Bevezetés az absztrakt algebrába

Kiss Emil

Bevezetés

Te jól tudod, a költő sose lódít:
az igazat mondd, ne csak a valódit.

József Attila: *Thomas Mann üdvözlése*

Ez a jegyzet egy most készülő könyv kézirata, amely az Eötvös Loránd Tudományegyetem Algebra és Számelmélet Tanszékének oktatási tapasztalatai alapján íródott. Bármilyen megjegyzést, javítást, kérést szívesen veszünk, sőt reméljük, hogy minél több ilyen megjegyzést kapunk, mert ez javítani fogja a könyv színvonalát. A megjegyzéseket az `ewkiss@cs.elte.hu` email-címre érdemes küldeni, de szívesen meghallgatjuk szóban is. A visszajelzések birtokában a jegyzetet folyamatosan javítjuk, és újabb anyagrészekkel bővítjük is. Ezért érdemes rendszeresen körülnézni a

`http://www.cs.elte.hu/~ewkiss/bboard/algebrabook/index.html`

web-címen, ahol `pdf` formátumban mindig megtalálható a legfrissebb változat, és néha egyéb hasznos megjegyzések is (például az ismert, értelemzavaró sajtóhibákról).

A könyv matematika tanárszakos, matematikus, és alkalmazott matematikus hallgatók számára készül. E három szakon az anyag mennyisége, felépítése, és így az előadás tempója, részletessége is különböző lehet. Sok esetben az előadó egyes számolásokat, meggondolnivalókat házi feladatnak ad azért, mert ezeket önálló munkával lehet csak igazán megérteni. A jegyzet azzal kínál segítséget, hogy benne vannak azok a részletek is, amelyek az előadáson nem mindig hangzanak el. Ezek sokszor magyarázatok, részletszámítások, de elsősorban az apróbetűs részekben szerepelnek mélyebb, előremutató, vagy filozófiai jellegű megjegyzések is.

Maximális érthetőségre törekedtünk, de ezen belül mindig úgy választottuk a tárgyalási módot, hogy a lehető legjobban előkészítse a legfontosabb absztrakt algebrai fogalmak bevezetését. Ezért a bevezető fejezeteket annak is érdemes átfutnia, aki már ismeri például a komplex számokat, vagy a polinomokat. Nagy hangsúlyt fektettünk arra, hogy elmagyarázzuk a „miért”-eket: azt, hogy az egyes fogalmak miért fontosak, miért így és nem máshogy definiáltuk őket, hogy a bizonyításokban miért éppen a leírt lépéseket tesszük, hogy lehetne-e másmerre haladni. Úgy gondoljuk, ez nemcsak az anyag alkalmazásához ad segítséget, hanem az önálló problémamegoldáshoz is. Aki a matematikát alkalmazza, azaz modelleket készít, annak el kell sajátítania a fogalomalkotás technikáját is.

Ha valaki matematikával foglalkozik, akár tanárként, akár kutatóként, akár alkalmazóként, mindig el kell döntenie, hogy a precízségnek mely szintje az, amely a maximális érthetőséget eredményezi saját maga és a környezete számára. Ha nem vagyunk elég precízek, akkor összemoshatunk különböző dolgokat, kimaradhatnak fontos feltételek, ami hibához, érthetetlenséghez vezet. Ha viszont túl precízek vagyunk, akkor a formalizmus mögött elsikkad a lényeg, az idő a kódolással/dekódolással, és nem az emberi gondolkozással telik. Az áttekinthetőség, és az ehhez kapcsolódó jó jelölés megtalálása minden matematikusnak elsőrendűen fontos feladata minden egyes problémában, mert hatékonyabbá teszi a gondolkodást és a kommunikációt. Az Olvasó feladata eldönteni, hogy ezt az egyensúlyt ebben a könyvben megtaláltuk-e.

A jegyzet formája annyiban szokatlan, hogy egyes számolási részletek, meggondolnivalók Kérdés, Gyakorlat, vagy akár Feladat formájában szerepelnek az „elméleti" szövegen belül is. Meggyőződésünk, hogy matematikát úgy lehet a legeredményesebben tanulni, ha minél több bizonyítást magunk találunk ki, és ha menet közben elgondolkozunk a dolgokon, mielőtt tovább olvasnánk. Az új forma ennek a lehetőségét próbálja megteremteni. Ha valaki nem boldogul egy ilyen Kérdés megválaszolásával, vagy ha ellenőrizni akarja magát, akkor érdemes a választ fellapoznia a jegyzet végén, mielőtt tovább haladna.

A matematikát nem elég megtanulni, meg is kell érteni azt. Ebben segítenek a könyvben szereplő Gyakorlatok (ezek általában könnyebbek), és a Feladatok (amelyek nehezebbek). Ezek legtöbbjéhez megoldást, és a Feladatokhoz ezen kívül útmutatást is adunk a jegyzet végén. Így a jegyzetben csaknem teljes egészében megtalálható a gyakorlatokon szerepelt anyag is, megoldásokkal együtt.

Vigyázzunk: a megoldások elolvasása nem helyettesíti az önálló gondolkodást. Ezen kívül a megértés és a begyakorlás két különböző dolog! A jegyzetben szereplő Gyakorlatok és Feladatok elsősorban az anyag megértését segítik. Ha nem elegendőek a begyakorlásra, akkor a Fagyejev-Szominszkij [**8**] és a Czédli-Szendrei-Szendrei [**6**] feladatgyűjteményekből érdemes további feladatokat megoldani, egyéni szükségletek szerint.

A jegyzet kiindulásképpen csak a középiskolai anyagra támaszkodik. Ahogy azonban haladunk előre, szükség lesz más, elsősorban számelméleti, kombinatorikai, és később lineáris algebrai ismeretekre is. Ezek elsajátításában segíthetnek az Irodalomjegyzékben szereplő művek, elsősorban Freud Róbert és Gyarmati Edit: *Számelmélet* [**11**], illetve Freud Róbert: *Lineáris algebra* [**10**] című művei. A szövegben természetesen mindig megemlítjük a szükséges előismereteket.

Köszönetemet szeretném kifejezni Freud Róbertnek, Pálfy Péter Pálnak, Fried Ervinnek, Szabó Endrének, Szabó Csabának, Pelikán Józsefnek, Ágoston Istvánnak, valamint hallgatóimnak (a legtöbbet segítők névsora, a teljesség igénye nélkül: Boros Balázs, Bérczi Kristóf, Csóka Endre, Finta Viktória, Gyenis Zalán, Haász Sándor, Kmecs Viktória, Salát Máté, Szabó Máté, Vicze Zsolt) a rengeteg szakmai segítségért, a sajtóhibák megtalálásáért, a könyv olvashatóbbá tételéért. Minden kedves Olvasónak hasznos, sikeres és kellemes időtöltést kívánunk.

I. rész

Elemi algebra

1. KOMPLEX SZÁMOK

. . . a zseniális Cerebron, egzakt módszerekkel boncolgatva a problémát, a sárkányok három faját fedezte fel: a nullás, az imaginárius, és a negatív sárkányokat. Mindezek, amint már említettük, nem léteznek, de mindegyik fajta egészen másképpen nem létezik.

Stanisław Lem: *Kiberiáda*
(Murányi Beatrix fordítása)

Mik azok a számok? Egy ősember valószínűleg kis pozitív egész számokra gondolna: egy, kettő, három, sok. A régi görögök csak a racionális számokat tekintették számnak. A törteket ismerték, de a végtelen tizedes törteket nem. A szakaszok hosszát csak geometriailag tudták összeadni, és még be is bizonyították, hogy az egységnégyzet átlójának hossza *nem szám*, hiszen nem lehet két egész hányadosaként kifejezni.

A számfogalom tehát fejlődött az emberiség történelme során. Párszáz éve derült ki, hogy a valós számok fogalmát érdemes tovább bővíteni, így kapjuk a komplex számokat. Ebben a fejezetben megmutatjuk, hogy a harmadfokú egyenlet megoldásához miért hasznos ezeket az újfajta számokat bevezetni, majd a komplex számok alapvető tulajdonságaival foglalkozunk. Rá fogunk jönni, hogy ezek a számolási szabályok ismerősek, mert hasonlóak ahhoz, ahogy valós számokkal, vagy (egyenletek rendezése során) ismeretleneket tartalmazó kifejezésekkel (úgynevezett polinomokkal) számolunk. Ez a hasonlóság vezet majd el a gyűrű fogalmához a következő fejezetben. Hasonló szabályok vonatkoznak arra az esetre is, amikor számelméleti problémák megoldásakor egész számokkal számolunk ugyan, de speciális módon, mert csak az eredmény egy bizonyos osztási maradéka, például a paritása érdekel bennünket.

1.1. Számolás maradékokkal

Ebben a szakaszban a maradékokkal való számolás hasznosságát illusztráljuk néhány feladattal, majd összefoglaljuk a rá vonatkozó szabályokat. Az alábbi két feladat nagyon különböző, de a megoldásuk ötlete hasonló.

1.1.1. Feladat. Igazoljuk, hogy egy 100×100-as sakktábla nem fedhető le 8×1-es dominókkal (egyrétűen és hézagmentesen).

1.1.2. Feladat. Megoldható-e az egész számok körében az $x^2 + 5y = 1002$ egyenlet?

Az első feladat megoldásához írjunk fel a sakktábla minden mezőjére egy-egy számot a következőképpen. A bal felső sarokba nullát írunk. Ezután a sor többi elemét úgy töltjük ki, hogy az előző mezőn lévő számhoz mindig 1-et hozzáadunk, de ha a 8-hoz érünk, akkor nem 8-at, hanem nullát írunk ismét. Ezt úgy fejezzük ki, hogy az 1 hozzáadását *modulo* 8 *végezzük el*. Ha már az első sor kész, akkor ebből kiindulva az összes oszlopot is hasonlóan készítjük el: lefelé haladva minden mező értékét megnöveljük 1-gyel modulo 8. Másképp fogalmazva: a (felülről számított) i-edik sor j-edik mezőjére írt szám az $i + j - 2$ maradéka 8-cal osztva. A bal felső sarok tehát így néz ki:

0	1	2	3	4	5	6	7	0	1
1	2	3	4	5	6	7	0	1	2
2	3	4	5	6	7	0	1	2	3
3	4	5	6	7	0	1	2	3	4
4	5	6	7	0	1	2	3	4	5
5	6	7	0	1	2	3	4	5	6
6	7	0	1	2	3	4	5	6	7
7	0	1	2	3	4	5	6	7	0
0	1	2	3	4	5	6	7	0	1
1	2	3	4	5	6	7	0	1	2

Könnyen látható, hogy *bármely* mezőről egyet jobbra vagy lefelé lépve a ráírt érték pontosan 1-gyel növekszik modulo 8. Helyezzünk most rá egy 8×1-es dominót erre a sakktáblára, akár vízszintesen, akár függőlegesen. Bármilyen számot takar is el a dominó bal felső sarka, a következő eltakart szám ennél eggyel nagyobb modulo 8, a következő még eggyel, és így tovább. Mivel a dominó nyolc négyzetből áll, mindenképpen a 0, 1, 2, 3, 4, 5, 6, 7 számokat takarja el, valamilyen sorrendben.

Most már könnyű belátni, hogy a kívánt lefedés nem lehetséges. Ha ugyanis létezne ilyen lefedés, akkor, mivel mindegyik dominó pontosan egy darab 0-t takar el, a sakktáblán annyi 0 szerepelne, mint amennyi a szükséges dominók száma. Ugyanennyi szerepelne az 1, 2, 3, 4, 5, 6, 7 számok mindegyikéből is. De ez nem így van, könnyű megszámolni, hogy a sakktáblára 1249 darab 0-t, de csak 1248 darab 7-est írtunk.

1.1.3. Gyakorlat. Mutassuk meg, hogy a sakktáblára több nullát írtunk, mint hetest, *anélkül, hogy megszámolnánk, melyikből hányat írtunk.*

A most alkalmazott gondolatmenet egy *indirekt bizonyítás* volt: feltételeztük, hogy a bizonyítandó állítás hamis (azaz, hogy létezik lefedés), és ebből *ellentmondásra* jutottunk (hiszen az jött ki, hogy $1248 = 1249$). Ezért a kiinduló állításunk sem lehetett hamis, tehát mégsincs ilyen lefedés. Ezt a bizonyítási módot lépten-nyomon alkalmazni fogjuk.

Az 1.1.2. Feladat megoldásához „modulo 5” fogunk számolni. A jobb oldalon álló 1002 szám maradéka 5-tel osztva 2. Mivel $5y$ maradéka nulla, olyan x-et kell találnunk, melyre

x^2 maradéka szintén 2. Meg fogjuk mutatni, hogy nincs ilyen x, tehát az egyenletnek nincs megoldása az egész számok között.

Ehhez elvileg végig kellene néznünk az összes egész számot, mindegyiket négyzetre emelni, és öttel elosztani. A nullától indulva a keletkező maradékok a következők lesznek:

0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	...
0,	1,	4,	4,	1,	0,	1,	4,	4,	1,	0,	1,	4,	4,	1,	...

Láthatjuk, hogy a sorozat 5-ösével periodikus. Így van-e ez akkor is, ha tovább folytatjuk a sorozatot, vagy ha a negatív x-eket is megvizsgáljuk? A válasz igenlő. Ennek belátásához az x számot osszuk el maradékosan 5-tel: $x = 5q + r$, ahol r a 0, 1, 2, 3, 4 valamelyike. Ekkor

$$x^2 = (5q + r)^2 = 25q^2 + 10q + r^2 = 5(5q^2 + 2q) + r^2 .$$

Vagyis az x^2 és az r^2 ugyanazt a számot adja maradékul! Ezért elég az r^2 lehetséges maradékait végignézni. Ezt már megtettük, és látjuk, hogy a 2 nem fordul elő közöttük, tehát a feladatot megoldottuk: az egyenletnek nincs egész megoldása.

Az előző feladatban az eredeti szám, azaz x helyett annak az 5-tel való osztási maradékával számoltunk. Ez óriási könnyebbség volt, mert végtelen sok szám helyett csak véges sokat — az öt lehetséges maradékot — kellett megvizsgálni. A megoldást az tette lehetővé, hogy szoros kapcsolat volt x^2 és r^2 maradéka között. Hasonló állítás igaz általában az összeadásra és a szorzásra is, durván fogalmazva összeg maradéka a maradékok összege, szorzat maradéka a maradékok szorzata lesz. Emiatt tetszőleges olyan egyenletet, amelyben az ismeretlenek egész számok, megpróbálhatunk úgy megvizsgálni, hogy „modulo 5 vesszük”, vagyis az ismeretlenek helyett azok 5-tel való osztási maradékával számolunk. Ha így nincs megoldás, akkor eredetileg sem lehetett. Persze az 5 helyett más „modulust” is kereshetünk, ha az egyenlet vizsgálatához az a célszerűbb.

Hogyan is végezzük ezeket a műveleteket a maradékok között? Foglaljuk össze táblázatosan az összeadást is és a szorzást is. Az a elemhez tartozó sor és a b elemhez tartozó oszlop metszéspontjában az a és b modulo 5 vett összege illetve szorzata szerepel:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ezekből a táblázatokból sok hasznos információ olvasható le. Például a szorzástábla „főátlójára” nézve látjuk azt a korábban már felhasznált tényt, hogy modulo 5 a 0, 1, 4 számoknak van „négyzetgyöke”, 2-nek és 3-nak pedig nincs. Máshogy fogalmazva: egy négyzetszám 5-tel osztva nem adhat sem 2-t, sem 3-at maradékul.

A fenti táblázatokkal két *új műveletet* definiáltunk a $\{0, 1, 2, 3, 4\}$ halmazon, vagyis a modulo 5 maradékok halmazán. E műveletek tulajdonságai nagyon hasonlítanak az eredeti

összeadás és szorzás tulajdonságaihoz. Foglaljuk össze ezeket a tulajdonságokat, de most már általában, az 5 helyett tetszőleges m modulust alkalmazva.

1.1.4. Definíció. Legyen m pozitív egész szám, és jelölje $\mathbb{Z}_m$ a $\{0, 1, \dots, m-1\}$ halmazt, vagyis a modulo m maradékok halmazát. Értelmezzük e számok között a *modulo m összeadást és szorzást* a következőképpen. Ha $a, b \in \mathbb{Z}_m$, akkor $a +_m b$ jelölje az (egész számok között kiszámított) $a + b$ összeg m-mel való osztási maradékát. Hasonlóképpen legyen $a *_m b$ az ab szorzat m-mel való osztási maradéka.

1.1.5. Állítás. *Legyen $m \geq 1$ egész és $x, y, z \in \mathbb{Z}_m$. A jobb áttekinthetőség kedvéért jelölje $+ = +_m$ a modulo m összeadást, $* = *_m$ pedig a modulo m szorzást.*

(1) $(x + y) + z = x + (y + z)$ *(az összeadás* ***asszociatív****).*
(2) $x + y = y + x$ *(az összeadás* ***kommutatív****).*
(3) $x + 0 = 0 + x = x$ *(azaz létezik* ***nullelem****, amelyet bármely elemhez hozzáadva azt az elemet kapjuk).*
(4) *Minden x-nek van* ***ellentettje****, azaz olyan y, melyre $x + y = y + x = 0$. (Ilyen y lesz a $-x$ maradéka modulo m.)*
(5) $(x * y) * z = x * (y * z)$ *(a szorzás asszociatív).*
(6) $x * y = y * x$ *(a szorzás kommutatív).*
(7) $x * 1 = 1 * x = x$ *(azaz létezik* ***egységelem****, amellyel bármely elemet megszorozva azt az elemet kapjuk).*
(8) $(x + y) * z = x * z + y * z$ (***disztributivitás****).*

Ezeket a tulajdonságokat most nem bizonyítjuk be (bár némelyiket könnyű ellenőrizni). A legtöbbjük következik az alábbi állításból, ami a modulo m műveletek és az egész számok közötti műveletek már emlegetett kapcsolatát írja le. Az állítás megfogalmazásához egy x egész szám m-mel való osztási maradékát egyszerűen csak felülvonással, vagyis $\overline{x}$-sal jelöljük. Ezt persze csak akkor tehetjük meg, ha már előre megbeszéltük, hogy mi az m modulus!

1.1.6. Állítás. *Ha $m \geq 1$ egész, $x, y \in \mathbb{Z}$, és felülvonás jelöli a modulo m maradék képzését, akkor*

$$\overline{x + y} = \overline{x} +_m \overline{y} \quad \text{és} \quad \overline{xy} = \overline{x} *_m \overline{y}\,.$$

Máshogy fogalmazva: összeg maradéka a maradékok (modulo m vett) összege, és szorzat maradéka a maradékok (modulo m vett) szorzata. Röviden: a modulo m maradékképzés összeg- és szorzattartó, azaz ***művelettartó****.*

Nem beszéltünk a kivonás és az osztás műveletéről. Elvégezhetjük-e ezeket is modulo m? A *kivonást* az összeadásból származtatjuk, hiszen $z = x - y$ az a szám, amelyre $z + y = x$. Szerencsére ezzel a művelettel nem kell külön foglalkoznunk, mert visszavezethető az ellentettképzésre. Valóban, az egész számok között $x - y$ megkapható úgy, mint $x + (-y)$ (szavakban: az y kivonása az y ellentettjének a hozzáadása). Ugyanez a helyzet akkor is, amikor modulo m számolunk.

1.1.7. Feladat. Igazoljuk az 1.1.6 és az 1.1.5 állításokat. Definiáljuk alkalmasan a kivonás $-_m$ műveletét, és mutassuk meg az $\overline{x-y} = \overline{x} -_m \overline{y}$ azonosságot.

Az *osztás* művelete ugyanúgy származik a szorzásból, mint ahogy a kivonás az összeadásból: $z = x : y$ az a szám, amelyre $z * y = x$. Ahogy a kivonás az ellentett képzésére, az osztás a *reciprok* (más néven *inverz*) képzésére vezethető vissza. Az y reciproka (vagy inverze) az az $u = 1/y$-nal (néha y^{-1}-gyel) jelölt szám, melyre $y * u = u * y = 1$ (az egységelem). Ha ezt ismerjük, akkor $x : y$ megkapható úgy, mint $x * u$ (szavakban: az y-nal való osztás a reciprokával való szorzás).

A reciprokképzés (és így az osztás) azonban nem végezhető el korlátlanul. Például a nullának egész biztosan nincs reciproka, hiszen $u * 0 = 0$ minden u-ra, és így soha nem kapunk 1-et. Az egész számok között csak az 1-nek és a -1-nek van olyan reciproka, ami szintén egész szám, tehát csak ezekkel lehet korlátlanul osztani. Mint az alábbi gyakorlat illusztrálja, modulo m számolva a helyzet ennél jobb egy kicsit.

1.1.8. Gyakorlat. Végezzük el a fenti modulo 5 szorzástábla alapján a $2 : 3$ osztást modulo 5. Tudunk-e osztani $\mathbb{Z}_5$ minden nem nulla elemével? Mi a helyzet modulo 6?

Az eddigiek alapján leszűrhetjük, hogy modulo m maradékokkal ugyanúgy a „szokásos szabályok” szerint számolhatunk, mint valós számokkal, bár az osztásnál óvatosnak kell lennünk. A következő gyakorlat további óvatosságra int.

1.1.9. Gyakorlat. Igaz-e modulo 5 illetve modulo 6, hogy szorzat csak akkor lehet nulla, ha valamelyik tényezője nulla? (Ezt a tulajdonságot ***nullosztómentességnek*** hívjuk.)

A tanulság, hogy meg kell majd vizsgálnunk pontosan, mit is értünk a „szokásos” számolási szabályokon: fel kell sorolnunk, hogy mit és hogyan szabad csinálnunk, amikor a műveleteket végezzük. Mielőtt ezt megtennénk, megismerkedünk két másik „struktúrával”, melyekben szintén a „szokásos” szabályok alapján lehet az összeadást és a szorzást elvégezni.

Aki már hallott *maradékosztályokról* számelméletből, az bizonyára ismerősnek találja a fentieket. Ha például modulo 5 nem maradékokkal, hanem maradékosztályokkal akarunk számolni, akkor nem a 2 maradékot tekintjük, hanem helyette a 2 maradékosztályát, vagyis az $5k + 2$ alakú számok halmazát. Bár ez matematikailag elegánsabb megközelítés, a műveletek definíciója ilyenkor kissé bonyolultabb lesz, mint az imént. A fellépő nehézségekről részletesen szólunk majd, amikor faktorgyűrűkről beszélünk az 5.1. Szakaszban. Az alkalmazások tekintetében a két módszer egyenértékű.

Gyakorlatok, feladatok

1.1.10. Gyakorlat. Melyek helyesek az alábbi gondolatmenetek közül?

(1) Belátjuk, hogy az $x^2 + 10y^2 = 6$ egyenletnek van megoldása az egész számok körében. Tekintsük az egyenletet modulo 5. Ekkor azt kapjuk, hogy $\overline{x} *_5 \overline{x} = 1$. Ennek van megoldása, például az $x = 1$. Tehát az eredeti egyenlet is megoldható.

(2) Ugyanez a gondolatmenet az $x^2 + 5y^2 = 6$ egyenlet esetén.

1.1.11. Gyakorlat. A modulo 5 műveleti táblázatok vizsgálatával igazoljuk, hogy $a^5 - a$ minden egész a-ra osztható 5-tel. Milyen a egészekre igaz, hogy $a^4 - 1$ osztható 5-tel?

1.1.12. Gyakorlat. Készítsük el a modulo 6 maradékok összeadás és szorzástábláját. Milyen a egészekre teljesülnek az alábbi oszthatóságok?

(1) $6 \mid a^6 - a$.
(2) $6 \mid a^5 - 1$.
(3) $6 \mid a^2 - 1$.

1.1.13. Gyakorlat. Bizonyítsuk be a modulo 8 szorzás felhasználásával, hogy minden páratlan szám négyzete 8-cal osztva 1-et ad maradékul. Mutassuk meg ezt az állítást közvetlen számolással is.

1.1.14. Gyakorlat. Adjunk meg a modulo 5 szorzástábla vizsgálatával olyan x és y egészeket, melyre $5x + 3y = 7$. Véges, vagy végtelen sok megoldás van?

1.1.15. Gyakorlat. Mely x egész számokra teljesül, hogy $5 \mid x^2 - 2x + 2$? És az, hogy $7 \mid x^2 - 2x + 2$?

1.1.16. Feladat. Mely x egészekre teljesül, hogy

(1) $101 \mid x^2 - 2x + 2$?
(2) $101 \mid x^2 - 13x - 3$?

1.1.17. Gyakorlat. A közönséges 8×8-as sakktáblából kivesszük az egyik átló két végpontján lévő két sarokkockát. Lefedhető-e a kapott alakzat 2×1-es dominókkal?

1.1.18. Feladat. Igazoljuk, hogy egy $k \times k$ méretű sakktábla akkor és csak akkor fedhető le $m \times 1$-es dominókkal, ha m osztója k-nak.

1.1.19. Feladat. Igazoljuk, hogy ha p is és $p^2 + 2$ is prímszám, akkor $p^3 + 4$ is az. Igaz-e, hogy ha p is és $p^2 + 5$ is prímszám, akkor $p^3 + 4$ is az?

1.2. A harmadfokú egyenlet megoldásának problémája

Ebben a szakaszban a harmadfokú egyenlet vizsgálata kapcsán bemutatjuk, hogy a valós számokat érdemes kibővíteni a megoldások meghatározása érdekében. Ehhez először gondoljuk végig, hogyan is oldjuk meg a másodfokú egyenletet. A megoldóképlet az egyenlet megoldását négyzetgyökvonásra vezeti vissza.

1.2.1. Gyakorlat. Az $y^2 + py + q = 0$ egyenletben vezessük be az $x = y - w$ ismeretlent. Hogyan válasszuk meg w értékét, ha azt akarjuk, hogy x értékét egy négyzetgyökvonással közvetlenül megkaphassuk?

A másodfokú egyenlet megoldásakor alkalmazott (az előző gyakorlatra adott válaszból adódó) $y = x - p/2$ (azaz $x = y + p/2$) helyettesítés azért működik, mert általa eltűnik az y-os tag, és mivel a $w = -p/2$ kifejezhető az eredeti egyenlet együtthatóiból, az átalakított egyenlet megoldásaiból az eredeti egyenlet megoldásait is megkaphattuk.

Próbáljuk most megoldani az

$$ay^3 + by^2 + cy + d = 0 \qquad (a \neq 0) \tag{1.1}$$

harmadfokú egyenletet. Most is megpróbálkozhatunk azzal, hogy az $x = y - w$ helyettesítéssel hozzuk az egyenletet egyszerűbb alakra. Ahhoz, hogy x^2-es tag ne szerepeljen, a $w = -b/3a$ értéket kell választanunk. De a megoldásokat most nem kapjuk meg közvetlenül köbgyökvonással, mert az egyenletben benne marad általában az x-es tag! Annyit azért elértünk, hogy (az a főegyütthatóval való osztás után) az egyenlet

$$x^3 + px + q = 0 \tag{1.2}$$

alakú lesz alkalmas p-re és q-ra, amelyek az eredeti egyenlet együtthatóiból a négy alapművelet segítségével kifejezhetők. Tudjuk azt is, hogy ennek az egyenletnek a megoldásaiból az eredeti egyenlet megoldásait megkaphatjuk $b/3a$ levonásával.

1.2.2. Gyakorlat. Mutassuk meg, hogy az (1.1) egyenlet esetében az $y = x - b/3a$ az egyetlen olyan helyettesítés, ami eltünteti az y^2 együtthatóját. Számítsuk ki az (1.2) egyenletben keletkező p és q értékét is.

Tehát elegendő ezt az új egyenletet megoldanunk. A megoldáshoz vezető ötletet az alábbi azonos átalakítás szolgáltatja:

$$(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = u^3 + v^3 + 3uv(u+v)\,,$$

azaz

$$(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0\,.$$

Ez az azonosság hasonlít a megoldandó egyenlet $x^3 + px + q = 0$ alakjához. Ha sikerülne az u és v számokat úgy megválasztani, hogy a

$$\left.\begin{aligned} -3uv &= p \\ -(u^3+v^3) &= q \end{aligned}\right\} \tag{1.3}$$

egyenletrendszer teljesüljön, akkor $x = u + v$ biztosan az egyenlet megoldása lenne.

1.2.3. Gyakorlat. Beláttuk-e, hogy az $x^3 + px + q = 0$ egyenlet minden megoldása $u + v$ alakban írható, ahol u és v kielégíti ezt az egyenletrendszert?

Hogyan lehetne megoldani ezt az egyenletrendszert? Az olyan egyenletrendszereket, ahol a két ismeretlen összege és szorzata adott, másodfokú egyenletre vezethetjük vissza.

1.2.4. Gyakorlat. Mutassuk meg, hogy ha a és b valós számok, akkor az

$$\left.\begin{aligned} x+y&=a\\ xy&=b\end{aligned}\right\}$$

egyenletrendszer megoldásai éppen a $z^2-az+b=0$ egyenlet megoldásai. Mi történik, ha ennek a másodfokú egyenletnek csak egy megoldása van?

Az (1.3) egyenletrendszerben u^3 és v^3 összege $-q$, szorzatuk pedig, az első egyenletet köbre emelve, $(-p/3)^3$. Ezért u^3 és v^3 a $z^2+qz-(p/3)^3=0$ másodfokú egyenlet megoldásai. Ezt a másodfokú egyenletet megoldva u és v értékét köbgyökvonással állapíthatjuk meg. A számolást elvégezve az úgynevezett *Cardano-képletet* kapjuk:

$$x=u+v=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(-\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(-\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}\,.$$

A négyzetgyök alatt álló $(q/2)^2+(p/3)^3$ kifejezést általában D betűvel fogjuk jelölni.

A Cardano-képletben tehát mindenhol $-q/2$ szerepel, ami a könnyebb megjegyezhetőséget segíti elő. Természetesen $(-q/2)^2$ helyett $(q/2)^2$ is írható. Másik megjegyzési lehetőség, hogy a köbgyökjelek alatti képletek „ritmusa” nagyon hasonlít a másodfokú egyenlet megoldóképletére.

Ahogy a másodfokú egyenlet esetében a négyzetgyökjel alatti kifejezést az egyenlet diszkriminánsának hívják, úgy néhány könyvben a fenti D-t is így nevezik. A 3.7. Szakaszban bevezetjük majd a diszkrimináns fogalmát magasabb fokú egyenletekre is, és meglátjuk, hogy a harmadfokú egyenlet esetében inkább a $-108D$ kifejezést érdemes diszkriminánsnak hívni (3.7.11. Gyakorlat).

Az 1.2.3. Kérdésre adott válasz szerint egyáltalán nem láttuk be, hogy a Cardano-képlet megadja a harmadfokú egyenlet összes gyökét. Gyanakvásra adhat okot, hogy mivel a valós számok körében minden számnak egy köbgyöke van, a képlet csak egyetlen megoldást szolgáltathat. Márpedig könnyen felírhatunk egy olyan harmadfokú egyenletet, aminek három valós megoldása van, például

$$(x-1)(x-4)(x+5)=x^3-21x+20=0\,.$$

Vajon az 1, 4 és -5 közül melyiket adja a Cardano-képlet? Ha behelyettesítünk, akkor $D=-243$, azaz negatív szám adódik. Ebből nem tudunk négyzetgyököt vonni, tehát az egyenlet egyik megoldását sem kapjuk meg!

Használhatatlan lenne a módszerünk? Mielőtt feladnánk, vizsgáljunk meg két másik egyenletet is. Az $x^3-9x-28=0$ esetben $D=169$, azaz

$$x=\sqrt[3]{14+13}+\sqrt[3]{14-13}=3+1=4\,.$$

Több megoldás nincs is (a valós számok között), mert

$$x^3-9x-28=(x-4)(x^2+4x+7)\,,$$

és a második tényezőnek nincs valós gyöke.

Lehet, hogy ha csak egy valós megoldás van, akkor a képlet ezt mindig megadja? Az előző példán felbátorodva próbálkozzunk meg az $x^3 - 3x - 52$ egyenlettel. Az eredmény

$$x = \sqrt[3]{26 + \sqrt{675}} + \sqrt[3]{26 - \sqrt{675}}\,,$$

kalkulátorral ezt (közelítőleg) kiszámítva $x = 4$ adódik. Szorzattá alakítással most is meggyőződhetünk arról, hogy az egyenlet egyetlen valós megoldása az $x = 4$. Tehát a fenti gyökös kifejezés nemcsak közelítőleg, hanem pontosan egyenlő 4-gyel! Ezt közvetlenül is be tudjuk látni, ha észrevesszük, hogy

$$26 + \sqrt{675} = 26 + 15\sqrt{3} = 2^3 + 3 \cdot 2^2 \cdot \sqrt{3} + 3 \cdot 2\sqrt{3}^2 + \sqrt{3}^3 = (2 + \sqrt{3})^3\,,$$

és ugyanígy $26 - \sqrt{675} = (2 - \sqrt{3})^3$. Ezért $x = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4$.

Térjünk most vissza az $x^3 - 21x + 20 = 0$ egyenletből kapott

$$x = \sqrt[3]{-10 + \sqrt{-243}} + \sqrt[3]{-10 - \sqrt{-243}}$$

eredményre. Felejtsük el, hogy nincs olyan valós szám, aminek a négyzete -243, és próbáljuk most is az előző módon elvégezni a köbgyökvonást. Annyit persze elfogadunk, hogy $(\sqrt{-3})^2 = -3$. Azt kapjuk, hogy

$$-10+\sqrt{-243} = -10+9\sqrt{-3} = 2^3+3\cdot 2^2\cdot\sqrt{-3}+3\cdot 2(\sqrt{-3})^2+(\sqrt{-3})^3 = (2+\sqrt{-3})^3\,,$$

és ugyanígy $-10 - \sqrt{-243} = (2 - \sqrt{-3})^3$. Ezért $x = (2 + \sqrt{-3}) + (2 - \sqrt{-3}) = 4$.

Vagyis az egyik megoldást ki tudjuk hozni a Cardano-képletből, ha hajlandók vagyunk formálisan számolni negatív számok négyzetgyökével, mert ezek a négyzetgyökök a végén kiesnek! Sőt, a „köbgyökvonást” másképp végezve a másik két megoldás is kijön:

1.2.5. Gyakorlat. „Mutassuk meg”, hogy

$$\left(-\frac{5}{2} + \frac{\sqrt{-3}}{2}\right)^3 = \left(\frac{1}{2} - \frac{3\sqrt{-3}}{2}\right)^3 = -10 + \sqrt{-243}\,.$$

A két új „köbgyököt” felhasználva $x_2 = (-5/2 + \sqrt{-3}/2) + (-5/2 - \sqrt{-3}/2) = -5$, illetve $x_3 = (1/2 - 3\sqrt{-3}/2) + (1/2 + 3\sqrt{-3}/2) = 1$ adódik.

Találtunk egy csóválódó farkat, keressük meg a kutyát! Szabad-e, és ha igen, milyen szabályok szerint szabad számolni ezekkel az újfajta kifejezésekkel? Igaz-e, hogy a Cardano-képlettel az összes harmadfokú egyenlet megoldható? Mi lesz a megoldások száma? Van-e a fenti trükkös eljárástól különböző, mechanikus módszer a köbgyökvonás elvégzésére? Mindezekre a kérdésekre a *komplex számok* bevezetése adja meg a választ. A Cardano-képlet pontos tárgyalására a 3.8. Szakaszban térünk majd vissza (az igazán mély megértése pedig, Galois-elmélet segítségével, a 6.10. Szakaszban következik majd be).

Gyakorlatok, feladatok

1.2.6. Gyakorlat. Elérhetjük-e alkalmas $x = y + w$ helyettesítéssel, hogy az (1.1) harmadfokú egyenletből az y-os tag, illetve a konstans tag (vagyis a d) tűnjön el?

1.2.7. Gyakorlat. Helyes-e az 1.2.4. Gyakorlatra adott következő megoldás? Ha $x+y=a$ és $xy=b$, akkor $(z-x)(z-y) = z^2-(x+y)z+xyz = z^2-az+b$. Tehát a $z^2-az+b=0$ egyenletnek megoldása x is és y is.

1.2.8. Gyakorlat. Melyik természetes számmal egyenlő $\sqrt[3]{7+\sqrt{50}} + \sqrt[3]{7-\sqrt{50}}$?

1.2.9. Gyakorlat. „Mutassuk meg”, hogy $\sqrt[4]{-4} = 1+\sqrt{-1}$. Keressük meg $\sqrt[4]{-4}$ három további értékét is.

1.2.10. Gyakorlat. Egy pozitív valós számból két négyzetgyök vonható. Ezért ha D értéke pozitív, akkor látszólag a Cardano-képletből négy megoldást nyerhetünk (hiszen mindkét négyzetgyökvonásnak kétféle eredménye lehet). Hogy lehet ez? Tényleg négy megoldása van ilyenkor a harmadfokú egyenletnek?

1.2.11. Gyakorlat. Az alábbi levezetés ellentmondáshoz vezet:

$$1 = \sqrt{1} = \sqrt{(-1)\cdot(-1)} = \sqrt{-1}\cdot\sqrt{-1} = -1\,.$$

Fel kell adnunk a $\sqrt{-1}$-et tartalmazó kifejezésekkel való számolás gondolatát?

1.2.12. Feladat. Igazoljuk Bolzano tételének[1] felhasználásával, hogy egy valós együtthatós harmadfokú egyenletnek mindig van valós megoldása.

1.3. Számolás komplex számokkal

A tervünk az, hogy olyan kifejezésekkel is tudjunk formálisan számolni, melyekben negatív számok négyzetgyökei is szerepelnek. Az 1.2.11. Gyakorlat azonban óvatosságra int. Meg kell pontosan mondanunk, milyen kifejezéseket akarunk vizsgálni, és megállapítani a számolás szabályait.

Hogy ne kelljen sokat írni, vezessük be a $\sqrt{-1} = i$ rövidítést. Látni fogjuk, hogy hasonló rövidítést nem kell bevezetnünk a többi negatív szám négyzetgyökére, például $\sqrt{-4}$ helyett írhatunk majd $2\sqrt{-1} = 2i$-t, mert e két szám négyzete ugyanaz. Mivel az összeadást és a szorzást is el akarjuk végezni, biztosan meg kell engednünk az olyan kifejezéseket, mint például $3+2i$, vagyis általában az $a+bi$ alakú kifejezéseket, ahol a és b valós számok. Ezekkel úgy fogunk számolni, mintha i egy ismeretlen lenne, de közben felhasználhatjuk, hogy $i^2 = \sqrt{-1}^2 = -1$.

[1] Az analízisből ismert Bolzano-tétel (lásd A.3.2. Tétel) azt mondja ki, hogy ha egy folytonos függvény (mint például $f(x) = ax^3+bx^2+cx+d$) bizonyos helyeken negatív, illetve pozitív értéket vesz fel, akkor e két hely között felveszi a nulla értéket is, azaz „valahol át kell metszenie az x-tengelyt”.

Tegyük föl, hogy az $a + bi$ alakú kifejezésekkel szabad a szokásos szabályok szerint számolni. Ekkor két ilyen kifejezést könnyű összeadni:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \, .$$

Sőt, össze is tudjuk szorozni őket:

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i \, ,$$

hiszen $i^2 = -1$.

A $\sqrt{-1}$-nek két értéke lesz (ez okozza a gondot például az 1.2.11. Gyakorlatban fellépő látszólagos ellentmondás során). Az i betű a két érték egyikét jelöli, egyszer s mindenkorra. Azonnal látjuk, hogy a másik érték $-i$, mert $(-i)(-i) = i^2 = -1$. A másik értékkel persze ugyanúgy kell számolni, és ennek később igen nagy hasznát vesszük, amikor az úgynevezett konjugálás tulajdonságait vizsgáljuk majd.

1.3.1. Gyakorlat. Át lehet-e alakítani a $2 + 3i$ kifejezést, hogy a végén $4 + 5i$ jöjjön ki?

Eddig a lehetőségeinket vizsgálgattuk, azt, hogy *ha* sikerülne számolni a negatív számok négyzetgyökeivel, akkor milyen szabályok kötnének bennünket. Most már eleget tudunk ahhoz, hogy végre *definiálhassuk* a komplex számokat.

1.3.2. Definíció. *Komplex számoknak* az $a+bi$ alakú formális kifejezéseket nevezzük, ahol a és b valós számok. Az $a + bi$ és a $c + di$ számokat akkor tekintjük egyenlőnek, ha $a = c$ és $b = d$. Az összeadást és a szorzást az alábbi képletekkel definiáljuk:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \, .$$

A komplex számok most definiált halmazát $\mathbb{C}$ jelöli. Emlékeztetőül megjegyezzük, hogy az egész, racionális, illetve valós számok halmaza rendre $\mathbb{Z}$, $\mathbb{Q}$ és $\mathbb{R}$.

Az 1.3.1. Gyakorlat megmutatta, hogy miért így definiáltuk komplex számok egyenlőségét, az előtte levő számolás pedig, hogy miért így definiáljuk a műveleteket. Definíciónk alkalmas arra, hogy a komplex számokkal számolni tudjunk, ami most az elsődleges célunk. Matematikai szempontból azonban nem kielégítő, mert nem eléggé precíz, és mert nem mutattuk meg, hogy a számolásokból nem jöhet ki ellentmondás. Az 1.6. Szakaszban visszatérünk majd ezekre a kérdésekre, és bepótoljuk a hiányosságokat.

Ha az $a + bi$ kifejezésben $b = 0$, akkor csak a-t írunk, és így láthatjuk, hogy a valós számok mind komplex számok is egyúttal (és komplex számként persze ugyanúgy kell őket összeadni és szorozni, mint valós számként). Hasonlóképpen $0 + bi$ helyett csak bi-t fogunk írni. Az ilyen alakú komplex számokat *(tisztán) képzetes*, vagy *imaginárius* számoknak nevezzük. A $z = a + bi$ komplex szám *valós része* $\mathrm{Re}(z) = a$, *képzetes része* pedig $\mathrm{Im}(z) = b$ (a jelölés a latin eredetű "reális rész", illetve "imaginárius rész" kifejezésekből származik). Külön is felhívjuk a figyelmet arra, hogy a képzetes rész valós szám, tehát b, és nem bi.

Foglaljuk össze azokat a szabályokat, amelyek a most definiált műveletekre érvényesek. Érdemes észrevenni, hogy ezek mennyire hasonlítanak mind a valós számok körében megszokott szabályokhoz, mind pedig a maradékokkal való számolás szabályaihoz, amiket az 1.1.5. Állításban soroltunk fel.

1.3.3. Állítás. *Tetszőleges $x, y, z \in \mathbb{C}$ számokra érvényesek az alábbiak.*

(1) $(x + y) + z = x + (y + z)$ *(az összeadás asszociatív).*
(2) $x + y = y + x$ *(az összeadás kommutatív).*
(3) $x + 0 = 0 + x = x$ *(azaz létezik nullelem).*
(4) *Minden x-nek van ellentettje, azaz olyan y, melyre $x + y = y + x = 0$. (Ha $x = a + bi$, akkor ilyen y lesz $-a + (-b)i$.)*
(5) $(xy)z = x(yz)$ *(a szorzás asszociatív).*
(6) $xy = yx$ *(a szorzás kommutatív).*
(7) $x \cdot 1 = 1 \cdot x = x$ *(azaz létezik egységelem).*
(8) $(x + y)z = xz + yz$ *(disztributivitás).*

Ezt az állítást nem bizonyítjuk be, mert következni fog a később tanultakból. Egy mintabizonyítást azonban érdemes mindenkinek önállóan elvégezni.

1.3.4. Gyakorlat. Mutassuk meg a fenti azonosságok közül a disztributivitást.

Mivel minden komplex számnak van ellentettje, az 1.1. Szakaszban írottak szerint a kivonást is el tudjuk végezni. Ugyanitt láttuk azt is, hogy az osztás elvégzéséhez azt kell megvizsgálnunk, mely komplex számoknak van reciproka.

1.3.5. Gyakorlat. Keressük meg az $1 + i$ komplex szám reciprokát, vagyis azt a z komplex számot, melyre $(1 + i)z = 1$.

Noha e gyakorlatot egyenletrendszer segítségével is megoldhatjuk, eljárhatunk elegánsabban is. Az osztást a tört alkalmas bővítésével érdemes elvégezni:

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i\,.$$

A nevezőben szereplő $a^2 + b^2$ kifejezés mindig pozitív, kivéve ha $a = b = 0$, hiszen nem nulla valós szám négyzete pozitív. Ezért a fenti számolás mindig elvégezhető, ha a és b egyike nem nulla. A komplex számok egyenlőségének definíciója alapján viszont $a + bi$ akkor nulla, ha $a = b = 0$, és így a kapott képlet minden nem nulla komplex szám esetében értelmes.

1.3.6. Állítás. *A komplex számok között minden nem nulla számmal lehet osztani.*

Bizonyítás. Beszorzással ellenőrizhető, hogy

$$(a+bi)\left(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i\right) = 1\,,$$

és így tényleg az $a + bi$ szám reciprokát kaptuk. □

1.3.7. Következmény. *A komplex számok között egy szorzat csak akkor lehet nulla, ha valamelyik tényezője nulla. (Ezt a tulajdonságot most is nullosztómentességnek nevezzük.)*

Bizonyítás. Tegyük föl, hogy $zw = 0$, de $z \neq 0$. Meg kell mutatnunk, hogy akkor $w = 0$. Mivel $z \neq 0$, van reciproka, vagyis egy olyan u, melyre $uz = 1$. Ekkor

$$w = 1 \cdot w = (uz)w = u(zw) = u \cdot 0 = 0\,.$$

Tehát $\mathbb{C}$ valóban nullosztómentes. □

Az a kifejezés, amivel osztáskor a történet bővítettük, olyan fontos, hogy önálló nevet kapott. A $z = a + bi$ komplex szám *konjugáltjának* a $\overline{z} = a - bi$ számot nevezzük. Tehát *az osztás konkrét elvégzésekor a nevező konjugáltjával érdemes bővíteni.* A nevezőben ilyenkor a $z\overline{z} = a^2 + b^2$ kifejezés keletkezik, amiről láttuk, hogy nemnegatív valós szám.

1.3.8. Gyakorlat. Mutassuk meg, hogy ha z valós szám, akkor $\sqrt{z\overline{z}}$ a z abszolút értéke.

Ezt az észrevétel lehetővé teszi, hogy az abszolút érték fogalmát komplex számokra is kiterjesszük. A következő szakaszban egy újabb, geometriai indokot is fogunk látni arra, hogy miért érdemes a komplex számok abszolút értékét az alábbi módon definiálni.

1.3.9. Definíció. A $z = a + bi$ komplex szám konjugáltján a $\overline{z} = a - bi$ komplex számot, abszolút értékén a $|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$ nemnegatív valós számot értjük.

Nagyon fontos megértenünk, hogy komplex számok között már *nem igaz, hogy az abszolút érték mindig a szám maga, vagy az ellentettje* (ami valósakra igaz volt). Komplex számok között *egyenlőtlenségeket sem írhatunk fel* (kivéve, ha véletlenül valósak), tehát nem beszélhetünk például pozitív komplex számokról. Ennek okát később (az 5.8. Szakaszban) fogjuk majd látni. Most összefoglaljuk a konjugálás és az abszolút érték néhány tulajdonságát. Ezek közül többen emlékeztetnek arra, amit az 1.1.6. Állításban műveletartásnak neveztünk.

1.3.10. Állítás. *Tetszőleges $z, w \in \mathbb{C}$ számokra érvényesek az alábbiak.*

(1) *A konjugálás kölcsönösen egyértelmű, és $\overline{\overline{z}} = z$.*
(2) *$z = \overline{z}$ akkor és csak akkor, ha z valós.*
(3) *$\overline{z + w} = \overline{z} + \overline{w}$ (a konjugálás összegtartó).*
(4) *$\overline{zw} = \overline{z}\,\overline{w}$ (a konjugálás szorzattartó).*
(5) *$|z| = 0$ akkor és csak akkor, ha $z = 0$.*
(6) *$|\overline{z}| = |z|$.*
(7) *$|zw| = |z||w|$ (az abszolút érték szorzattartó).*

Bizonyítás. Az állítások mindegyikét könnyen be lehet látni úgy, hogy a $z = a + bi$ és $w = c+di$ helyettesítés után elvégezzük a műveleteket. Ezeket a számolásokat az Olvasóra hagyjuk, és csak annak a megmutatására szorítkozunk, hogy az abszolút érték szorzattartása hogyan következik abból, hogy a konjugálás szorzattartó. Nyilván

$$|zw|^2 = zw\,\overline{zw} = zw\,\overline{z}\,\overline{w} = z\overline{z}w\overline{w} = |z|^2|w|^2\,.$$

Mivel az abszolút érték nemnegatív, négyzetgyököt vonhatunk. □

Zárásként hadd említsük meg, hogy a komplex számokat nemcsak az algebrában használják. Egyes geometriai alakzatok sokkal jobban megérthetők, ha a leírásukra komplex változókat is használunk (az alakzat „valósban fekvő darabja" csupán a jéghegy csúcsa). A kvantummechanikában komplex értékű valószínűségek adják meg a részecskék állapotát. Az univerzum egyes modelljeiben az időt komplex szám jeleníti meg. Később megmutatjuk, hogy mi a komplex számoknak az a „nagyon jó" tulajdonsága, ami több ilyen alkalmazást lehetővé tesz.

Gyakorlatok, feladatok

1.3.11. Gyakorlat. Számítsuk ki az alábbi kifejezések értékét.

(1) $(1+i)(3-2i)$, $1/i$, $(1+i)/(3-2i)$.
(2) $|\overline{(4+i)}/(4+i)|$, $|(1+1526i)^{100}/(1-1526i)^{100}|$.
(3) $(1+i)^2$, $(1+i)^{1241}$.

1.3.12. Gyakorlat. Oldjuk meg az alábbi egyenleteket a komplex számok között.

(1) $x^2+1=0$.
(2) $x^2=-12$.
(3) $x^2+2x+2=0$.
(4) $x^2+2ix-1=0$.

1.3.13. Feladat. Határozzuk meg azokat a $c+di$ számokat (c és d valós), melyek négyzete $20i-21$. Oldjuk meg az $x^2+(i-2)x+(6-6i)=0$ egyenletet a komplex számok körében. E példa alapján adjunk általános eljárást a négyzetgyökvonásra, és a másodfokú egyenlet megoldására.

1.3.14. Gyakorlat. Oldjuk meg az alábbi egyenleteket a komplex számok között.

(1) $x^2=i$.
(2) $x^2+3x+4=0$.
(3) $x^2-(2+i)x+7i-1=0$.
(4) $(2+i)x^2-(5-i)x+2-2i=0$.
(5) $x=(3+2i)\overline{x}$.
(6) $x=2\cdot\mathrm{Re}(x)$.

1.3.15. Gyakorlat. Mutassuk meg, hogy a konjugálás szorzattartó.

1.3.16. Gyakorlat. Melyek igazak az alábbi állítások közül?

(1) A konjugálás tartja a kivonást.
(2) Az abszolút érték tartja az összeadást.
(3) Az abszolút érték tartja az osztást.

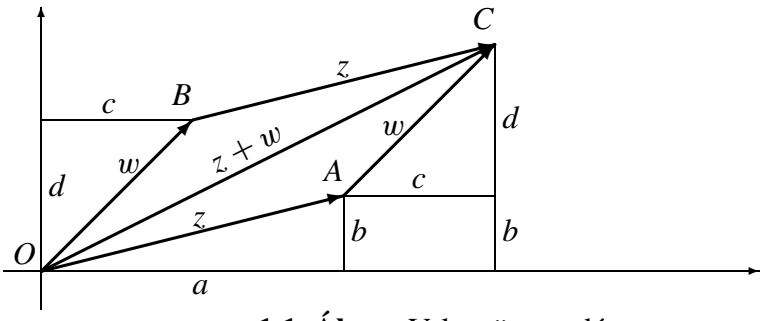
1.4. A komplex számok trigonometrikus alakja

A komplex számokat egyenletek megoldására akartuk használni. Ehhez a négy alapműveleten kívül gyökvonásra biztosan szükség van. Az 1.3.13. Feladat megoldásakor láttuk, hogy a komplex számok jobbak, mint a valósak a négyzetgyökvonás szempontjából, mert itt minden számból lehet négyzetgyököt vonni. Azt is láttuk azonban, hogy ez eléggé komplikált számolással jár, és a módszer már a köbgyökvonás elvégzéséhez is használhatatlanul bonyolultnak tűnik.

> Az ilyen zsákutcákból a matematikában nem egyszer úgy kecmergünk ki, hogy félretesszük az eredeti problémát, és egy másik, látszatra teljesen új témával kezdünk foglalkozni. Gyakran megesik, hogy ennek során váratlanul ötleteket kapunk az eredeti probléma megválaszolására is. Most is ezt az utat követjük, és „melléktermékként" nemcsak a gyökvonás módszerét fedezzük fel, hanem geometriai feladatok megoldásához is hasznos eszközre lelünk.

Az új téma amivel foglalkozunk, a következő: ha a valós számokat a számegyenesen tudjuk ábrázolni, akkor érdemes-e a komplex számokat is hasonló módon lerajzolni? A tapasztalatok azt mutatják, hogy erre a sík bizonyul alkalmasnak. Írjuk rá az $a + bi$ számot a sík (a, b) pontjára. Ez azért hasznos, mert a komplex számok műveletei nagyon ismerősek lesznek geometriából!

Akár fizikából, akár geometriából, mindannyian ismerjük a *vektorok* fogalmát. Foglaljuk össze, mit is tudunk ezekről. A vektorokat az irányított szakaszokból kapjuk úgy, hogy az egyenlő hosszú és egyforma állású irányított szakaszokat egyenlőnek, ugyanannak a vektornak tekintjük. Ezért néha érdemes csak azokat a szakaszokat vizsgálni, amelyek kezdőpontja az origóban van. Ekkor *helyvektorokról* beszélünk. A helyvektorokat szokás a végpontjukkal azonosítani, vagyis a sík (a, b) pontját vektornak is tekinthetjük: annak a vektornak, ami az origóból (a, b)-be mutat.

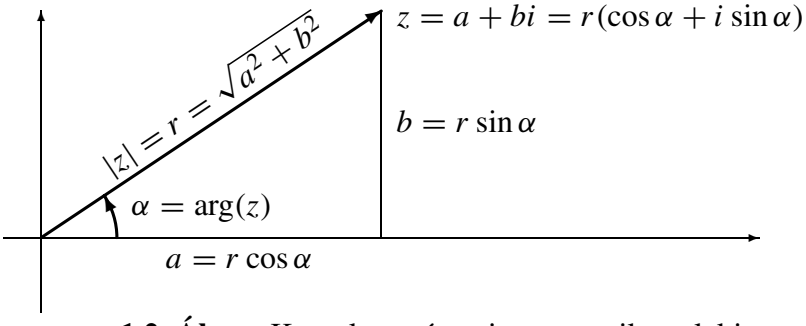


1.1. Ábra. Vektorösszeadás

Vektorokat úgy adunk össze, hogy egymás után fűzzük őket. Helyvektorok esetében ezt úgy lehet lefordítani, hogy az A és B pontba mutató vektorok összege akkor mutat a C pontba, ha az $OACB$ négyszög (esetleg elfajuló) paralelogramma. Ha kiszámoljuk a pontok koordinátáit, akkor ebből az adódik, hogy az (a, b) és (c, d) helyvektorok összege $(a + c, b + d)$. Vegyük észre, hogy ugyanezzel a képlettel kell összeadni a komplex számokat is!

1.4.1. Állítás. *A komplex számok összeadása a vektorösszeadásnak felel meg. Pontosabban: két komplex szám összegének megfelelő helyvektor a két komplex számnak megfelelő helyvektorok összege.*

A komplex számok szorzásának képlete első ránézésre nem utal geometriai kapcsolatra. Ahhoz, hogy a kapcsolatot felfedezzük, érdemes észrevenni, hogy minden nem nulla helyvektort egyértelműen meghatároz az origótól való távolsága, vagyis a *hossza*, továbbá az x-tengely pozitív felétől mért, irányított *szöge*. Például az $1-i$ szöge 315° (vigyázzunk, nem 45°). A z komplex szám szögét néha z árkuszának vagy *argumentumának* is nevezik, és ilyenkor $\arg(z)$-vel jelölik. Ez a szög egyértelműen meghatározott, ha kikötjük, hogy $0 \le \arg(z) < 2\pi = 360^\circ$ legyen.



1.2. Ábra. Komplex szám trigonometrikus alakja

Az 1.2. ábrából leolvashatjuk a következő összefüggéseket. Ha a $z = a + bi \neq 0$ szám hossza r és szöge α, akkor nyilván

$$a = r\cos\alpha \qquad \text{és} \qquad b = r\sin\alpha\,,$$

azaz $z = r\cos\alpha + ir\sin\alpha = r(\cos\alpha + i\sin\alpha)$. Ezt a felírást a $z \neq 0$ szám *trigonometrikus alakjának*, a $z = a + bi$ felírást *algebrai alaknak* nevezzük. Vegyük észre, hogy

$$|z|^2 = a^2 + b^2 = r^2(\cos^2\alpha + \sin^2\alpha) = r^2\,,$$

azaz *komplex szám hossza ugyanaz, mint az abszolút értéke.* Mindezt persze leolvashatjuk az ábráról is, ha Pitagorasz tételét alkalmazzuk. A nulla komplex számnak sem szöge, sem trigonometrikus alakja nincs.

1.4.2. Tétel. *Tetszőleges z és w komplex számokra $|z+w| \le |z| + |w|$ teljesül. Ezt* háromszög-egyenlőtlenségnek *nevezzük. Egyenlőség akkor van, ha z és w párhuzamosak, és egyenlő állásúak.*

Bizonyítás. Ha a z és w vektorokat összefűzéssel adjuk össze, akkor egy olyan OAC háromszöget kapunk, melyre $\overrightarrow{OA} = z$, $\overrightarrow{AC} = w$ és $\overrightarrow{OC} = z + w$. Vagyis az állítás valóban a háromszögegyenlőtlenségnek felel meg. Egyenlőség akkor van, ha a háromszög elfajuló, mégpedig úgy, hogy az A csúcs az OC szakaszra esik. □

A háromszög-egyenlőtlenséget algebrailag is be lehet bizonyítani, ha z-t és w-t algebrai alakban írjuk fel, és átrendezünk. Ekkor a híres Cauchy-Bunyakovszkij-Schwarz egyenlőtlenségre vezethetjük vissza az állítást. Ez a kapcsolat, és mindkét egyenlőtlenség sokkal általánosabban, úgynevezett euklideszi vektorterekben is teljesül. Az érdeklődő Olvasó a [**10**] könyv 8.2. Szakaszában nézhet mindennek utána.

A trigonometrikus alak jelentőségét akkor érthetjük meg igazán, ha ilyen alakban szorozzuk össze a komplex számokat. Legyen $z = r(\cos\alpha + i\sin\alpha)$ és $w = s(\cos\beta + i\sin\beta)$. Ekkor

$$zw = rs(\cos\alpha\cos\beta - \sin\alpha\sin\beta) + rs(\cos\alpha\sin\beta + \sin\alpha\cos\beta)i\ ,$$

ami az ismert addíciós képletek miatt $rs(\cos(\alpha+\beta) + i\sin(\alpha+\beta))$. Látszólag tehát beláttuk, hogy *komplex számok szorzásakor hosszuk összeszorzódik, szögük összeadódik.* Azt eddig is tudtuk, hogy az abszolút érték szorzattartó, a szögekre vonatkozó észrevétel azonban új.

Itt azonban valamire vigyáznunk kell. Komplex szám szögét 0 és 360° fok közöttinek definiáltuk. A most kapott képlet tehát szigorúan véve nem mindig trigonometrikus alak, mert az $\alpha+\beta$ szög túllépheti a 360 fokot. Például ha $-i$-t, aminek a hossza 1, szöge 270°, önmagával szorozzuk, akkor a fenti képletből a

$$(-i)^2 = \cos 540^\circ + i\sin 540^\circ$$

adódik. Ez persze ugyanaz, mint $\cos 180^\circ + i\sin 180^\circ = -1$, hiszen a sin és a cos függvény is 360° szerint periodikus. A legegyszerűbben úgy szabadulhatunk meg ettől a problémától, ha a trigonometrikus alakban megengedünk tetszőleges szöget, de ennek ára az, hogy a trigonometrikus alakban szereplő szög csak „modulo 360°" lesz egyértelmű.

1.4.3. Gyakorlat. Mutassuk meg, hogy

$$r(\cos\alpha + i\sin\alpha) = s(\cos\beta + i\sin\beta) \neq 0$$

akkor és csak akkor, ha $r = s \neq 0$, és $\alpha - \beta$ a 360° egész számú többszöröse.

A másik út az, ha az 1.1.4. Definícióhoz hasonlóan szögekre is bevezetjük a „modulo 360" összeadás fogalmát. Ha $0 \leq \alpha, \beta < 360$ (ezek most valós számok), akkor $\alpha +_{360} \beta$ értéke legyen $\alpha+\beta$, ha ez 360-nál kisebb, különben pedig $\alpha+\beta-360$.

1.4.4. Állítás. *Komplex számok szorzásakor hosszuk összeszorzódik, szögük pedig összeadódik (modulo 360°). A $z = r(\cos\alpha + i\sin\alpha) \neq 0$ számmal való szorzás tehát forgatva nyújtás: az origó körül α szöggel forgat, és az origóból r-szeresre nyújt.*

A komplex számok azért előnyösebbek a geometriai feladatok megoldásakor, mint a vektorok, mert nemcsak a vektorösszeadást, hanem a forgatásokat és nyújtásokat is fel lehet írni velük, méghozzá könnyebben kezelhető formában, mintha koordináta-geometriával számolnánk. A fejezet végén több feladattal próbáljuk meg illusztrálni ezeket az előnyöket.

1.4.5. Gyakorlat. Adjunk képletet két komplex szám hányadosára a trigonometrikus alak felhasználásával.

A szorzásra levezetett képlet segítségével hatványozni is tudunk, hiszen az ismételt szorzás. Nevezetesen

$$[r(\cos\alpha + i\sin\alpha)]^n = r^n(\cos n\alpha + i\sin n\alpha)\,.$$

Ezt az összefüggést *Moivre képletének* nevezzük. (Sokszor így hívják a trigonometrikus alakban felírt számok szorzásának szabályát is.) Hatványozáskor tehát a szöget a kitevővel kell szorozni, a hosszat pedig a kitevőre kell emelni. Ha a valós számokhoz hasonlóan a hatványozást negatív egész kitevőkre is kiterjesztjük, vagyis z^0 értékét 1-nek, z^{-n} értékét pedig $1/z^n$-nek definiáljuk, akkor az 1.4.5. Gyakorlat alapján könnyű meggondolni, hogy Moivre képlete minden egész kitevőre érvényes lesz.

Gyakorlatok, feladatok

1.4.6. Gyakorlat. Ha z és w komplex számok, mi a geometriai jelentése a $\overline{z}$ számnak, a $z-w$ vektornak, illetve a $|z-w|$ számnak?

1.4.7. Gyakorlat. Rajzoljuk le a komplex számsíkon a következő halmazokat:

(1) $\{z\in\mathbb{C} : \mathrm{Re}(z+3+2i)\le -2\}$.
(2) $\{z\in\mathbb{C} : \mathrm{Re}(z+1)\ge \mathrm{Im}(z-3i)\}$.
(3) $\{z\in\mathbb{C} : |z-i-1|\le 3\}$.
(4) $\{z\in\mathbb{C} : |z-3+2i| = |z+4-i|\}$.
(5) $\{z\in\mathbb{C} : z+\overline{z} = -1\}$.
(6) $\{z\in\mathbb{C} : 1/z = \overline{z}\}$, illetve $\{z\in\mathbb{C} : (1/z)+8 = \overline{z}\}$.
(7) $\{z\in\mathbb{C} : |z| = iz\}$.
(8) $\{z\in\mathbb{C} : \mathrm{Im}((z-1)/(z+1)) = 0\}$, illetve $\{z\in\mathbb{C} : \mathrm{Re}((z-1)/(z+1)) = 0\}$.

1.4.8. Gyakorlat. Írjuk fel az alábbi komplex számokat trigonometrikus alakban:

(1) $1+i$ és $1-i$.
(2) $\sqrt{3}+i$ és $-1-\sqrt{3}i$.
(3) $\cos(60^\circ) - i\sin(60^\circ)$.
(4) $\cos(30^\circ) - i\sin(60^\circ)$.

1.4.9. Gyakorlat. A sík mely geometriai transzformációinak felelnek meg a komplex számok halmazának alábbi leképezései:

(1) $z\to 3z+2$.
(2) $z\to (1+i)z$.
(3) $z\to 1/\overline{z}$.

1.4.10. Gyakorlat. Legyenek $z=a+bi$ és $w=c+di$ különböző komplex számok. Írjuk fel az alábbi „alakzatok egyenletét” komplex számok segítségével. Az eredményben ne szerepeljen a, b, c, d, csak z és w.

(1) A z-t w-vel összekötő szakasz felezőpontja.
(2) A z-t w-vel összekötő szakasz felező merőlegese.

(3) A z középpontú, w-t tartalmazó körvonal.
(4) Az origóból z-be mutató vektor $+90$ fokos elforgatottja.
(5) A w-ből z-be mutató vektor $+90$ fokos elforgatottja.
(6) A z pont w körüli $+90$ fokos elforgatottja.
(7) Annak a négyzetnek a csúcsai, amelynek a z-t w-vel összekötő szakasz átlója.
(8) Annak a két szabályos háromszögnek a középpontja, melyeknek az adott két szám két csúcsa.

1.4.11. Feladat. Egy négyszög oldalaira kifelé négyzeteket rajzolunk. Kössük össze az átellenes oldalakra rajzolt négyzetek középpontjait. Mutassuk meg, hogy az így kapott két szakasz merőleges, és egyenlő hosszú.

1.4.12. Feladat. Írjunk egy háromszög mindegyik oldalára kifelé egy szabályos háromszöget. Igazoljuk, hogy ezek középpontjai szabályos háromszöget alkotnak.

1.4.13. Feladat. Mutassuk meg, hogy a z_1, z_2, z_3, z_4 páronként különböző komplex számok akkor és csak akkor vannak egy körön vagy egyenesen, ha kettősviszonyuk, vagyis a

$$(z_1\,,\,z_2\,,\,z_3\,,\,z_4) = \frac{z_3 - z_1}{z_3 - z_2} \Big/ \frac{z_4 - z_1}{z_4 - z_2}$$

kifejezés valós szám.

1.4.14. Feladat. Igazoljuk Ptolemaiosz tételét: ha egy négyszög oldalainak hossza rendre a, b, c, d, átlóinak hossza pedig e és f, akkor $ac + bd \geq ef$, és egyenlőség akkor és csak akkor áll, ha a négyszög (konvex) húrnégyszög.

1.4.15. Feladat. Hozzuk zárt alakra a $\sin x + \sin 2x + \ldots + \sin nx$ összeget.

1.5. Egységgyökök és rendjeik

Moivre képlete alapján már el tudjuk végezni komplex számok között a gyökvonást. Ehhez a megoldást trigonometrikus alakban keressük. Ha tehát $z = r(\cos\alpha + i\sin\alpha)$ nem nulla szám, és $n \geq 1$ egész, akkor olyan w számot keresünk, amelyre $w^n = z$. Azonnal láthatjuk, hogy $w_0 = \sqrt[n]{r}(\cos(\alpha/n) + i\sin(\alpha/n))$ jó lesz, hiszen ezt a számot n-edik hatványra emelve z-t kapjuk vissza.

1.5.1. Gyakorlat. Ahhoz, hogy w_0 értékét kiszámítsuk, n-edik gyököt kell vonni r-ből. Miért egyszerűbb dolog ez, mint egy általános komplex számból vonni n-edik gyököt?

A z szám *összes* n-edik gyökét közvetlen számolással is megkereshetjük.

1.5.2. Gyakorlat. Igazoljuk, hogy a $z = r(\cos\alpha + i\sin\alpha)$ szám n-edik gyökei pontosan a

$$w = \sqrt[n]{r}\left(\cos\frac{\alpha + 2k\pi}{n} + i\sin\frac{\alpha + 2k\pi}{n}\right)$$

alakú számok, ahol $0 \leq k < n$ egész szám.

A közvetlen számolás helyett a következőképpen is eljárhatunk. Legyen w a z tetszőleges n-edik gyöke. A fenti w_0 számra ekkor $w_0^n = z = w^n$, ahonnan $(w/w_0)^n = 1$. Jelöljük a w/w_0 hányadost ε-nal, akkor tehát $\varepsilon^n = 1$. Így ha sikerülne meghatározni az ilyen ε számokat, akkor az összes keresett w-t is megkapnánk a $w = \varepsilon w_0$ összefüggésből.

1.5.3. Definíció. Az $\varepsilon \in \mathbb{C}$ számot n-edik *komplex egységgyöknek* nevezzük, ha $\varepsilon^n = 1$.

Például az i szám negyedik egységgyök, hiszen $i^2 = -1$, és ezért $i^4 = 1$. Az i szám hatványai tehát

i^1,	i^2,	i^3,	i^4,	i^5,	i^6,	i^7,	i^8,	...
i,	-1,	$-i$,	1,	i,	-1,	$-i$,	1,	...

Vagyis a hatványok periodikusan ismétlődnek. Ha lerajzoljuk őket, egy négyzetet kapunk, melynek a középpontja az origó, és az egységkörbe írható. Ezeket az észrevételeket rövidesen általánosítani fogjuk, és akkor az is kiderül majd, hogy az i, -1, $-i$, 1 számok az 1 szám *összes* negyedik gyöke, vagyis az összes negyedik egységgyök.

Az n-edik egységgyököket trigonometrikus alakban keressük meg. Mivel $\varepsilon^n = 1$, és az abszolút érték szorzattartó, $|\varepsilon|^n = 1$, azaz $|\varepsilon| = 1$. Tehát $\varepsilon = \cos\alpha + i\sin\alpha$, és így

$$\cos n\alpha + i\sin n\alpha = \varepsilon^n = 1 = 1(\cos 0 + i\sin 0)\,.$$

Az 1.4.3. Gyakorlat miatt $n\alpha = 2k\pi$ alkalmas k egészre. Tehát $\alpha = 2k\pi/n$.

1.5.4. Tétel. *Az n-edik egységgyökök száma pontosan n, ezek az*

$$\varepsilon_k = \cos(2k\pi/n) + i\sin(2k\pi/n) = \varepsilon_1^k$$

képlettel definiált $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n = 1$ számok. Ha $z = r(\cos\alpha + i\sin\alpha)$ nem nulla komplex szám, akkor egyik n-edik gyöke

$$w_0 = \sqrt[n]{r}(\cos(\alpha/n) + i\sin(\alpha/n))\,,$$

a többi n-edik gyökét pedig úgy kapjuk meg, hogy a w_0 számot végigszorozzuk az n-edik egységgyökökkel. Minden nem nulla komplex számnak pontosan n darab n-edik gyöke van a komplex számok között, és ezek egy origó középpontú szabályos sokszög csúcsaiban helyezkednek el.

Bizonyítás. Ha lerajzoljuk az $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n = 1$ számokat a síkon, akkor egy szabályos n-szöget kapunk, amelynek természetesen mind különbözők a csúcsai. Viszont $\varepsilon_{n+1} = \varepsilon_1$, $\varepsilon_{n+2} = \varepsilon_2$, és így tovább, vagyis körbe-körbe járunk a szabályos n-szög csúcsain. Általában ha k-nak az n-nel való osztási maradéka r, akkor nyilván $\varepsilon_k = \varepsilon_r$. Az $\varepsilon_k = \varepsilon_1^k$ összefüggés nyilvánvalóan következik Moivre képletéből. Végül a z szám n-edik gyökei azért alkotnak szabályos n-szöget, mert ez w_0-lal szorzással, azaz forgatva nyújtással kapható az egységgyökök által alkotott sokszögből. □

Az n-edik komplex egységgyököket „ugyanúgy kell szorozni, ahogy a modulo n maradékokat összeadni”. Valóban, amikor az ε_k és ε_ℓ számokat szorozzuk össze, akkor a szögeket modulo 360° kell összeadni, és ezért az indexek modulo n adódnak össze. Képlettel felírva:

$$\varepsilon_{k+n\ell} = \varepsilon_k \varepsilon_\ell \,.$$

Még máshogy fogalmazva a $k \mapsto \varepsilon_k$ leképezés (kölcsönösen egyértelmű, és) művelettartó a $\mathbb{Z}_n$ halmaz és az n-edik egységgyökök halmaza között akkor, ha az első esetben a modulo n összeadást, a másodikban pedig a komplex számok szorzását tekintjük műveletnek. (De mondhatjuk azt is, hogy a $\mathbb{Z}$-ből $\mathbb{C}$-be vezető $k \mapsto \varepsilon_k$ leképezés művelettartó, ha az első művelet az összeadás, a második a szorzás, hiszen $\varepsilon_{k+\ell} = \varepsilon_k \varepsilon_\ell$ is teljesül. Ez a leképezés azonban már nem kölcsönösen egyértelmű.)

A fejezet hátralévő részében a komplex szám *rendjének* a fogalmával ismerkedünk meg. Ez a téma kicsit nehezebb az eddigieknél, ezért az Olvasó megteheti, hogy előreszalad a polinomokhoz, és ide akkor tér vissza, amikor már kicsit jobban beleszokott az új gondolkodásmódba. A most következő anyagra legközelebb a körosztási polinomok vizsgálatakor, azután pedig a csoportelméleti elemrend tárgyalásakor lesz szükség.

Az ε_1 komplex számról beláttuk, hogy hatványai periodikusan ismétlődnek. Vizsgáljunk most meg ebből a szempontból egy tetszőleges z nem nulla komplex számot. „Tipikus esetben” a z szám összes egész kitevőjű hatványa páronként különböző lesz. Ilyen szám például a $z = 2$, hiszen az $1, 2, 4, 8, \ldots$ és $1, 1/2, 1/4, 1/8, \ldots$ számok között nincs két egyenlő.

1.5.5. Gyakorlat. Mely valós $z \neq 0$ számokra fordulhat elő, hogy $z^k = z^\ell$, noha $k \neq \ell$?

Tegyük föl, hogy z-nek vannak egyenlő hatványai is: $z^k = z^\ell$, noha $k \neq \ell$. Ekkor $z^{k-\ell} = z^{\ell-k} = 1$, így vannak olyan kitevők, melyekre z-t emelve 1-et kapunk. Ezeket hívjuk *jó kitevőknek*.

$$\boxed{n \text{ jó kitevője } z\text{-nek, ha } z^n = 1.}$$

Mivel a $k - \ell$ és $\ell - k$ jó kitevők egyike pozitív, van pozitív jó kitevő is. Legyen d a *legkisebb* pozitív jó kitevő. Osszuk el $k - \ell$-et maradékosan d-vel: $k - \ell = dq + r$, ahol $0 \leq r < d$. Ekkor

$$1 = z^{k-\ell} = z^{dq+r} = (z^d)^q z^r = 1^q z^r = z^r \,.$$

Tehát r is jó kitevő. Mivel d a legkisebb pozitív jó kitevő volt, és $r < d$, az r már nem lehet pozitív. Ezért $r = 0$, vagyis $d \mid k - \ell$. Beláttuk tehát, hogy ha $z^k = z^\ell$, akkor $d \mid k - \ell$.

Ennek az állításnak a megfordítása is igaz. Ha $d \mid k - \ell$, akkor $z^{k-\ell}$ hatványa $z^d = 1$-nek, és így $z^{k-\ell} = 1$, vagyis $z^k = z^\ell$. Szavakban megfogalmazva: z két hatványa akkor és csak akkor egyenlő, ha a kitevők különbsége a d szám többszöröse.

Tehát z hatványai d szerint periodikusak! Hiszen $z, z^2, \ldots, z^d = 1$ még páronként különböző (mert e d-nél kisebb kitevők különbsége nem lehet d-vel osztható), de már $z^{d+1} = z$, $z^{d+2} = z^2$, és így tovább. Így z-nek pontosan d darab különböző hatványa van. Ezt a d számot a z *rendjének* nevezzük.

1.5.6. Definíció. Egy z komplex szám különböző (egész kitevős) hatványainak a számát a z *rendjének* nevezzük. Ez vagy pozitív egész, vagy ∞. A rendet $o(z)$-vel jelöljük.

1.5.7. Tétel. *A z számnak vagy bármely két egész kitevőjű hatványa különböző (ilyenkor a rendje végtelen), vagy pedig a hatványok a rend szerint periodikusan ismétlődnek. A rend a legkisebb pozitív „jó" kitevő, vagyis a legkisebb olyan pozitív egész, melyre a számot emelve* 1*-et kapunk. Továbbá*

$$\boxed{z^k = z^\ell \iff o(z) \mid k-\ell, \quad \textit{speciálisan} \quad z^k = 1 \iff o(z) \mid k.}$$

A jó kitevők tehát pontosan a rend többszörösei.

Az Olvasónak *a lehető legmelegebben ajánljuk,* hogy a fentiek jobb megértése érdekében ismételje át a rendnek a számelméletben használt, analóg fogalmát (lásd például [**11**], 3.2. Szakasz). Röviden összefoglaljuk a legfontosabb tudnivalókat.

Legyen $z \in \mathbb{Z}_m$ olyan szám, amely m-hez relatív prím. Hatványozzuk z-t a modulo m szorzás szerint. A hatványok periodikusan ismétlődni fognak. Nevezzük z rendjének modulo m (jele $o_m(z)$) a z szám modulo m különböző hatványainak a számát. A rend most is a legkisebb pozitív „jó" kitevő, vagyis a legkisebb olyan pozitív egész, melyre a számot a $*_m$ szorzás szerint hatványozva 1-et kapunk. Az elemi számelméletben szívesebben használnak mindennek a kifejezésére kongruenciákat. Ezen a nyelven fogalmazva tehát tetszőleges m-hez relatív prím z egészre

$$\boxed{z^k \equiv z^\ell \ (m) \iff o_m(z) \mid k-\ell, \quad \text{speciálisan} \quad z^k \equiv 1 \ (m) \iff o(z) \mid k.}$$

A jó kitevők tehát pontosan a rend többszörösei.

Fontos észrevennünk, hogy nem minden n-edik komplex egységgyök rendje n. Például az 1 rendje 1, noha az 1 minden n-re n-edik egységgyök. A negyedik egységgyökök közül az i és $-i$ rendje 4, a -1 rendje 2, az 1 rendje pedig 1. A hatodik egységgyökök rendjeit a 3.1. ábrán szemléltettük (123. oldal). Próbáljuk most általánosan meghatározni az n-edik egységgyökök rendjeit. Ebben a következő feladat lesz a segítségünkre.

1.5.8. Feladat. Egy bolha ugrál körbe egy n-szög csúcsain, úgy, hogy minden ugrásnál k csúcsnyit lép előre. Hány lépés után jut vissza a kiindulóponthoz? Hány kört tesz meg ezalatt? Hány csúcsot érint összesen?

1.5.9. Tétel. *Ha a z komplex szám rendje véges, és k egész szám, akkor*

$$\boxed{o(z^k) = \frac{o(z)}{(o(z), k)}\,.}$$

Ez a hatvány rendjének képlete.

Bizonyítás. Legyen $o(z) = n$, és írjuk fel a z hatványait sorban egy n-szög csúcsaira. Helyezzünk rá egy bolhát a $z^n = 1$-nél levő csúcsra. Amikor a z^k számot hatványozzuk, akkor mindig azokra a csúcsokra jutunk, ahol a bolha lesz, amikor k-asával ugrál (az első ugrás után a z^k-ban, azután a $(z^k)^2$-ben, és így tovább). A z^k rendje a hatványainak a száma, vagyis a bolha által érintett csúcsok száma, ami az előző feladat szerint $n/(n, k)$. □

A képlettel ellenőrizhetjük, hogy mivel $o(i) = 4$, azért valóban $o(i^2) = 4/(4, 2) = 2$, és $o(i^3) = 4/(4, 3) = 4$. Általában, ha

$$\varepsilon_k = \cos(2k\pi/n) + i \sin(2k\pi/n) = \varepsilon_1^k ,$$

akkor már láttuk, hogy ε_1-nek n különböző hatványa van, tehát a rendje n, és így a képlet szerint

$$o(\varepsilon_k) = o(\varepsilon_1^k) = \frac{n}{(n, k)} .$$

Ezt praktikusabban is megfogalmazhatjuk. Az ε_k képletében egyszerűsítsük le a k/n törtet. Ekkor elérhetjük, hogy k és n relatív prímek legyenek. Ilyenkor pedig a fenti képlet n-et ad eredményül. Ez az észrevétel igen hasznos konkrét számoláskor, feladatmegoldáskor, ezért egy külön állításba foglaljuk.

1.5.10. Állítás. *Egy $z \neq 0$ komplex szám rendje akkor és csak akkor véges, ha abszolút értéke* 1, *szöge pedig a 2π racionális többszöröse. Ha ez a racionális szám egyszerűsíthetetlen tört alakjában felírva p/q (ahol $q > 0$), akkor a z rendje q.*

1.5.11. Definíció. Az n rendű komplex számokat *primitív n-edik egységgyököknek* nevezzük.

Ezek mind az n-edik egységgyökök között vannak, és a fenti képlet szerint pontosan azok az ε_k számok lesznek primitív n-edik egységgyökök, melyekre $(k, n) = 1$.

1.5.12. Tétel. *A primitív n-edik egységgyökök pontosan az*

$$\varepsilon_k = \cos(2k\pi/n) + i \sin(2k\pi/n)$$

alakú számok, ahol k és n relatív prímek, és $0 \leq k < n$. Számuk $\varphi(n)$, ahol φ a számelméletből ismert Euler-függvény (lásd A.4.1. Definíció). Egy komplex szám akkor és csak akkor n-edik primitív egységgyök, ha a hatványai pontosan az összes n-edik egységgyökök.

Bizonyítás. Csak az utolsó állítást nem láttuk be az eddigiek során. Ha ε primitív n-edik egységgyök, akkor a rendje n, ezért n különböző hatványa van. Ezek mind n-edik egységgyökök, és mivel abból is n darab van, mindet meg kell kapjuk. Megfordítva, ha ε hatványai pont az n-edik egységgyökök, akkor n különböző hatványa van, és így a rendje n. □

A rend fogalmának bevezetésével befejeztük a komplex számokkal való ismerkedést. Noha láttunk néhány geometriai alkalmazást, és a gyökvonás sem probléma többé, a harmadfokú egyenlettel kapcsolatos kérdéseket még nem tisztáztuk. Erre akkor kerül majd sor, amikor már eleget fogunk tudni polinomokról is. Mostantól kezdve *szám* alatt mindig komplex számot értünk.

Gyakorlatok, feladatok

1.5.13. Gyakorlat. Oldjuk meg az alábbi egyenleteket a komplex számok között:

(1) $x^3 = 1$.
(2) $x^4 = -4$.
(3) $x^8 = \sqrt{3} - i$.
(4) $x^n = -1$.

1.5.14. Gyakorlat. Mennyi a rendje az

$$1 + i, \quad (1 + i)/\sqrt{2}, \quad \cos(\sqrt{2}\pi) + i \sin(\sqrt{2}\pi), \quad \cos(336^\circ) + i \sin(336^\circ)$$

számoknak? Melyek ezek között az egységgyökök? Mely n-ekre lesznek ezek a számok n-edik egységgyökök? És primitív n-edik egységgyökök?

1.5.15. Gyakorlat. Mutassuk meg, hogy minden egységgyök pontosan egy n-re lesz primitív n-edik egységgyök, de végtelen sok n-re lesz n-edik egységgyök.

1.5.16. Gyakorlat. Mutassuk meg, hogy ha $n > 0$ egész, $\varepsilon \in \mathbb{C}$, és $\varepsilon^n = i$, akkor ε rendje véges, és néggyel osztható.

1.5.17. Gyakorlat. Ha ε primitív 512-edik egységgyök, mennyi lehet $o(-i\varepsilon)$?

1.5.18. Feladat. Hogyan függ össze egy komplex szám és az ellentettjének a rendje? (Először kis n számokra vizsgáljuk meg).

1.5.19. Gyakorlat. Szorozzuk össze a hatodik egységgyököket a negyedik egységgyökökkel az összes lehetséges módon. Hány különböző számot kapunk? Mi a helyzet, ha a hatodik és a hetedik egységgyököket szorozzuk össze?

1.5.20. Gyakorlat. Legyenek m és n pozitív egészek.

(1) Hány közös gyöke van az $x^n = 1$ és $x^m = 1$ egyenleteknek $\mathbb{C}$-ben?
(2) Mutassuk meg, hogy egy n-edik és egy m-edik egységgyök szorzata nm-edik egységgyök.
(3) Bizonyítsuk be, hogy egy n-edik és egy m-edik primitív egységgyök szorzata akkor és csak akkor nm-edik primitív egységgyök, ha m és n relatív prímek.

1.5.21. Gyakorlat. Mennyi az n-edik egységgyökök összege, szorzata és négyzetösszege?

Az alábbi feladatokban használjuk fel a 2.2.37. Gyakorlatban bizonyított binomiális tételt.

1.5.22. Feladat. Hozzuk „zárt alakra” a következő összeget:

$$\binom{1867}{0} + \binom{1867}{4} + \binom{1867}{8} + \binom{1867}{12} + \dots .$$

(Az utolsó tagban alul 1864 szerepel, de ezt nem kell kiírni, mert egy binomiális együttható értéke megállapodás szerint nulla, ha alul nagyobb szám van, mint fölül.)

1.5.23. Feladat. Fejezzük ki $\cos x$ és $\sin x$ segítségével $\sin 7x$-et. Általánosítsuk a kapott képletet.

1.6. A komplex számok precíz bevezetése

Bizonyára sok Olvasónk hallott már Gödel nevezetes tételéről, amely nagyon durva fogalmazásban ezt állítja: nem lehet bebizonyítani, hogy a matematikában soha nem fog felbukkanni ellentmondás. (Ezt, sajnos, teljes szabatossággal be lehet bizonyítani.) Így teljes biztonságot nem érhetünk el a komplex számok bevezetésekor sem. De ha az igényeinket lejjebb adjuk, akkor sem lehetünk elégedettek a komplex számok eddig használt, szemléletes bevezetésével. Eleve zavaró például az, hogy még mielőtt összeadást és szorzást definiáltunk volna, már magában a komplex szám $a + bi$ definíciójában mindkettő szerepel. Márpedig a matematikában nem definiálhatunk egyetlen fogalmat sem Münchausen-módra, saját maga segítségével.

Érdemes tehát a komplex számok fogalmát egy fokkal precízebben bevezetni, mint ahogy eddig tettük, hogy ne adjon félreértésre alkalmat, hogy meggyőzhessük magunkat arról: ha a valós számokkal való számolás során nem lehet baj (ellentmondás), akkor a komplex számok használata esetében sem lesz. Természetesen mindez csak a szemléletesség rovására történhet. Ezért úgy kell ügyeskednünk, hogy a bevezetés végére érve az eddig szemléletesen használt fogalmakat, jelöléseket továbbra is ugyanúgy használhassuk, ne keletkezzenek felesleges bonyodalmak.

A komplex számok precíz bevezetése magasabb fokú matematikai érettséget igényel, mint amit a könyv eddigi részeiben feltételeztünk. Meggyőződésünk, hogy először a komplex számokkal (sőt, esetleg a polinomokkal) való számolás gyakorlati fogásait célszerű elsajátítani. Ezért *ezt a szakaszt teljes egészében apró betűs résznek érdemes tekinteni.* Csak a jobb olvashatóság kedvéért nem szerepel ebben a formában. A könyv első olvasásakor az Olvasó nyugodtan átugorhatja, annál is inkább, mert a konstrukció igazán tanulságos mozzanatai később újra és újra megjelennek majd. Először a polinomok precíz bevezetésekor (2.3. Szakasz), később a hányadostest, vagy az egyszerű algebrai tesbővítés konstrukciójakor. Sőt, a faktorgyűrűk vizsgálatakor a komplex számok bevezetésére is egy alternatív, ugyancsak precíz módszert lelünk majd.

Abból indulunk ki, ahogy a komplex számok egyenlőségét definiáltuk. A komplex számokat a valós és képzetes részük egyértelműen meghatározza, és ezek tetszőleges valós számok lehetnek. Így az $a + bi$ komplex számra gondolva egy olyan matematikai objektumot kell keresnünk, amelyet az a és b számok (a sorrendre is tekintettel) egyértelműen meghatároznak. Ilyen objektum az (a, b) rendezett pár (de akinek jobban tetszik, gondolhat helyette a sík megfelelő pontjára is, és akkor egy füst alatt a komplex számok geometriai kapcsolatát is megkapja). Tehát a nem szemléletes, de jól kezelhető definíció a következő:

1.6.1. Definíció. Komplex számon egy $z = (a, b)$ rendezett párt értünk, ahol a és b valós számok. A $z = (a, b)$ komplex szám *valós része* a, *képzetes része* b.

A műveleteket is könnyen definiálhatjuk, ha suttyomban az (a, b) helyére odaképzeljük az $a + bi$-t, és így „átkódoljuk” az 1.3.2. Definíciót:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b)(c, d) = (ac - bd, ad + bc)\,.$$

A komplex számok között most nincsenek ott a valós számok, hiszen azok nem rendezett párok. Az a valós számot $a + 0 \cdot i$-ként írtuk fel komplex számként, ehelyett az $(a, 0)$ párra

kell gondolnunk. Az ilyen párokkal ugyanúgy kell számolni, mint a valós számokkal, hiszen a fenti képletek szerint

$$(a, 0) + (c, 0) = (a + c, 0)$$
$$(a, 0)(c, 0) = (ac, 0)\,.$$

Másképp fogalmazva, a

$$\varphi : a \mapsto (a, 0)$$

leképezés (amely kölcsönösen egyértelmű a valós számok és az $(a, 0)$ alakú komplex számok között) tartja az összeadást és a szorzást is. Ezért az a számot *azonosítjuk* a neki megfelelő $(a, 0)$ komplex számmal. (Ennek az azonosításnak vannak precíz technikái, amivel a halmazelméletben ismerkedhetünk meg.)

Látszólag nincs ott az újsütetű komplex számok között az i sem. A szemléletes definíció szerint persze $i = 0 + 1 \cdot i$, és így bevezethetjük az

$$i = (0, 1)$$

jelölést. Ekkor a szorzás szabálya miatt

$$i^2 = (0, 1)(0, 1) = (-1, 0)\,,$$

amit a -1 számmal azonosítottunk. Magyarul $i^2 = -1$, immár precízen. Végül az összeadás és a szorzás szabálya szerint

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1)\,,$$

ezt a számot pedig éppen $a + bi$-vel azonosítottuk. Így a komplex számok tényleg az $a + bi$ alakú kifejezések, melyekkel a műveleteket úgy kell végezni, ahogyan már megszoktuk.

1.7. Összefoglaló

A modulo m maradékok $\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$ halmazán bevezettük a *modulo m összeadás és szorzás* fogalmát (1.1.4. Definíció), és felderítettük ezek alapvető tulajdonságait (1.1.5. Állítás). Megállapítottuk, hogy ezek nagyon hasonlítanak a számok közötti műveletek tulajdonságaira, valamint hogy *művelettartó* az a leképezés, amely minden egész számhoz a mod m maradékát rendeli (1.1.6. Állítás). A kivonást az ellentett hozzáadásaként, az osztást a reciprokkal (inverzzel) való szorzásként definiáltuk. Az ellentett mindig létezik, a reciprok azonban nem. Nyitva maradt a *nullosztómentesség* kérdése is: egy szorzat lehet-e nulla úgy, hogy egyik tényezője sem nulla. A maradékokkal való számolást felhasználtuk kombinatorikai és számelméleti feladatok megoldására.

Megbeszéltük a harmadfokú egyenlet megoldási ötletét, és ebből levezettük a Cardano-képletet, bár az még nem derült ki, hogy ez megadja-e az egyenlet összes megoldását. Konkrét példák alapján azt tapasztaltuk, hogy ha az egyenletnek csak egy valós gyöke van, akkor azt a képlet megadja, de három valós gyök esetén ezeket csak úgy tudjuk megkapni, ha hajlandók vagyunk formálisan számolni negatív számok négyzetgyökeivel.

Hogy a negatív számok négyzetgyökeivel való számolást precízzé tegyük, bevezettük a *komplex számokat*, mint $a + bi$ alakú formális kifejezéseket, ahol $i^2 = -1$. Felfedeztük az összeadás és a szorzás szabályait és tulajdonságait (1.3.2. Definíció, 1.3.3. Állítás), melyek szintén nagyon hasonlítanak a számok közötti műveletek tulajdonságaihoz. A valós számokat is ($a + 0 \cdot i$ alakú) komplex számnak képzeljük, és ezentúl „szám" alatt komplex számot értünk. Megmutattuk, hogy minden nem nulla komplex számmal lehet osztani (1.3.6. Állítás): a törtet a nevező *konjugáltjával* kell bővíteni. Ebből levezettük a nullosztómentességet is (1.3.7. Állítás). Kiterjesztettük az *abszolút érték* fogalmát komplex számokra (de leszögeztük, hogy komplex számok között nem értelmezünk egyenlőtlenségeket). Összefoglaltuk a konjugálás és az abszolút érték tulajdonságait (1.3.10. Állítás).

A komplex számokat a sík pontjaival, illetve az ezekbe az origóból mutató helyvektorokkal azonosítottuk. Ekkor a komplex számok összeadása a vektorösszeadásnak felel meg. Egy komplex szám abszolút értéke az origótól való távolsága, és emiatt teljesül a *háromszög-egyenlőtlenség* (1.4.2. Tétel). Definiáltuk nem nulla komplex szám *szögét*, és *trigonometrikus alakját*. Megállapítottuk, hogy komplex számok szorzásakor a hosszak összeszorzódnak, a szögek pedig (mod 2π) összeadódnak (1.4.4. Állítás). Így képletet kaptunk a gyors hatványozásra (pozitív és negatív egész kitevők esetében). Az a következmény, hogy egy komplex számmal való szorzás egy forgatva nyújtás, lehetővé teszi, hogy komplex számokat használjunk geometriai feladatok megoldásához.

Megállapítottuk, hogy egy nem nulla komplex számnak minden n pozitív egészre pontosan n darab n-edik gyöke van, amelyek egy origó középpontú szabályos sokszög csúcsaiban helyezkednek el. A *gyökvonást* trigonometrikus alakban célszerű elvégezni (1.5.2. Gyakorlat). Azokat az ε komplex számokat, amelyekre $\varepsilon^n = 1$ teljesül, *n-edik egységgyököknek* neveztük. Ezek a $\cos(2k\pi/n) + i\sin(2k\pi/n)$ alakú számok, összesen n darab n-edik egységgyök van. Ha egy számnak ismerjük az egyik n-edik gyökét, akkor az összes n-edik gyökeit az n-edik egységgyökökkel való szorzással kapjuk (1.5.4. Tétel).

Egy $z \neq 0$ komplex szám $o(z)$ *rendje* a különböző hatványainak a száma. Ez vagy végtelen, ebben az esetben z bármely két egész kitevőjű hatványa különböző, vagy egy pozitív r szám, ebben az esetben z hatványai r szerint periodikusan ismétlődnek, vagyis

$$\boxed{z^k = z^\ell \iff o(z) \mid k - \ell}$$

(1.5.7. Tétel). Speciálisan z^n akkor és csak akkor 1, ha $o(z) \mid n$ (ezek a z szám „jó" kitevői). Egy z komplex szám rendje akkor és csak akkor véges, ha a szám egységgyök, vagyis ha hossza 1, szöge pedig a 2π racionális számszorosa. Ha ez a racionális szám p/q, és $(p, q) = 1$, akkor z rendje q (1.5.10. Állítás). Mindez a hatvány rendjének

$$\boxed{o(z^k) = \frac{o(z)}{(o(z), k)}}$$

képletéből következik (1.5.9. Tétel).

Egy szám *primitív* n-edik egységgyök, ha rendje n. Ezek a $\cos(2k\pi/n) + i\sin(2k\pi/n)$ alakú számok, ahol $(k, n) = 1$. Összesen $\varphi(n)$ darab primitív n-edik egységgyök van

(itt $\varphi(n)$ a számelméletből ismert Euler-függvény). Egy szám akkor és csak akkor n-edik primitív egységgyök, ha hatványai pontosan az összes n-edik egységgyökök (1.5.12. Tétel).

Végül mutattunk egy lehetséges módot a komplex számok precíz bevezetésére. Az $a + bi$-nek képzelt számot az (a, b) rendezett párként definiáltuk, és az ezek közötti műveleteket az 1.3.2. Definíció alapján adtuk meg (1.6.1. Definíció). Az a valós számot azonosítottuk az $(a, 0)$ komplex számmal, ezt azért tehettük meg, mert az összeadást és a szorzást mindkettővel „ugyanúgy" kell végezni. Ily módon a valós számok is komplex számokká váltak. Az $i = (0, 1)$ jelölést használva $(a, b) = a + bi$ adódott, és így precízzé tettük a komplex számok korábbi, szemléletes definícióját.

2. POLINOMOK

...de az a + b-t és a nullát, ami nem is nulla,
és az x-nek titokzatos hánytorgásait...

Fekete István: *Téli berek*

2.1. A polinom fogalma

Amikor közönséges egyenleteket kell megoldanunk, az ismeretlennel *formálisan* számolunk. Például az

$$\frac{x^2+x+1}{x+1} = x$$

egyenlet esetében nem próbálunk az x helyébe konkrét számokat helyettesíteni, hanem olyan átrendezést hajtunk végre, ami minden egyes x-re helyes. Így a fenti egyenletből $x+1$-gyel átszorozva

$$x^2+x+1 = x^2+x$$

adódik. Ezt az átalakítást akkor is helyesnek érezzük, ha tudjuk, hogy ez utóbbi egyenletnek nincs megoldása (hiszen $1 = 0$-ra vezet), tehát semmilyen konkrét x számra nem teljesül egyik felírt egyenlőség sem.

Ahogy tehát a komplex számok bevezetése kapcsán megállapítottuk, hogy milyen szabályok szerint szabad számolni negatív számok négyzetgyökeivel, úgy érdemes most is megvizsgálni, hogy az „ismeretlen, meghatározatlan számokat" tartalmazó kifejezéseket hogyan kezelhetjük.

Miért van erre szükség? Hiszen az egyenletmegoldást már a középiskolában begyakoroltuk. A válasz ismét az, hogy szeretnénk sok problémára közös megoldási módszert találni. Ilyen például egy egyenlet megoldóképlete. Más esetben olyan, minél egyszerűbb kifejezést kell felírnunk, ami adott helyeken adott értékeket vesz fel (így kereshet például egy fizikus törvényt, szabályszerűséget a mérési eredményeihez). Ilyenkor ismernünk kell a felírandó kifejezések tulajdonságait. Az is előfordul, hogy meg szeretnénk bizonyosodni: egy bonyolult egyenletnek nincs már más megoldása, mint amiket megtaláltunk. Ehhez jól jönne egy olyan tétel, ami megmondja, hogy egy egyenletnek, az alakjától függően, maximum hány megoldása lehet.

De szükség lehet *negatív eredmények* bizonyítására is. A matematikában nagyon hasznos ismerni a *módszereink korlátait* is, hogy tudjuk: egy-egy probléma megoldásához kell-e új

módszert kifejleszteni. Fontos példa ilyen korlátra, hogy a legalább ötödfokú egyenletek esetében már nem létezik olyan általános megoldóképlet, amely a négy alapművelet és gyökvonás segítségével megadja az egyenlet gyökeit. Ennek a bizonyításához precízen tudnunk kell, mit is értünk egyenlet, megoldóképlet alatt, és mik ezeknek a tulajdonságai.

A komplex számokhoz hasonlóan arra törekszünk, hogy az Olvasó minél hamarabb el tudjon kezdeni számolni polinomokkal. Ezért a lehető legpraktikusabban vezetjük be ezt a fogalmat. A precíz bevezetés megtalálható a 2.3. Szakaszban.

Elsőként az olyan kifejezéseket vesszük górcső alá, amelyekben számokon kívül csak egy x „ismeretlen" szerepel, és csak három műveletet használhatunk: összeadást, kivonást és szorzást. A komplex számok bevezetésekor észrevettük, hogy minden i-t tartalmazó, a fenti három művelettel felírt kifejezés $a + bi$ alakra egyszerűsíthető. Középiskolás tapasztalatunk az, hogy a zárójelek felbontásával, és x hatványai szerinti rendezéssel az x-et tartalmazó, e három művelettel felírt kifejezések a következő alakra hozhatók:

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n\,,$$

ahol $a_0, \ldots, a_n$ számok (mostani tudásunkkal persze már komplex számok is lehetnek), és $n \geq 0$ egész szám. Az ilyen kifejezéseket *polinomoknak* nevezzük. Az x a polinomban szereplő *határozatlan*. Az a_jx^j kifejezések a polinom *tagjai*, az a_i számok pedig a polinom *együtthatói*. Az a_0 a polinom *konstans tagja*.

Mivel formálisan számolunk, x-ről semmi mást nem tételezhetünk fel, csak azt, ami minden számra érvényes. Ezért $0 \cdot x$ természetesen nulla lesz, de a fenti képletben semmilyen más egyszerűsítési lehetőséget nem várhatunk. A $0 \cdot x^k$ tagot néha érdemes lesz kiírni, néha meg érdemes lesz elhagyni. Így tehát az $1 + x^2$ és az $1 + 0 \cdot x + x^2 + 0 \cdot x^3$ polinomokat egyenlőnek tekintjük. A legegyszerűbb, ha minden polinomba odaképzeljük a ki nem írt x-hatványokat is, nulla együtthatóval. Ekkor polinomok egyenlőségét a következőképpen definiálhatjuk.

2.1.1. Definíció. Két polinomot akkor és csak akkor tekintünk egyenlőnek, ha a megfelelő együtthatóik megegyeznek, vagyis ha minden $k \geq 0$ egészre az x^k együtthatója a két polinomban ugyanaz.

Ha a fenti f polinomban mindegyik a_i együttható nulla, akkor a *nullapolinomot* kapjuk (ez nem tévesztendő össze a 0 számmal, de mindkettőt 0 jelöli). Ha $f \neq 0$, akkor hagyjuk el a polinom jobb oldaláról a nulla együtthatójú tagokat. Így

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_kx^k$$

adódik, ahol $a_k \neq 0$. Ebben az esetben a k kitevő a polinom *foka*, az a_kx^k a polinom *főtagja*, az a_k szám pedig a polinom *főegyütthatója*. Egy polinom *normált*, ha főegyütthatója 1. Tehát csak a nem nulla polinomoknak értelmezzük a fokát. Az f polinom fokát $\mathrm{gr}(f)$-fel jelöljük (a *gradus* a „fok" szó latin megfelelője). Sok könyvben a $\deg(f)$ jelölést alkalmazzák (mert a „fok" angolul *degree*). Egyenlő polinomoknak természetesen ugyanaz

a foka (ha létezik). Az f helyett mindegyik jelölésben írhatunk $f(x)$-et is, ha fel akarjuk tüntetni, hogy x a határozatlan.

Ahhoz, hogy eldönthessük, tényleg minden vizsgált kifejezés a fenti alakra hozható-e, elegendő azt ellenőrizni, hogy a fenti alakú polinomokat összeadva, kivonva, és összeszorozva szintén ilyen alakú kifejezést kapunk. A komplex számok bevezetéséhez hasonlóan fontos lesz konkrétan kiszámolni az összeg és a szorzat képletét.

Két polinom összegének kiszámításához a kisebb fokú polinom végére írjunk nulla tagokat úgy, hogy a következő alakot kapjuk:

$$f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n\,, \qquad g = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n\,.$$

Tehát feltehető, hogy ugyanaz az n szám szerepel a két polinomban (de ekkor csak annyit tudunk, hogy polinomjaink foka legfeljebb n, tehát ilyenkor már nem tehetjük föl, hogy a két főegyüttható nem nulla). Ez a felírás azért hasznos, mert az összeadást könnyen elvégezhetjük:

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_n + b_n)x^n\,.$$

Hasonló képlet adja két polinom különbségét is.

2.1.2. Állítás. *Két polinom összegének a foka legfeljebb akkora, mint a két polinom fokai közül a nagyobb (pontosabban a nem kisebb). Képletben:* $\mathrm{gr}(f+g) \le \max(\mathrm{gr}(f), \mathrm{gr}(g))$. *Ha a két polinom foka különböző, akkor egyenlőség áll.*

Természetesen az összeg fokáról csak akkor beszélhetünk, ha az létezik, vagyis ha az összeg nem a nullapolinom.

Bizonyítás. Az f és g felírásában (hacsak nem $f = g = 0$) feltehetjük, hogy a két főegyüttható egyike, mondjuk a_n, nem nulla. Ha $b_n = 0$, akkor az összeg főegyütthatója is a_n lesz. Ha azonban mindkét polinom foka n, akkor elképzelhető, hogy $a_n + b_n = 0$. □

2.1.3. Gyakorlat. Szorozzuk össze az $a_0+a_1x+a_2x^2$ és $b_0+b_1x+b_2x^2+b_3x^3$ polinomokat, bontsuk fel a zárójelet, rendezzük az eredményt x hatványai szerint, végül állapítsuk meg az eredmény fokát.

A polinomok szorzásakor a következő felírás lesz hasznos:

$$f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n\,, \qquad g = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m\,,$$

ahol $a_n \neq 0$ és $b_m \neq 0$. (Ha valamelyik tényező a nullapolinom, akkor a szorzat nyilván szintén nulla.) Szorozzuk össze ezt a két polinomot.

2.1.4. Gyakorlat. Mutassuk meg, hogy az $(a_1 + \ldots + a_n)(b_1 + \ldots + b_m)$ szorzat egyenlő az nm darab a_ib_j szám összegével.

A fenti észrevétel alapján az f és g szorzásánál a zárójelet úgy bonthatjuk ki, hogy az első összeg minden tagját megszorozzuk a második összeg minden tagjával, majd a kapott szorzatokat összeadjuk. Ezt az $(n+1)(m+1)$ tagú összeget szeretnénk x hatványai szerint rendezni. Egy x^k-os tag úgy tud keletkezni, hogy egy x^i-s és egy x^j-s tagot szorzunk össze, ahol $i+j=k$. Így az fg szorzatban x^k együtthatója

$$c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \ldots + a_{k-1}b_1 + a_kb_0\,. \tag{2.1}$$

Látszólag c_k egy $k+1$ tagú összeg, de valójában az összegnek lehet kevesebb tagja. Például ha $k = m+n$, akkor az a_0b_{n+m} tag nem fog szerepelni, mert b indexe csak nullától m-ig halad. Ezt a gondot azonban könnyen kiküszöbölhetjük, ha megállapodunk abban, hogy nullának tekintjük $b_{m+1}, b_{m+2}, \ldots$, és ugyanúgy $a_{n+1}, a_{n+2}, \ldots$ értékét (ahogy már a polinomok egyenlőségének 2.1.1. Definíciója előtt is tettük). Ezzel a fenti (2.1) képlet mindkét formája helyessé válik.

Az x^{n+m} tag együtthatója tehát egy $n+m+1$ tagú összeg, de ennek csak egyetlen nem nulla tagja van: a_nb_m. Valóban, a tagok a_ib_j alakúak, ahol $i+j=n+m$, és ha $i>n$, akkor $a_i=0$, ha viszont $i<n$, akkor $j>m$, vagyis $b_j=0$. Ez az egyetlen a_nb_m tag viszont nem lesz nulla, mert egyik tényezője sem az. Ez bizonyítja a következő állítást.

2.1.5. Állítás. *Az fg szorzat főegyütthatója a_nb_m, foka $n+m$. Tehát nem nulla polinomok szorzásakor a fokok összeadódnak:* $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$. *Így a szorzatpolinom nem nulla, vagyis polinomok szorzására is érvényes a nullosztómentesség.*

A polinomokkal is a szokásos szabályok szerint számolhatunk. Foglaljuk össze bizonyítás nélkül ezeket a — remélhetőleg már ismerős — szabályokat.

2.1.6. Állítás. *Legyenek f, g, h tetszőleges polinomok.*

(1) $(f+g)+h = f+(g+h)$ *(az összeadás asszociatív).*
(2) $f+g = g+f$ *(az összeadás kommutatív).*
(3) $f+0 = 0+f = f$ *(azaz létezik nullelem).*
(4) *Minden f-nek van ellentettje, azaz olyan g, melyre $f+g = g+f = 0$. (Ilyen g lesz az a polinom, melynek együtthatói az f együtthatóinak ellentettjei.)*
(5) $(fg)h = f(gh)$ *(a szorzás asszociatív).*
(6) $fg = gf$ *(a szorzás kommutatív).*
(7) $f\cdot 1 = 1\cdot f = f$ *(azaz létezik egységelem).*
(8) $(f+g)h = fh+gh$ *(disztributivitás).*

A (3) állításban szereplő 0 a nullapolinomot jelöli (és nem a 0 számot). Hasonlóképpen a (7) állításban szereplő 1 jel polinom, és nem szám: az a polinom, amelynek minden együtthatója nulla, kivéve a konstans tagot, ami 1. Általában tetszőleges c számot polinomnak is tekinthetünk. Ezek a *konstans polinomok*, azaz a nulladfokú polinomok és a nullapolinom. A konstans polinomokat ugyanúgy kell összeadni és szorozni, mint a megfelelő számokat.

Mivel minden polinomnak létezik ellentettje, a kivonás is korlátlanul elvégezhető (mint az ellentett hozzáadása). Korábban láttuk, hogy az osztást (a maradékokkal való számolásnál is, a komplex számoknál is) a reciprokképzésre, vagyis az inverz elemmel való szorzásra vezethetjük vissza. Így van ez a polinomoknál is, de csak nagyon kevés polinomnak van reciproka.

2.1.7. Állítás. *Az f polinomnak akkor és csak akkor van inverze (reciproka) a polinomok között, ha f nem nulla konstans polinom.*

Bizonyítás. Ha $c \neq 0$ konstans polinom, akkor inverze az $1/c$ konstans polinom (és így minden polinom eloszthető vele: az együtthatóit kell c-vel elosztani). Tegyük most fel, hogy az f polinomnak van inverze. Ez azt jelenti, hogy létezik olyan g polinom, hogy $fg = 1$. Így egyik tényező sem nulla, vagyis képezhetjük a szereplő polinomok fokát. Mivel szorzásnál a fokok összeadódnak, azt kapjuk, hogy

$$\mathrm{gr}(f) + \mathrm{gr}(g) = \mathrm{gr}(fg) = \mathrm{gr}(1) = 0\,.$$

Ezért f és g foka is nulla kell, hogy legyen, vagyis f csak konstans polinom lehet. □

Mielőtt továbblépnénk, bevezetünk egy jelölést, amit sokszor használunk majd a későbbiekben. Egy soktagú összeg jelölésére eddig a ... szimbólumot használtuk, például $a_1 + a_2 + \ldots + a_n$ jelentette azt, hogy az a_i számokat össze kell adni, miközben az i index 1-től n-ig fut. Ezzel a jelöléssel azonban több probléma is lehet. Ha az a_i egy bonyolult kifejezés, akkor esetleg kényelmetlen, vagy áttekinthetetlen leírni több tagot is (ahogy az imént három konkrét tagot is leírtunk: a_1-et, a_2-t és a_n-et). Esetleg nem is könnyű kitalálni, mire gondolhat az, aki mondjuk az $a_1 + a_3 + \ldots + a_n$ összeget írta le. Vajon itt a páratlan indexű a_i számokat kell összeadni? E problémák áthidalására a következő jelölés szolgál.

2.1.8. Definíció. A

$$\sum_{j=1}^{n} a_j$$

úgynevezett *szumma jelölés* azt jelenti, hogy a j változó 1-től n-ig fut, és minden értékére össze kell adni a szumma jel jobb oldalán álló a_j kifejezést. A

$$\prod_{j=1}^{n} a_j$$

produktum jelölés a szumma jelöléstől abban különbözik, hogy itt az a_j kifejezéseket össze kell szorozni.

Vagyis a fenti definícióban az $a_1 + a_2 + \ldots + a_n$ összeg, illetve az $a_1 a_2 \ldots a_n$ szorzat tömör jelölése szerepel. Sokszor előfordul, hogy a szummázás nem $i = 1$-től n-ig, hanem $i = m$-től n-ig megy. Sőt, azt is megtehetjük, hogy a szumma jel alá egy feltételt írunk, és

akkor a szummázást azokra az indexekre kell végrehajtani, amelyekre ez a feltétel teljesül. Például

$$\sum_{p\,<\,1000,\ p\ \text{prím}} p^2$$

az 1000-nél kisebb prímszámok négyzetösszege. Az új jelöléssel a szorzatpolinomnak a (2.1) képletben szereplő általános együtthatóját többféleképpen is felírhatjuk:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j$$

(a második szummában hallgatólagosan azt feltételeztük, hogy i és j nemnegatív egészek).

Ebben a szakaszban megismerkedtünk az egyhatározatlanú polinomok fogalmával, és néhány alapvető tulajdonságukkal. Sokszor előfordul, hogy több ismeretlenünk is van (és esetleg több egyenlet). Célszerű lenne tehát polinomnak tekinteni mondjuk az

$$x^2y^2 - 6xy^4 + \pi x - ix^2 + y + 2$$

kifejezést is. Az eddigiekhez hasonló módon definiálhatnánk a *többhatározatlanú* polinomok fogalmát, és levezethetnénk a műveleti szabályokat. Azonban a képleteink egyre bonyolultabbak lennének, és különben sem hasznos dolog sokszor végigcsinálni lényegében ugyanazt. Ezért más utat fogunk keresni.

Ezt az új utat a következő probléma megoldása jelöli ki: nullosztómentes-e a szorzás a többhatározatlanú polinomok között? Elvileg előfordulhatna, hogy amikor a szorzást elvégezzük, akkor a zárójel felbontása után keletkező összes tag kipotyog. Láttuk, hogy az egyhatározatlanú polinomok között ez nem történhet meg, az oka az volt, hogy ha a polinomok legmagasabb fokú tagjai a_nx^n és b_mx^m, akkor csak egyetlen x^{n+m}-es tag keletkezik a szorzásnál, és ezért az biztosan nem fog kiesni.

Többhatározatlanú polinomnál azonban vigyáznunk kell: a fenti polinomban x^2y^2-et vagy xy^4-t tekintsük-e magasabb fokú tagnak? Úgy érdemes eljárni, hogy kijelöljük az egyik határozatlant, mondjuk az x-et, és a polinomot az x hatványai szerint rendezzük:

$$(y^2 - i)x^2 + (-6y^4 + \pi)x + (y + 2)\,.$$

Az együtthatók most már nem számok, hanem y polinomjai, de ez nem gond, hiszen *számolni* azokkal is tudunk! Beszélhetünk főegyütthatóról is, ez most $y^2 - i$. A nullosztómentességhez az kell, hogy a két összeszorzott polinom főegyütthatójának szorzata ne legyen nulla, és ez igaz, mert y polinomjairól már beláttuk a nullosztómentességet.

A többhatározatlanú polinomok vizsgálatához tehát arra van szükség, hogy a polinomokat általánosan vezessük be: az együtthatókról ne tegyük fel, hogy számok, hanem csak azt, hogy *a szokásos szabályok szerint lehet velük számolni.* Ez más területen is kamatozna, például számelméleti feladatoknál, mert itt néha olyan egyenleteket kell megoldani, ahol az együtthatókkal modulo m kell számolni. Az is elképzelhető, hogy egy-egy alkalmazásban csak az egész, vagy csak a racionális együtthatójú polinomokat célszerű megengednünk.

E problémák megoldása érdekében a most következő két szakaszban (2.2 és 2.3) egy kitérőt teszünk.

Az Olvasó bátran megteheti, hogy ezt a kitérőt egyelőre átugorja, és a polinomokat továbbra is úgy tekinti, hogy az együtthatóik komplex számok. Ha így tesz, akkor ezzel a szemlélettel megértheti a 2.4. Szakaszban leírtak lényegét, de ha a többhatározatlanú polinom fenti, szemléletes „definícióját" elfogadja, akkor a polinomokról szóló további anyag jelentős részét is. Természetesen fog majd találkozni furcsa jelenségekkel (például azzal, hogy a nullosztómentesség általánosabb körülmények között nem mindig teljesül), ezért előbb-utóbb mindenképpen érdemes lesz majd visszatérnie a következő két szakaszhoz, és ezek megértése után még egyszer átvennie az anyagot.

Gyakorlatok, feladatok

2.1.9. Gyakorlat. Végezzük el az alábbi műveleteket a komplex együtthatós polinomok körében, és állapítsuk meg az eredmény fokát.
a) $(x^3 + 3x^2 + 2) - (x^3 + 3x - 4)$.
b) $(x^2 + ix + 3)(x^2 + i)$.

2.1.10. Gyakorlat. Mivel egyenlő az $(a_1 + b_1) \dots (a_n + b_n)$ szorzat? (Először $n = 3$-ra fejtsük ki.) Mi történik, ha sok tényezőt szorzunk össze, amelyek mindegyike soktagú összeg?

2.1.11. Gyakorlat. Igazoljuk a

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij}$$

azonosságot.

2.2. A szokásos számolási szabályok

Az előző szakaszban megállapítottuk, hogy a polinomokat úgy lenne érdemes bevezetni, hogy az együtthatóikról semmi mást nem teszünk föl, mint hogy azokkal a szokásos szabályok szerint számolni lehet. Ezeket a „szokásos" szabályokat már három ízben megfogalmaztuk: az 1.1.5, 1.3.3 és 2.1.6. Állításokban. Kézenfekvő tehát most már *általában* megfogalmazni őket, hogy ne kelljen még ötödször, hatodszor, hetedszer leírni ugyanazt, hanem egy szóval hivatkozhassunk rájuk. Ez a szakasz az új elnevezések bevezetését, felsorolását tartalmazza.

Adott tehát egy R halmaz, amin műveleteket (összeadást, szorzást) értelmezünk valamilyen módon. Egy kétváltozós $*$ művelet tehát semmi egyebet nem jelent, mint hogy R bármely két a és b elemét „össze tudjuk műveletezni" (összeadni, összeszorozni), és az $a * b$ eredmény szintén az R halmaznak egy eleme lesz. Vagyis egy kétváltozós művelet egy tetszőleges kétváltozós függvény az R halmazon, amely szintén az R halmazba képez.

Nagyon vigyázzunk arra, amikor egy műveletet megadunk, hogy azt tényleg *minden elempárra, egyértelműen* definiáljuk. Ezt mindig elsőnek érdemes ellenőrizni. Például a kivonás *nem művelet* a pozitív számok halmazán, hiszen a $3 - 5$ eredménye nincs benne ebben a halmazban. Viszont művelet lesz az egész számok halmazán, hiszen bármely két egész szám különbsége is egész szám

Most áttekintjük a műveletek már ismerős tulajdonságait.

2.2.1. Definíció. Legyen $*$ kétváltozós művelet az R halmazon. Azt mondjuk, hogy ez

(1) *asszociatív*, ha tetszőleges $x, y, z \in R$ esetén $(x * y) * z = x * (y * z)$;
(2) *kommutatív*, ha tetszőleges $x, y \in R$ esetén $x * y = y * x$.

Az asszociativitás azt jelenti, hogy a háromtényezős szorzatokat zárójelek nélkül írhatjuk fel (de a sorrendre ügyelnünk kell). Ebből már (nem könnyen, de) be lehet bizonyítani, hogy a több tényezős szorzatok felírásakor sem kell zárójeleket használni. Az Olvasó esetleg meg is próbálkozhat a bizonyítással.

2.2.2. Feladat. Mutassuk meg, hogy ha $*$ asszociatív művelet, akkor az $a_1 * a_2 * \ldots * a_n$ szorzatot akárhogyan is zárójelezzük, az eredmény mindig ugyanaz lesz.

Asszociatív műveletre az egyik legfontosabb, eddig még nem szerepelt példa az, amikor függvényeket helyettesítünk egymásba.

2.2.3. Definíció. Legyen X tetszőleges halmaz, és R az összes X-et X-be képző (egyváltozós) függvények halmaza. Ha $f, g \in R$, akkor $f \circ g$ azt a függvényt jelöli, amikor f-be g-t helyettesítünk, vagyis először g-t, majd f-et alkalmazzuk. Képlettel kifejezve

$$(f \circ g)(x) = f\big(g(x)\big)$$

tetszőleges $x \in X$ esetén. Az $f \circ g$ neve az f és g *kompozíciója*.

Az analízisben néha kompozíció helyett *összetett függvény* képzéséről beszélnek. Ez a művelet általában nem kommutatív. Nem mindegy, hogy a csirkét előbb megkopasztjuk, és azután megsütjük, vagy előbb megsütjük, és azután megkopasztjuk. A kompozíció művelete azonban mindig asszociatív.

2.2.4. Gyakorlat. Mutassuk meg, hogy a kompozíció művelete asszociatív. Adjunk példát két geometriai transzformációra, ami azt mutatja, hogy a kompozíció nem kommutatív.

A kommutativitás azt jelenti, hogy a sokténYezős szorzatok esetében is mindegy a tényezők sorrendje.

2.2.5. Feladat. Mutassuk meg, hogy ha $*$ asszociatív és kommutatív művelet, akkor az $a_1 * a_2 * \ldots * a_n$ szorzat tényezőit bármilyen sorrendben is írjuk fel, az eredmény mindig ugyanaz lesz.

Az összeadás „szokásos tulajdonságai” között mindig felsoroltuk azt, hogy van egy „nulla” nevű elem, amihez bármely x számot hozzáadva ezt az x számot kapjuk eredményül. A szorzásnál ugyanezt a tulajdonságot emlegettük, csak ott egységelemről beszéltünk nullelem helyett. Általános művelet esetén (ami lehet összeadás, szorzás, vagy egész más is), célszerű egy új nevet bevezetni, amit mindig használhatunk.

2.2.6. Definíció. Legyen $*$ kétváltozós művelet az R halmazon. Azt mondjuk, hogy az $e \in R$ *neutrális* (=semleges) *elem*, ha tetszőleges $x \in R$ esetén $e * x = x * e = x$. Ha a művelet jele $+$, akkor általában *nullelemről* beszélünk, és a 0 jelet használjuk. Ha viszont a művelet szorzás (amit a leggyakrabban egyszerűen egymás mellé írással jelülünk), akkor a neutrális elemet *egységelemnek* hívjuk, és 1-gyel jelöljük.

2.2.7. Gyakorlat. Melyik függvény lesz a kompozícióra nézve neutrális elem?

Nemkommutatív művelet esetében szokás *bal oldali neutrális elemről* is beszélni, ha csak azt követeljük meg, hogy $e*x = x$ teljesüljön minden x-re. Hasonlóan *e jobb oldali neutrális elem*, ha minden x-re $x * e = x$. Ebben a könyvben vizsgálunk ugyan fontos nemkommutatív műveleteket, de az egyoldali neutrális elem csak ritkán fog szerepet játszani.

2.2.8. Feladat. Mutassuk meg, hogy tetszőleges műveletre nézve legfeljebb egy neutrális elem lehet.

Több konkrét példán is láttuk már, hogy a kivonást az ellentett hozzáadásaként, az osztást pedig a reciprokkal való szorzásként definiálhatjuk. Ezért most, amikor ezeket a fogalmakat általában vezetjük be, elsőnek az ellentett, illetve a reciprok képzésével kell foglalkoznunk. Ez a két név valójában ugyanazt a fogalmat takarja (csak a művelet más).

2.2.9. Definíció. Legyen e neutrális elem a $*$ műveletre nézve. Ha $u * v = e$, akkor azt mondjuk, hogy u *balinverze* v-nek, v pedig *jobbinverze* u-nak. Ha $v * u = e$ is teljesül, akkor azt mondjuk, hogy u és v egymás *inverzei*. Ha egy elemnek van kétoldali inverze, akkor *invertálhatónak* nevezzük. Ha a művelet a $+$, akkor inverz helyett *ellentettről* beszélünk. Ilyenkor a $v = -u$ jelölést alkalmazzuk. Ha a művelet jele a szorzás (vagy egymás mellé írás), akkor u inverzét u^{-1}-gyel jelöljük.

2.2.10. Feladat. Legyen $*$ asszociatív, de nem feltétlenül kommutatív művelet, melynek van neutrális eleme.

(1) Mutassuk meg, hogy ha egy u elemnek van balinverze is és jobbinverze is, akkor ez a kettő egyenlő (és így u invertálható). Speciálisan ha egy elemnek van kétoldali inverze, akkor ez az egyetlen balinverze és az egyetlen jobbinverze, vagyis *az inverz egyértelmű.*

(2) Ha az u és v elemek is invertálhatók, akkor igazoljuk, hogy $u*v$ (kétoldali) inverze

$$(u * v)^{-1} = v^{-1} * u^{-1}\,.$$

Tehát invertáláskor a tényezők sorrendje megfordul!

2.2.11. Gyakorlat. Legyen X egy halmaz és S az X-ből X-be vezető függvények halmaza. Jelölje e az X halmaz identikus leképezését (amely minden elemet saját magába visz). Mutassuk meg, hogy az $f, g \in S$ függvények akkor és csak akkor inverzek e-re nézve a 2.2.9. Definíció értelmében, ha a „szokásos" értelemben e két függvény egymás inverze. Mely $f \in S$ függvényeknek van bal-, illetve jobbinverze?

Az összeadásra vonatkozó „szokásos számolási szabályokat" úgy foglaltuk össze, hogy a most definiált tulajdonságokból többet is felhasználtunk. Érdemes külön nevet is adni a tulajdonságok ilyen csoportjainak.

2.2.12. Definíció. Ha egy nem üres halmazon értelmezett egy asszociatív művelet, akkor *félcsoportról* beszélünk.

Ha egy félcsoportban minden elemmel lehet osztani, akkor azt csoportnak nevezzük. Ehhez persze elegendő, ha minden elemnek van inverze.

2.2.13. Definíció. Egy G nem üres halmaz *csoport*, ha értelmezett rajta egy $*$ művelet a következő tulajdonságokkal.

(1) A $*$ művelet asszociatív.
(2) Van neutrális eleme.
(3) G minden elemének van inverze.

Mint láttuk, a neutrális elem egyértelmű, és az inverz létezése természetesen erre a neutrális elemre vonatkozik. Az inverzképzést szokásosabb külön (egyváltozós) műveletként bevezetni. Ennek előnyéről szólunk majd a 8.4. Szakaszban. Most az a fontos számunkra, hogy a fent megfogalmazott definíció a lehető legegyszerűbb legyen. Ha inverzről esik szó, akkor ebbe ezentúl automatikusan beleértjük, hogy létezik a megfelelő neutrális elem is.

A csoport definíciójában tehát nem tesszük föl, hogy a művelet kommutatív. A g és h elemeket *felcserélhetőnek*, nevezzük, ha $g * h = h * g$. Ha bármely két elem felcserélhető, azaz ha a művelet kommutatív, akkor a csoportot *kommutatív csoportnak*, vagy *Abel-csoportnak* hívjuk. Nagyon gyakori, hogy Abel-csoportok esetében a műveletet $+$ jelöli. Ilyenkor tehát v ellentettje $-v$, és definiálhatjuk a *kivonást* az $u - v = u + (-v)$ képlettel.

Ha a csoport nem kommutatív, akkor viszont inkább egymás mellé írással jelöljük a műveletet. Ilyenkor osztásról nem lesz szó, mert u és v hányadosát kétféleképpen is definiálhatnánk: $v^{-1}u$-nak is és uv^{-1}-nek is. (Néha beszélnek ennek megfelelően balosztásról és jobbosztásról.)

A bal és jobb oldali osztás közötti elvi különbséget érdekesen illusztrálja az osztás általános iskolában tanított kétféle fogalma. Ha egy étteremben 10 asztal van, és mindegyiknél négy vendég ül, akkor az étteremben $4 \cdot 10 = 40$ vendég van. Természetesen $4 \cdot 10 = 10 \cdot 4$, hiszen a szorzás az egész számok között kommutatív. De e két szorzatnak mégis más a *jelentése*, ha megállapodunk, hogy az első tényező mindig a csoportok létszámát, a második pedig a csoportok számát jelenti. Ha a kérdés az (40 vendég esetén), hogy „ha minden asztalnál négyen

ülnek, hány asztal van", akkor ezt a feladatot *bennfoglalásnak* nevezik. Ha viszont az a kérdés, hogy „ha tíz asztal van, hányan ülnek egy asztalnál", akkor *részekre osztásnak*. Az első esetben balosztásról van szó (4-gyel), a másodikban jobbosztásról (10-zel). Persze a kommutativitás miatt ugyanannak a két számnak a bal és a jobb oldali hányadosa ugyanaz lesz, tehát számolnunk ugyanúgy kell, de a számolás értelme más a két esetben. Nemkommutatív műveletnél az eredmény is lehet más.

Most röviden összefoglaljuk, hogy az eddig megismert konkrét műveletek milyen tulajdonságúak, de már az újonnan született nyelvünkön. Azt javasoljuk, hogy az Olvasó ellenőrizze az alábbi állításokat.

2.2.14. Állítás. *Kommutatív csoportot alkotnak:*

(1) *A komplex számok az összeadásra:* $\mathbb{C}^+$.
(2) *A nem nulla komplex számok a szorzásra:* $\mathbb{C}^\times$.
(3) *A valós számok az összeadásra:* $\mathbb{R}^+$.
(4) *A nem nulla valós számok a szorzásra:* $\mathbb{R}^\times$.
(5) *A racionális számok az összeadásra:* $\mathbb{Q}^+$.
(6) *A nem nulla racionális számok a szorzásra:* $\mathbb{Q}^\times$.
(7) *Az egész számok az összeadásra:* $\mathbb{Z}^+$.
(8) *A komplex együtthatós polinomok az összeadásra:* $\mathbb{C}[x]^+$.
(9) *A* $\{0, 1, \ldots, m-1\}$ *halmaz a modulo* m *összeadásra:* $\mathbb{Z}_m^+$.
(10) *Az* $\{1, 2, 3, 4\}$ *halmaz a modulo* 5 *szorzásra:* $\mathbb{Z}_5^\times$ *(ezt a jelölést majd később magyarázzuk meg).*

A felsorolt csoportok között persze összefüggés van. Ha tudjuk, hogy hogyan kell összeadni a komplex számokat, akkor ebből megkaphatjuk, hogy hogyan kell összeadni a valósakat, a racionálisakat, az egészeket, hiszen ezek mind részhalmazai a komplex számoknak.

2.2.15. Definíció. Legyen G egy csoport. Ha H részhalmaza G-nek, amely maga is csoport a G-beli műveletre nézve, akkor azt mondjuk, hogy H *részcsoportja* G-nek. Ezt úgy jelöljük, hogy $H \leq G$.

Például $\mathbb{Z}^+ \leq \mathbb{Q}^+ \leq \mathbb{R}^+ \leq \mathbb{C}^+$ és $\mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times$. Ugyanakkor $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet. Ugyanúgy $\mathbb{Z}_5^+$ nem részcsoportja $\mathbb{Z}^+$-nak, mert itt is más a művelet: $2+4 = 6$, de $2+_5 4 = 1$. (Erre különösen kell figyelnünk akkor, ha az egyszerűbb jelölés kedvéért $+_5$ helyett $+$-t írunk).

Általában hogyan lehet ellenőrizni, hogy egy részhalmaz részcsoport-e? A legelső kérdés, hogy egyáltalán *el tudjuk-e végezni a műveletet a* H *halmazon belül*. Ha például $G = \mathbb{R}^+$, és H a -10 és 10 közötti számokból áll, akkor ebben a H halmazban nem is tudjuk elvégezni az összeadást, az *kivezet belőle*: például $8, 9 \in H$, de $8+9 \notin H$. Elsőként tehát azt kell ellenőriznünk, hogy a H részhalmaz *zárt-e* G műveletére.

Az asszociativitást nem kell megvizsgálnunk, az automatikusan öröklődik, hiszen a bővebb G halmazon már tudjuk, hogy teljesül. A következő kérdés, hogy van-e H-nak neutrális eleme, és hogy elvégezhető-e benne az inverzképzés. Be lehet látni, hogy egy

részcsoport neutrális eleme ugyanaz kell, hogy legyen, mint az eredeti csoporté, és így az inverzet is ugyanúgy kell kiszámítani. Az alábbi állításban összefoglaljuk, hogyan célszerű ellenőrizni, hogy egy részhalmaz részcsoport-e.

2.2.16. Feladat. Mutassuk meg, hogy ha G csoport egy $*$ műveletre, akkor egy $H \subseteq G$ részhalmaz akkor és csak akkor részcsoport, ha

(1) H zárt a $*$ műveletre, azaz $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$;
(2) H tartalmazza G neutrális elemét;
(3) H zárt a G-beli inverzképzésre, azaz ha $h \in H$, akkor $h^{-1} \in H$.

Igazoljuk azt is, hogy tetszőleges H részcsoport neutrális eleme ugyanaz, mint G neutrális eleme.

Következő célunk a „többszörös”, illetve „hatvány” fogalmának általánosítása. Mindkét esetben arról van szó, hogy egy műveletet (a többszörös esetében az összeadást, hatványozás esetében a szorzást) sokszor végzünk el.

2.2.17. Definíció. Legyen $*$ asszociatív művelet az R halmazon, és $a \in R$. Ekkor tetszőleges n pozitív egészre legyen

$$a^n = a * a * \ldots * a \quad (n \text{ tényező}).$$

Ha $*$-ra nézve van egy e neutrális elem, akkor legyen $a^0 = e$. Végül ha a invertálható, és inverze b, akkor legyen

$$a^{-n} = b^n .$$

Ezek az a elem egész kitevőjű *hatványai*. Ha a műveletet $+$ jelöli, akkor hatvány helyett *többszörösről* beszélünk, és az na írásmódot alkalmazzuk.

Most áttekintjük a hatványozás ismert azonosságait.

2.2.18. Gyakorlat. Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Mutassuk meg a következőket.

(1) a^{-n} az a^n inverze.
(2) $a^m a^n = a^{m+n}$.
(3) $(a^m)^n = a^{mn}$.
(4) Ha a és b felcserélhetők, azaz $ab = ba$, akkor $(ab)^n = a^n b^n$.

A „szokásos” számolási szabályokban egyszerre szerepelt összeadás és szorzás is, ezeket a disztributivitás kapcsolta össze. Az ilyen struktúrát gyűrűnek nevezzük.

2.2.19. Definíció. Az R *gyűrű*, ha az R halmazon értelmezett egy összeadásnak nevezett $+$ jelű művelet is, és egy szorzásnak nevezett, általában egymás mellé írással jelölt művelet is, a következő tulajdonságokkal.

(1) R az összeadásra nézve Abel-csoport.
(2) R a szorzásra nézve félcsoport (azaz a szorzás asszociatív).

(3) Érvényes a *disztributivitás*: tetszőleges $x, y, z \in R$ esetén

$$(x + y)z = xz + yz \qquad \text{és} \qquad z(x + y) = zx + zy.$$

A gyűrűbeli szorzást nem definiáltuk kommutatívnak (ezért kellett két disztributív azonosságot is felírni), és azt sem tettük fel, hogy van rá nézve egységelem. Ha a szorzás kommutatív, akkor *kommutatív gyűrűről*, ha van egységelem, akkor *egységelemes gyűrűről* beszélünk.

Az összeadásra kapott csoportot az R *additív csoportjának* nevezzük, és R^+-szal jelöljük. Egységelemes gyűrűben van értelme annak, hogy egy elem invertálható-e vagy sem. A 2.2.10. Feladatból kapjuk, hogy az R invertálható elemei csoportot alkotnak az R-beli szorzásra, melynek egységeleme a gyűrű egységelemével egyenlő. Ez az R *multiplikatív csoportja*, jele $R^\times$.

Azt a gyűrűt, aminek a nulla az egyetlen eleme, *nullgyűrűnek* nevezzük. Ezt nem tekintjük egységelemes gyűrűnek. A többi egységelemes gyűrű esetében az egységelem különbözik a nullelemtől, és ilyenkor a multiplikatív csoportban nem lehet benne a nulla (más szóval a nullával soha nem lehet osztani). Mindez a következő állításból következik.

2.2.20. Feladat. Mutassuk meg, hogy egy gyűrűben a nullával való szorzás mindig nullát ad eredményül, és így egy invertálható elem (speciálisan az egységelem) nem lehet nullával egyenlő. Igazoljuk azt is, hogy tetszőleges r és s elemekre $r(-s) = (-r)s = -(rs)$.

Az olyan kommutatív, egységelemes gyűrűket, amelyben *minden nem nulla elemmel lehet osztani,* testnek nevezzük. (A nullgyűrű tehát nem test, mert nem is egységelemes.)

2.2.21. Definíció. Ha egy gyűrű nem nulla elemei csoportot alkotnak a szorzásra, akkor a gyűrűt *ferdetestnek* hívjuk. Ha egy ferdetest kommutatív, akkor *testről* beszélünk.

2.2.22. Állítás. *Kommutatív, egységelemes gyűrűt alkotnak:*

(1) *A komplex számok:* $\mathbb{C}$.
(2) *A valós számok:* $\mathbb{R}$.
(3) *A racionális számok:* $\mathbb{Q}$.
(4) *Az egész számok:* $\mathbb{Z}$.
(5) *A komplex együtthatós polinomok:* $\mathbb{C}[x]$.
(6) *A* $\{0, 1, \ldots, m-1\}$ *halmaz a modulo* m *összeadásra és szorzásra:* $\mathbb{Z}_m$.

A felsoroltak közül $\mathbb{C}$, $\mathbb{R}$ *és* $\mathbb{Q}$ *testek is.*

Azt, hogy mikor lesz $\mathbb{Z}_m$ test, nemsokára megvizsgáljuk. A fenti példákban, a csoportokhoz hasonlóan, többször előfordul, hogy az egyik gyűrű részhalmaza egy másiknak.

2.2.23. Definíció. Legyen R egy gyűrű. Ha S részhalmaza R-nek, amely maga is gyűrű az R-beli műveletekre nézve, akkor azt mondjuk, hogy S *részgyűrűje* R-nek. Ezt úgy jelöljük, hogy $S \leq R$. Ha R és S testek, akkor *résztestről* beszélünk. Ilyenkor azt is mondjuk, hogy az R test *bővítése* az S testnek.

Például $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ résztestek, és $\mathbb{Z}$ részgyűrűje $\mathbb{Q}$-nak. Azt, hogy egy részhalmaz részgyűrű, illetve résztest-e, szintén a műveletekre való zártság vizsgálatával ellenőrizhetjük, a műveleti azonosságokkal (asszociativitás, disztributivitás) nem kell foglalkoznunk.

2.2.24. Feladat. Mutassuk meg, hogy ha R gyűrű, akkor egy $S \subseteq R$ részhalmaz akkor és csak akkor részgyűrű, ha

(1) S zárt az R összeadására és szorzására, azaz $r_1, r_2 \in S$ esetén $r_1 + r_2$ és $r_1 r_2 \in S$;
(2) S tartalmazza R nullelemét;
(3) S zárt az R-beli ellentettképzésre, azaz ha $r \in S$, akkor $-r \in S$.

Ha R test, akkor az S részgyűrű pontosan akkor résztest, ha

(4) S tartalmazza R egységelemét;
(5) S zárt az R-beli inverzképzésre, azaz ha $0 \neq r \in S$, akkor $r^{-1} \in S$.

Tetszőleges S részgyűrű nulleleme ugyanaz, mint R nulleleme, és ha R test, akkor tetszőleges S résztest egységeleme ugyanaz, mint R egységeleme.

Megjegyezzük, hogy általában egy részgyűrű egységeleme különbözhet a gyűrű egységelemétől (lásd a 2.2.35. Gyakorlatot és a 2.4.24. Feladatot).

Az eddig vizsgált konkrét gyűrűk többségében fontos észrevétel volt, hogy egy szorzat csak úgy lehet nulla, ha valamelyik tényezője nulla. Ilyen például $\mathbb{C}$ összes részgyűrűje, de a $\mathbb{Z}_6$ gyűrű nem ilyen, mert itt a nem nulla 2 és 3 elemek szorzata nulla lesz.

2.2.25. Definíció. Ha egy R gyűrűben $uv = 0$, de sem u, sem v nem nulla, akkor azt mondjuk, hogy u bal oldali, v pedig jobb oldali *nullosztó*. Az R *nullosztómentes,* ha nincsen benne nullosztó, vagyis $uv = 0$-ból $u = 0$ vagy $v = 0$ következik.

Egy u elem tehát akkor bal oldali nullosztó, ha nem nulla, és van olyan v nem nulla elem, amelyre $uv = 0$ teljesül.

2.2.26. Gyakorlat. Igazoljuk, hogy ha egy R gyűrű egy $u \neq 0$ eleme nem bal oldali nullosztó, akkor szabad vele balról egyszerűsíteni, azaz tetszőleges $r, s \in R$ esetén $ur = us$-ből $r = s$ következik. Igaz-e az állítás megfordítása?

Ezzel elérkeztünk ahhoz a ponthoz, hogy beláthatjuk első absztrakt algebrai tételünket.

2.2.27. Tétel. *Minden ferdetest nullosztómentes.*

Bizonyítás. Most is, a későbbiekben is, gyakran fogunk olyan bizonyításokkal találkozni, ahol az „aprómunkát" már korábban elvégeztük, és csak ellenőrizni kell egy korábbi bizonyításról, hogy az ott szereplő gondolatok valójában az általánosabb állítást is kiadják. Lapozzuk fel annak bizonyítását, hogy a komplex számok között érvényes a nullosztómentesség (1.3.7. Következmény). Vegyük észre, hogy az ottani gondolatmenet szó szerint elmondható a mostani körülmények között is, még azt sem használtuk fel, hogy a szorzás kommutatív lenne (amit most nem is tettünk fel). Csak a „reciprok" szó helyett kell „inverz"-et írnunk. □

2.2.28. Gyakorlat. Mutassuk meg, hogy ha az R egységelemes gyűrű r elemének van balinverze, akkor az r nem bal oldali nullosztó.

2.2.29. Állítás. *A $\mathbb{Z}_m$ gyűrű akkor és csak akkor nullosztómentes, ha m prímszám, és ebben az esetben test is.*

Bizonyítás. Ha m összetett szám, azaz $m = ab$, ahol $1 < a, b < m$, akkor $a *_m b = 0$, vagyis nullosztókat találtunk. Ha viszont m prímszám, és $u *_m v = 0$, ahol $0 \leq u, v < m$, akkor $m \mid uv$, és így m prímtulajdonsága miatt $m \mid u$ vagy $m \mid v$. Az első esetben az u, a második esetben a v lesz nulla. Tehát $\mathbb{Z}_m$ nullosztómentes. Az, hogy $\mathbb{Z}_m$ test, ha m prímszám, az alábbi feladat megoldásából következik. □

2.2.30. Feladat. Mutassuk meg, hogy a $\mathbb{Z}_m$ gyűrű egy u eleme akkor és csak akkor invertálható, ha u és m relatív prímek. Határozzuk meg a $\mathbb{Z}_m$ gyűrűben a nullosztókat is.

Ennek alapján már megérthetjük, hogy a $\mathbb{Z}_5^\times$ csoport, azaz $\mathbb{Z}_5$ multiplikatív csoportja miért az 1, 2, 3, 4 elemekből áll.

A magyar nyelvű szakirodalomban általában *integritási tartománynak* hívják a nullosztómentes és kommutatív gyűrűket. A most következő, polinomokkal kapcsolatos vizsgálatokban elsősorban ilyen gyűrűkkel fogunk foglalkozni, amelyek azonban rendszerint egységelemesek is. Erre nincs bevett magyar terminológia. A rövidség kedvéért szokásos gyűrűnek nevezzük őket.

2.2.31. Definíció. Azt mondjuk, hogy R *szokásos gyűrű*, ha kommutatív, egységelemes és nullosztómentes.

Az utolsó fogalom, amit precízen definiálni szeretnénk, a művelettartás. Erre is sok példát láttunk, ilyen volt a komplex konjugálás, a modulo m maradék képzése, vagy az egységgyököknél használt $k \mapsto \varepsilon_k$ megfeleltetés. Mindezekben az a közös, hogy két halmazon egy-egy művelet van adva, továbbá a két halmaz között egy leképezés. A művelettartás azt fejezi ki, hogy *mindegy az, hogy először a műveletet végezzük el, és azután alkalmazzuk a leképezést, vagy fordítva.*

2.2.32. Definíció. Legyen $\varphi : A \to B$ egy leképezés, továbbá $*$ az A halmazon, $\bullet$ pedig a B halmazon értelmezett kétváltozós művelet. Azt mondjuk, hogy φ (ezekre a műveletekre nézve) *művelettartó*, ha tetszőleges $x, y \in A$ esetén

$$\varphi(x * y) = \varphi(x) \bullet \varphi(y) .$$

Vigyázzunk, mindig oda kell figyelnünk arra, hogy egy adott φ leképezés *mely* műveleteket tartja. Például legyen R és S két gyűrű. A kettő között haladó $\varphi : R \to S$ leképezést akkor szokás művelettartónak vagy *gyűrűhomomorfizmusnak* nevezni, ha az összeadást és a szorzást is tartja, vagyis ha

$$\varphi(r + s) = \varphi(r) + \varphi(s) \quad \text{és} \quad \varphi(rs) = \varphi(r)\varphi(s) .$$

Szó sincs tehát olyasféle „vegyes” művelettartásról, hogy $\varphi(rs) = \varphi(r) + \varphi(s)$.

A művelettartás (illetve a lényegében ugyanezt kifejező homomorfizmus) az algebra talán legfontosabb fogalma. Ennek az általános fogalomnak azonban most, a polinomok tárgyalásakor még nem lesz akkora jelentősége, mint a gyűrűknek és a testeknek. Ezért az Olvasót arra biztatjuk, hogy a művelettartás fenti definícióját vesse össze a korábban szerepelt konkrét példákkal, de ezzel a fogalommal most csak néhány feladat erejéig foglalkozunk.

Gyakorlatok, feladatok

2.2.33. Gyakorlat. Az S halmazon tekintsük az $x * y = x$ képlettel definiált $*$ műveletet. Mutassuk meg, hogy félcsoportot kaptunk, és határozzuk meg a bal oldali, illetve a jobb oldali neutrális elemeket.

2.2.34. Gyakorlat. Az alábbi struktúrák gyűrűk-e? Ha igen, kommutatívak-e, egységelemesek-e, nullosztómentesek-e, testek-e? Amelyek gyűrűk, azokban határozzuk meg az invertálható elemeket.

(1) $\{a + bi \,:\, a, b \in \mathbb{Q}\}$ a szokásos összeadásra és szorzásra nézve.
(2) $\mathbb{G} = \{a + bi \,:\, a, b \in \mathbb{Z}\}$ a szokásos összeadásra és szorzásra nézve (ezek az úgynevezett *Gauss-egészek*).
(3) $\{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}\}$ a szokásos összeadásra és szorzásra nézve.
(4) $\{a + b\sqrt[3]{2} \,:\, a, b \in \mathbb{Q}\}$ a szokásos összeadásra és szorzásra nézve.
(5) Tetszőleges Abel-csoport, a szorzást úgy definiáljuk, hogy minden szorzat nulla.
(6) Egy X halmaz összes részhalmaza, ahol az összeadás a szimmetrikus differencia képzése, a szorzás pedig a metszetképzés. (Két halmaz szimmetrikus differenciája azokból az elemekből áll, amelyek a két halmaz közül pontosan egyben vannak benne.)

2.2.35. Gyakorlat. Mutassuk meg, hogy a $\mathbb{Z}_6$ gyűrűben $R = \{0, 2, 4\}$ részgyűrűt alkot. Egységelemes gyűrű-e, illetve test-e az R gyűrű?

2.2.36. Gyakorlat. Legyen R gyűrű, $r, s \in R$, és m, n egész számok. Mutassuk meg a következő állításokat. (Az nr többszörös fogalmát az összeadásra nézve a 2.2.17. Definícióban értelmeztük).

(1) $(-n)r$ az nr ellentettje.
(2) $mr + nr = (m + n)r$.
(3) $n(mr) = (nm)r$.
(4) $n(r + s) = nr + ns$.
(5) $n(rs) = (nr)s = r(ns)$.

2.2.37. Gyakorlat. Bizonyítsuk be tetszőleges a, b valós számokra az alábbi, úgynevezett *binomiális tételt*:

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j =$$

$$= a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \ldots + \binom{n}{n-1} a b^{n-1} + b^n \,.$$

Az állításban szereplő *binomiális együtthatókat* a A.2.2. Tételben definiáltuk. Mutassuk meg, hogy az állítás érvényben marad akkor is, ha az a és b egy tetszőleges R kommutatív gyűrű elemei. Hogyan kell ekkor érteni a binomiális együtthatókkal való szorzást?

2.2.38. Feladat. Jelölje $\mathbb{Z}[\sqrt{2}]$ az $a + b\sqrt{2}$ alakú számok gyűrűjét a $\mathbb{C}$-beli összeadásra és szorzásra, ahol $a, b \in \mathbb{Z}$. Igazoljuk, hogy ebben végtelen sok invertálható elem van.

2.2.39. Feladat. Ha R kommutatív, egységelemes gyűrű, akkor tekintsük az $a + bi$ alakú formális kifejezéseket, ahol $a, b \in R$ (ezeket nevezhetnénk R feletti komplex számoknak). A műveleteket ugyanúgy végezzük, mint a közönséges komplex számok esetén. Testet kapunk-e, ha $R = \mathbb{Z}_3$, illetve ha $R = \mathbb{Z}_5$?

2.2.40. Gyakorlat. Döntsük el az alábbi $\varphi : R_1 \to R_2$ leképezésekről, hogy tartják-e a megadott műveleteket.

(1) $R_1 = \mathbb{R}^+$, $R_2 = \mathbb{R}^\times$, $\varphi(x) = 2^x$.
(2) $R_1 = \mathbb{R}^+$, $R_2 = \mathbb{C}^\times$, $\varphi(x) = \cos x + i \sin x$.
(3) $R_1 = \mathbb{C}^+$, $R_2 = \mathbb{C}^+$, $\varphi(x) = |x|$.
(4) $R_1 = \mathbb{Z}_{100}^+$, $R_2 = \mathbb{Z}_{100}^+$, $\varphi(x) = 60 *_{100} x$.
(5) $R_1 = \mathbb{Z}_{100}^+$, $R_2 = \mathbb{Z}_{100}^+$, $\varphi(x) = 60x$.

2.2.41. Feladat. Legyen $\varphi : G_1 \to G_2$ művelettartó leképezés két csoport között. Mutassuk meg, hogy φ az egységelemet az egységelembe viszi, és inverz képe a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

2.2.42. Feladat. Igazoljuk, hogy az $\{a + bi \mid a, b \in \mathbb{Q}\}$ és $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ testek között nincs kölcsönösen egyértelmű, művelettartó (azaz összeg- és szorzattartó) leképezés.

2.2.43. Gyakorlat. Legyen G egy kommutatív csoport, amelyben a műveletet $+$ jelöli, és $a_1, \ldots, a_n \in G$. Igazoljuk, hogy $1 \leq k \leq n$ esetén

$$\sum_{j=1}^{k} a_i + \sum_{j=k+1}^{n} a_i = \sum_{j=1}^{n} a_i \,.$$

Igaznak érezzük ezt akkor is, ha $k = n-1$? És ha $k = n$? Hány tagja van ebben az esetben a bal oldalon szereplő összegeknek? Hogyan érdemes értelmeznünk az egytagú összeget? És a nulla tagú *üres összeget*? Hogyan érdemes definiálni az *üres szorzatot*?

2.3. A polinomok alaptulajdonságai

Ebben a szakaszban a polinomokra vonatkozó alapvető fogalmakat ismételjük át, de most már olyan általánosságban, ahogy azt a későbbiek megkívánják. Ezután az érdeklődő Olvasók számára vázoljuk, hogy hogyan lehet a polinomok fogalmát precízen bevezetni.

2.3.1. Definíció. Legyen R egységelemes, kommutatív gyűrű. Ekkor $R[x]$ jelöli az R-beli együtthatós, x határozatlanú polinomok, vagyis az

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

alakú formális kifejezések halmazát, ahol $a_i \in R$. Ezeket *R fölötti* polinomoknak is mondjuk. Polinomok egyenlőségét, fokát, összegét és szorzatát ugyanúgy definiáljuk, ahogy a 2.1. Szakaszban tettük.

2.3.2. Tétel. *Ha R egységelemes, kommutatív gyűrű, akkor $R[x]$ is az, amely tartalmazza az R gyűrűt, mint konstans polinomokat. Polinomok összegének foka legfeljebb annyi lehet, mint a tagok fokainak maximuma. Ha R nullosztómentes, akkor nem nulla polinomok szorzatának foka a fokok összege lesz. Ilyenkor $R[x]$ is nullosztómentes, és az $R[x]$ (szorzásra) invertálható elemei azok a konstans polinomok, amelyek R-ben invertálhatóak.*

Bizonyítás. A műveleti azonosságokat (asszociativitást, kommutativitást) nem számoljuk ki (kivéve a disztributivitást a 2.3.4. Gyakorlatban). Az $R[x]$ nulleleme nyilván a nullapolinom, egységeleme pedig a konstans 1 polinom, ahol 1 az R egységeleme. Ha R nullosztómentes, akkor a 2.1.5. Állítás bizonyítása most is működik, mert a szorzatpolinom főegyütthatója, mint két nem nulla R-beli elem szorzata, nem lesz nulla. Az összeg és szorzat fokáról szóló állítások is a korábbi módon bizonyíthatók, az invertálható elemek meghatározásához pedig a 2.1.7. Állítás bizonyítása ad mintát. □

E szakasz hátralévő részét (a gyakorlatok kivételével) apró betűs résznek érdemes tekinteni. A komplex számok precíz bevezetését az 1.6. Szakaszban írtuk le. Most ehhez hasonlóan megmutatjuk, hogy hogyan lehet a polinomokat is precízen bevezetni. A két felépítés rendkívül hasonló, de technikailag a komplex számok bevezetése az egyszerűbb, és ezért azt érdemes először elolvasni. Az Olvasó a most következőket is nyugodtan átugorhatja a könyv első olvasásakor.

A „formális kifejezés” szemléletes fogalmát nehéz precízen kezelni, és ezért ami most következik, az nem szemléletes, viszont precíz lesz. Amikor majd más struktúrákban (például csoportokban) beszélünk polinomokról, akkor mégsem kerülhetjük meg, hogy a formális kifejezés fogalmát precízzé tegyük. Erre a 8.2. Szakaszban kerül sor.

Abból indulunk ki, ahogy a polinomok egyenlőségét definiáltuk. Egy polinomot az együtthatói határoznak meg, vagyis az $a_0, a_1, a_2, \ldots$ számok (vagy általában gyűrűelemek). Mivel a polinom véges sok tagú összeg, az a_j számok valamettől kezdve mindannyian nullák lesznek. Tehát a nem szemléletes, de jól kezelhető definíció a következő:

2.3.3. Definíció. Legyen R kommutatív, egységelemes gyűrű. Ekkor R feletti polinomon egy olyan

$$(a_0, a_1, \ldots, a_k, \ldots)$$

sorozatot értünk, ahol $a_j \in R$ minden $j \geq 0$ egészre, és van olyan n egész, hogy $j \geq n$ esetén $a_j = 0$. (Természetesen ez az n szám más polinom esetében más lehet.)

Kézenfekvőek ennek alapján a következő fogalmak: nullapolinom (mindegyik $a_j = 0$), polinom foka (ez n, ha $a_n \neq 0$, de a_j már nulla minden $j > n$ esetén), főegyüttható (n-edfokú polinomnál a_n), konstans tag (az a_0). A műveleteket is könnyen definiálhatjuk, hiszen korábban már kiszámoltuk az összeg és szorzat együtthatóit. Ha tehát

$$f = (a_0, a_1, \ldots, a_k, \ldots) \quad \text{és} \quad g = (b_0, b_1, \ldots, b_k, \ldots)\,,$$

akkor legyen

$$f + g = (a_0 + b_0, a_1 + b_1, \ldots, a_k + b_k, \ldots)\,,$$

és

$$fg = (c_0, c_1, \ldots, c_k, \ldots)\,,$$

ahol c_k értékét a (2.1) formula szolgáltatja (38. oldal). Persze le kell ellenőrizni, hogy az összeg és szorzat is polinom-e, azaz, hogy valamettől kezdve csupa nulla elemek szerepelnek-e ebben a két sorozatban, de ez nyilván így van.

A polinomjaink között most nincsenek ott R elemei, hiszen a c elem nem ugyanaz, mint a megfelelő $(c, 0, 0, \ldots)$ konstans polinom. Azonban a konstans polinomokkal ugyanúgy kell számolni, mint R elemeivel, hiszen

$$(c, 0, 0, \ldots) + (d, 0, 0, \ldots) = (c + d, 0, 0, \ldots)$$

és

$$(c, 0, 0, \ldots)(d, 0, 0, \ldots) = (cd, 0, 0, \ldots)$$

teljesül az összeadás és a szorzás definíciója miatt. Másképp fogalmazva, a

$$\varphi : c \mapsto (c, 0, 0, \ldots)$$

leképezés (amely kölcsönösen egyértelmű R elemei és a konstans polinomok halmaza között) tartja az összeadást és a szorzást is. Ezért a c elemet *azonosítjuk* a neki megfelelő konstans polinommal.

Nincs ott a polinomjaink között az x határozatlan sem. Ha belegondolunk, az x polinom konstans tagja 0, az x-es tag együtthatója 1 (az R egységeleme, ezért volt fontos, hogy R egységelemes legyen), és a többi együttható nulla. Tehát ha a

$$(0, 1, 0, 0, 0, \ldots)$$

polinomot x-szel *jelöljük*, akkor a szorzás szabálya miatt

$$x^2 = (0, 0, 1, 0, 0, \ldots)\,, \qquad x^3 = (0, 0, 0, 1, 0, 0, \ldots)\,,$$

és így tovább, továbbá

$$(c, 0, 0, \ldots)x^3 = (0, 0, 0, c, 0, 0, \ldots)\,,$$

(és ugyanígy a többi kitevőre is), végül pedig az összeadás definíciója miatt

$$(a_0, a_1, \ldots, a_k, \ldots) = (a_0, 0, \ldots) + (a_1, 0, 0, \ldots)x + \ldots + (a_k, 0, 0, \ldots)x^k + \ldots$$

(ez persze csak véges sok tagú összeg, mert valamettől kezdve $a_j = 0$, és innentől kezdve a megfelelő tagokat nem kell kiírni). Mivel $(a_k, 0, 0, \ldots)$-t azonosítottuk a_k-val, az

$$a_0 + a_1 x + \ldots + a_k x^k + \ldots$$

alakot kapjuk, ami már a polinomok korábban megszokott formája.

Ezen a ponton tehát visszakapcsolódhatunk a korábbi tárgyalás menetébe, megmutathatjuk, hogy a polinomok tényleg gyűrűt alkotnak, és a többi hasonló állítást is.

Gyakorlatok, feladatok

2.3.4. Gyakorlat. Bizonyítsuk be az $R[x]$ polinomgyűrűben a disztributív azonosságot.

2.3.5. Gyakorlat. Részgyűrűt alkotnak-e

(1) $\mathbb{C}[x]$ páros fokú elemei és a 0 a $\mathbb{C}[x]$-ben?
(2) $\mathbb{R}[x]$ legalább huszadfokú elemei és a 0 az $\mathbb{R}[x]$-ben?

2.3.6. Gyakorlat. Gyűrűt alkotnak-e $\mathbb{C}[x]$ elemei a szokásos összeadásra, és a kompozícióra, mint szorzásra?

2.3.7. Gyakorlat. Legyen m rögzített nemnegatív egész szám. Az $f \in \mathbb{Z}[x]$ polinomhoz rendeljük hozzá azt az $\overline{f} \in \mathbb{Z}_m[x]$ polinomot, amelyet f-ből úgy kapunk, hogy minden együtthatóját modulo m vesszük. Mutassuk meg, hogy az $f \to \overline{f}$ leképezés összeg- és szorzattartó, vagyis gyűrűhomomorfizmus $\mathbb{Z}[x]$-ből $\mathbb{Z}_m[x]$-be.

2.3.8. Gyakorlat. Ha R és S gyűrűk, és $\varphi : R \to S$ gyűrűhomomorfizmus, akkor mutassuk meg, hogy $a_0+a_1x+\ldots+a_nx^n \mapsto \varphi(a_0)+\varphi(a_1)x+\ldots+\varphi(a_n)x^n$ is gyűrűhomomorfizmus $R[x]$-ből $S[x]$-be.

2.4. Polinomfüggvények és gyökök

Ebben a szakaszban általános polinomokkal foglalkozunk, amelyek együtthatói tetszőlegesek (azaz egy kommutatív, egységelemes R gyűrű elemei) lehetnek. Gyűrűn ezért most kommutatív és egységelemes gyűrűt értünk. Akinek ez az általánosság még nehézséget okoz, az nyugodtan képzelje, hogy az R elemei, vagyis a szereplő polinomok együtthatói (komplex) számok.

A polinomokkal formálisan számolunk ugyan, de sokszor konkrét számokat is be akarunk helyettesíteni az x helyére. Ha $f = a_0 + a_1 x + \ldots + a_n x^n$, és $b \in R$, akkor legyen

$$f^*(b) = a_0 + a_1 b + \ldots + a_n b^n \in R\,.$$

Ebben a jelölésben a $*$ feleslegesnek látszik (később el is hagyjuk majd). Itt arra szolgál, hogy figyelmeztessen bennünket: a b nem határozatlan immár, hanem egy konkrét R-beli

elem. E jelölés azonban azt is mutatja, hogy f^* egy *függvény*nek is felfogható, amely R-ből R-be képez. Ez nem ismeretlen dolog középiskolából sem, hiszen például az x^2 polinomot sokszor függvénynek képzeltük, sőt le is rajzoltuk a grafikonját.

2.4.1. Definíció. Ha $f \in R[x]$ egy polinom, akkor azt az $f^* : R \to R$ függvényt, amelyet a fenti képlet definiál, az f-hez tartozó *polinomfüggvénynek* nevezzük.

Bár egy f polinom mint formális kifejezés, és az f^* polinomfüggvény nyilván nem ugyanaz, esetleg valaki arra gondolhat, hogy gyakorlati szempontból nincs nagy különbség közöttük, hiszen például az x^2 valós feletti grafikonjából visszakaphatjuk az x^2 polinomot. Nézzük meg, igaz marad-e ez, ha a $\mathbb{Z}_2$ gyűrű felett dolgozunk. Ennek csak két eleme van, így a „grafikon" mindössze két pontból áll. A polinomfüggvényeket tehát táblázatosan is megadhatjuk:

f	$f^*(0)$	$f^*(1)$
x^2	0	1
x^3	0	1
x	0	1
$x+1$	1	0
0	0	0
x^2+x	0	0
1	1	1
x^2+x+1	1	1

Itt bizony sok egybeesés van, például az x, x^2 és x^3 polinomokhoz is ugyanaz a polinomfüggvény tartozik. Persze ez nem meglepő: a $\{0, 1\}$ halmazból önmagába csak négy függvény létezik egyáltalán, hiszen 0-nál is és 1-nél is csak kétféle függvényérték lehetséges. Mind a négy lehetséges függvény szerepel is a fenti táblázatban, azaz $\mathbb{Z}_2$ *fölött minden függvény polinomfüggvény.* Polinom viszont végtelen sok van $\mathbb{Z}_2$ fölött (például $x, x^2, x^3, \ldots, x^k, \ldots$ csupa különböző polinomok). Egyik fontos célunk, hogy megvizsgáljuk: milyen összefüggés van általában egy polinom és a hozzá tartozó polinomfüggvény között, mikor határozza meg az utóbbi az előbbit.

Első lépésként vizsgáljuk meg, hogy mit kapunk eredményül, ha összeg-, illetve szorzatpolinomba helyettesítünk. A polinomok közötti műveleteket pontosan azzal a szándékkal definiáltuk, hogy az alábbi állítás igaz legyen.

2.4.2. Gyakorlat. Mutassuk meg, hogy ha $f, g \in R[x]$, és $b \in R$, akkor

$$(f+g)^*(b) = f^*(b) + g^*(b) \qquad \text{és} \qquad (fg)^*(b) = f^*(b)g^*(b)\,.$$

A középiskolában függvényekkel is végeztünk műveleteket. Például az $x \sin x$ az a függvény volt, ami az x helyen az x és a $\sin x$ szorzatát veszi fel. Ennek alapján a polinomfüggvények összegét és szorzatát is definiálhatjuk. Az alábbi definíció megemésztéséhez nagyon ajánljuk a 2.4.23. Gyakorlatot.

2.4.3. Definíció. Legyen R gyűrű, és p, q két függvény, ami R-et R-be képzi. Ekkor $p+q$, illetve pq az a függvény, ami tetszőleges $b \in R$ helyen $p(b) + q(b)$-t, illetve $p(b)q(b)$-t vesz fel. Képletben:

$$(p+q)(b) = p(b) + q(b) \qquad \text{és} \qquad (pq)(b) = p(b)q(b)\,.$$

Az $f+g$, illetve fg neve az f és g függvények *pontonkénti* összege, illetve szorzata.

Most egy viszonylag gyors eljárást mutatunk polinomba való behelyettesítésre. Példaként legyen $f(x) = 3x^4+2x^3+x+2$, és helyettesítsünk be $b = 2$-t. A szükséges szorzások számát nagymértékben lecsökkenthetjük, ha a polinomot a következőképpen alakítjuk át:

$$f(x) = \Big(\big((3x+2)x+0\big)x+1\Big)x+2$$

A részletszámításokat „belülről kifelé haladva” egy táblázatba írjuk:

	3	2	0	1	2
$b=2$	3	$3\cdot 2+2=8$	$8\cdot 2+0=16$	$16\cdot 2+1=33$	$33\cdot 2+2=68=f^*(b)$

Az eljárás tehát a következő:

(1) A táblázat felső sorába felírjuk sorban a polinom együtthatóit, a főtagtól a konstans tagig. (Vigyázzunk közben arra, hogy a nulla együtthatókat is be kell írni a táblázatba, akkor is, ha azokat a polinomban nem írtuk ki.)
(2) Az alsó sorba bemásoljuk a főegyüttható, a főegyüttható alá. A sor elejére oda szokás írni a behelyettesítendő b értéket is.
(3) Az alsó sort balról jobbra haladva töltjük ki. Az utoljára kitöltött mezőben talált értéket megszorozzuk b-vel, majd hozzáadjuk a következő, üres mező fölött található együtthatót, és az eredményt beírjuk ebbe az üres mezőbe.
(4) Az $f^*(b)$ értékét az alsó sor végéről olvashatjuk le.

Általában tehát a következő, úgynevezett *Horner-elrendezést* kapjuk:

	a_n	$\dots$	a_{j+1}	a_j	$\dots$	a_1	a_0
b	$c_{n-1}=a_n$	$\dots$	c_j	$c_{j-1}=c_jb+a_j$	$\dots$	c_0	$f^*(b)=c_0b+a_0$

2.4.4. Gyakorlat. Mutassuk meg általában is, hogy a Horner-elrendezés az $f^*(b)$ értéket számítja ki. Igazoljuk az alábbi összefüggést:

$$f(x) = (x-b)(c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_1x + c_0) + f^*(b)\,,$$

ahol $f(x) = a_nx^n + \ldots + a_0$, és $c_{n-1}, \ldots, c_0$ a táblázatban kiszámított értékek.

Ezek szerint minden $f \in R[x]$ polinom tetszőleges $b \in R$ esetén felírható

$$f(x) = (x-b)q(x) + f^*(b)$$

alakban alkalmas $q \in R[x]$ polinomra. Ezt az észrevételt (amely önmagában is elegendő a következő állítás bizonyításához) később általánosítani fogjuk, amikor a polinomok közötti *maradékos osztásról* beszélünk majd a 3.2. Szakaszban.

2.4.5. Definíció. Azt mondjuk, hogy $b \in R$ *gyöke* az $f \in R[x]$ polinomnak, ha $f^*(b) = 0$.

2.4.6. Állítás. *A $b \in R$ akkor és csak akkor gyöke az $f \in R[x]$ polinomnak, ha*

$$f(x) = (x - b)q(x)$$

alkalmas $q \in R[x]$ polinomra.

Bizonyítás. Ha f ilyen alakban írható, akkor b nyilvánvalóan gyöke f-nek. Megfordítva, ha b gyöke f-nek, akkor a Horner-elrendezés alsó sorában szereplő számok egy megfelelő q polinom együtthatóit szolgáltatják (a 2.4.4. Gyakorlat miatt). □

Ha b gyöke f-nek, akkor az $x - b$ kifejezést az f polinom b-hez tartozó *gyöktényezőjének* nevezzük, az előző állítás a *gyöktényező kiemelhetőségéről szóló tétel*.

Ha egy polinomnak több gyöke is van, akkor megpróbálhatunk egyszerre több gyöktényezőt is kiemelni. Ehhez nagyon fontos, hogy az R gyűrű *nullosztómentes* legyen. Ha ez nem teljesül, akkor furcsa dolgok történhetnek. Például a $\mathbb{Z}_8$ gyűrű felett tekintsük az $x^2 - 1$ polinomot. Ennek gyökeit akár úgy is megállapíthatjuk, hogy végigpróbálgatjuk a $\mathbb{Z}_m$ nyolc elemét. Az eredmény, hogy ennek gyökei a négy páratlan szám, azaz 1, 3, 5, 7. A gyöktényezőket kiemelve azonban *kétféle* felbontást kapunk:

$$x^2 - 1 = (x - 1)(x - 7) = (x - 3)(x - 5)\,.$$

A polinom tehát két, lényegesen különböző módon is felbontható gyöktényezők szorzatára, és egyszerre csak két gyöktényezőt tudunk szerepeltetni a lehetséges négy közül. A problémát az okozza, hogy ha az $(x - 1)(x - 7)$ alakba az $r = 3$ gyököt behelyettesítjük, akkor $0 = 2 *_8 4$ adódik, tehát a nullosztómentesség hiánya teszi lehetővé, hogy az 1-en és a 7-en kívül még legyen gyök.

2.4.7. Tétel. *Egy nullosztómentes (egységelemes, kommutatív) R gyűrű (speciálisan egy test) felett a gyöktényezők egyszerre is kiemelhetők: minden nem nulla $f \in R[x]$ polinom felírható*

$$f(x) = (x - b_1) \dots (x - b_k)q(x)$$

alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k$ az f-nek az ***összes*** *R-beli gyökei, és q-nak egyáltalán nincs gyöke R-ben. Ezért* ***nullosztómentes gyűrű felett egy polinomnak legfeljebb annyi gyöke lehet, mint a foka.***

Bizonyítás. Egy gyöktényező kiemelésekor a fok eggyel csökken (hiszen nullosztómentes gyűrűben polinomok szorzásakor a fokok összeadódnak). Emeljünk ki f-ből addig gyöktényezőket, ameddig lehet. Vagyis ha

$$f(x) = (x - b_1) \dots (x - b_m)q_m(x)\,,$$

de q_m-nek még van gyöke R-ben, akkor q_m-ből emeljünk ki egy további gyöktényezőt. Ezt csak véges sokszor lehet csinálni, mert q_m foka minden lépésnél csökken. Ezért előbb-utóbb eljutunk az

$$f(x) = (x - b_1) \dots (x - b_k)q(x)$$

alakhoz, ahol már q-nak nincs gyöke R-ben. Ha b gyöke f-nek, akkor ezt behelyettesítve

$$0 = (b - b_1) \dots (b - b_k) q^*(b)$$

adódik. Mivel R nullosztómentes, valamelyik tényező nulla. De $q^*(b) \neq 0$, tehát van olyan j, hogy $b - b_j = 0$, azaz $b = b_j$. Megfordítva, a b_j nyilván gyöke f-nek (hiszen az R gyűrűben a nullát bármelyik elemmel szorozzuk meg, nullát kapunk). Tehát f gyökei pontosan $b_1, \dots, b_k$.

Az utolsó állítás bizonyításához írjuk fel a fokszámokat:

$$\mathrm{gr}(f) = \mathrm{gr}(x - b_1) + \dots + \mathrm{gr}(x - b_k) + \mathrm{gr}(q) = k + \mathrm{gr}(q).$$

Ezért tényleg $\mathrm{gr}(f) \geq k$. □

2.4.8. Gyakorlat. Az előző bizonyításban mely állítások maradnak érvényesek, ha az R gyűrűről nem tesszük fel a nullosztómentességet? A fokszámokkal kapcsolatos érveléseknél is kihasználtuk-e a nullosztómentességet, vagy csak b behelyettesítésekor?

Annak igazolásához, hogy egy polinomnak legfeljebb annyi gyöke lehet, mint amennyi a foka, nemcsak a nullosztómentesség szükséges, hanem a kommutativitás is. Bár nemkommutatív gyűrűk fölött a polinomok definíciójával is gondok merülnek föl, az $x^2 + 1$-et minden egységelemes gyűrű fölött nyilván polinomnak tekinthetjük. Az 5.10.11. Feladatban meglátjuk majd, hogy van olyan nullosztómentes gyűrű (az úgynevezett kvaterniók ferdeteste), amelyben ennek a polinomnak végtelen sok gyöke van.

2.4.9. Gyakorlat. Igazoljuk, hogy ha R nullosztómentes gyűrű, akkor minden nem konstans $f \in R[x]$ polinom minden $c \in R$ értéket csak véges sok R-beli helyen vehet föl.

Most már könnyű belátni, hogy ha két polinom „elég sok” helyen megegyezik, akkor azonosak.

2.4.10. Következmény [A polinomok azonossági tétele]. *Ha egy R nullosztómentes gyűrű felett adott két, legfeljebb n-edfokú polinom, amelyek több mint n (R-beli) helyen megegyeznek, akkor a két polinom egyenlő (vagyis együtthatóik is megegyeznek).*

Bizonyítás. Legyen f és g a két polinom. Ha $f - g$ nem a nullapolinom, akkor van foka, ami legfeljebb n lehet. Ugyanakkor $f - g$-nek gyöke minden olyan $b \in R$, ahol f és g megegyezik (azaz $f(b) = g(b)$). Tehát $f - g$-nek több, mint n gyöke van, de foka legfeljebb n, és ez ellentmond az előző tételnek. Az ellentmondást abból kaptuk, hogy feltettük: $f - g$ nem a nullapolinom. Ezért $f - g$ a nullapolinom, azaz $f = g$. □

Ez a bizonyítás akkor is működik, ha f vagy g a nullapolinom, noha a tételben ezt elvileg nem engedtük meg, mert f és g fokáról beszéltünk. Néha ezért megállapodnak abban, hogy (noha a nullapolinomnak nincs foka), a legfeljebb n-edfokú polinomok közé mégiscsak odaértjük a nullapolinomot is. Egy ilyesfajta megállapodás sokat egyszerűsíthet egy-egy tétel szövegén, és könnyebben megjegyezhetővé teheti azt.

2.4.11. Következmény. *Végtelen nullosztómentes gyűrű felett minden polinomot egyértelműen meghatároz a hozzá tartozó polinomfüggvény, véges gyűrű felett viszont nem.*

Bizonyítás. Ha R végtelen, és $f^* = g^*$, akkor f és g végtelen sok helyen megegyezik (mert R minden elemén megegyezik). Tehát az azonossági tétel miatt $f = g$. Ha R véges, akkor csak véges sok függvény van R-ből R-be, tehát csak véges sok polinomfüggvény van. Polinom viszont végtelen sok van, tehát nem tartozhat minden polinomhoz más és más polinomfüggvény. □

A polinomfüggvények tárgyalását ezzel befejeztük. Reménykedvén, hogy már mindenki pontosan érti a különbséget polinom és polinomfüggvény között, ezentúl jelölésben nem különböztetjük meg a kettőt, például egyszerűen $f(r)$-rel jelöljük az f polinom r helyen felvett helyettesítési értékét. Zárásként röviden, két feladat formájában, megemlítjük az *interpoláció* problémáját.

Olyan polinomfüggvényt fogunk keresni, amely adott helyeken adott értékeket vesz fel. Ezek a helyek egy T test páronként különböző elemei, jelölje őket $a_1, \ldots, a_n$, a felveendő értékeket pedig $b_1, \ldots, b_n$. Az azonossági tétel miatt a legfeljebb $n-1$-edfokú polinomok között legfeljebb egy olyan f polinom létezik, melyre $f(a_j) = b_j$ minden j-re. Meg fogjuk mutatni, hogy mindig van ilyen polinom. A legegyszerűbb konstrukció a *Lagrange-interpoláció*, amit a következő feladatban írunk le.

2.4.12. Gyakorlat. Legyenek $a_1, \ldots, a_n$ páronként különböző elemei a T testnek.

(1) Melyek azok az $n-1$-edfokú polinomok, melyeknek az a_j kivételével az $a_1, \ldots, a_n$ mindegyike gyöke?
(2) Melyik az az f_j polinom, ami az előző (1)-beli kívánalmakon kívül még azt is teljesíti, hogy $f_j(a_j) = 1$?
(3) Ha $b_1, \ldots, b_n \in T$, akkor hogyan lehetne az f_j polinomokból és a b_j elemekből egy olyan f polinomot összekombinálni, amelyre $f(a_j) = b_j$ minden j-re?

E módszer előnye, hogy a keresett interpolációs polinomra képletet kapunk. Hátránya viszont a következő. Képzeljük el, hogy az interpoláció célja az, hogy mérési eredményekhez polinomot illesszünk. Ha új mérési eredmény érkezik, akkor a Lagrange-féle technikával elölről kell kezdenünk a számolást. *Newton módszere* azt teszi lehetővé, hogy a már meglevő polinomunkat úgy módosítsuk, hogy az új helyen is a kívánt értéket vegye fel.

2.4.13. Gyakorlat. Tegyük fel, hogy a legfeljebb $n-2$-edfokú f polinom teljesíti, hogy $f(a_j) = b_j$, ha $j = 1, 2, \ldots, n-1$.

(1) Mi az általános alakja az olyan $n-1$-edfokú g polinomoknak, melyekre teljesül, hogy $f + g$ az a_j helyen szintén a b_j értéket veszi fel, ha $j = 1, 2, \ldots, n-1$?
(2) Hogyan kell g-t megválasztani, hogy $(f + g)(a_n) = b_n$ is teljesüljön?

Többváltozós függvényeket többhatározatlanú polinomokkal interpolálhatunk, erről a 2.6.11. Feladatban lesz szó.

Gyakorlatok, feladatok

2.4.14. Gyakorlat. A Horner elrendezés segítségével döntsük el, hogy a 2 szám gyöke-e az $f(x) = x^6 - 4x^4 + x^3 - x^2 + 4$ polinomnak, és írjuk is fel $f(x)$-et $(x-2)g(x) + f(2)$ alakban.

2.4.15. Gyakorlat. Az $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \ldots + b^{k-1})$ ismert (és beszorzással igazolható) azonosság felhasználásával adjunk új bizonyítást a gyöktényező kiemelhetőségéről szóló tételre (2.4.6. Állítás).

2.4.16. Feladat. Mutassuk meg, hogy ha T test és $b \in T$, akkor minden $T[x]$-beli f polinom egyértelműen fölírható $x - b$ polinomjaként, melynek foka ugyanaz, mint az f foka.

2.4.17. Feladat. Mely m-ekre van $\mathbb{Z}_m[x]$-ben olyan polinom, amelynek több gyöke van, mint a foka?

2.4.18. Gyakorlat. Adjunk meg olyan legfeljebb harmadfokú komplex együtthatós polinomot, amelyre $f(0) = 3$, $f(1) = 3$, $f(4) = 15$ és $f(-1) = 0$.

2.4.19. Feladat. Tegyük fel, hogy az $f \in \mathbb{C}[x]$ polinom minden racionális helyen racionális értéket vesz fel. Következik-e ebből, hogy f racionális együtthatós? Igaz-e az állítás, ha „racionális" helyett mindenütt „egész" szerepel?

2.4.20. Feladat. Létezik-e olyan $f \in \mathbb{Z}[x]$ polinom, melyre $f(10) = 400$, $f(14) = 440$ és $f(18) = 520$?

2.4.21. Feladat. Tegyük fel, hogy n egész alapponthoz keresünk interpolációs polinomot, és az itt felvett értékek maguk is egészek, de a kapott legfeljebb $n-1$-edfokú interpolációs polinom mégsem egész együtthatós. Lehetséges-e, hogy az interpoláció egy magasabb fokú, de egész együtthatós polinommal is elvégezhető?

2.4.22. Feladat. Mutassuk meg, hogy ha R kommutatív, egységelemes gyűrű, amely felett az interpoláció korlátlanul elvégezhető, akkor R test.

2.4.23. Gyakorlat. Legyen R (mint eddig is) kommutatív, egységelemes gyűrű. Ellenőrizzük az alábbi állításokat.

(1) Az R-ből R-be menő függvények egységelemes, kommutatív gyűrűt alkotnak a pontonkénti összeadásra és szorzásra (2.4.3. Definíció), ami nem nullosztómentes.
(2) Ez az összeadás és szorzás nem vezet ki a polinomfüggvények közül, és azok is egységelemes, kommutatív gyűrűt alkotnak erre a két műveletre.
(3) Ha $b \in R$ egy rögzített elem, akkor az $f \mapsto f^*(b)$ leképezés összeg- és szorzattartó az $R[x]$ és az R gyűrűk között (röviden: a b *behelyettesítése* gyűrűhomomorfizmus).
(4) Igazoljuk, hogy az $f \mapsto f^*$ leképezés összeg- és szorzattartó az $R[x]$ és a polinomfüggvények gyűrűje között (azaz a polinomfüggvény képzése gyűrűhomomorfizmus).

2.4.24. Feladat. Legyen R a valós számokon értelmezett, valós értékű függvények gyűrűje a pontonkénti műveletekre. Mutassuk meg, hogy R-nek van olyan S részgyűrűje, amely egységelemes, de S egységeleme nem ugyanaz, mint R egységeleme. Előfordulhat ez a jelenség nullosztómentes R gyűrűben is? (Lásd a 2.2.35. Gyakorlatot is.)

2.5. A gyöktényezős alak

Az előző szakaszban láttuk, hogy ha R nullosztómentes (és mint polinomok vizsgálatakor lényegében mindig, kommutatív és egységelemes) gyűrű, akkor egy polinom gyökeihez tartozó gyöktényezők egyszerre is kiemelhetők. A 2.4.7. Tételben akár olyan szerencsénk is lehet, hogy q már konstans polinom, azaz a végeredmény a következő lesz:

$$f(x) = c(x - b_1)(x - b_2)\dots(x - b_n)\,,$$

ahol c egy nem nulla konstans. Ezt az f *gyöktényezős alakjának* hívjuk.

2.5.1. Gyakorlat. Mutassuk meg, hogy a gyöktényezős alakban szereplő c az f polinom főegyütthatója, az n szám pedig az f foka.

Ez a „szerencse” szükségszerűen bekövetkezik, ha az R gyűrűben minden nem konstans polinomnak már van gyöke.

2.5.2. Feladat. Mutassuk meg, hogy ha egy R (egységelemes, kommutatív) gyűrűben minden nem konstans polinomnak van gyöke, akkor R test.

2.5.3. Definíció. Azt mondjuk, hogy a T test *algebrailag zárt*, ha $T[x]$ minden nem konstans polinomjának van T-ben gyöke.

Algebrailag zárt test fölött tehát minden polinom gyöktényezős alakban írható. A valós számok teste nem algebrailag zárt, hiszen például az $x^2 + 1$ polinomnak nincsen benne gyöke. Pontosan azért vezettük be a komplex számokat, hogy ezt a problémát kiküszöböljük. Láttuk, hogy a komplex számok testében a gyökvonás mindig elvégezhető, vagyis az $x^n - a$ polinomnak mindig van gyöke. A komplex számok konstrukciója azonban még ennél is jobban sikerült.

2.5.4. Tétel [Az algebra alaptétele]. *A komplex számok teste algebrailag zárt.*

Ezt a tételt csak később, a Galois-elmélet egy alkalmazásaként bizonyítjuk (6.6.10. Tétel). Rá kell azonban mutatnunk, hogy az algebra alaptétele valójában az analízis tétele! Ennek az az oka, hogy a valós számok bevezetésekor folytonossági meggondolások játszanak szerepet. A komplex számokon értelmezett függvények vizsgálatában is fontos szerepet kap az analízis. A komplex függvénytan apparátusával az algebra alaptételére több, nagyon egyszerű és roppant elegáns bizonyítást kaphatunk.

A gyöktényezős alakban ugyanaz a tényező többször is szerepelhet. Ha ezeket összevonjuk, akkor a következő alakot kapjuk:

$$f(x) = c(x - d_1)^{k_1}(x - d_2)^{k_2}\dots(x - d_m)^{k_m}\,,$$

ahol a $d_1, \ldots, d_m$ már páronként különbözők. Ezt az összevont formát *kanonikus alaknak* nevezzük, a k_j számot pedig a d_j gyök *multiplicitásának* hívjuk. Másképp fogalmazva azt mondjuk, hogy d_j az f-nek k_j*-szeres gyöke*. A fokszámokat felírva látjuk, hogy

$$k_1 + k_2 + \ldots + k_n = \mathrm{gr}(f)\,.$$

Ezt úgy szokás fogalmazni, hogy egy polinomnak, ha gyöktényezős alakra hozható, *multiplicitásokkal számolva pontosan annyi gyöke van, mint a foka.*

Ezekkel az elnevezésekkel súlyos probléma lenne, ha az f polinomot máshogy is fel tudnánk írni gyöktényezős alakban. Ha előfordulhatna olyasmi, hogy $(x-1)^2(x-2)^3 = (x-1)^3(x-2)^2$ akkor nem tudhatnánk, hogy a 2 szám most kétszeres, vagy háromszoros gyök-e. Ilyesmi azonban nem fordulhat elő, mert *a kanonikus alak egyértelmű,* amit azonnal be fogunk látni.

A többszörös gyökök fenti definíciójával más baj is van: nem elég általános. Ha valós együtthatós polinomokat akarunk vizsgálni, akkor az

$$f(x) = (x-1)^2(x-2)^3(x^2+1)^2(x^2+3)^5$$

ugyan nem hozható kanonikus alakra $\mathbb{R}$ fölött, mégis úgy érezzük, hasznos lenne azt mondani, hogy e polinomnak a 2 szám háromszoros gyöke. Mi lenne akkor a többszörös gyök „helyes" definíciója? Azt érdemes észrevenni, hogy ha a fenti polinomból elvesszük az $(x-2)^3$ gyöktényezőt, akkor a maradék résznek a 2 már nem gyöke.

2.5.5. Definíció. Legyen R szokásos gyűrű. Azt mondjuk, hogy az $f \in R[x]$ polinomnak a $b \in R$ elem (pontosan) k*-szoros gyöke* (vagy, hogy a b gyök *multiplicitása* k), ha

$$f(x) = (x-b)^k q(x)$$

alakban írható, ahol a $q \in R[x]$ polinomnak b már nem gyöke.

Itt k nemnegatív egészet jelöl. Célszerű megengedni a $k = 0$ esetet is, mert így könnyebben fogalmazhatunk meg majd bizonyos eredményeket. Persze a „nullaszoros gyök" helyett azt mondjuk majd, hogy b „nem gyöke" a polinomnak.

2.5.6. Gyakorlat. Mutassuk meg, hogy ha R nullosztómentes, akkor

(1) gyök multiplicitása egyértelműen meghatározott (vagyis az előző definíció adott f és b mellett csak egyetlen k-ra teljesülhet);
(2) ha az f polinomnak van gyöktényezős alakja, akkor a többszörös gyök most adott definíciója ugyanaz, mint amiről fentebb beszéltünk.

Ebből már nyilvánvaló, hogy egy nullosztómentes gyűrű felett a kanonikus alak egyértelmű (ezt más eszközökkel újra belátjuk majd, amikor a polinomok számelméletét tanulmányozzuk). Valóban, a fenti kanonikus alakban a d_j elemek azért egyértelműen meghatározottak, mert ezek pontosan f gyökei, a k_j kitevők pedig az előbbi 2.5.6. Gyakorlat miatt lesznek egyértelműek. Többszörös gyökök meghatározására két eljárást is tanulunk majd (a 3.6, illetve 3.7. Szakaszokban).

Utolsó témaként a *gyökök és együtthatók közötti összefüggéseket* tekintjük át.

2.5.7. Gyakorlat. Számítsuk ki x alábbi két polinomjának az együtthatóit:

$$(x-b_1)(x-b_2)(x-b_3) \qquad \text{és} \qquad (x-b_1)(x-b_2)(x-b_3)(x-b_4)\,.$$

Az előző gyakorlat megoldását általában végezve a következő képleteket kapjuk.

2.5.8. Tétel. *Ha az R kommutatív, egységelemes gyűrű feletti f polinomra*

$$f(x) = (x-b_1)\dots(x-b_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - + \ldots + (-1)^n \sigma_n\,,$$

akkor a gyökök és együtthatók közötti összefüggések a következők:

$$\sigma_1 = b_1 + b_2 + \ldots + b_n \qquad \text{tagok száma: } \binom{n}{1} = n$$

$$\sigma_2 = b_1b_2 + \ldots + b_1b_n + b_2b_3 + \ldots + b_{n-1}b_n \qquad \text{tagok száma: } \binom{n}{2}$$

$$\sigma_k = b_1b_2\dots b_k + \ldots \qquad \text{tagok száma: } \binom{n}{k}$$

$$\sigma_n = b_1b_2\dots b_n \qquad \text{tagok száma: } \binom{n}{n} = 1\,.$$

A σ_k úgy keletkezik, hogy a $b_1, \dots, b_n$ közül az összes lehetséges módon kiválasztunk k darabot, a kiválasztott b_i-ket összeszorozzuk, majd a kapott szorzatokat összeadjuk. Szokás a σ_0-ról is beszélni, és (a fenti f főegyütthatójaként) konstans 1-nek tekinteni.

(Az itt szereplő $\binom{n}{k}$ binomiális együtthatót a A.2.2. Tételben definiáltuk.) A most kapott képletekben hasznos lesz, ha $b_1, \dots, b_n$-et határozatlanoknak, és nem R-beli elemeknek tekintjük. Ekkor σ_k ezen határozatlanok (többhatározatlanú) polinomjává válik. Ezeket később *elemi szimmetrikus polinomoknak* fogjuk nevezni.

Célszerű a gyökök és együtthatók összefüggését általános együtthatójú polinomra is átfogalmazni.

2.5.9. Következmény. *Tegyük fel, hogy*

$$f(x) = a_0 + a_1x + \ldots + a_nx^n = a_n(x-b_1)\dots(x-b_n)\,.$$

Ekkor $0 \le k \le n$ esetén

$$a_k = a_n(-1)^{n-k}\sigma_{n-k}(b_1, \dots, b_n)\,,$$

vagyis

$$\sigma_k(b_1, \dots, b_n) = (-1)^k a_{n-k}/a_n\,.$$

Bizonyítás. Az állítás azonnal adódik, ha az $(x-b_1)\dots(x-b_n)$ szorzatot az előző tétel szerint kifejtjük, és a két oldal együtthatóit összehasonlítjuk. □

Gyakorlatok, feladatok

2.5.10. Gyakorlat. Írjuk fel az $x^4 + 4$ polinomot gyöktényezős alakban, és ellenőrizzük beszorzással az eredményt. Hogyan lehetne ezt a polinomot valós együtthatós polinomok szorzatára bontani?

2.5.11. Gyakorlat. Hányszoros gyöke az $x^4 - x^3 - x + 1$ polinomnak az 1? A Horner-elrendezést használjuk.

2.5.12. Gyakorlat. Mutassuk meg, hogy ha két n-edfokú komplex együtthatós polinom n (komplex) helyen megegyezik (vagyis a két polinom ugyanazt az értéket veszi fel), és a főegyütthatóik egyenlők, akkor a polinomok is egyenlők.

2.5.13. Feladat. Fejezzük ki az $x_1^2 + x_2^2 + \ldots + x_n^2$ négyzetösszeget a $\sigma_1(x_1, x_2, \ldots, x_n)$ és a $\sigma_2(x_1, x_2, \ldots, x_n)$ segítségével.

2.5.14. Gyakorlat. Határozzuk meg a $2x^4 + 2x + 3$ polinom komplex gyökeinek összegét, szorzatát, négyzetösszegét, és a gyökök reciprokainak összegét.

2.5.15. Feladat. Legyenek $\varepsilon_1, \ldots, \varepsilon_n$ az összes n-edik egységgyökök.

(1) Bontsuk gyöktényezős alakra az $x^4 - 1$ polinomot.
(2) Bizonyítsuk be, hogy $x^n - 1 = (x - \varepsilon_1) \ldots (x - \varepsilon_n)$.
(3) A gyökök és együtthatók összefüggése alapján számítsuk ki az n-edik egységgyökök összegét, négyzetösszegét és szorzatát.
(4) Az egységsugarú körbe írt szabályos n-szög egy csúcsából az összes többi csúcsba húzott szakaszok hosszát összeszoroztuk. Bizonyítsuk be, hogy az eredmény n-nel egyenlő.

2.5.16. Gyakorlat. Értelmezhető-e egy polinomfüggvény gyökeinek a multiplicitása?

2.5.17. Feladat. Mutassuk meg, hogy véges test nem lehet algebrailag zárt.

2.6. Többhatározatlanú polinomok

Ahogy korábban már megbeszéltük, többhatározatlanú polinomon olyan kifejezéseket szeretnénk érteni, amelyek az $x_1, \ldots, x_n$ határozatlanokból és valamilyen R gyűrű elemeiből épülnek fel összeadás, kivonás és szorzás segítségével. Azt gondoljuk, hogy ezek

$$f(x_1, \ldots, x_n) = \sum r_{m_1,m_2,\ldots,m_n} x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$$

alakban írhatók fel, ahol az $r_{m_1,m_2,\ldots,m_n}$ együtthatók R-nek elemei, $m_1, m_2, \ldots, m_n$ pedig nemnegatív egészek. A polinom *tagjainak* a fenti összeg tagjait nevezzük (feltételezve, hogy a lehetséges összevonásokat már elvégeztük, tehát semelyik $x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ sem szerepelhet több együtthatóval). Azt szeretnénk, hogy ezeket az együtthatókat a polinom

egyértelműen meghatározza. Láttuk (a 2.1. Szakasz végén) azt is, hogy magát a definíciót érdemesebb úgy megalkotni, hogy a fenti „polinomot" az egyik határozatlan szerint rendezzük. Ekkor az együtthatók is polinomok lesznek, amelyekben azonban már eggyel kevesebb a határozatlan.

2.6.1. Definíció. Az R (kommutatív, egységelemes) gyűrű feletti, $x_1, \dots x_n$-határozatlanú (vagy röviden csak n-határozatlanú) polinomok $R[x_1, \dots, x_n]$ gyűrűjét n szerinti indukcióval definiáljuk: ez nem más, mint $(R[x_1, \dots, x_{n-1}])[x_n]$. Az indukció kezdőlépése a már ismert $R[x_1]$ polinomgyűrű.

Ebben a definícióban úgy képzeltük, hogy a polinomokat az x_n határozatlan szerint rendezzük. Eszünkbe juthatna, hogy mondjuk az x_1 határozatlan szerint rendezzük őket, és akkor az $R[x_2, \dots, x_n][x_1]$ gyűrűhöz jutnánk. Ez formailag más, mint az $R[x_1, \dots, x_{n-1}][x_n]$ (pláne ha még a „sorozatos" precíz bevezetéshez is ragaszkodunk). De a két gyűrű mégis, a lényeget tekintve ugyanaz. (Később az ilyesmit úgy fogalmazzuk majd, hogy a két gyűrű *izomorf*, lényegében „ugyanazok" az elemeik, és „ugyanúgy" kell bennük számolni, precízen: van közöttük kölcsönösen egyértelmű, művelettartó megfeleltetés.) Most azonban minderre még semmi szükség nincs, mert a fenti többértelműség semmiféle gyakorlati problémát nem fog okozni.

2.6.2. Állítás. *Az n-határozatlanú polinomok gyűrűje kommutatív és egységelemes. Ha R nullosztómentes, akkor $R[x_1, \dots, x_n]$ is az, és az invertálható elemei azok a konstans polinomok, amelyek R-ben invertálhatóak.*

Bizonyítás. Teljes indukcióval azonnal következik a 2.3.2. Tételből. Természetesen a konstans polinomok továbbra is R elemei, amelyeket (sőt az n-nél kevesebb határozatlanú polinomokat is) n-határozatlanú polinomoknak képzeljük. □

A fenti $rx_1^{m_1}x_2^{m_2}\dots x_n^{m_m}$ tag *fokát* $m_1 + \dots + m_m$-nek definiáljuk. Az f polinom fokán a benne szereplő tagok fokainak maximumát értjük. Vigyázzunk, ez *nem ugyanaz*, mint amikor a polinomot mondjuk x_n polinomjának tekintve számítjuk ki a fokát. Például

$$f = x^2y + y^3x$$

foka 2, ha f-et x polinomjának tekintjük, 3, ha y polinomjának tekintjük, és 4 a fenti értelemben. Tehát ha fokszámról beszélünk, mindig meg kell mondanunk, milyen értelemben gondoljuk, vagyis hogy a polinomot többhatározatlanúnak, vagy egyhatározatlanúnak képzeljük (és az utóbbi esetben melyik határozatlan szerint rendezünk).

Egy polinomot *homogénnek* nevezünk, ha minden tagjának ugyanaz a foka. Ha f polinom, akkor gyűjtsük össze a k-adfokú tagjait, és jelöljük ezek összegét f_k-val. Nyilván f_k homogén polinom, és f az f_k polinomok összege. Ezért minden polinom egyértelműen felbontható homogén polinomok összegére. Az f_k-t az f polinom k-adfokú *homogén komponensének* hívjuk.

Ha f-ben nincs egyáltalán k-edfokú tag, akkor f_k-t nullának értjük (lásd az üres összegről írottakat a 2.2.43. Gyakorlatban).

2.6.3. Gyakorlat. Mutassuk meg, hogy ha f és g többhatározatlanú polinomok az R nullosztómentes gyűrű fölött, akkor az fg polinom k-adfokú homogén komponense

$$f_0 g_k + f_1 g_{k-1} + \ldots + f_k g_0 = \sum_{i=0}^{k} f_i g_{k-i} \,.$$

Speciálisan fg foka az f és g fokainak összege.

A következő szakaszban belátjuk első komolyabb tételünket, az úgynevezett szimmetrikus polinomok alaptételét. A bizonyításhoz egy új fogalom bevezetésére van szükség: általánosítanunk kell a főtag fogalmát többváltozós polinomokra.

Vegyünk egy $f \in R[x_1, \ldots, x_n]$ polinomot, ennek tagjai $r x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ alakúak. A kitevők $(m_1, \ldots, m_n)$ sorozatát egy n „jegyű" telefonszámnak képzelhetjük (az analógia annyiban sántít, hogy a „jegyek", vagyis az m_j számok akármekkorák lehetnek). Rakjuk ezeket a telefonszámokat növekvő sorrendbe a szokásos módon, és írjuk fel az f polinom tagjait ebben a sorrendben. Például ha

$$f(x_1, x_2, x_3) = x_1 x_2^4 - i x_1^2 x_3 + x_1 x_2 x_3 - 3x_2^3 + x_3^2 + 2x_1^2 + x_1 x_2 x_3^3 \,, \tag{2.2}$$

akkor a kapott „telefonszámok" $x_1 x_2^4 = x_1 x_2^4 x_3^0 \mapsto 140$ (a nulla kitevőket is ki kell írni!), azután sorban haladva 201, 111, 030, 002, 200, 113. A „növekvő" sorrend 002, 030, 111, 113, 140, 200, 201. Az f ennek megfelelő felírása a következő:

$$x_3^2 - 3x_2^3 + x_1 x_2 x_3 + x_1 x_2 x_3^3 + x_1 x_2^4 + 2x_1^2 - i x_1^2 x_3 \,.$$

Az általános szabály tehát az, hogy először az első „jegyeket" kell sorba rakni, azután a második jegyeket, és így tovább. Hasonló elv szerint rendezzük egy lexikonban a címszavakat is (ábécé sorrendben), és ezért ennek a sorrendnek *lexikografikus rendezés* a neve.

2.6.4. Definíció. Legyenek r és s nem nulla elemei az R szokásos gyűrűnek. Azt mondjuk, hogy a

$$P = r x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n} \qquad \text{és} \qquad Q = s x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$$

tagok közül az első lexikografikusan kisebb a másodiknál, ha az első olyan j indexnél, ahol az $(m_1, \ldots, m_n)$ és $(k_1, \ldots, k_n)$ sorozatok eltérnek, $m_j < k_j$ teljesül. Másképp fogalmazva: van olyan $1 \le j \le n$, hogy $m_1 = k_1, m_2 = k_2, \ldots, m_{j-1} = k_{j-1}$, de $m_j < k_j$. Erre a fogalomra a $P \prec Q$ jelölést fogjuk használni. Azt is írjuk majd, hogy $P \preceq Q$, ha $P \prec Q$, vagy P és Q az együtthatójuktól eltekintve megegyezik (vagyis a kitevősorozatuk ugyanaz).

A lexikografikus rendezés szoros kapcsolatban van azzal, ahogy polinomjainkat indukcióval definiáltuk. A kapcsolatot a következő gyakorlat írja le. Ez az összefüggés magyarázza, hogy a lexikografikus rendezést a fokszám valamiféle általánosításának, finomításának tekinthetjük.

2.6.5. Gyakorlat. Ha adott egy $f \in R[x_1, \dots, x_n]$ polinom, akkor rendezzük x_1 hatványai szerint (és írjuk is le a konstans taggal kezdve, fokszám szerint növekvő sorrendben). Az együtthatók $R[x_2, \dots, x_n]$ elemei lesznek, ezeket rendezzük x_2 hatványai szerint. A kapott együtthatókat x_3 hatványai szerint. És így tovább, végül „legbelül" x_n hatványai szerint rendezünk. Mutassuk meg, hogy ha a zárójeleket kibontjuk, de a sorrendet nem változtatjuk meg, akkor f tagjai lexikografikusan növekvő sorrendben lesznek.

Ha két egyhatározatlanú polinomot összeszorzunk, akkor a szorzat főtagja a két polinom főtagjainak szorzata lesz. Szeretnénk ezt az állítást többhatározatlanú polinomokra is általánosítani. Egy n-határozatlanú polinom (lexikografikus értelemben vett) *főtagján* a nem nulla tagjai közül azt értjük, ami a lexikografikus értelemben a legnagyobb. Például az imént vizsgált (2.2)-beli f polinom főtagja $-ix_1^2x_3$. A következő lemma segít meghatározni a szorzatpolinom főtagját.

2.6.6. Lemma. *Legyenek P', P, Q', Q egytagú, n-határozatlanú polinomok, melyeknek az együtthatója* 1. *Tegyük fel, hogy $P' \preceq P$ és $Q' \preceq Q$ teljesül. Ekkor $P'Q' \preceq PQ$. Ha itt egyenlőség áll, akkor $P' = P$ és $Q' = Q$.*

Bizonyítás. Legyen

$$P' = x_1^{m'_1}x_2^{m'_2}\dots x_n^{m'_n},\ P = x_1^{m_1}x_2^{m_2}\dots x_n^{m_n},\ Q' = x_1^{k'_1}x_2^{k'_2}\dots x_n^{k'_n},\ Q = x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}.$$

Ekkor

$$P'Q' = x_1^{m'_1+k'_1}x_2^{m'_2+k'_2}\dots x_n^{m'_n+k'_n} \quad \text{és} \quad PQ = x_1^{m_1+k_1}x_2^{m_2+k_2}\dots x_n^{m_n+k_n}.$$

Arra vagyunk kíváncsiak, hogy hol tér el először ez a két kitevősorozat.

Nézzük meg először azt az egyszerű esetet, amikor $P' = P$. Ha $Q' = Q$, akkor nyilván $P'Q' = PQ$. Ha $Q' \neq Q$, akkor jelölje j azt az indexet, ahol Q' és Q kitevősorozata először eltér: $k'_i = k_i$ ha $i < j$, de $Q' \prec Q$ miatt $k'_j < k_j$. Tudjuk, hogy $P' = P$, ezért minden i-re $m'_i = m_i$. Tehát a $P'Q'$ és a PQ kitevősorozata is a j-edik helyen tér el először: $m'_i + k'_i = m_i + k_i$ ha $i < j$, viszont $m'_j + k'_j < m_j + k_j$. Ezért $P'Q' \prec PQ$.

Ha az előző bekezdés gondolatmenetében felcseréljük P-t Q-val és P'-t Q'-vel, akkor az adódik, hogy $P' \prec P$ és $Q' = Q$ esetén is $P'Q' \prec PQ$. Tehát már csak akkor kell bizonyítanunk az állítást, amikor $P' \prec P$ és $Q' \prec Q$.

Ebben az esetben azt állítjuk, hogy $P'Q'$ és PQ kitevősorozata ott fog először eltérni, ahol előbb van eltérés P és P', illetve Q és Q' sorozata között. Valóban, legyen j az az index, ahol P sorozata először eltér P' sorozatától, és ℓ az az index, ahol Q' sorozata először eltér Q sorozatától. Feltehetjük, hogy $j \leq \ell$ (vagyis hogy P' előbb kezd eltérni P-től, mint Q' a Q-tól), hiszen ellenkező esetben megcserélhetjük P-t Q-val és P'-t Q'-vel. Nyilván $i < j$ esetén $m'_i = m_i$ és $k'_i = k_i$, tehát ilyenkor $m'_i + k'_i = m_i + k_i$. Mivel $P' \prec P$, tudjuk, hogy $m'_j < m_j$. Ugyanakkor $j < \ell$ esetén $k'_j = k_j$, ha pedig $j = \ell$, akkor $k'_j < k_j$. Mindkét esetben azt kapjuk, hogy $m'_j + k'_j < m_j + k_j$. Tehát tényleg $P'Q' \prec PQ$. □

2.6.7. Következmény. *Ha R nullosztómentes, és $f, g \in R[x_1, \dots x_n]$, akkor fg főtagja az f és g főtagjainak szorzata.*

Így újabb bizonyítást kaptunk arra, hogy $R[x_1, \dots x_n]$ nullosztómentes.

Bizonyítás. Legyen az f főtagja rP és a g főtagja sQ, ahol r és s az R gyűrű nem nulla elemei. Amikor f-et és g-t összeszorozzuk, akkor f egy tetszőleges $r'P'$ tagját megszorozzuk g egy tetszőleges $s'Q'$ tagjával, majd összevonjuk azokat a tagokat, amelyek csak az együtthatójukban különböznek. Nyilván $P' \preceq P$ és $Q' \preceq Q$. Az előző lemma szerint $P'Q' \preceq PQ$, vagyis a szorzatpolinomban $rsPQ$-nál lexikografikusan nagyobb tag nem keletkezhet. Azt kell még megnéznünk, hogy az összevonások során nem eshet-e ki az $rsPQ$ tag. A lemma szerint azonban $P'Q' \prec PQ$, kivéve ha $P' = P$ és $Q' = Q$. Ezért $rsPQ$ semmivel sem vonható össze, és így nem is tud kiesni. Az R nullosztómentessége miatt $rs \neq 0$, és így fg főtagja tényleg f és g főtagjainak szorzata. □

A főtagok az összeadásra is hasonlóan viselkednek, mint az egyváltozós polinomoknál. Ha két polinom főtagja nemcsak együtthatójában tér el, akkor összegüknek a főtagja a két főtag közül a lexikografikus értelemben nagyobbik lesz. Ha viszont a két főtag csak az együtthatóban tér el, akkor az összeg főtagját ezekből összevonással kapjuk, kivéve, ha ez a tag kiesik, ilyenkor a főtag lexikografikusan csökken, sőt akár a nullapolinom is lehet az eredmény (aminek nincs is főtagja).

Gyakorlatok, feladatok

2.6.8. Gyakorlat. Az alábbi $p(x_1, x_2, x_3, x_4)$ polinomot bontsuk fel homogén polinomok összegére, ezeket rendezzük lexikografikusan, és állapítsuk meg a p^7 polinomban egyrészt a lexikografikusan legnagyobb tagot, másrészt a legnagyobb fokú tagok közül a lexikografikusan legnagyobb tagot.

$$ix_1x_2x_3x_4^2 - x_1^2x_3^3 + 3x_1^3x_2 + \pi x_1^2x_2^3 + x_4 - x_1^2x_2^2x_3 + 2x_1^2x_2x_3x_4 - 6x_1^2x_2^2x_4\,.$$

2.6.9. Gyakorlat. Definiáljuk precízen egy n-változós polinomhoz tartozó n-változós polinomfüggvény fogalmát, és igazoljuk, hogy $f, g \in R[x_1, \dots, x_n]$ és $\mathbf{b} \in R^n$ esetén

$$f(\mathbf{b}) \pm g(\mathbf{b}) = (f \pm g)(\mathbf{b}) \quad \text{és} \quad f(\mathbf{b})g(\mathbf{b}) = (fg)(\mathbf{b})\,.$$

Általánosítsuk a pontonkénti műveletek 2.4.3. Definícióját többváltozós függvényekre is, és igazoljuk, hogy a 2.4.23. Gyakorlat állításai érvényben maradnak többváltozós polinomokra.

2.6.10. Feladat. Igaz-e végtelen, nullosztómentes (szokásos) gyűrű fölött a többváltozós polinomok azonossági tétele (vagyis hogy a polinomfüggvény egyértelműen meghatározza a polinomot)?

2.6.11. Feladat. Általánosítsuk az interpolációt többhatározatlanú polinomokra. Mutassuk meg, hogy véges test esetében minden véges sok változós függvény polinomfüggvény.

2.7. Szimmetrikus polinomok

Gyakran előfordul, hogy egy többhatározatlanú polinom *szimmetrikus*. Ilyen például a háromváltozós

$$x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + x_1 + x_2 + x_3 - x_1x_2x_3$$

polinom. Ebben a három határozatlan szerepe teljesen egyenrangú: ha például x_2-t és x_3-at kicseréljük, a polinom változatlan marad. Ugyanakkor

$$x_1^2x_2 + x_2^2x_3 + x_3^2x_1$$

nem szimmetrikus, mert például x_1 és x_2 cseréjekor a következőbe megy át:

$$x_2^2x_1 + x_1^2x_3 + x_3^2x_2\,,$$

ami nem az eredeti polinom, hiszen ebben például $x_1^2x_2$ nem szerepel.

2.7.1. Definíció. Az $f \in R[x_1, \ldots, x_n]$ polinomot szimmetrikus polinomnak nevezzük, ha bármely két határozatlant kicserélve a polinom önmagába megy át.

Nyilván szimmetrikus polinomok összege, különbsége és szorzata is szimmetrikus, és így a szimmetrikus polinomok részgyűrűt alkotnak a polinomok között. A gyökök és együtthatók összefüggésében (a 2.5.8. Tételben) szereplő σ_k kifejezések is szimmetrikus polinomok.

2.7.2. Definíció. Az $x_1, \ldots, x_n$ határozatlanú, k-adik *elemi szimmetrikus polinom* úgy keletkezik, hogy az $x_1, \ldots, x_n$ közül az összes lehetséges módon kiválasztunk k darabot, a kiválasztott x_i-ket összeszorozzuk, majd a kapott szorzatokat összeadjuk. E polinom jele $\sigma_k(x_1, \ldots, x_n)$, ahol $1 \leq k \leq n$. A σ_0 polinomot konstans 1-nek definiáljuk. (Néha használják $k > n$ esetén a $\sigma_k = 0$ konvenciót is).

Az elemi szimmetrikus polinomok azért fontosak, mert segítségükkel az összes többi szimmetrikus polinomot ki lehet fejezni, méghozzá egyértelműen. (Ezt illusztrálja például a 2.5.14. Gyakorlat.) De mit értünk azalatt, hogy „ki lehet fejezni”? Milyen műveleteket használhatunk eközben? Milyen értelemben egyértelmű ez a „kifejezés”? Vizsgáljunk meg először egy konkrét példát. Legyen

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - ix_1x_2x_3\,.$$

A 2.5.13. Feladat megoldásakor rájöttünk, hogy a négyzetösszeggel hogyan érdemes bánni:

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3)\,.$$

Itt már csupa elemi szimmetrikus polinom szerepel. Tehát végül is

$$f = \sigma_1^2 - 2\sigma_2 - i\sigma_3\,.$$

Azaz f kifejezésekor összeadást és kivonást használtunk, f együtthatóiból és az elemi szimmetrikus polinomokból kiindulva.

De polinomnak azokat a kifejezéseket neveztük, amelyek a határozatlanokból és az alapgyűrű elemeiből az összeadás, kivonás és szorzás ismételt használatakor keletkeznek.

Vagyis azt mondhatjuk, hogy f-et az elemi szimmetrikus polinomok *polinomjaként* írtuk fel. Valóban, ha

$$F(y_1, y_2, y_3) = y_1^2 - 2y_2 - iy_3 \in \mathbb{C}[y_1, y_2, y_3]\,,$$

akkor a fenti képlet szerint

$$f = F(\sigma_1, \sigma_2, \sigma_3)\,,$$

(az egyenlőséget úgy kell érteni, hogy a két oldal, mint x_1, x_2, x_3 polinomja, megegyezik). Most már nem lehet gondunk az egyértelműség megfogalmazása sem: arról van szó, hogy $f(x_1, x_2, x_3)$ az $F(y_1, y_2, y_3)$ polinomot egyértelműen meghatározza.

2.7.3. Tétel [A szimmetrikus polinomok alaptétele]. *Legyen R szokásos gyűrű. Ekkor minden $f \in R[x_1, \ldots, x_n]$ szimmetrikus polinom egyértelműen felírható az elemi szimmetrikus polinomok polinomjaként. Ez azt jelenti, hogy létezik pontosan egy $F \in R[y_1, \ldots, y_n]$ polinom, melyre*

$$f(x_1, \ldots, x_n) = F(\sigma_1, \ldots, \sigma_n)\,.$$

A F együtthatói a f együtthatóiból összeadás és kivonás segítségével kaphatók.

Bizonyítás. Egyben eljárást is fogunk adni arra, hogy egy konkrét polinomot hogyan fejezzünk ki az elemi szimmetrikus polinomokkal.

2.7.4. Gyakorlat. Mutassuk meg, hogy ha az

$$ry_1^{k_1} y_2^{k_2} \ldots y_n^{k_n} \in R[y_1, \ldots, y_n]$$

polinomban az y_i helyére a $\sigma_i(x_1, \ldots, x_n)$ elemi szimmetrikus polinomot helyettesítjük, akkor

$$rx_1^{k_1+\ldots+k_n} x_2^{k_2+\ldots+k_n} \ldots x_{n-1}^{k_{n-1}+k_n} x_n^{k_n}$$

lesz az eredmény főtagja.

Látjuk, hogy a kapott főtagban a kitevők sorozata csökkenő. Ez nem véletlen, hanem így van minden szimmetrikus polinomban.

2.7.5. Gyakorlat. Mutassuk meg, hogy ha az $f \in R[x_1, \ldots, x_n]$ szimmetrikus polinom főtagja

$$rx_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}\,,$$

akkor $m_1 \geq m_2 \geq \ldots \geq m_n$, és f minden tagjában mindegyik határozatlan kitevője legfeljebb m_1 lehet. Igazoljuk, hogy az f polinomnak legfeljebb $(m_1 + 1)^n$ tagja lehet.

Legyen hát adva egy $f \in R[x_1, \ldots, x_n]$ szimmetrikus polinom. Le szeretnénk vonni belőle egy

$$g = s\sigma_1^{k_1} \sigma_2^{k_2} \ldots \sigma_n^{k_n}$$

alakú polinomot úgy, hogy a főtagja kiessen, de ne is termelődjön közben az eredeti főtagnál lexikografikusan nagyobb tag. Ha f főtagja $rx_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$, akkor az előző két gyakorlat szerint, ha s-et r-nek választjuk, a k_i számokat pedig úgy, hogy

$$k_1 + \ldots + k_n = m_1\,, \quad k_2 + \ldots + k_n = m_2\,, \quad \ldots\,, \quad k_{n-1} + k_n = m_{n-1}\,, \quad k_n = m_n$$

legyen, akkor f és g főtagja meg fog egyezni. Mivel $m_1 \geq m_2 \geq \ldots \geq m_n$, a k_i számokat meg is lehet így választani, a következőképpen:

$$k_1 = m_1 - m_2\,, \quad k_2 = m_2 - m_3\,, \quad \ldots\,, \quad k_{n-1} = m_{n-1} - m_n\,, \quad k_n = m_n\,.$$

Az $f - g$ szintén szimmetrikus polinom. Ha nulla, akkor készen vagyunk, hiszen g már az elemi szimmetrikus polinomok polinomja. Ha nem, akkor is tudjuk, hogy $f - g$ főtagja már lexikografikusan kisebb, mint f eredeti főtagja volt. Abban reménykedünk, hogy ezt az eljárást ismételgetve véges sok lépésben már a nulla polinomhoz jutunk, ami azt jelenti, hogy az eredeti polinomot felírtuk az elemi szimmetrikus polinomok polinomjaként.

A fenti 2.7.5. Gyakorlat mutatja, hogy az eljárás során soha nem fog m_1-nél nagyobb kitevő előfordulni. Vagyis mindegyik kitevő $m_1 + 1$-féle lehet: $0, 1, \ldots, m_1$ valamelyike. Ezért az eljárás során keletkező főtagból sem lehet több, mint $(m_1 + 1)^n$, azaz csak véges sok. Az eljárás tehát tényleg véges sok lépésben véget ér, és így $f(x_1, \ldots, x_n)$-et sikerült $F(\sigma_1, \ldots, \sigma_n)$ alakban előállítani.

Mik lesznek a kapott F polinom együtthatói? Az első lépésben g-nek, mint $\sigma_1, \ldots, \sigma_n$ polinomjának az egyetlen együtthatója r lesz, ami a kiinduló f-nek is együtthatója. Az $f - g$-nek (mint $x_1, \ldots, x_n$ polinomjának) együtthatói az f együtthatóiból összeadással és kivonással keletkeznek. A második lépésben az $f - g$ egyik együtthatóját használjuk fel az új, második g felírásakor, és így tovább. Ezért a végén kapott $F(\sigma_1, \ldots, \sigma_n)$ együtthatói tényleg megkaphatók f együtthatóiból összeadás és kivonás segítségével.

Most rátérünk az egyértelműség bizonyítására. Tegyük fel, hogy $F, G \in R[y_1, \ldots, y_n]$ két olyan polinom, amelybe mindegyik y_i helyébe σ_i-t helyettesítve, és a műveleteket elvégezve, a kapott $F(\sigma_1, \ldots, \sigma_n)$ és $G(\sigma_1, \ldots, \sigma_n)$, mint $x_1, \ldots, x_n$ polinomjai, egyenlőek lesznek. Meg kell mutatnunk, hogy akkor F és G, mint az $y_1, \ldots, y_n$ polinomjai, eredetileg is egyenlőek voltak. Kényelmesebb az F és G polinomok $H = F - G$ különbségével dolgozni. Most tehát azt tudjuk, hogy $H(\sigma_1, \ldots, \sigma_n)$, mint az $x_1, \ldots, x_n$ polinomja, azonosan nullává válik, és meg kell mutatnunk, hogy ez csak akkor lehet, ha már $H(y_1, \ldots, y_n)$ is a nullapolinom volt. Másképp fogalmazva: ha veszünk egy $H(y_1, \ldots, y_n)$ nem nulla polinomot, akkor meg kell keresnünk a $H(\sigma_1, \ldots, \sigma_n)$-nek egy olyan tagját, ami nem tud kiesni, ha a műveleteket elvégezzük. Azt javasoljuk az Olvasónak, hogy először az alábbi speciális esetben maga végezze el a számolást (de mindenképpen nézze meg a megoldást) mielőtt tovább haladna.

2.7.6. Gyakorlat. Legyen

$$H(y_1, y_2, y_3) = 30y_1y_3^3 - y_2^5\,.$$

Helyettesítsük be mindegyik y_i helyére a három határozatlanú $\sigma_i(x_1, x_2, x_3)$ elemi szimmetrikus polinomot, és adjuk meg az eredménynek egy nem nulla tagját.

Vegyük a $H(y_1, \ldots, y_n)$ polinom egy tetszőleges $ry_1^{k_1} \ldots y_n^{k_n}$ tagját. Helyettesítsük be a σ_i-ket, és számítsuk ki a $\sigma_1^{k_1}\sigma_2^{k_2} \ldots \sigma_n^{k_n}$ polinom főtagját:

$$P = x_1^{k_1+\ldots+k_n} x_2^{k_2+\ldots+k_n} \ldots x_{n-1}^{k_{n-1}+k_n} x_n^{k_n}\,.$$

2.7.7. Állítás. *A H különböző tagjaiból a fenti eljárással kapott P főtagok különbözők lesznek. (Feltételezzük természetesen, hogy $H(y_1, \dots, y_n)$-ben már összevontuk azokat a tagokat, amelyek csak az együtthatójukban különböznek.)*

Bizonyítás. Az állítás bizonyításához tegyük fel, hogy $s y_1^{\ell_1} \dots y_n^{\ell_n}$ a $H(y_1, \dots, y_n)$ polinomnak egy másik tagja. Ekkor a $\sigma_1^{\ell_1}\sigma_2^{\ell_2}\dots\sigma_n^{\ell_n}$ főtagja

$$Q = x_1^{\ell_1+\dots+\ell_n} x_2^{\ell_2+\dots+\ell_n} \dots x_{n-1}^{\ell_{n-1}+\ell_n} x_n^{\ell_n}.$$

Ha $P = Q$, akkor az x_n kitevőjét megvizsgálva látjuk, hogy $k_n = \ell_n$. Az x_{n-1} kitevőjét nézve $k_{n-1}+k_n = \ell_{n-1}+\ell_n$. De már tudjuk, hogy $k_n = \ell_n$, és így $k_{n-1} = \ell_{n-1}$. A gondolatmenetet tovább folytatva végül az x_1 kitevőjének vizsgálatával $k_1 = \ell_1$ adódik. De akkor a H polinom $r y_1^{k_1} \dots y_n^{k_n}$ és $s y_1^{\ell_1} \dots y_n^{\ell_n}$ tagjai csak az együtthatójukban különböznek, ami lehetetlen. Ezzel az állítást beláttuk. □

A $H(y_1, \dots, y_n)$ tagjaiból kapott főtagok tehát mind különböznek, és így van közöttük olyan, amely lexikografikusan nagyobb a többinél. Legyen ez a fenti $r y_1^{k_1} \dots y_n^{k_n}$-ből keletkező, P-vel jelölt tag. Megmutatjuk, hogy rP nem eshet ki a $H(\sigma_1, \dots, \sigma_n)$ polinomból (sőt, ez lesz a főtagja). Valóban, $r\sigma_1^{k_1}\sigma_2^{k_2}\dots\sigma_n^{k_n}$ főtagja rP, ha pedig H-nak egy másik, $s y_1^{\ell_1} \dots y_n^{\ell_n}$ tagját vesszük, akkor az ebből keletkező $s\sigma_1^{\ell_1}\sigma_2^{\ell_2}\dots\sigma_n^{\ell_n}$ főtagja P választása miatt P-nél lexikografikusan kisebb (és így a többi tagja is kisebb). Ezzel a szimmetrikus polinomok alaptételének a bizonyítását befejeztük. □

Az alaptétel szerint az

$$s_k(x_1, \dots, x_n) = x_1^k + x_2^k + \dots + x_n^k \qquad (k \geq 0)$$

hatványösszegeket is ki lehet fejezni a szimmetrikus polinomokkal. Erre nem mutatunk explicit képlet, hanem csak egy olyan összefüggést, amiből az $s_1, s_2, s_3, \dots$ hatványösszegeket sorra ki lehet számítani.

2.7.8. Tétel [Newton–Girard-formulák]. *Az $s_k = s_k(x_1, \dots, x_n)$ és $\sigma_k = \sigma_k(x_1, \dots, x_n)$ polinomokra $k \geq n$ esetén*

$$s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} - + \dots + (-1)^{n-1}\sigma_{n-1}s_{k-n+1} + (-1)^n \sigma_n s_{k-n} = 0,$$

ha viszont $k \leq n$, akkor

$$s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} - + \dots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k k\sigma_k = 0.$$

Bizonyítás. Az elemi szimmetrikus polinomokat definiáló

$$(x - x_1)\dots(x - x_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - + \dots + (-1)^n \sigma_n$$

azonosságba helyettesítünk x helyére x_j-t. Ekkor a bal oldalon nullát kapunk, ezért

$$x_j^n - \sigma_1 x_j^{n-1} + \sigma_2 x_j^{n-2} - + \dots + (-1)^n \sigma_n = 0.$$

Szorozzuk ezt meg x_j^{k-n}-nel, és adjuk össze a kapott azonosságokat a $j = 1, 2, \ldots, n$ értékekre. Ekkor az első Newton–Girard-formulát kapjuk.

A második formulát n szerinti indukcióval bizonyítjuk be, $n = k$-tól elindulva. Ahhoz, hogy ezt megérthessük, ismét egy gyakorlatot érdemes végigszámolni.

2.7.9. Gyakorlat. Írjuk föl a Newton–Girard-formulát, amikor $n = 3$ és $k = 2$:

$$s_2(x_1, x_2, x_3) - \sigma_1(x_1, x_2, x_3)s_1(x_1, x_2, x_3) + 2\sigma_2(x_1, x_2, x_3) = 0\,.$$

Ha itt x_3 helyébe nullát helyettesítünk, a Newton–Girard-formulának melyik esetét kapjuk? Az a már bebizonyított esetek közé tartozik? Mit kapunk általában, ha az $s_i(x_1, \ldots, x_n)$, illetve $\sigma_i(x_1, \ldots, x_n)$ polinomokban x_n helyére nullát írunk?

Ha $n = k$, akkor a második Newton–Girard-formula ugyanaz, mint az első (tehát már beláttuk). Az indukció során feltesszük, hogy az állítás igaz $n-1$-re (ahol $n - 1 \geq k$), és belátjuk, hogy n-re is igaz.

2.7.10. Lemma. *Tegyük fel, hogy az $f \in R[x_1, \ldots, x_n]$ polinomban nincs olyan tag, amelyben mindegyik határozatlan előfordul. Ha f-re teljesül az, hogy bármelyik határozatlan helyébe nullát helyettesítve f-ből a nullapolinom lesz, akkor f maga is a nullapolinom.*

A lemma állítása nyilvánvaló, hiszen ha f-nek lenne egy nem nulla tagja, akkor a feltétel szerint ebben nem szerepel valamelyik x_j határozatlan, tehát ez a tag megmarad akkor is, amikor x_j helyébe írunk nullát. A lemmát alkalmazzuk a második Newton–Girard-formula bal oldalán álló polinomra. Mivel ez homogén k-adfokú, egyetlen tagban sem szerepelhet mindegyik változó (hiszen $k < n$). Helyettesítsünk x_n helyébe nullát. A 2.7.9. Gyakorlat szerint ekkor a Newton–Girard-formula eggyel kevesebb változós alakját kapjuk, amiről az indukciós feltevés miatt tudjuk, hogy igaz. Ugyanez történik akkor is, ha x_n helyett egy másik változó helyébe írunk nullát, hiszen polinomjaink szimmetrikusak. A lemma feltételei tehát teljesülnek, ami a második Newton–Girard-formulát bizonyítja. □

Ez a gondolatmenet megmagyarázza azt is, hogy miért a k szám szerepel a második Newton–Girard-formula végén: a $k = n$ esetben ez öröklődik az első formulából, utána pedig n növelésével nem változik meg.

Gyakorlatok, feladatok

2.7.11. Gyakorlat. Igaz-e, hogy szimmetrikus polinom minden homogén komponense is szimmetrikus?

2.7.12. Gyakorlat. Ha egy három határozatlanú szimmetrikus polinom lexikografikusan legnagyobb tagja $x_1^2x_2^2x_3$, akkor lehet-e tagja $x_1x_2^3x_3$? Szerepelhet-e hatodfokú tag? Hány tag lehet legfeljebb? Amikor elemi szimmetrikusakkal írjuk fel, mi az eljárás első lépése?

2.7.13. Gyakorlat. A 2.6.8. Gyakorlatban szereplő p polinomban helyettesítsük be mindegyik x_i helyére a négy határozatlanú σ_i elemi szimmetrikus polinomot, és adjuk meg az eredménynek egy olyan tagját, amelynek nem nulla az együtthatója.

2.7.14. Gyakorlat. Írjuk fel az elemi szimmetrikus polinomok polinomjaként az alábbi polinomot:

$$f(x_1, \ldots, x_n) = \sum_{1 \le i \ne j \le n} x_i^2 x_j \,.$$

2.7.15. Gyakorlat. Határozzuk meg az $x^n + x + 1$ polinom (komplex) gyökeinek köbösszegét, és a gyökök reciprokainak összegét ($n \ge 2$).

2.7.16. Gyakorlat. Legyenek a, b, c az $x^3 + 3x + 1$ polinom gyökei. Írjuk fel azt a két harmadfokú normált polinomot, melynek gyökei a^2, b^2, c^2, illetve $a + b, a + c, b + c$.

2.7.17. Feladat. Legyen $f \in R[x_1, \ldots, x_n]$ egy homogén k-adfokú szimmetrikus polinom, melyben minden határozatlan legfeljebb az m-edik hatványon szerepel. Mutassuk meg, hogy ha $\sigma_1^{k_1} \ldots \sigma_n^{k_n}$ nem nulla együtthatóval szerepel az f-nek az elemi szimmetrikus polinomokkal való felírásában, akkor

$$k_1 + k_2 + \ldots + k_n \le m \,,$$
$$k_1 + 2k_2 + \ldots + nk_n = k \,.$$

Hogyan segítenek ezek a képletek az f polinom elemi szimmetrikus polinomokkal való előállításában?

2.8. Összefoglaló

A komplex együtthatós polinomok olyan formális kifejezések, amelyek határozatlanokból („ismeretlenekből", „változókból"), és komplex számokból keletkeznek összeadás, kivonás és szorzás felhasználásával. Egy határozatlan esetén minden polinom a zárójelek kibontásával $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ alakra hozható. Két ilyen alakban felírt polinom akkor *egyenlő*, ha a megfelelő együtthatóik megegyeznek (2.1.1. Definíció). Definiáltuk polinomok összegét és szorzatát, amelyek a szokásos számolási szabályoknak tettek eleget (2.1.6. Állítás). Bevezettük a polinom *fokának* a fogalmát, és megmutattuk, hogy az összeg foka legfeljebb a tagok fokainak maximuma lehet (2.1.2. Állítás), szorzat foka pedig a tényezők fokainak összege, és ezért a polinomok szorzása nullosztómentes (2.1.5. Állítás). Ebből levezettük, hogy a komplex együtthatós polinomok között csak a nem nulla konstans polinomoknak létezik inverze (2.1.7. Állítás).

Felmerült az igény, hogy egy polinom együtthatói ne csak számok, hanem például mod m maradékok, vagy (a többhatározatlanú polinomok kényelmes bevezetéséhez) akár polinomok is lehessenek, szóval mindenféle, amivel a „szokásos szabályok szerint" számolni szoktunk. Ezért definiáltuk a kétváltozós művelet általános fogalmát, és több fontos tulajdonságát (asszociativitás, kommutativitás, neutrális elem, inverz, hatvány és többszörös: 2.2.1, 2.2.6, 2.2.9, 2.2.17. Definíciók). Ezekből a tulajdonságokból felépítettük a félcsoport, a *csoport*, a *gyűrű* és a *test* fogalmát (2.2.12, 2.2.13, 2.2.19, 2.2.21. Definíciók). Szó

volt részstruktúrákról (részcsoport, részgyűrű) is. Bevezettük a nullosztó fogalmát általános gyűrűben (2.2.25. Definíció), és megmutattuk, hogy minden ferdetest nullosztómentes (2.2.27. Tétel). Szokásos gyűrűnek neveztük a kommutatív egységelemes, nullosztómentes gyűrűket, mert ezek azok, ahol az összeadás, kivonás, szorzás a „szokásos" tulajdonságokkal rendelkezik. Röviden művelettartó leképezésekről is beszéltünk (2.2.32. Definíció).

A 2.3. Szakaszban kommutatív, egységelemes gyűrű felett értelmeztünk polinomokat, és megállapítottuk, hogy ha a gyűrű nullosztómentes is, akkor általában is igazak maradnak a komplex együtthatós polinomokra megismert alaptulajdonságok. A 1.6. Szakasz mintájára a polinomok precíz bevezetésének egy módjáról is szó esett.

Egy R gyűrű feletti polinom esetében definiáltuk, hogy hogyan lehet behelyettesíteni az R gyűrű elemeit, és bevezettük a *gyök* és a *gyöktényező* fogalmát (2.4.5. Definíció). A Horner-elrendezés lehetővé tette az elemek gyors behelyettesítését, és a gyöktényezők kiemelését (2.4.6. Állítás). Megmutattuk, hogy nullosztómentes gyűrű felett a gyöktényezők egyszerre is kiemelhetők, és ezért *egy polinomnak legfeljebb annyi gyöke lehet, mint a foka* (2.4.7. Tétel). Ebből adódott a polinomok azonossági tétele (2.4.10. Következmény), amely szerint ha két polinom több helyen megegyezik, mint a fokuk, akkor a két polinom (együtthatóról együtthatóra) egyenlő. Bevezettük a *polinomfüggvény* fogalmát (2.4.1. Definíció), és megmutattuk, hogy végtelen gyűrű felett ez meghatározza a polinomot, de véges gyűrű felett nem. Szót ejtettünk a Lagrange- és Newton-interpolációról is.

Ha egy polinomból az összes gyöktényezőt kiemelve csak egy konstans marad (ez szükségképpen a polinom főegyütthatója lesz), akkor azt mondjuk, hogy a polinomot *gyöktényezős alakra* bontottuk. Ez mindig bekövetkezik *algebrailag zárt* alaptest esetén: ezek azok a testek, amelyekben minden nem konstans polinomnak van gyöke (2.5.3. Definíció). A komplex számok teste is algebrailag zárt, ez az algebra alaptétele (2.5.4. Tétel), amelyet egyelőre nem tudtunk bebizonyítani. Bevezettük a gyök multiplicitásának, azaz a *többszörös gyöknek* a fogalmát (2.5.5. Definíció). A gyöktényezős alak beszorzásával kaptuk *a gyökök és együtthatók közötti összefüggéseket* (2.5.8. Tétel, 2.5.9. Következmény).

A *többhatározatlanú polinomokat* indukcióval olyan egyhatározatlanú polinomként definiáltuk, amelyek együtthatói eggyel kevesebb határozatlanú polinomok (2.6.1. Definíció). Nullosztómentes gyűrű felett ezek is nullosztómentes gyűrűt alkotnak, melynek invertálható elemei az invertálható konstans polinomok lesznek. Definiáltuk többhatározatlanú polinom fokát, és a homogén polinomokat. Bevezettük egy polinom tagjainak *lexikografikus rendezését* (2.6.4. Definíció). Megmutattuk, hogy nullosztómentes gyűrű felett két polinom szorzatának lexikografikusan legnagyobb tagja (azaz főtagja) a két tényező főtagjainak szorzata (2.6.7. Következmény).

Egy polinomot *szimmetrikusnak* nevezünk, ha bármely két határozatlan cseréjekor önmagába megy át. Ilyenek a gyökök és együtthatók összefüggéseiből kapott elemi szimmetrikus polinomok (2.7.2. Definíció). Beláttuk a *szimmetrikus polinomok alaptételét*, mely szerint minden szimmetrikus polinom egyértelműen felírható az elemi szimmetrikus polinomok polinomjaként (2.7.3. Tétel). Végül levezettük a hatványösszegeket az elemi szimmetrikus polinomokból rekurzívan előállító Newton–Girard-formulákat (2.7.8. Tétel).

3. A POLINOMOK SZÁMELMÉLETE

Ha van két nem egyenlő számunk, a kisebbet váltakozva mindig kivonjuk a nagyobból, és a maradék sosem osztja a megelőző számot, míg csak nem az egység a maradék, akkor az eredeti számok relatív prímek.

Euklidész: *Elemek*
(Mayer Gyula fordítása)

Könyvünk eddigi részében lényegében csak középiskolai ismeretekre támaszkodtunk. Ez most sem változik meg, de a polinomok számelméletének tárgyalásakor nagyon hasznos, ha az Olvasó már rendelkezik néhány alapvető ismerettel az egész számok számelméletéről. Ezek az ismeretek megszerezhetők például Freud Róbert és Gyarmati Edit [**11**] könyvének első fejezetéből. Konkrétan érdemes átvenni az oszthatóság alaptulajdonságait, az egység fogalmát, a legnagyobb közös osztó definícióját és meghatározását az euklideszi algoritmussal, a felbonthatatlan és prímszám közötti különbséget, és végül a számelmélet alaptételét, bizonyítással együtt.

3.1. Számelméleti alapfogalmak

Az egész számok között a számelmélet alaptétele teszi lehetővé, hogy egy szám szorzatra bontásait áttekintsük. Ugyanígy fontos tudnunk azt is, hogy polinomokat hogyan lehet szorzattá bontani. Például x^2+1 a komplex együtthatós polinomok között felbontható:

$$x^2+1=(x+i)(x-i)\,.$$

Vizsgáljuk meg, hogyan bontható föl a valós együtthatós polinomok között. Ha

$$x^2+1=f(x)g(x)\,,$$

akkor f és g fokainak összege kettő. Ha f elsőfokú lenne, azaz $f(x)=ax+b$, ahol $a\neq 0$, akkor a valós $-b/a$ szám gyöke lenne x^2+1-nek, ami lehetetlen. Ezért a fenti felbontásban f és g egyike konstans polinom kell, hogy legyen. Tehát csak olyasféle felbontás létezik, mint például

$$x^2+1=(2/3)\big((3/2)x^2+(3/2)\big)\,.$$

Ez a felbontás nem érdekes, hiszen nem mond semmi újat az x^2+1 polinomról. Példánk azt mutatja, hogy $\mathbb{C}[x]$ és $\mathbb{R}[x]$ „számelmélete" másmilyen, vagyis minden egyes R gyűrű esetében az $R[x]$ polinomgyűrűt külön kell megvizsgálni számelméleti szempontból.

3.1.1. Gyakorlat. Határozzuk meg az x^2-2 polinom összes lehetséges felbontásait a valós együtthatós, illetve a racionális együtthatós polinomok gyűrűjében.

3.1.2. Gyakorlat. Határozzuk meg az x^2+1 polinom felbontásait $\mathbb{Z}_2[x]$-ben és $\mathbb{Z}_3[x]$-ben.

Számelméleti kérdéseket nem csak az egész számok és a polinomok között érdemes vizsgálni. Például az úgynevezett *Gauss-egészek* az $a+bi$ alakú komplex számok, ahol a és b egészek (2.2.34. (2) Gyakorlat). Ezek között is érvényes a számelmélet alaptételének megfelelő állítás, és ennek felhasználásával érdekes egész számokra vonatkozó problémákat oldhatunk meg (például kideríthetjük, mely egész számok állnak elő két négyzetszám összegeként).

Ha ilyen sokféle gyűrűben kell számelmélettel foglalkozni, akkor az a gazdaságos hozzáállás, ha a fogalmakat egy általános gyűrűben definiáljuk, és általános tételeket bizonyítunk. Az alábbiakban mindig az egész számok $\mathbb{Z}$ gyűrűjét tartsuk szem előtt főpéldaként.

3.1.3. Definíció. Legyen R kommutatív gyűrű. Azt mondjuk, hogy az $r \in R$ elem *osztja* az $s \in R$ elemet, ha van olyan $t \in R$, hogy $rt = s$. Az oszthatóság jele $r \mid s$. Azt, hogy $r \mid s$, úgy is mondjuk, hogy r *osztója* s-nek, illetve hogy s *többszöröse* r-nek.

Az áthúzott oszthatóság jel azt jelenti: nem osztható. Néha fontos feltüntetnünk a jelölésben is, hogy melyik gyűrűben értjük az oszthatóságot, ilyenkor $r \mid s$ helyett $r \mid_R s$-et írunk. Például $2 \nmid_{\mathbb{Z}} 3$, de $2 \mid_{\mathbb{Q}} 3$ (hiszen $2 \cdot (3/2) = 3$). Hasonlóképpen $2 \nmid_{\mathbb{Z}[x]} 3x+1$, de $2 \mid_{\mathbb{Q}[x]} 3x+1$.

3.1.4. Gyakorlat. Legyen R kommutatív gyűrű, és $r, s, t \in R$. Igazoljuk az alábbiakat.

(1) Ha $r \mid s$ és $r \mid t$, akkor $r \mid s \pm t$.
(2) Ha $r \mid s$, akkor $r \mid st$ (sőt $rt \mid st$).
(3) Ha $r \mid s$ és $s \mid t$, akkor $r \mid t$ (az oszthatóság *tranzitív*).
(4) Ha R egységelemes, akkor $r \mid r$ minden $r \in R$ esetén (az oszthatóság *reflexív*).

3.1.5. Gyakorlat. Igazoljuk, hogy a nulla csak a nullának osztója (azaz $0 \mid s \implies s = 0$), de minden elemnek többszöröse (azaz $r \mid 0$ minden $r \in R$ esetén). Egy testben mikor teljesül az $r \mid s$ oszthatóság?

3.1.6. Gyakorlat. Igazoljuk, hogy ha n egész szám, akkor egy $p \in \mathbb{Z}[x]$ polinom akkor és csak akkor osztható ($\mathbb{Z}[x]$-ben) n-nel, ha minden együtthatója osztható ($\mathbb{Z}$-ben) n-nel. Általánosítsuk a feladatot $\mathbb{Z}$ helyett tetszőleges R kommutatív, egységelemes gyűrűre.

Az egész számok között megszoktuk, hogy egy szám és ellentettje oszthatóság szempontjából ugyanúgy viselkedik. A valós együtthatós polinomok között azonban egy f polinom kétszerese (fele, sőt $\sqrt{2}$-szöröse, π-szerese) is ugyanúgy viselkedik, mint f. Valóban $f \mid 2f$ és $2f \mid f$ is igaz (utóbbi azért, mert az $1/2$ is valós szám), és így f-nek és $2f$-nek ugyanazok az osztói is, és a többszörösei is.

3.1.7. Definíció. Legyen R kommutatív gyűrű. Azt mondjuk, hogy az $r, s \in R$ elemek egymás *asszociáltjai*, ha egymás osztói (vagyis $r \mid s$ és $s \mid r$ is teljesül). Az asszociáltság jele $r \sim s$.

Az „asszociált” szó helyett tehát ezt is mondhatjuk: „oszthatóság szempontjából egyformán viselkedő, megkülönböztethetetlen”. Így szóba jönne a következő definíció is: r és s asszociáltak, ha tetszőleges $t \in R$ esetén $r \mid t$ és $s \mid t$ ugyanakkor teljesül (vagyis ha a két elemnek ugyanazok a többszöröseik). Így az asszociáltság nem egységelemes gyűrűben is reflexív lenne (vö. 3.1.31. Gyakorlat). Az Olvasónak érdemes végiggondolnia, hogy egységelemes gyűrűben, ahol tehát minden elem osztója önmagának, az oszthatóság tranzitivitása miatt ez ugyanaz az asszociáltság-fogalom, mint ami a fenti 3.1.7. Definícióban szerepel.

3.1.8. Gyakorlat. Mutassuk meg, hogy ha R egységelemes, kommutatív gyűrű, akkor

(1) Minden $r \in R$ esetén $r \sim r$ (az asszociáltság *reflexív*).
(2) Ha $r \sim s$, akkor $s \sim r$ (az asszociáltság *szimmetrikus*).
(3) Ha $r \sim s$ és $s \sim t$, akkor $r \sim t$ (az asszociáltság *tranzitív*).

Tegyük fel, hogy r és s asszociáltak. Ekkor $re = s$ és $se' = r$ teljesül alkalmas $e, e' \in R$ elemekre. Innen $ree' = se' = r$. Ha R egységelemes és nullosztómentes, akkor $r \neq 0$ esetén r-rel egyszerűsíthetünk, és $ee' = 1$ adódik. Ezt úgy is fogalmazhatjuk, hogy $e \mid 1$.

3.1.9. Definíció. Legyen R kommutatív, egységelemes gyűrű. Azt mondjuk, hogy az $e \in R$ elem *egység*, ha az egységelemnek (vagyis az 1 elemnek) osztója.

Ne tévesszük össze tehát az egység és az egységelem fogalmát! Az egységelem az az $1 \in R$ elem, amelyre $1r = r1 = r$ teljesül minden $r \in R$ esetén. Az egységek ennek az osztói, vagyis az R invertálható elemei (lásd a 2.2.9. Definíciót). Az egységek tehát az $R^\times$ halmaznak, azaz R multiplikatív csoportjának az elemei. (Az „egység” és „invertálható” szavak kommutatív, egységelemes gyűrűben szinonimák, de számelméleti ízű vizsgálatokban inkább az egység szó használatos.) Például $\mathbb{Z}$ egységei 1 és -1.

Az R egy eleme tehát pontosan akkor egység, ha R minden elemének osztója. Azt gondolhatnánk, hogy érdemesebb az egységet így definiálni, mert akkor a fogalom nem egységelemes gyűrűben is értelmessé válna. Azonban a 3.1.31. Gyakorlat szerint nem egységelemes, de nullosztómentes gyűrűben nem lehetnek egységek ebben a kiterjesztett értelemben sem.

3.1.10. Állítás. *Tegyük fel, hogy R kommutatív, egységelemes, nullosztómentes (azaz szokásos) gyűrű. Ekkor tetszőleges $r \in R$ asszociáltjai pontosan az egységszeresei.*

Bizonyítás. A nulla asszociáltja nyilván csak a nulla lehet. Ha $r \neq 0$ és $s \in R$ asszociáltja r-nek, akkor az imént beláttuk, hogy s az r-nek egységszerese. Megfordítva, ha e egység, azaz $ee' = 1$ alkalmas e'-re, akkor r és re asszociáltak, hiszen $(re)e' = r$ miatt $re \mid r$. □

3.1.11. Gyakorlat. Igazoljuk, hogy $\mathbb{Z}[x]$ egységei az 1 és -1 konstans polinomok, $\mathbb{R}[x]$ egységei pedig a nem nulla konstans polinomok. Általában mutassuk meg, hogy ha R szokásos gyűrű, akkor $R[x]$ egységei pontosan R egységei lesznek (mint konstans polinomok). Speciálisan tehát test fölötti polinomgyűrű egységei a nem nulla konstans polinomok.

A következő célunk a számelmélet alaptételének megfelelő állítás megfogalmazása tetszőleges gyűrűben. Az egyszerűség és a jobb érthetőség kedvéért *mostantól a számelméleti vizsgálatok során feltesszük, hogy minden gyűrű kommutatív, nullosztómentes és egységelemes, azaz szokásos gyűrű.* (Néhány feladatban azért meg fogjuk vizsgálni, hogy ezek a feltevések mindig szükségesek-e.)

A számelmélet alaptétele durván fogalmazva azt mondja ki, hogy minden számot egyértelműen föl lehet bontani olyan számok szorzatára, amik tovább már nem bonthatók. A „tovább már nem bontható" szám fogalmát azonban pontosan definiálnunk kell, hiszen például a 7, amit az egész számok között „tovább már nem bonthatónak" gondolunk, igenis felbontható:

$$7 = 1 \cdot 7 = 7 \cdot 1 = (-1) \cdot (-7) = (-7) \cdot (-1) \,.$$

Azonban másféle felbontás nincs, ezek pedig ugyanúgy érdektelenek, mint ahogy a fenti példában érdektelen volt, amikor az $x^2 + 1$ polinomból kiemeltük a $2/3$-ot. Ezekben az „érdektelen" felbontásokban az a közös, hogy egy egységet emelünk ki, és ami megmarad, az az eredeti elemnek egy asszociáltja. Az ilyen felbontást triviálisnak nevezzük.

3.1.12. Definíció. Legyen R szokásos gyűrű, és $0 \neq r = bc$, ahol $r, b, c \in R$. Azt mondjuk, hogy az r elemnek ez a felbontása *triviális*, ha b és c egyike r-nek asszociáltja. Ami ezzel ekvivalens: b és c közül a másik egység.

Egy elem tehát akkor lesz „tovább már nem bontható", ha nincs nemtriviális felbontása (azaz ha van is felbontása, az csak triviális lehet). Ilyen tulajdonságú elem az 1 és a -1 is az egész számok között, de ezeket mégsem tekintjük építőkőnek akkor, ha egy általános számot akarunk minél jobban szétbontani. Ezért a most következő definícióban az egységeket is kizárjuk.

3.1.13. Definíció. Legyen R szokásos gyűrű. A $p \in R$ elemet *felbonthatatlannak* vagy *irreducibilisnek* nevezzük, ha nem nulla, nem egység, és p-nek nincs nemtriviális felbontása.

A fenti példák szerint a 7 szám felbonthatatlan $\mathbb{Z}$-ben, az $x^2 + 1$ polinom pedig felbonthatatlan, más szóval irreducibilis $\mathbb{R}[x]$-ben, de nem irreducibilis $\mathbb{C}[x]$-ben.

Az „irreducibilis" és „felbonthatatlan" szavak tehát ugyanazt jelentik. Ha a vizsgált gyűrű elemei számok (például egészek vagy Gauss-egészek), akkor szokásosabb a „felbonthatatlan" szót használni. Ha viszont egy $R[x]$ polinomgyűrűben dolgozunk, akkor inkább az „irreducibilis polinom" kifejezést használjuk. Ahelyett, hogy „f irreducibilis $R[x]$-ben" sokszor azt fogjuk mondani, hogy „f irreducibilis R *fölött*". Ha egy nem nulla és nem egység polinom nem irreducibilis, akkor *reducibilisnek* is hívjuk majd.

3.1.14. Definíció. Azt mondjuk, hogy az R gyűrűben érvényes a számelmélet alaptétele (azaz hogy R *alaptételes*), ha R minden nem nulla és nem egység eleme sorrendtől és asszociáltságtól eltekintve egyértelműen felírható R irreducibilis elemeinek szorzataként.

Külön is felhívjuk a figyelmet arra, hogy csak a nem nulla és nem egység elemeket akarjuk felbontani irreducibilisek szorzatára. Szokásos gyűrűben mást nem is lehet: a nulla

minden felbontásában lesz nulla tényező, ami nem irreducibilis, egy egység felbontásában pedig minden tényező egység lesz.

Most precízen megfogalmazzuk, mit is jelent a felbontás egyértelműsége. A 15 számot az egész számok között négyféleképpen bonthatjuk felbonthatatlanok szorzatára:

$$15 = 3 \cdot 5 = 5 \cdot 3 = (-3) \cdot (-5) = (-5) \cdot (-3) \,.$$

Az első felbontásból az utolsót úgy kapjuk meg, hogy megcseréljük a sorrendet, majd mindkét tényezőnek vesszük egy-egy asszociáltját. Ezt általánosítva a felbontás egyértelműsége a következőt jelenti. Bárhogy is vesszük az r elemnek két

$$r = p_1 \dots p_k = q_1 \dots q_\ell$$

felbontását irreducibilisek szorzatára, a tényezők száma ugyanannyi (tehát $k = \ell$), és a két felbontás tényezői egymással párba állíthatók úgy, hogy a párok tagjai egymás asszociáltjai legyenek. Ezt a párba állítást még formálisabban úgy fogalmazhatjuk, hogy létezik olyan g kölcsönösen egyértelmű megfeleltetése az $\{1, 2, \dots, k\}$ halmaznak önmagába úgy, hogy p_i és párja, azaz $q_{g(i)}$ asszociáltak.

Az egész számok alaptétel szerinti felbontásában össze szokás vonni az „egyforma" felbonthatatlanokat, ekkor kapjuk egy szám *kanonikus alakját*. A polinomok gyöktényezős alakjának vizsgálatakor is beszéltünk kanonikus alakról hasonló értelemben. Mi is lesz a -4 szám kanonikus alakja?

$$-4 = 2 \cdot (-2) = (-2) \cdot 2 = -2^2 = -(-2)^2 \,,$$

vagyis az asszociált felbonthatatlanokat csak úgy tudjuk összevonni, ha egy -1-es tényező is megmarad! Ezért a kanonikus alakban meg kell engednünk egy egység tényezőt is.

3.1.15. Definíció. Az $r \neq 0$ elem *kanonikus alakja*

$$r = e p_1^{\alpha_1} \dots p_m^{\alpha_m} \,,$$

ahol e egység, a p_i páronként nem asszociált felbonthatatlan elemek, az α_i pedig nemnegatív egész számok.

Kanonikus alakja az egységeknek is van, például a fenti képletben vehetjük az $m = 0$ értéket. Az elemi számelméletből tudjuk, hogy az α_i kitevőkről néha érdemes feltenni, hogy mindegyik pozitív (ez a helyzet például, ha az Euler-féle φ függvény képletét akarjuk alkalmazni), néha viszont célszerű megengedni a nulla kitevőket is (ha több szám kanonikus alakjában ugyanazokat a felbonthatatlan elemeket akarjuk szerepeltetni, például a legnagyobb közös osztó meghatározásakor).

3.1.16. Gyakorlat. A közönséges pozitív egész számok kanonikus alakjának vizsgálatakor a számelméletben miért nem szokás az egységtényezőről beszélni? Mely negatív egész számok felírásakor lehet elkerülni az egységtényezőt?

3.1.17. Gyakorlat. Fogalmazzuk meg pontosan, hogy milyen értelemben egyértelmű a kanonikus alak, és bizonyítsuk is be az állítást.

Ebben a fejezetben még nem foglalkozunk azzal a kérdéssel, hogy általános gyűrűben hogyan (és milyen feltételek mellett) lehet bebizonyítani a számelmélet alaptételét. Annyit azonban megteszünk, hogy röviden átismételjük azt az utat, ahogy az egész számok gyűrűjében az alaptétel bebizonyítható, mert ez elvezet bennünket néhány fontos fogalomhoz.

Az egész számok között megmutattuk, hogy elvégezhető a maradékos osztás, és ennek felhasználásával az euklideszi algoritmus, amellyel előállítható tetszőleges két a és b szám (a, b) *legnagyobb közös osztója*. Az euklideszi algoritmusból azt is láttuk, hogy (a, b) felírható $ax + by$ alakban, ahol x és y alkalmas egész számok. Ebből levezettük, hogy az egész számok körében minden felbonthatatlan p elem *prímtulajdonságú*, azaz ha p osztója egy szorzatnak, akkor osztója valamelyik tényezőnek is. A prímtulajdonságból könnyen következik a számelmélet alaptételének egyértelműségi állítása. A felbontás létezésének bizonyításához azt használtuk fel, hogy ha egy számot nemtriviálisan szorzatra bontunk, akkor a tényezők (abszolút értékben) kisebbek, mint az eredeti szám (abszolút értéke).

A most szóba került fogalmak közül elsőként a legnagyobb közös osztót vizsgáljuk meg. Általános gyűrűben nem beszélhetünk arról, hogy az egyik gyűrűelem „nagyobb" lenne a másiknál. Szerencsére az egész számok esetében megtanultuk, hogy két szám legnagyobb közös osztója nemcsak nagyságra a legnagyobb a közös osztók között, hanem oszthatóság tekintetében is: a legnagyobb közös osztó ugyanis minden közös osztónak többszöröse. Ez a definíció már tetszőleges gyűrűre átvihető. Hogy ezt a különbséget hangsúlyozzuk, legnagyobb közös osztó helyett kitüntetett közös osztóról fogunk beszélni.

3.1.18. Definíció. Legyen R szokásos gyűrű és $r, s \in R$. Azt mondjuk, hogy egy $t \in R$ elem *kitüntetett közös osztója* r-nek és s-nek, ha t közös osztó (azaz $t \mid r$ és $t \mid s$), és t minden közös osztónak többszöröse (azaz ha $t' \mid r$ és $t' \mid s$, akkor $t' \mid t$). Az r és s *relatív prímek*, ha a kitüntetett közös osztójuk egység.

3.1.19. Gyakorlat. Mutassuk meg, hogy ha a kitüntetett közös osztó létezik, akkor asszociáltság erejéig egyértelműen meghatározott.

Ez az állítás lehetővé teszi, hogy jelölést vezessünk be a kitüntetett közös osztóra, ami ugyanúgy (r, s) lesz, ahogy egész számok esetében. Fontos észben tartanunk azonban, hogy ez az elem csak asszociáltság erejéig meghatározott. Az egész számok között ezt a problémát úgy oldottuk meg, hogy a legnagyobb közös osztónak mindig a nemnegatív értékét vettük. Hasonlóképpen test fölötti polinomok között néha szokás a kitüntetett közös osztónak azt az értékét venni, amely normált polinom. Általános gyűrűben ilyen egyszerűsítés nem lehetséges.

3.1.20. Gyakorlat. Legyen R alaptételes gyűrű.

(1) Mutassuk meg, hogy R bármely két elemének létezik „közös kanonikus alakja", amelyben ugyanazok a felbonthatatlanok szerepelnek, csak esetleg más (és esetleg nulla) kitevővel.
(2) Hogyan jellemezhetjük r és s közös kanonikus alakja segítségével azt, hogy r osztója s-nek? Mennyi az osztók száma?

(3) Mutassuk meg, hogy R bármely két elemének van kitüntetett közös osztója, és adjunk is rá képletet a két szám közös kanonikus alakja segítségével.
(4) Általánosítsuk a *kitüntetett közös többszörös* fogalmát is szokásos gyűrűre. Mutassuk meg, hogy ez asszociáltság erejéig egyértelmű, hogy alaptételes gyűrűben mindig létezik, és adjunk rá képletet a kanonikus alak segítségével.
(5) Hogyan kell módosítani a kapott képleteket, ha kettőnél több szám kitüntetett közös osztóját, illetve kitüntetett közös többszörösét akarjuk kiszámítani?

Az r és s elemek kitüntetett közös többszörösét $[r, s]$ fogja jelölni, ez az elem is csak asszociáltság erejéig meghatározott.

3.1.21. Definíció. Legyen R szokásos gyűrű és $p \in R$. Azt mondjuk, hogy p *prímtulajdonságú* (vagy egyszerűen csak prím), ha nem nulla, nem egység, és tetszőleges $r, s \in R$ esetén ha $p \mid rs$, akkor $p \mid r$ vagy $p \mid s$.

3.1.22. Gyakorlat. Mutassuk meg, hogy minden prímtulajdonságú elem felbonthatatlan, és ha R alaptételes, akkor minden felbonthatatlan eleme prím.

Most következő célunk az, hogy a legfontosabb polinomgyűrűkben bebizonyítsuk a számelmélet alaptételét, és hogy minél többet megtudjunk arról, mik az irreducibilis polinomok ezekben a gyűrűkben.

Gyakorlatok, feladatok

3.1.23. Gyakorlat. Igaz-e a $2x \mid 3x^2$ oszthatóság rendre a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ fölötti polinomok gyűrűjében?

3.1.24. Gyakorlat. Legyen R szokásos gyűrű, és $r \mid s$ két eleme. Mi lesz a kitüntetett közös osztójuk? Mi lesz r és 0 kitüntetett közös osztója?

3.1.25. Gyakorlat. Legyen R szokásos gyűrű. A nullának lehet benne nemtriviális felbontása? Teljesül-e rá, hogy csak akkor osztója egy szorzatnak, ha valamelyik tényezőjének osztója? Mi a helyzet az egységekkel?

3.1.26. Gyakorlat. Igazoljuk, hogy ha R alaptételes gyűrű, akkor tetszőleges $r, s, t \in R$ esetén (rt, st) és $(r, s)t$ asszociáltak (ez *a kitüntetett közös osztó kiemelési tulajdonsága*). Vezessük le ezt a tulajdonságot akkor is, ha R alaptételessége helyett azt tudjuk, hogy tetszőleges r és s esetén (r, s) felírható $rx + sy$ alakban alkalmas $x, y \in R$ elemekre.

3.1.27. Gyakorlat. Legyen R szokásos gyűrű, amelyben bármely két elemnek van kitüntetett közös osztója, és erre érvényes a kitüntetett közös osztó kiemelési tulajdonsága.

(1) Mutassuk meg, hogy ha egy elem osztója egy szorzatnak, de relatív prím az egyik tényezőhöz, akkor osztója a másik tényezőnek. Képletben: ha $r \mid st$ és $(r, s) \sim 1$, akkor $r \mid t$.
(2) Igazoljuk, hogy R minden irreducibilis eleme prím.

3.1.28. Feladat. Legyen R szokásos gyűrű, amelyben mindegyik irreducibilis elem prím. Mutassuk meg, hogy R-ben érvényes a számelmélet alaptételének egyértelműségi állítása.

3.1.29. Gyakorlat. Igazoljuk, hogy ha R alaptételes gyűrű, akkor tetszőleges $r, s \in R$ esetén $(r, s)[r, s]$ és rs asszociáltak.

3.1.30. Gyakorlat. Legyen R az $a + bi$ alakú számok gyűrűje a szokásos összeadásra és szorzásra, ahol $a, b \in \mathbb{Z}$ (ezek a Gauss-egészek, lásd 2.2.34. (2) Gyakorlat). Határozzuk meg 2-nek és $1 + 3i$-nek az összes kitüntetett közös osztóját R-ben.

3.1.31. Feladat. Mutassuk meg, hogy a páros számok gyűrűjében nincsen olyan elem, amely minden elemnek osztója (ebben a gyűrűben), és nincsen prímtulajdonságú elem sem. Mik lesznek az asszociált elempárok? Igazoljuk, hogy minden nem nulla elem felírható irreducibilisek szorzataként, de ez a felbontás nem mindig egyértelmű. Általánosítsuk a kapott észrevételeket nullosztómentes, kommutatív, de nem egységelemes gyűrűre.

3.1.32. Gyakorlat. Mutassuk meg, hogy a $\mathbb{Z}[x]$ gyűrűben a 2 és x elemeknek az 1 kitüntetett közös osztója, de ez nem írható föl $2p(x) + xq(x)$ alakban, ahol $p, q \in \mathbb{Z}[x]$.

3.1.33. Feladat. Legyen R az $a + bi\sqrt{5}$ alakú számok részgyűrűje $\mathbb{C}$-ben, ahol $a, b \in \mathbb{Z}$.

(1) Mutassuk meg, hogy a 3 ebben a gyűrűben felbonthatatlan, de nem prím.
(2) Létezik-e R-ben a 3-nak és a $2 + i\sqrt{5}$-nek kitüntetett közös osztója?
(3) Igaz-e R-ben a kitüntetett közös osztó kiemelési tulajdonsága (3.1.26. Gyakorlat)?

3.1.34. Feladat. Tekintsük az $\mathbb{R}[x, y]$ polinomgyűrűnek azokat az elemeit, amelyekben minden nem konstans tag legalább harmadfokú, de nem szerepel x^2y^2-es tag. Mutassuk meg, hogy ezek egy R részgyűrűt alkotnak, amely szokásos gyűrű, de nincs bármely két elemének kitüntetett közös osztója.

3.1.35. Gyakorlat. Legyen R azoknak a valós együtthatós „polinomoknak" a halmaza, amelyekben az x határozatlan kitevői nemcsak nemnegatív egész számok, hanem tetszőleges nemnegatív valós számok lehetnek. Mutassuk meg, hogy R elemei között az összeadás és szorzás a szokásos polinomokhoz hasonlóan elvégezhető, és így R szokásos gyűrű lesz, amelyben azonban az x nem bontható fel felbonthatatlanok szorzatára.

3.2. A maradékos osztás

Az előző szakaszban láttuk, hogy egész számok között a számelmélet alaptételét végső soron a maradékos osztás létezésének köszönhetjük. Test fölötti polinomgyűrűben szintén elvégezhető a maradékos osztás, és ezért itt is igaz lesz az alaptétel.

3.2.1. Tétel. *Legyen R szokásos gyűrű. Ekkor $R[x]$-ben minden olyan $g \in R[x]$ polinommal lehet maradékosan osztani, amelynek főegyütthatója invertálható. Ez azt jelenti, hogy tetszőleges $f \in R[x]$ polinomhoz léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = gq + r$, és vagy $r = 0$, vagy r foka kisebb g fokánál. A q és r polinomok egyértelműen meghatározottak.*

A most felírt maradékos osztásban a q polinomot *hányadosnak*, az r polinomot pedig *maradéknak* nevezzük. Az $r = 0$ esetet azért kellett külön vennünk, mert a nullapolinomnak nincsen foka.

Bizonyítás. Mint majd konkrét példákon látni fogjuk, polinomok között az osztást ahhoz hasonlóan kell elvégezni, ahogyan egész számok között (kézzel) maradékosan osztunk, még a jelölés is hasonló lesz. A most következő bizonyítás is ezt az eljárást követi: f foka szerinti indukcióval bizonyítjuk q és r létezését. Az $f = 0$ esetet ekkor külön meg kell nézni, de az rendben van, hiszen a $0 = g \cdot 0 + 0$ megfelelő lesz. Ha f foka kisebb g fokánál, akkor az $f = g \cdot 0 + f$ előállítás lesz megfelelő, és így az indukció kezdőlépését is megtettük.

Tegyük most fel, hogy f egy n-edfokú polinom, és hogy az n-nél kisebb fokú polinomokra már igaz az állítás. Jelölje f főtagját ax^n és g főtagját bx^m (ahol tehát b invertálható eleme R-nek). Mivel az m-nél kisebb fokú f polinomokra már beláttuk az állítást, feltehetjük, hogy $n \geq m$. Legyen $f_0 = f - (a/b)x^{n-m}g$. Ez értelmes, hiszen b-vel lehet osztani. A kivonásnál f főtagja kiesik, és így f_0 foka kisebb, mint n (vagy f_0 a nullapolinom). Az indukciós feltevés miatt f_0 maradékosan eloszthető g-vel: $f_0 = gq_0 + r$, ahol $r = 0$, vagy r foka kisebb g fokánál. De innen

$$f = f_0 + (a/b)x^{n-m}g = g\big(q_0 + (a/b)x^{n-m}\big) + r\,,$$

tehát f is eloszthető maradékosan g-vel.

Az egyértelműség bizonyításához tegyük fel, hogy f-et kétféleképpen is elosztottuk maradékosan g-vel:

$$f = gq_1 + r_1 = gq_2 + r_2\,,$$

ahol mind r_1, mind r_2 vagy nulla, vagy g-nél kisebb fokú polinom. Átrendezéssel

$$g(q_1 - q_2) = r_2 - r_1\,.$$

A jobb oldalon álló $r_2 - r_1$ polinom vagy nulla, vagy g-nél kisebb fokú. Ha $q_1 - q_2 \neq 0$, akkor viszont a bal oldalon álló polinom foka legalább annyi, mint g foka, hiszen szorzásnál a fokok összeadódnak, ami ellentmondás. Ezért $q_1 - q_2 = 0$, de akkor nyilván $r_2 - r_1 = 0$, és így a két maradékos osztásban a hányados és a maradék is ugyanaz. □

A tételből látjuk, hogy speciálisan test fölött minden nem nulla polinommal lehet maradékosan osztani. A bizonyításban szereplő $(a/b)x^{n-m}$ tag f és g főtagjainak hányadosa, ez lesz a keresett q hányados főtagja. Az osztás elvégzésekor ezzel kell beszorozni g-t, az eredményt f-ből kivonni, és a kapott polinommal ismételni az eljárást. Akkor állunk meg, amikor f foka már g foka alá csökken. Példaként osszuk el a $2x^3+2x^2+3x+2$ polinomot x^2+1-gyel:

$$\begin{array}{r} 2x^3+\ 2x^2+3x+2\ :\ x^2+1=\boxed{2x+2} \\ \underline{-(2x^3+\quad 0\ \ +2x)} \\ 2x^2+\ x\ +2 \\ \underline{-\,(2x^2+\ 0\ \ +2)} \\ \boxed{x} \end{array}$$

Láthatjuk, hogy a hányados $2x+2$, a maradék pedig x.

Az osztásnál kapott hányados és maradék együtthatói természetesen az R gyűrű elemei. Ennek az észrevételnek, és a tétel egyértelműségi állításának van egy fontos következménye. Képzeljük el, hogy f és g racionális együtthatós polinomok, és g osztója f-nek a $\mathbb{C}[x]$ gyűrűben, vagyis létezik egy olyan $q \in \mathbb{C}[x]$ polinom, melyre $gq = f$. Azt állítjuk, hogy q minden együtthatója racionális szám, és így g már $\mathbb{Q}[x]$-ben is osztója f-nek.

Ez következik abból, ahogy az osztást végezzük, hiszen az $f : g$ kiszámításakor csak a négy alapműveletre van szükség, és megkapjuk q együtthatóit. Elegánsabb azonban az állítást a következőképpen bizonyítani. Osszuk el maradékosan f-et g-vel $\mathbb{Q}[x]$-ben:

$$f = gq_1 + r_1\,,$$

ahol $q_1, r_1 \in \mathbb{Q}[x]$ (és $r_1 = 0$ vagy $\mathrm{gr}(r_1) < \mathrm{gr}(g)$). Vessük össze ezt az

$$f = gq + 0$$

összefüggéssel. Ez két maradékos osztás $\mathbb{C}[x]$-ben. Az egyértelműség miatt tehát $q = q_1$, vagyis q tényleg racionális együtthatós.

Ugyanez a gondolatmenet működik abban az esetben is, ha $\mathbb{Q}$ vagy $\mathbb{C}$ helyett a valós számok teste szerepel. Az alábbi állítást ezért általánosan mondjuk ki: a $\mathbb{C}$ szerepét T, a $\mathbb{Q}$ szerepét S fogja játszani.

3.2.2. Állítás. *Legyen T test, és S részteste T-nek. Ha $f, g \in S[x]$, és g osztója f-nek $T[x]$-ben, akkor osztója $S[x]$-ben is.*

A kitüntetett közös osztó meghatározására szolgáló euklideszi algoritmus a maradékos osztáson alapszik, ezért tetszőleges test fölötti polinomgyűrűben is elvégezhető. Ezt az eljárást röviden átismételjük. Legyen T test, és $f, g \in T[x]$ két polinom. Készítsük el az alábbi maradékos osztásokat:

$$\begin{aligned} f &= gq_1 &&+ r_1 \\ g &= r_1q_2 &&+ r_2 \\ r_1 &= r_2q_3 &&+ r_3 \\ &\dots \\ r_{n-2} &= r_{n-1}q_n &&+ r_n \\ r_{n-1} &= r_nq_{n+1} &&+ 0\,. \end{aligned}$$

Az itt szereplő $r_1, r_2, \dots$ maradékok foka egyre csökken, és mivel ezek a fokok nemnegatív egész számok, előbb-utóbb a maradék nulla lesz. A jelölést úgy választottuk, hogy r_n

legyen az utolsó nem nulla maradék. Az egész számokra tanult bizonyítás szó szerint átvihető: r_n az f és g kitüntetett közös osztója lesz.

3.2.3. Gyakorlat. Mutassuk meg, hogy a fenti eljárásban kapott legutolsó nem nulla maradék, vagyis az r_n polinom az f és g polinomok kitüntetett közös osztója, és ez előállítható $fp + gq$ alakban, ahol p és q alkalmas $T[x]$-beli polinomok.

3.2.4. Feladat. Az euklideszi algoritmus fenti vázlatában több pontatlanság is van. Keressük meg, és javítsuk ki ezeket.

Mint tudjuk, a kitüntetett közös osztó csak asszociáltság erejéig egyértelmű. Azt is láttuk (a 3.1.11. Gyakorlatban), hogy egy test fölött két polinom akkor és csak akkor asszociált, ha egymás konstansszorosai. Néha meg szokás állapodni abban, hogy az (f, g) jelölés a kitüntetett közös osztók közül az egyetlen normált polinomot jelöli.

3.2.5. Gyakorlat. Mutassuk meg, hogy két racionális együtthatós polinom $\mathbb{Q}[x]$-beli kitüntetett közös osztója $\mathbb{C}[x]$-ben is kitüntetett közös osztó. Általánosítsuk az állítást.

Most még egy bizonyítást adunk arra, hogy test fölötti polinomgyűrűben létezik a kitüntetett közös osztó. Ez a bizonyítás egyszerűbb, mint a fenti, és bevezeti azt a módszert, amellyel később a számelméleti kérdéseket gyűrűkben vizsgálni fogjuk. Hátránya, hogy segítségével nem lehet kiszámítani a kitüntetett közös osztót, erre a célra továbbra is az euklideszi algoritmust használjuk majd.

3.2.6. Tétel. *Legyen T test. Ekkor tetszőleges két T fölötti f és g polinomnak létezik az (f, g) kitüntetett közös osztója. Ha h is egy T fölötti polinom, akkor h pontosan akkor írható föl $fp + gq$ alakban alkalmas $p, q \in T[x]$ polinomokkal, ha $(f, g) \mid h$.*

Bizonyítás. Jelölje I az $fp + gq$ alakban felírható polinomok halmazát, ahol $p, q \in T[x]$. Ennek a halmaznak több érdekes tulajdonsága is van. Például zárt az összeadásra. Valóban, ha $h_1, h_2 \in I$, akkor

$$h_1 = fp_1 + gq_1 \quad \text{és} \quad h_2 = fp_2 + gq_2$$

alkalmas $p_1, p_2, q_1, q_2 \in T[x]$ polinomokra. De akkor

$$h_1 + h_2 = f(p_1 + p_2) + g(q_1 + q_2)\,,$$

ami azt mutatja, hogy $h_1 + h_2 \in I$.

Az I másik fontos tulajdonsága, hogy minden elemének az összes többszörösét (polinomszorosát) is tartalmazza (ez tehát több, mintha csak azt mondanánk, hogy részgyűrű). Valóban, ha $h \in I$, azaz $h = fp + gq$, és $r \in T[x]$ egy tetszőleges polinom, akkor

$$hr = f(pr) + g(qr) \in I\,.$$

Válasszunk ki most I-ből egy olyan h_0 polinomot, aminek a foka a lehető legkisebb. Megmutatjuk, hogy az I elemei pont a h_0 többszörösei. Azt az előbb láttuk, hogy h_0

többszörösei benne vannak I-ben. Megfordítva, ha $h \in I$ tetszőleges, akkor osszuk el h-t maradékosan h_0-lal:

$$h = h_0 q + r \,,$$

ahol $r = 0$, vagy r foka kisebb, mint h_0 foka. Az első esetben készen is vagyunk, hiszen azt akarjuk belátni, hogy h többszöröse h_0-nak. Ha $r \neq 0$, akkor

$$r = h - h_0 q \in I \,,$$

hiszen I-ben benne van $-h_0 q$ is (hiszen ez h_0 többszöröse), és benne van h is, tehát benne van a kettő összege is. De ez lehetetlen, mert r foka kisebb, mint h_0 foka, és h_0 foka a lehető legkisebb volt az I-beli elemek fokai között. Tehát beláttuk, hogy I tényleg a h_0 többszöröseiből áll.

Most azt mutatjuk meg, hogy h_0 kitüntetett közös osztója f-nek és g-nek. Nyilván $f \in I$ (mert $f = f \cdot 1 + g \cdot 0$), és hasonlóképpen $g \in I$. Így h_0 osztója f-nek és g-nek. Tegyük most fel, hogy $k \in T[x]$ közös osztója f-nek és g-nek, be kell látni, hogy $k \mid h_0$. De ez nyilvánvaló, hiszen $h_0 \in I$, azaz h_0 felírható $fp + gq$ alakban. Tehát h_0 tényleg f és g kitüntetett közös osztója.

Végül vegyük észre, hogy menet közben beláttuk a tétel utolsó állítását is. Az I halmaz ugyanis azokból a h polinomokból áll, amik felírhatók $fp + gq$ alakban, és éppen azt mutattuk meg, hogy ezek a polinomok $h_0 = (f, g)$ többszörösei. □

3.2.7. Feladat. Az előző bizonyításban van egy apró pontatlanság. Keressük ezt meg, és tegyük teljessé a gondolatmenetet.

Az eddig elmondottakból már könnyen következik az, hogy minden test fölötti polinomgyűrű alaptételes, vagyis minden polinom egyértelműen bontható irreducibilisek szorzatára. Először tisztázzuk, hogy test fölött mit is jelent az irreducibilitás.

3.2.8. Állítás. *Legyen T test. Egy $f \in T[x]$ polinom akkor és csak akkor irreducibilis T fölött, ha nem konstans, és nem bontható fel két alacsonyabb fokú T-beli együtthatós polinom szorzatára.*

Bizonyítás. Test fölött az egységek a nem nulla konstans polinomok (3.1.11. Gyakorlat). Tehát egy polinom triviális felbontásai azok, amikor az egyik tényező konstans, és így a nemtriviális felbontások azok, amikor egyik tényező sem konstans. Ez ugyanazt jelenti, mintha azt mondanánk, hogy mindkét tényező az eredeti polinomnál alacsonyabb fokú kell, hogy legyen, hiszen a tényezők fokainak összege az eredeti polinom foka. □

Vigyázzunk, a most adott jellemzés általános gyűrű fölött már nem működik. Ezzel a jelenséggel a 3.4. Szakaszban fogunk érdemben foglalkozni, most csak egy gyakorlat erejéig mutatjuk be.

3.2.9. Gyakorlat. Irreducibilis-e a $2x$ polinom $\mathbb{Z}$ fölött?

3.2.10. Tétel. *Legyen T test. Ekkor $T[x]$-ben érvényes a számelmélet alaptétele.*

Ennek a tételnek a bizonyítását most csak két feladat formájában, vázlatosan ismertetjük. Ennek egyrészt az az oka, hogy a gondolatmenet lényegében ugyanaz, mint az egész számok esetében, másrészt pedig az, hogy később a gyűrűelméleti részben egy olyan általános eredményt bizonyítunk majd, amelynek ez a tétel speciális esete lesz.

3.2.11. Feladat. Mutassuk meg, hogy ha T test, akkor $T[x]$-ben minden irreducibilis polinom prímtulajdonságú. Vezessük le ebből a számelmélet alaptételének egyértelműségi állítását.

3.2.12. Feladat. Mutassuk meg, hogy ha T test, akkor minden nem konstans $T[x]$-beli polinom felbontható irreducibilis polinomok szorzatára.

Az euklideszi algoritmusnak másik fontos alkalmazása, hogy lehetővé teszi két polinom közös gyökeinek megkeresését. Természetesen ez akkor izgalmas, ha a gyököket különkülön nem tudjuk meghatározni.

3.2.13. Állítás. *Legyen R szokásos gyűrű és $f, g \in R[x]$. Ha létezik az (f, g) kitüntetett közös osztó, akkor ennek az R-beli gyökei pontosan az f és g közös gyökei.*

Bizonyítás. Ha $b \in R$ gyöke (f, g)-nek, akkor gyöke mindegyik többszörösének is, azaz f-nek is és g-nek is. Ha viszont $b \in R$ közös gyöke f-nek és g-nek, akkor $x - b$ osztója mindkét polinomnak, és így a kitüntetett közös osztójuknak is. □

Gyakorlatok, feladatok

3.2.14. Gyakorlat. Osszuk el maradékosan az $x^3 - 2$ polinomot $2x^2 + 2x - 3$-mal.

3.2.15. Gyakorlat. Az alábbi f és g polinomoknak határozzuk meg a kitüntetett közös osztóját az euklideszi algoritmussal, és az eredményt a visszahelyettesítési eljárással írjuk fel $fp + gq$ alakban, ahol p és q alkalmas polinomok.

(1) $f(x) = 3x^3 + 6x^2 + 6x + 3$ és $g(x) = 2x^4 + 2x^2 + 2$.
(2) $f(x) = x^5 - 1$ és $g(x) = x^3 - 1$.

3.2.16. Gyakorlat. Elvégezhető-e $\mathbb{Z}[x]$-ben az $x : 2$ maradékos osztás? Vagyis léteznek-e olyan $q, r \in Z[x]$ polinomok, hogy $x = 2q(x) + r(x)$, és $r = 0$, vagy r foka kisebb a 2 fokánál?

3.2.17. Gyakorlat. Tegyük fel, hogy f és $g \neq 0$ egész együtthatós polinomok. Igaz-e, hogy g akkor és csak akkor osztója f-nek $\mathbb{Z}[x]$-ben, ha az $f : g$ maradékos osztást $\mathbb{Q}[x]$-ben elvégezve a hányados egész együtthatós, és a maradék nulla?

3.2.18. Gyakorlat. Legyen T test, és S rész***gyűrűje*** T-nek. Tegyük fel, hogy $f, g \in S[x]$, és g főegyütthatója invertálható S-ben. Mutassuk meg, hogy ha g osztója f-nek $T[x]$-ben, akkor osztója $S[x]$-ben is.

3.2.19. Gyakorlat. Vezessük le a gyöktényező kiemelhetőségéről szóló 2.4.6. Állítást a maradékos osztás tételéből.

3.2.20. Gyakorlat. Mi lesz a maradék, ha az $x^4 + x^2 + 1$ polinomot elosztjuk $x^2 + x + 1$-gyel? A kapott eredményt indokoljuk meg számolás nélkül is. Hogyan lehetne általánosítani a kapott észrevételt?

3.2.21. Gyakorlat. Mi a maradék, ha $x^{64} + x^{54} + x^{14} + 1$-et osztjuk $x^2 - 1$-gyel, illetve $x^2 + 1$-gyel?

3.2.22. Gyakorlat. Ha b közös gyöke az f és g (szokásos gyűrű fölötti) polinomoknak, és h kitüntetett közös osztója f-nek és g-nek, akkor mi lesz a b gyök multiplicitása h-ban?

3.2.23. Feladat. Határozzuk meg az egész számok gyűrűjében az összes olyan nem üres I részhalmazt, amely zárt az összeadásra, és bármely elemének mindegyik többszörösét is tartalmazza. Hogyan használhatnánk fel a kapott eredményt a komplex szám rendjére vonatkozó 1.5.7. Tétel egyszerűbb bizonyítására?

3.3. Gyökök és irreducibilitás

Általában nehéz feladat egy polinomról eldönteni, hogy irreducibilis-e. A későbbiekben (az úgynevezett Galois-elmélet keretében) új eszközöket találunk majd az irreducibilitás vizsgálatára. Most először azt tekintjük át, hogy egy test fölötti polinom irreducibilitása hogyan függ össze azzal: van-e gyöke az adott testben. Emlékeztetjük az Olvasót a 3.2.8. Állításra, mely szerint egy *test fölötti* polinom akkor és csak akkor irreducibilis, ha nem konstans, és *nem bontható fel két alacsonyabb fokú polinom szorzatára.*

3.3.1. Állítás. *Test fölött egy elsőfokú polinom mindig irreducibilis.*

Bizonyítás. Elsőfokú polinomot nem lehet alacsonyabb fokúak szorzatára bontani, hiszen két nulladfokú polinom szorzata is nulladfokú. □

3.3.2. Állítás. *Legyen T test.* ***Ha*** *egy legalább másodfokú $T[x]$-beli polinomnak* ***van gyöke*** *T-ben,* ***akkor nem irreducibilis*** *T fölött.*

Bizonyítás. Legyen $b \in T$ gyöke egy $f \in T[x]$ polinomnak. Ekkor a hozzá tartozó $x - b$ gyöktényező kiemelhető f-ből. Ha f legalább másodfokú, akkor ezzel f-et két alacsonyabb fokú polinom szorzatára bontottuk. □

Ennek az észrevételnek a kapcsán az embernek az az érzése támadhat, hogy az irreducibilitás eldöntéséhez elég a gyököket megkeresni. De ez nem így van! ***Abból, hogy egy polinomnak nincs gyöke, még nem következik, hogy irreducibilis!*** A legegyszerűbb példa az $(x^2 + 1)^2$ polinom a racionális test fölött. Ennek még valós gyöke sincs, és nyilván nem irreducibilis, hiszen eleve szorzatként adtuk meg. A gyökök ismerete tehát nem csodafegyver az irreducibilitás eldöntéséhez, de hasznos, mert ha véletlenül találunk gyököt, akkor már készen is vagyunk.

3.3.3. Állítás. *Legyen T test. Ekkor egy $f \in T[x]$ polinomnak akkor és csak akkor van gyöke T-ben, ha van* ***elsőfokú*** *tényezője.*

Bizonyítás. Azt már láttuk, hogy ha van gyök, akkor a megfelelő gyöktényező kiemelhető. Megfordítva, tegyük fel, hogy $f = gh$, ahol $g(x) = ax + b$ egy elsőfokú polinom. Ekkor $-b/a$ gyöke f-nek. □

A gyök létezése tehát elsőfokú tényezőt jelent. Egy reducibilis polinom azonban bomolhat csupa egynél magasabb fokú tényezőre is, és *ezért* nem biztos, hogy van gyöke. Van azonban egy speciális helyzet, amikor elegendő a polinom gyökeit ellenőrizni az irreducibilitás eldöntéséhez.

3.3.4. Állítás. *Legyen T test. Ha egy* ***másod- vagy harmadfokú*** *$T[x]$-beli polinomnak nincs gyöke T-ben, akkor irreducibilis T fölött.*

Bizonyítás. Egy másodfokú polinomot alacsonyabb fokú tényezők szorzatára csak úgy lehet felbontani, hogy mindkét tényező elsőfokú lesz. Hasonlóképpen egy harmadfokú polinomot alacsonyabb fokúak szorzatára csak úgy bonthatunk, hogy az egyik tényező elsőfokú, a másik pedig másodfokú lesz. Mindkét esetben lesz tehát elsőfokú tényező, és így az előző állítás szerint gyök is. □

Most, hogy az irreducibilitás és a gyökök viszonyát tisztáztuk, megpróbáljuk tudásunkat alkalmazni néhány konkrét test esetében.

3.3.5. Tétel. *A komplex számok teste fölött (és általában egy algebrailag zárt T test fölött) az irreducibilis polinomok pontosan az elsőfokúak.*

Bizonyítás. Ez nyilvánvaló az eddigiekből, hiszen algebrailag zárt test fölött minden nem konstans polinomnak van gyöke. □

A valós számok teste fölötti irreducibilitás vizsgálatához egy nagyon hasznos segédállításra van szükségünk.

3.3.6. Lemma. *Legyen f valós együtthatós polinom, és z egy komplex gyöke f-nek. Ekkor z konjugáltja is gyöke f-nek, sőt z és $\overline{z}$ ugyanannyiszoros gyökök.*

Bizonyítás. Legyen $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. Ennek gyöke a z, tehát

$$a_0 + a_1 z + \ldots + a_n z^n = 0\,.$$

Vegyük mindkét oldal konjugáltját. Tudjuk, hogy összeg konjugáltja a konjugáltak összege, és ezért a bal oldalon álló összeget tagonként konjugálhatjuk. De a konjugálás szorzattartó is, ezért az eredmény ez lesz:

$$\overline{a_0} + \overline{a_1}\,\overline{z} + \ldots + \overline{a_n}\,\overline{z}^n = \overline{0}\,.$$

Valós szám konjugáltja önmaga, tehát $\overline{0} = 0$ és $\overline{a_j} = a_j$. Így a bal oldalon $f(\overline{z})$ áll, a jobb oldalon 0, tehát $\overline{z}$ tényleg gyöke f-nek.

A lemma második állítását f foka szerinti indukcióval bizonyítjuk. Ha z valós, azaz $z = \overline{z}$, akkor az állítás nyilvánvaló. Ha nem, azaz ha $z \neq \overline{z}$, akkor a z és $\overline{z}$ gyökökhöz tartozó gyöktényezők (a 2.4.7. Tétel miatt) egyszerre is kiemelhetők:

$$f(x) = (x - z)(x - \overline{z})q(x)$$

alkalmas $q \in \mathbb{C}[x]$ polinomra. Azonban

$$g(x) = (x - z)(x - \overline{z}) = x^2 - (z + \overline{z})x + z\overline{z}$$

valós együtthatós polinom, hiszen $z\overline{z} = |z|^2$ és $z+\overline{z} = 2\,\mathrm{Re}\,z$ valós számok. A 3.2.2. Állítás (igazából a maradékos osztás egyértelműsége) miatt q is valós együtthatós polinom. Az indukciós feltevés miatt tehát q-nak z és $\overline{z}$ ugyanannyiszoros (esetleg nullaszoros) gyöke, és így ugyanez igaz f-re is. □

3.3.7. Tétel. *A valós számok teste fölött az irreducibilis polinomok pontosan az elsőfokúak, és azok a másodfokúak, melyeknek nincs valós gyöke.*

Bizonyítás. A felsorolt polinomokról a korábbi állításokban már beláttuk, hogy irreducibilisek. Tegyük fel, hogy f irreducibilis polinom $\mathbb{R}$ fölött. Ekkor nem konstans, és így van egy z komplex gyöke. Ha ez valós, akkor f csak elsőfokú lehet. Ha z nem valós, akkor az előző bizonyításban láttuk, hogy a valós együtthatós $g(x) = (x - z)(x - \overline{z})$ kiemelhető f-ből, és a megmaradó q polinom is valós együtthatós. Mivel f irreducibilis, $q(x)$ csak konstans lehet, és így f tényleg másodfokú, melynek gyökei nem valósak. □

3.3.8. Következmény. *Páratlan fokú valós együtthatós polinomnak van valós gyöke.*

Bizonyítás. Bontsuk a polinomot irreducibilisek szorzatára $\mathbb{R}$ fölött. Ezek első- vagy másodfokúak. Mindegyik tényező nem lehet másodfokú, mert a polinom foka páratlan. Tehát van elsőfokú tényező, és így valós gyök is. □

Ez a bizonyítás természetesen használja az algebra alaptételét. Már említettük, hogy az algebra alaptételének bizonyításához valamennyi analízis-tudás is szükséges, és ha komplex függvénytant is használhatunk, akkor nagyon egyszerű lesz a bizonyítás. Van azonban egy elegáns bizonyítás Galois-elmélet felhasználásával is, ezt a 6.6.10. Tételben fogjuk bemutatni. Az abban felhasznált analízis-ismeretek minimálisak: semmi másra nincs szükség, mint a fenti, 3.3.8. Következményre. Ezért ezt célszerű elemien, az algebra alaptételének felhasználása nélkül is bebizonyítani. Egy ilyen bizonyítás olvasható az A.3. Függelékben (lásd A.3.4. Tétel).

A racionális számok teste fölött már nem tudjuk olyan könnyen leírni az irreducibilis polinomokat, mint $\mathbb{C}$ és $\mathbb{R}$ fölött. Itt vannak akárhányadfokú irreducibilis polinomok is: nemsokára látni fogjuk, hogy például $x^n - 2$ irreducibilis $\mathbb{Q}$ fölött tetszőleges $n \geq 1$ esetén. A most bizonyított eredmények mégis segíthetnek néha, mert ha találunk egy racionális gyököt, akkor tudjuk, hogy a polinom nem lehet irreducibilis (kivéve ha elsőfokú). Az alábbiakban egy eljárást ismertetünk a racionális gyökök megkeresésére.

Ha adott egy racionális együtthatós polinom, akkor szorozzuk be az együtthatók nevezőivel. Így egy egész együtthatós polinomot kapunk, amelynek a gyökei ugyanazok, mint a

kiinduló polinomé. Így elegendő az egész együtthatós polinomok racionális gyökeit megkeresni. Erre szolgál az alábbi állítás.

3.3.9. Tétel [Racionális gyökteszt]. *Tegyük fel, hogy a p/q már nem egyszerűsíthető tört gyöke az f egész együtthatós polinomnak. Ekkor a számláló (azaz p) osztja f konstans tagját, a nevező (azaz q) pedig osztja f főegyütthatóját.*

Azt nem állítjuk, hogy a feltételnek eleget tevő törtek tényleg gyökei az f polinomnak! De csak véges sok törtről van szó, mert a főegyütthatónak és a konstans tagnak is (ha nem nulla) véges sok osztója van. Így ezeket a törteket egyenként végigpróbálgathatjuk: mindegyiket behelyettesíthetjük (például a Horner-elrendezéssel) az f polinomba. Ezzel megkapjuk az f összes racionális gyökét.

Bizonyítás. Az, hogy a tört már nem egyszerűsíthető, azt jelenti, hogy p és q relatív prím egész számok. Legyen $f(x) = a_0 + a_1x + \ldots + a_nx^n$. Ekkor p/q-t behelyettesítve, majd q^n-nel beszorozva

$$a_0q^n + a_1pq^{n-1} + \ldots + a_np^n = 0$$

adódik. Ebben az összegben mindegyik tag osztható p-vel, kivéve esetleg a legelsőt. Mivel a 0 is osztható p-vel, ezért a legelső tag is, tehát $p \mid a_0q^n$. De p és q relatív prímek, és így $p \mid a_0$. Ugyanezzel a módszerrel kapjuk a $q \mid a_n$ oszthatóságot is. □

3.3.10. Gyakorlat. Hogyan alkalmazhatjuk a racionális gyöktesztet egy olyan polinom racionális gyökeinek a megkeresésére, amelynek a konstans tagja nulla?

A $\mathbb{Q}$ fölötti irreducibilitás eldöntésében néha segíthet az, ha a polinomnak a komplex gyökeit ismerjük. Ennek a módszernek az illusztrálására egy példát dolgozunk ki.

3.3.11. Példa. Mutassuk meg, hogy $x^4 + 36$ irreducibilis $\mathbb{Q}$ fölött.

Határozzuk meg a polinom komplex gyökeit. A -36 számból (például trigonometrikus alak segítségével) negyedik gyököt vonva az eredmény $\sqrt{3}(\pm 1 \pm i)$. A gyöktényezős alak tehát a következő:

$$x^4 + 36 = \big(x - \sqrt{3} - \sqrt{3}i\big)\big(x - \sqrt{3} + \sqrt{3}i\big)\big(x + \sqrt{3} - \sqrt{3}i\big)\big(x + \sqrt{3} + \sqrt{3}i\big)\,.$$

Egyik gyök sem valós, és így ha $x^4 + 36$ felbomlik $\mathbb{Q}$ fölött, akkor csak két másodfokú polinom szorzata lehet: $x^4 + 36 = f(x)g(x)$. Az f és g gyökei összesen kiadják a fenti négy komplex gyököt. Mivel f és g valós együtthatósak, gyökeik konjugáltak kell, hogy legyenek. Ezért f és g egyike

$$r\big(x - \sqrt{3} - \sqrt{3}i\big)\big(x - \sqrt{3} + \sqrt{3}i\big) = r\big(x^2 - 2\sqrt{3}x + 6\big)\,,$$

a másik pedig

$$s\big(x + \sqrt{3} - \sqrt{3}i\big)\big(x + \sqrt{3} + \sqrt{3}i\big) = s\big(x^2 + 2\sqrt{3}x + 6\big)\,,$$

alkalmas r és s valós számokra, ahol $rs = 1$ (a beszorzást, a 2.5.10. Gyakorlat megoldásához hasonlóan, az $(a - b)(a + b) = a^2 - b^2$ azonosság felhasználásával érdemes

elvégezni). Mivel f és g racionális együtthatós, a fenti első polinom főegyütthatója, azaz r is racionális szám. Racionális továbbá ebben a polinomban x együtthatója, azaz $-2r\sqrt{3}$ is, ami lehetetlen, hiszen akkor $r \neq 0$ miatt $\sqrt{3}$ is racionális lenne. Ezért $x^4 + 36$ tényleg irreducibilis $\mathbb{Q}$ fölött.

Gyakorlatok, feladatok

3.3.12. Gyakorlat. Bontsuk fel a következő polinomokat az $\mathbb{R}$ fölött irreducibilis polinomok szorzatára: $x^4 - 1$, $x^4 + 1$, $x^4 + 9$, $x^6 - 4x^3 + 3$.

3.3.13. Gyakorlat. Bontsuk fel a $6(x^2 - 2)(x^2 + 1)$ polinomot $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ fölött felbonthatatlanok szorzatára.

3.3.14. Gyakorlat. Adjuk meg az összes olyan tizenkettedfokú valós együtthatós polinomot, melynek az $1 + i$ hatszoros gyöke.

3.3.15. Gyakorlat. Adjuk meg a $2x^3 + 3x + 5$ polinom racionális gyökeit, és bontsuk $\mathbb{Q}$ fölött irreducibilisek szorzatára.

3.3.16. Gyakorlat. Legyen c pozitív egész szám. Mi annak a szükséges és elégséges feltétele, hogy $x^4 + c$ irreducibilis legyen $\mathbb{R}$, illetve $\mathbb{Q}$ fölött? Mi a helyzet negatív c esetén?

3.3.17. Gyakorlat. Határozzuk meg a $\mathbb{Z}_2$ test fölött a legfeljebb negyedfokú irreducibilis polinomokat.

3.3.18. Feladat. Legyen $p \in \mathbb{Z}$ pozitív prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p-szerese nulla. Bizonyítsuk be, hogy tetszőleges $r, s \in R$ elemekre

$$(r + s)^p = r^p + s^p ,$$

azaz R-ben tagonként lehet p-edik hatványra emelni. Vezessük le ebből a kis Fermat-tételt (miszerint $b^p - b$ osztható p-vel minden b egészre). Mutassuk meg, hogy tetszőleges $f \in \mathbb{Z}_p[x]$ polinomra $f(x^p) = f(x)^p$.

3.3.19. Gyakorlat. Irreducibilisek-e az alábbi polinomok?

(1) $\mathbb{Z}_2$ fölött $x^8 + x^2 + 1$, $x^5 + x + 1$, $x^5 + x^3 + 1$, $x^5 + x^4 + x^3 + 1$.
(2) $\mathbb{Z}_{17}$ fölött $x^2 + 1$, $x^4 + 1$, $x^8 + 1$, $x^{17} + 1$, $x^{17} + 2$.

3.3.20. Feladat. Bontsuk fel az $x^4 - 10x^2 + 1$ polinomot $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ fölött felbonthatatlanok szorzatára.

3.4. Egész együtthatós polinomok

Ebben a szakaszban a $\mathbb{Z}[x]$ számelméletét vizsgáljuk. Erről a gyűrűről is be fogjuk látni, hogy igaz benne az alaptétel, de másképp, mint test fölötti polinomokra, mert $\mathbb{Z}[x]$-ben nem végezhető el korlátlanul a maradékos osztás. A kapott eredmények segíteni fognak a $\mathbb{Q}$ fölötti irreducibilitás vizsgálatában is.

A $\mathbb{Q}$ és $\mathbb{Z}$ számelmélete közötti első különbséggel már szembesült az, aki megoldotta a 3.2.9. Gyakorlatot. A $2x$ polinom $\mathbb{Q}$ fölött irreducibilis, de $\mathbb{Z}$ fölött nem az, mert itt a $2 \cdot x$ felbontás nem triviális: a 2 egység $\mathbb{Q}$ fölött, de nem egység $\mathbb{Z}$ fölött.

Ha tehát egy egész együtthatós polinomot $\mathbb{Z}$ fölött akarunk felbontani, akkor úgy érdemes kezdeni, hogy kiemeljük belőle azt az egész számot, amit lehet, vagyis az együtthatóinak a legnagyobb közös osztóját. Például

$$180x^3 + 72x + 120 = 12(15x^3 + 6x + 10)\,.$$

A megmaradó polinomot primitívnek fogjuk nevezni. Tehát $15x^3 + 6x + 10$ már primitív polinom.

3.4.1. Definíció. Egy egész együtthatós nem nulla polinomot *primitívnek* nevezünk, ha együtthatóinak legnagyobb közös osztója 1.

E definíció egytagú polinom esetében azt jelenti, hogy az egyetlen nem nulla együttható ± 1 (ez felel meg annak a szemléletnek, hogy a polinomból csak egységet lehessen kiemelni). De ezt nem szükséges külön kikötni, mert együtthatók legnagyobb közös osztóján az $(a, 0) = a$ összefüggés miatt nem változtat, ha nulla együtthatókat is közéjük veszünk.

A polinomból kiemelt egész számot úgy bontjuk fel, mint az egész számok között. Ez azért lesz megfelelő, mert az egészek közötti felbonthatatlan számok a polinomok között is felbonthatatlanok.

3.4.2. Gyakorlat. Mutassuk meg, hogy a felbonthatatlan egész számokat konstans polinomnak képzelve $\mathbb{Z}[x]$-ben is felbonthatatlan elemeket kapunk.

A számelmélet alaptétele kapcsán láttuk, hogy a felbonthatatlan egész számok prímtulajdonságúak. A $\mathbb{Z}[x]$-beli alaptétel bizonyításának első lépése az, hogy belátjuk: ezek a számok prímtulajdonságúak $\mathbb{Z}[x]$-ben is.

3.4.3. Lemma [Első Gauss Lemma]. *Ha p prímszám, akkor $\mathbb{Z}[x]$-ben mint konstans polinom is prímtulajdonságú.*

Bizonyítás. A lemmára két bizonyítást is adunk. Az első elemi számolás lesz. A második elegánsabb, felhasználja a modulo p számolásról tanultakat. Azt tudjuk, hogy p nem nulla, és nem ± 1, tehát $\mathbb{Z}[x]$-ben sem egység. Tegyük fel, hogy $p \mid fg$, ahol $f, g \in \mathbb{Z}[x]$. Meg kell mutatni, hogy $p \mid f$ vagy $p \mid g$.

Az első bizonyításban felírjuk f és g együtthatóit, és elvégezzük a szorzást. Legyen

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \quad \text{és} \quad g(x) = b_0 + b_1 x + \ldots + b_m x^m\,.$$

Tegyük fel, hogy p nem osztója sem f-nek, sem g-nek, azaz mindkét polinomnak van p-vel nem osztható együtthatója. Válasszuk ki mindkét polinomban a legnagyobb indexű ilyen együtthatót, legyenek ezek a_i és b_j. Tudjuk, hogy fg-ben az x^{i+j} együtthatója

$$a_0b_{i+j} + a_1b_{i+j-1} + \ldots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \ldots + a_{i+j}b_0$$

(ahol a szokásos konvenció szerint $a_{n+1} = a_{n+2} = \ldots = 0$ és $b_{m+1} = b_{m+2} = \ldots = 0$). Az összeg tagjai egy kivétellel mind p-vel oszthatók, mert az a_i választása (az i maximalitása) miatt $a_{i+1}, \ldots, a_{i+j}$, a b_j választása miatt pedig $b_{j+1}, \ldots, b_{i+j}$ osztható p-vel. A kimaradó a_ib_j viszont nem osztható p-vel, mert a_i és b_j nem osztható p-vel, és p prímszám. Tehát a fenti összeg nem osztható p-vel. Ez lehetetlen, mert ez az összeg a p-vel osztható fg polinom egyik együtthatója. Ez az ellentmondás bizonyítja az állítást.

A második bizonyítást az elsőből származtathatjuk, ha észrevesszük, hogy az elmondott gondolatmenet mennyire hasonlít annak bizonyításához, hogy szorzatpolinom foka a fokok összege. Ezt a hasonlóságot ki is aknázhatjuk, ha az f és g polinomokat (pontosabban az együtthatóikat) modulo p vesszük. Ekkor ugyanis az iménti gondolatmenetben kiválasztott a_i az f polinom főegyütthatójává, a b_j pedig a g polinom főegyütthatójává válik.

A második bizonyítás tehát a következőképpen hangzik. Vegyük az f, g és fg polinomokat modulo p, az eredményt jelölje $\overline{f}$, $\overline{g}$, $\overline{fg} \in \mathbb{Z}_p[x]$. Ekkor $\overline{fg} = \overline{f}\,\overline{g}$ (a 2.3.7. Gyakorlat miatt). Mivel $p \mid fg$, az $\overline{fg}$ a nullapolinom. De $\mathbb{Z}_p$ test, és így $\mathbb{Z}_p[x]$ nullosztómentes. Tehát $\overline{f}$ és $\overline{g}$ egyike nulla, vagyis f és g egyike osztható p-vel. □

Néha az előző állítás alábbi következményét is „első Gauss-lemma" néven emlegetik.

3.4.4. Következmény [Első Gauss Lemma, első következmény]. *Primitív polinomok szorzata is primitív.*

Bizonyítás. Tegyük fel, hogy $f, g \in \mathbb{Z}[x]$ primitív polinomok. Azt kell megmutatni, hogy fg nem osztható egységtől különböző egész számmal. Ha osztható lenne, akkor lenne egy p prímosztója is. Az előző lemma miatt ekkor $p \mid f$ vagy $p \mid g$, ami nem lehet, hiszen f és g primitívek. □

3.4.5. Következmény [Első Gauss Lemma, második következmény]. *Legyen f primitív (egész együtthatós) polinom. Ha g olyan racionális együtthatós polinom, melyre $h = fg$ egész együtthatós, akkor g is egész együtthatós. Speciálisan ha f osztója egy h egész együtthatós polinomnak $\mathbb{Q}[x]$-ben, akkor f osztója h-nak $\mathbb{Z}[x]$-ben is.*

Bizonyítás. Hozzuk g együtthatóit közös nevezőre, és emeljük ki a számlálókból a legnagyobb közös osztójukat. Így a $g = (s/t)g_0$ felbontást kapjuk, ahol g_0 már primitív (egész együtthatós) polinom, és az s, t egész számokról az s/t törtet egyszerűsítve feltehetjük, hogy relatív prímek. A $h = fg$ egyenlőséget t-vel megszorozva kapjuk, hogy $th = sfg_0$. Ha p prímosztója t-nek, akkor $p \mid sfg_0$, az első Gauss-lemma miatt tehát $p \mid s$, vagy $p \mid f$, vagy $p \mid g_0$. Mindhárom lehetetlen, az első azért, mert t és s relatív prímek, a másik kettő azért, mert f és g_0 primitívek. A t számnak nincs tehát prímosztója, vagyis t egység, és így $g = (s/t)g_0$ tényleg egész együtthatós polinom. □

Az előző bizonyításban láttuk, hogy minden racionális együtthatós polinom felbontható egy racionális szám, és egy egész együtthatós primitív polinom szorzatára. Az alábbi gyakorlat ennek a felbontásnak az egyértelműségét fogalmazza meg.

3.4.6. Gyakorlat. Mutassuk meg, hogy minden nem nulla racionális együtthatós polinom felírható egy egész együtthatós primitív polinom és egy racionális szám szorzataként, és a felbontásban szereplő primitív polinom $\mathbb{Z}$ fölötti asszociáltság erejéig egyértelműen meghatározott.

A $\mathbb{Z}[x]$-beli alaptételt a $\mathbb{Q}[x]$-beli alaptétel segítségével fogjuk bizonyítani. Ehhez meg kell vizsgálnunk, hogy egy adott polinomnak „mennyivel több" felbontása van $\mathbb{Q}$, mint $\mathbb{Z}$ fölött. Ha a polinom $f(x) = x^2 - 1$, akkor ennek $\mathbb{Q}$ fölött felbontása lesz például a következő:

$$x^2 - 1 = \big((2/3)x - (2/3)\big)\big((3/2)x + (3/2)\big)\,.$$

Mindannyian érezzük, hogy ez „valójában" az $(x-1)(x+1)$ felbontás, csak „el van bonyolítva" úgy, hogy az első tényezőt $2/3$-dal, a másodikat $3/2$-del beszoroztuk. Gauss második lemmája azt mondja ki, hogy minden $\mathbb{Q}$ fölötti felbontás egy $\mathbb{Z}$ fölötti felbontás hasonló „elbonyolításával" keletkezik.

3.4.7. Lemma [Második Gauss Lemma]. *Tegyük fel, hogy az $f \neq 0$ egész együtthatós polinomot felbontottuk a racionális együtthatós g és h polinomok szorzatára. Ekkor g és h megszorozható alkalmas racionális számokkal úgy, hogy a kapott g_0 és h_0 polinomok egész együtthatósak legyenek, és $f = g_0 h_0$ teljesüljön.*

Bizonyítás. Írjuk föl a g és h polinomokat rg_1 és sh_1 alakban, ahol r, s racionális számok, g_1 és h_1 egész együtthatós primitív polinomok. Ekkor $f = (rs)(g_1 h_1)$. Az első Gauss-lemma első következménye miatt $g_1 h_1$ primitív polinom, a második következménye miatt tehát $n = rs$ egy egész együtthatós polinom, azaz egész szám. Így a $g_0 = ng_1$ és $h_0 = h_1$ választás megfelel a követelményeknek. □

3.4.8. Tétel. *Egy egész együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ fölött, ha*

(1) *vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),*
(2) *vagy egy (nem konstans) primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.*

Bizonyítás. A $\mathbb{Z}$-beli felbonthatatlan számokról láttuk, hogy mint konstans polinomok szintén felbonthatatlanok. Tegyük fel, hogy f nem konstans primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis. Ha $f = gh$ egy felbontás, ahol $g, h \in \mathbb{Z}[x]$, akkor a $\mathbb{Q}$ fölötti irreducibilitás miatt g és h egyike egység $\mathbb{Q}$-ban, vagyis konstans, és így egész szám (hiszen g és h egész együtthatós). Mivel f primitív, ez az egész szám csak egység lehet, és így az $f = gh$ felbontás $\mathbb{Z}[x]$-ben is triviális. Tehát f irreducibilis $\mathbb{Z}$ fölött.

Megfordítva, tegyük fel, hogy f irreducibilis polinom $\mathbb{Z}[x]$-ben. Ekkor f felírható nk alakban, ahol n egész szám, és k primitív polinom. Mivel f irreducibilis, ez a felbontás triviális. Így vagy n egység (és akkor f primitív), vagy k egység (és akkor f konstans).

Ha f konstans, akkor nyilván felbonthatatlannak kell lennie $\mathbb{Z}$-ben, hiszen a $\mathbb{Z}$-beli nemtriviális felbontások egyben $\mathbb{Z}[x]$-beli nemtriviális felbontások is. Ha f nem konstans primitív polinom, akkor meg kell mutatnunk, hogy nemcsak $\mathbb{Z}$, hanem $\mathbb{Q}$ fölött is irreducibilis.

Tegyük fel, hogy f előáll a nála alacsonyabb fokú (és ezért nem konstans), racionális együtthatós g és h polinomok szorzataként. A második Gauss-lemma miatt ekkor f felírható g_0h_0 alakban is, ahol ezek már egész együtthatós polinomok, és g_0 foka megegyezik g fokával, h_0 foka pedig h fokával. Tehát f_0 és g_0 egyike sem konstans, és így ez nemtriviális felbontás $\mathbb{Z}$-ben is, ami ellentmond f irreducibilitásának $\mathbb{Z}$ fölött. □

Az alaptétel bizonyításához már csak egy észrevételre van szükség.

3.4.9. Állítás. *A $\mathbb{Z}[x]$ gyűrű minden irreducibilis eleme prímtulajdonságú.*

Bizonyítás. Az előző tétel miatt ez az irreducibilis elem vagy egy konstans $\mathbb{Z}$-beli prím, vagy egy primitív f polinom, amely $\mathbb{Q}$ fölött irreducibilis. Az első esetben az első Gauss-lemma pont az állítást mondja ki. A második esetben tegyük fel, hogy f osztója $\mathbb{Z}[x]$-ben a gh szorzatnak, ahol g és h egész együtthatós polinomok. Mivel $\mathbb{Q}[x]$-ben igaz az alaptétel, f prímtulajdonságú $\mathbb{Q}[x]$-ben, tehát f osztója g-nek vagy h-nak $\mathbb{Q}[x]$-ben. Az első Gauss-lemma második következménye miatt ez az oszthatóság $\mathbb{Z}[x]$-ben is fönnáll. Így f tényleg prímtulajdonságú. □

3.4.10. Tétel. *A $\mathbb{Z}[x]$ gyűrűben érvényes a számelmélet alaptétele.*

Bizonyítás. Az alaptétel egyértelműségi állítása következik abból, hogy a felbonthatatlan elemek prímtulajdonságúak (lásd 3.1.28. Feladat). Azt kell tehát csak megmutatni, hogy minden f egész együtthatós polinom, amely nem nulla és nem egység, felbontható irreducibilisek szorzatára. Az f polinomot felírhatjuk egy n egész szám és egy g primitív polinom szorzataként, és az n számot felbonthatjuk $\mathbb{Z}$-ben felbonthatatlanok szorzatára, ezek a tényezők $\mathbb{Z}[x]$-ben is felbonthatatlanok lesznek. Tehát elég azt megmutatni, hogy $\mathbb{Z}[x]$ minden primitív, nem konstans g polinomja felírható irreducibilisek szorzataként.

Tegyük fel, hogy ez az állítás nem igaz, legyen g minimális fokú ellenpélda. Ha g maga irreducibilis, akkor önmaga, mint egytényezős felbontás megfelelő lesz. Ha nem, akkor $g = hk$ alakban írható, ahol k és h egyike sem egység. Mivel g primitív, a h és k is primitív polinomok. Így egyikük sem lehet konstans (mert akkor egység lenne), és ezért mindketten g-nél alacsonyabb fokúak. Mivel g foka minimális volt, h és k már felbomlik irreducibilisek szorzatára, de akkor ezt a két felbontást összeszorozva g-t is felbontottuk irreducibilisek szorzatára. Ez az ellentmondás bizonyítja a tételt. □

Az eddigiektől vérszemet kapva megkérdezhetjük, alaptételes-e a $\mathbb{Z}[x, y]$ vagy a $\mathbb{Q}[x, y]$ polinomgyűrű. A válasz igenlő, és a meglepő az, hogy ezt lényegében már be is bizonyítottuk! Például $\mathbb{Q}[x, y]$ úgy tekinthető, mint $\mathbb{Q}[y][x]$, ahol $\mathbb{Q}[y]$-ról tudjuk, hogy alaptételes gyűrű. Ha a most elhangzott bizonyítást el tudnánk mondani $\mathbb{Z}$ helyett $\mathbb{Q}[y]$-ra is, akkor készen lennénk.

Azt kell megvizsgálni, hogy a fenti bizonyításban a $\mathbb{Z}$ milyen tulajdonságait használtuk, és ezek teljesülnek-e $\mathbb{Q}[y]$-ban is. Az alaptételt sokszor, de az $\mathbb{Q}[y]$-ban is teljesül. Használtuk a $\mathbb{Z}_p$ fogalmát is, de csak egy második bizonyításban, tehát ezt nem muszáj általánosítanunk. (Ennek ellenére ez lehetséges, az új fogalmat *faktorgyűrű* néven vezetjük majd be.) Amiről még rengeteget beszéltünk, azok a racionális számok, vagyis a $\mathbb{Z}$ elemeiből készített törtek. De probléma ezzel sincs, hiszen olyan törtekről, amiben az y is szerepel, a középiskolában is sok szó esett, egyenletrendezés kapcsán számoltunk ilyenekkel, bár nem definiáltuk őket pontosan (ezeket, tehát két polinom hányadosát *racionális törtfüggvényeknek* hívják). A *hányadostestről* szóló szakaszban precízen be fogjuk bizonyítani, hogy bármilyen szokásos gyűrű esetében használhatjuk a törteket a szokásos tulajdonságokkal.

Mindezt megelőlegezve, az eddigiek gondos áttanulmányozásával láthatjuk, hogy valójában a közvetkező tételt bizonyítottuk be.

3.4.11. Tétel. *Ha R alaptételes (szokásos) gyűrű, akkor az $R[x]$ polinomgyűrűben is érvényes a számelmélet alaptétele.*

Ezt az áttanulmányozást természetesen csak a hányadostest pontos fogalmának ismeretében lesz majd érdemes elvégezni. Mindenesetre az algebrai szemléletmód erejét mutatja, hogy az alábbi állítás bizonyításához most már a kisujjunkat sem kell mozdítanunk: n szerinti teljes indukcióval azonnal következik az előző tételből.

3.4.12. Következmény. *A $\mathbb{Z}[x_1, \ldots, x_n]$, továbbá tetszőleges T test esetén a $T[x_1, \ldots, x_n]$ gyűrű is alaptételes.*

Gyakorlatok, feladatok

3.4.13. Gyakorlat. Bontsuk $\mathbb{Z}$ fölött irreducibilisek szorzatára a $30x^3 - 30$ polinomot.

3.4.14. Gyakorlat. Mutassuk meg, hogy ha R szokásos gyűrű, és $R[x]$ alaptételes, akkor az R gyűrű is az.

3.4.15. Gyakorlat. Adjunk második bizonyítást arra a tényre, hogy $\mathbb{Z}$ fölött minden polinom irreducibilisek szorzatára bontható úgy, hogy egy $\mathbb{Q}$ fölötti felbontásból indulunk ki, és azt módosítjuk.

3.4.16. Gyakorlat. Bizonyítsuk be, hogy az $f, g \in \mathbb{Z}[x]$ polinomok $\mathbb{Z}[x]$-beli legnagyobb közös osztója a következő eljárással határozható meg. Alkalmazzuk az euklideszi algoritmust $\mathbb{Q}$ fölött, és a kapott racionális együtthatós polinomot írjuk fel rh alakban, ahol $r \in \mathbb{Q}$ és $h \in \mathbb{Z}[x]$ primitív polinom. Határozzuk meg f és g együtthatóinak a legnagyobb közös osztóját, ez legyen n. Ekkor f és g legnagyobb közös osztója nh. Hogyan módosítható ez az eljárás, ha két $\mathbb{C}[x, y]$-beli polinom legnagyobb közös osztóját keressük?

3.4.17. Gyakorlat. Mutassuk meg, hogy minden test alaptételes gyűrű. A 3.4.11. Tétel szerint ekkor $T[x]$ is alaptételes. Második bizonyítást kaptunk-e ezzel arra, hogy test fölötti polinomgyűrű alaptételes?

3.5. Irreducibilitás a racionális számtest fölött

A komplex és a valós test fölött át tudtuk tekinteni az összes irreducibilis polinomot, az egész számok gyűrűje fölötti irreducibilitást pedig visszavezettük a racionális számtest fölötti irreducibilitás kérdésére. A racionális számok fölött akárhányadfokú irreducibilis polinomok léteznek, és egy adott polinomról egyáltalán nem könnyű megállapítani, hogy irreducibilis-e, vagy sem. Az irreducibilitás eldöntésére létezik hatékony algoritmus mind $\mathbb{Q}$, mind a véges testek fölött (és így például a `Maple` program meg tudja mondani egy-egy konkrét polinomról, hogy irreducibilis-e), de ennek tárgyalása messze meghaladná e könyv kereteit. Egy nem hatékony algoritmust ír le a 3.5.17. Feladat.

Most néhány olyan elemi módszert mutatunk, amellyel az irreducibilitás kérdése megvizsgálható, és amelyek elegendőek lesznek a későbbi alkalmazásokhoz. Az első ilyen ötlet az úgynevezett Schönemann-Eisenstein kritérium, amivel, ha szerencsénk van, egy-egy konkrét polinomról megállapíthatjuk, hogy irreducibilis. A bizonyításban használni fogjuk az alábbi segédállítást.

3.5.1. Gyakorlat. Legyen T test, és $r \neq 0$ egy eleme. Mutassuk meg, hogy az rx^n polinom osztói $T[x]$-ben pontosan az sx^m alakú polinomok, ahol $0 \neq s \in T$ és $m \leq n$.

3.5.2. Tétel [A Schönemann-Eisenstein irreducibilitási kritérium]. *Legyen f egy egész együtthatós nem konstans polinom.* ***Ha*** *létezik olyan p prímszám, amelyre*

(1) *p nem osztja f főegyütthatóját;*
(2) *p osztja f összes többi együtthatóját;*
(3) *p^2 nem osztja f konstans tagját,*

akkor *f irreducibilis $\mathbb{Q}$ fölött.*

Mielőtt az állítást bebizonyítanánk, néhány fontos megjegyzést teszünk.

(1) Az állítás megfordítása nem igaz! Például az $x + 1$ polinom irreducibilis $\mathbb{Q}$ fölött, de nincs hozzá megfelelő p prímszám. Tehát ez a kritérium nem ad eljárást az irreducibilitás eldöntésére: ha alkalmazható, akkor a polinom irreducibilis, de ha nem alkalmazható, akkor az irreducibilitást nem tudjuk, és új ötlet után kell néznünk.
(2) Az állítás egész együtthatós polinomokról szól ugyan, de racionális együtthatós polinomokra is alkalmazható lehet, ha a nevezőkkel felszorzunk.
(3) Vigyázzunk: ez a kritérium csak $\mathbb{Q}$ fölötti (és nem $\mathbb{Z}$ fölötti) irreducibilitást biztosít. Például a $9x + 18$ polinomra érvényes a feltétel (ha $p = 2$), és ez a polinom irreducibilis is $\mathbb{Q}$ fölött, de nem irreducibilis $\mathbb{Z}$ fölött (hiszen nem primitív).
(4) A kritérium alapján láthatjuk, hogy az $x^n - 2$ polinom irreducibilis $\mathbb{Q}$ fölött (és így $\mathbb{Z}$ fölött is, hiszen primitív). Vagyis tényleg van akármilyen fokú irreducibilis polinom $\mathbb{Q}$ és $\mathbb{Z}$ fölött.
(5) A kritérium általánosítható alaptételes gyűrűre (lásd 5.6.8. Gyakorlat).

Bizonyítás. Az első Gauss-lemma (3.4.3. Lemma) bizonyításánál először egy együtthatókkal való számolást mutattunk be, majd ennek elemzésével rájöttünk, hogy a polinom modulo p vizsgálatával a számolás elkerülhető. Most fordítva járunk el: a számolásmentes

bizonyítást mutatjuk be, és az Olvasót a 3.5.3. Gyakorlatban kérjük meg arra, hogy ezt a bizonyítást fordítsa le elemi számolásra. Ha valakinek a modulo p gondolkodás még nehézséget okoz, az megteheti, hogy a Schönemann-Eisenstein kritérium bizonyításaként előbb ennek a gyakorlatnak a megoldását olvassa el.

Tegyük fel tehát, hogy az f polinom és a p prímszám teljesítik a feltételeket, de f mégsem irreducibilis $\mathbb{Q}$ fölött, vagyis az f-nél alacsonyabb fokú, racionális együtthatós g és h polinomok szorzatára bontható. A második Gauss-lemma (3.4.7. Lemma) miatt feltehetjük, hogy g és h egész együtthatós.

Vegyük az f, g, h polinomokat (tehát az együtthatóikat) modulo p, a kapott polinomokat jelölje $\overline{f}$, $\overline{g}$ és $\overline{h}$. Ekkor $\overline{fg} = \overline{f}\ \overline{g}$ (a 2.3.7. Gyakorlat miatt). Ha f főtagja $a_n x^n$, akkor, mivel f többi együtthatója p-vel osztható, az $\overline{f}$ polinom $\overline{a_n}x^n$ lesz (ahol $\overline{a_n} \neq 0$ az a_n maradéka modulo p). Az előző, 3.5.1. Gyakorlat miatt $\overline{a_n}x^n$ minden osztója sx^m alakú alkalmas $s \in \mathbb{Z}_p$-re és $m \leq n$ egészre. Speciálisan

$$\overline{g}(x) = ux^k \quad \text{és} \quad \overline{h}(x) = vx^\ell$$

alkalmas $u, v \in \mathbb{Z}_p$-re. Mivel $\mathbb{Z}_p$ nullosztómentes, a $\overline{g}$ és a $\overline{h}$ fokainak összege az $\overline{f}$ foka, vagyis $k + \ell = n$. De $k = \mathrm{gr}(\overline{g}) \leq \mathrm{gr}(g)$, hiszen ha a g polinomot modulo p vesszük, akkor foka nem nőhet (akkor csökkenhetne, ha a főegyütthatója osztható lenne p-vel). Hasonlóképpen látjuk, hogy $\ell \leq \mathrm{gr}(h)$. Mivel f-et eredetileg két alacsonyabb fokú polinom szorzatára bontottuk fel, k és ℓ mindketten n-nél kisebbek, és mivel összegük n, egyikük sem lehet nulla. Ez azt jelenti, hogy $\overline{g} = ux^k$ konstans tagja nulla, vagyis g konstans tagja osztható p-vel, és ugyanígy h konstans tagja is osztható p-vel. De akkor f konstans tagja, amely g és h konstans tagjainak a szorzata, osztható p^2-tel. Ez ellentmond a feltételeknek. □

3.5.3. Gyakorlat. A fenti gondolatmenetet elemezve adjunk a Schönemann-Eisenstein kritériumra olyan elemi bizonyítást, ami nem használja a $\mathbb{Z}_p[x]$ polinomgyűrűt.

Vigyázzunk, azzal a technikával, hogy „vegyük a felbontást modulo p”, óvatosan kell bánni! Például megtörténhet, hogy egy nemtriviális felbontás triviálissá válik mod p. A következő gyakorlatban összefoglaltunk néhány lehetséges anomáliát.

3.5.4. Gyakorlat. Legyen p egy prímszám, $f \in \mathbb{Z}[x]$ egy n-edfokú polinom, ahol $n \geq 1$, és $0 < k < n$. Legyen $\overline{f} \in \mathbb{Z}_p[x]$ az f modulo p véve. Az alábbi állítások közül melyek igazak?

(1) Ha f irreducibilis $\mathbb{Z}$ fölött, akkor $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött.
(2) Ha $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött, akkor f irreducibilis $\mathbb{Q}$ fölött.
(3) Ha $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött, és $\overline{f}$ foka n, akkor f irreducibilis $\mathbb{Z}$ fölött.
(4) Ha $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött, és $\overline{f}$ foka n, akkor f irreducibilis $\mathbb{Q}$ fölött.
(5) Ha f-nek van $\mathbb{Z}$ fölött k-adfokú tényezője, akkor $\overline{f}$-nak is van k-adfokú tényezője.
(6) Az előző állítás akkor, ha azt is tudjuk, hogy $\overline{f}$ foka n.

Néha előfordul, hogy a Schönemann-Eisenstein kritérium közvetlenül nem alkalmazható, de egy kis átalakítás után igen. Például legyen $f(x) = x^4 + 1$, és számítsuk ki az $f(x+1)$ polinomot:

$$f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2\,.$$

Itt $p = 2$-vel már alkalmazható a kritérium, tehát $f(x+1)$ irreducibilis. De akkor f is az lesz, a következő gyakorlat állítása miatt.

3.5.5. Gyakorlat. Legyen f racionális együtthatós polinom. Mutassuk meg, hogy f akkor és csak akkor irreducibilis $\mathbb{Q}$ fölött, ha valamelyik eltoltja (vagyis az $f(x+c)$ polinom alkalmas $c \in \mathbb{Q}$-ra) irreducibilis $\mathbb{Q}$ fölött. Érvényes marad az állítás más testek fölött is? Mi a helyzet, ha az $x \to x + c$ helyettesítés helyett az $x \to ax + b$ helyettesítést hajtjuk végre, ahol $a \neq 0$?

3.5.6. Feladat. Legyen p prímszám és $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$. Mutassuk meg, hogy $f(x+1)$ teljesíti a Schönemann-Eisenstein kritérium feltételeit a p prímre, és így f irreducibilis $\mathbb{Q}$ fölött.

A következő gyakorlatban egy másik esetet látunk, amikor a polinom mod p vizsgálata segít az irreducibilitás eldöntésében.

3.5.7. Gyakorlat. Mutassuk meg, modulo 3 vizsgálódva, hogy $6x^4 + 3x + 1$ irreducibilis $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Vegyük észre, hogy noha az előző gyakorlatban szereplő $f(x) = 6x^4 + 3x + 1$ polinomra nem alkalmazható a Schönemann-Eisenstein kritérium, de ha f együtthatóit fordított sorrendben írjuk fel, akkor a kapott polinomra már igen. Ebből már következik az irreducibilitás, ennek megmutatása az előző gyakorlat megoldásának egyszerű általánosítása.

3.5.8. Gyakorlat [A fordított Schönemann-Eisenstein kritérium]. Tegyük föl, hogy f egy egész együtthatós, nem konstans polinom. Igazoljuk, hogy ha létezik olyan p prímszám, amelyre

(1) p nem osztja f konstans tagját;
(2) p osztja f összes többi együtthatóját;
(3) p^2 nem osztja f főegyütthatóját,

akkor f irreducibilis $\mathbb{Q}$ fölött.

A fordított Schönemann-Eisenstein kritérium egy másik bizonyításának is tekinthető az úgynevezett reciprok polinomokról szóló alábbi állítás.

3.5.9. Feladat. Legyen T test, és $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in T[x]$, ahol a_0 és a_n nem nulla. Legyen $g(x) = a_n + a_{n-1}x + \ldots + a_0 x^n$. Mutassuk meg, hogy

(1) A g polinom T-beli gyökei pontosan az f gyökeinek a reciprokai (multiplicitással számolva is).
(2) Az f akkor és csak akkor irreducibilis T felett, ha g az.

A g polinomot az f-hez tartozó *reciprok polinomnak* is nevezzük. Szokás azt is mondani, hogy f reciprok polinom, ha a hozzá tartozó reciprok polinom maga az f.

Még egy példát mutatunk arra, hogy egy polinom mod p és $\mathbb{Z}$ fölötti felbontásainak együttes vizsgálata hogyan döntheti el az irreducibilitás kérdését.

3.5.10. Példa. Mutassuk meg, hogy $f(x) = x^4 + x^2 + x + 1$ irreducibilis $\mathbb{Q}$ fölött.

Az f polinomot $\mathbb{Z}_2$ fölött szorzatra lehet bontani, az eredmény $(x+1)(x^3+x^2+1)$. Az x^3+x^2+1 irreducibilis $\mathbb{Z}_2$ fölött, hiszen harmadfokú, és nincsen $\mathbb{Z}_2$-ben gyöke. Vagyis a polinomunk $\mathbb{Z}_2$ fölött egy elsőfokú és egy harmadfokú irreducibilis szorzata lesz, és a felbontás egyértelműsége miatt $\mathbb{Z}_2$ fölött nem lehet két másodfokú polinom szorzatára bontani. Ezek szerint f-et $\mathbb{Z}$ fölött sem lehet két másodfokú szorzatára bontani (hiszen ha lenne ilyen felbontás, akkor azt vehetnénk modulo 2). Ha tehát $\mathbb{Z}$ fölött f nem irreducibilis, akkor csak egy első- és egy harmadfokú szorzatára lehet bontható. Az elsőfokú tényező racionális gyököt jelentene, ilyen azonban a racionális gyökteszt szerint nincsen (az 1 és a -1 ugyanis nem gyök). Ezért f irreducibilis $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Végül egy utolsó módszert mutatunk az irreducibilitás eldöntésére. Azért hagytuk a végére, mert csak ritkán alkalmazható, általában nagyon bonyolult számolásra vezet. A módszer abban áll, hogy a polinomot általános együtthatókkal bontjuk szorzatra, a szorzást elvégezve pedig az együtthatók összehasonlításával egy egyenletrendszert kapunk. Ennek az egyenletrendszernek a megoldásában néha számelméleti megfontolások is segítenek.

Példaként ismét a fenti $f(x) = x^4 + x^2 + x + 1$ polinomot választjuk. Ennek nincs racionális gyöke, tehát ha felbomlik, akkor csak két másodfokú polinom szorzat lehet:

$$x^4 + x^2 + x + 1 = (ax^2 + bx + c)(ux^2 + vx + w)\,,$$

ahol a, b, c, u, v, w-ről (a második Gauss-lemma miatt) feltehetjük, hogy egész számok. Beszorozva, és az együtthatókat összehasonlítva a következő egyenletrendszert kapjuk:

$$au = 1\,,\ av + bu = 0\,,\ aw + bv + cu = 1\,,\ bw + cv = 1\,,\ cw = 1\,.$$

Szerencsére ezt az egyenletrendszert könnyű megoldani. Mivel $au = 1$, csak $a = u = 1$ vagy $a = u = -1$ lehetséges, ahonnan a második egyenletből $v + b = 0$. Hasonlóképpen az utolsó két egyenletből $c = w = b + v = 1$ vagy $c = w = b + v = -1$ adódik, és ez lehetetlen, mert $b + v = 0$.

3.5.11. Gyakorlat. Felbonthatatlan-e $\mathbb{Z}[x]$-ben az $x^4 + x + 1$ polinom?

A `Maple` programban a `factor` parancs segítségével bonthatunk polinomokat irreducibilisek szorzatára.

Néhány módszer az irreducibilitás eldöntésére $\mathbb{Q}$ és $\mathbb{Z}$ fölött

(1) Egy nem konstans polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ fölött, ha irreducibilis $\mathbb{Q}$ fölött, és primitív.
(2) Ha egy egész együtthatós nem konstans polinom reducibilis $\mathbb{Q}$ fölött, akkor két alacsonyabb fokú *egész együtthatós* polinom szorzatára is felbontható.
(3) Ha egy legalább másodfokú polinomnak van racionális gyöke, akkor nem irreducibilis $\mathbb{Q}$ fölött. Egy másod- vagy harmadfokú polinom pontosan akkor irreducibilis $\mathbb{Q}$ fölött, ha nincs racionális gyöke (használjuk a racionális gyöktesztet). A racionális gyökök az elsőfokú tényezőknek felelnek meg.
(4) Bontsuk föl a polinomot $\mathbb{C}$ vagy $\mathbb{R}$ fölött, és használjuk a felbontás egyértelműségét (lásd a 3.3.11. Példát).
(5) A (fordított) Schönemann-Eisenstein kritérium.
(6) Egy $f \in \mathbb{Q}[x]$ polinom akkor és csak akkor irreducibilis $\mathbb{Q}$ fölött, ha egy eltoltja ($f(x+c)$, $c \in \mathbb{Q}$) az.
(7) Ha $f \in \mathbb{Z}[x]$, akkor vizsgáljuk modulo p, ahol p prímszám.
(8) Bontsuk föl a polinomot általános együtthatókkal, és oldjuk meg a kapott egyenletrendszert.
(9) Az úgynevezett *körosztási polinomok* irreducibilisek (ezekről a 3.9. Szakaszban lesz szó).
(10) Negyedfokú polinom esetében vizsgálhatjuk az úgynevezett harmadfokú rezolvenst (lásd 3.8.9. Feladat).

E módszereknek sokszor a kombinációja az, ami célhoz vezet. Az alábbi feladatokban néha csak annyi a nehézség, hogy megtaláljuk, milyen irányba induljunk el.

Gyakorlatok, feladatok

3.5.12. Gyakorlat. Az alább felsorolt polinomok közül melyekre alkalmazható közvetlenül a Schönemann-Eisenstein kritérium: $x^{11}+2x+18$, $x^{11}+2x+12$, $x^{11}+12x+5$, $x^{11}+24$, $x^{11}+72$. Mely n egészekre felel meg az $x^{11}+n$ polinom?

3.5.13. Gyakorlat. Irreducibilisek-e az alábbi polinomok?

(1) $\mathbb{C}$, illetve $\mathbb{R}$ fölött x^7+x+1, x^2-2, x^2+x+1.
(2) $\mathbb{Q}$ fölött $3x^7-6x^6+6x^2+3x-2$, $3x^7+x^6+6x^2+2x-2$, $3x^7-6x^6+6x^2+2x-2$, $x^{16}+1$, $x^{16}+2$, x^4-14x^2+9, x^4-x^2+1, $3x^7+6x-18$, x^5+4, x^3+9, x^3+3, $x^{10}-x^5+1$, $x^{10}+10$, x^4+25, x^4+2, x^4+4x+1, x^4-2x+1, $2x^4+2x^2+1$, $x^6-10x+10$, $x^4+x^3+x^2+1$.
(3) $\mathbb{Z}$ fölött $x^4+2x+27$, $3x^7+6x-18$, x^6+1, x^3+7x-3, $x^4+3x^3+x^2+1$.

3.5.14. Feladat. Van-e olyan $f(x)$ egész együtthatós polinom, hogy minden $g(x)$ egész együtthatós, nem konstans polinomra az $f\big(g(x)\big)$ polinom irreducibilis legyen $\mathbb{Q}$ fölött?

3.5.15. Feladat. Legyen $f(x, y) = x^9 + x^3y^3 + y^2 + y \in \mathbb{C}[x, y]$, és jelölje $\mathbb{C}(y)$ az $f(y)/g(y)$ alakú racionális törtfüggvényekből álló testet ($f, g \in \mathbb{C}[y]$).

(1) Primitív-e f, mint $\mathbb{C}[y]$ fölötti polinom?
(2) Következik-e a Schönemann-Eisenstein tételből, hogy f irreducibilis $\mathbb{C}(y)$ fölött?
(3) Irreducibilis-e f a $\mathbb{C}[x, y]$-ban?

3.5.16. Feladat. Annak felhasználásával, hogy $x^3 - 2$ irreducibilis $\mathbb{Q}$ fölött, mutassuk meg, hogy $\sqrt[3]{4}$ nem írható fel $a + b\sqrt[3]{2}$ alakban, ahol a és b racionális számok.

3.5.17. Feladat. Mutassuk meg, hogy van olyan (nem feltétlenül gyors vagy hatékony) eljárás, amellyel egy egész együtthatós polinom összes egész együtthatós osztóját meg lehet határozni (és így az is eldönthető, hogy a polinom irreducibilis-e $\mathbb{Z}$ illetve $\mathbb{Q}$ fölött).

3.6. A derivált és a többszörös gyökök

Aki tanult már analízist, az ismerheti a differenciálszámítás rendkívül hasznos apparátusát. Ha egy függvény, például a valós együtthatós

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

polinomhoz tartozó polinomfüggvény maximumát vagy minimumát akarjuk meghatározni, akkor elkészítjük ennek a függvénynek az úgynevezett *deriváltját*, amely a következő lesz:

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1 .$$

A derivált gyökei szoros kapcsolatban állnak az eredeti függvény szélsőértékeivel.

Mi nem a szélsőértékeket, hanem az f polinom többszörös gyökeit szeretnénk megkeresni. A derivált fogalma ehhez is segítséget nyújt, mert *az f többszörös gyökei a deriváltjának is gyökei lesznek.* Ahhoz, hogy ezt az állítást beláthassuk, a polinomot gyöktényezős alakban kellene felírni, és így deriválni. Szükségünk lenne tehát egy szabályra, amely megmondja, hogy szorzatot hogyan kell deriválni. Az analízis ebben is a segítségünkre van, hiszen az ismert Leibniz-szabály szerint

$$(fg)' = f'g + fg'$$

teljesül tetszőleges f és g polinomfüggvényekre (sőt általában differenciálható függvényekre is). Ennek alapján például ha f-nek az 1 legalább háromszoros gyöke, vagyis ha

$$f(x) = (x-1)^3 g(x) ,$$

akkor

$$f'(x) = \big((x-1)^3\big)' g(x) + (x-1)^3 g'(x) .$$

Könnyű látni, hogy $(x-1)^3$ deriváltja $3(x-1)^2$, és így f'-ből kiemelhető $(x-1)^2$. Vagyis az 1 szám az f deriváltjának legalább kétszeres gyöke lesz.

Nagyon fontos észrevennünk a következőt. A deriváltat ugyan folytonossági megfontolásokkal származtatják, de a fenti gondolatmenetben a deriválásnak csak a számolási szabályait használtuk! Reménykedhetünk hát, hogy a fenti számolást ki lehet terjeszteni a valós helyett például véges testekre is, ahol a folytonossági megfontolások hasznavehetetlenek, de a számolási szabályok esetleg érvényesek maradnak. Így apparátust kapnánk tetszőleges test fölött a többszörös gyökök vizsgálatára. Most ezt az ötletet fogjuk kivitelezni.

3.6.1. Definíció. Legyen R szokásos gyűrű, és

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

egy $R[x]$-beli polinom. Ekkor f *formális deriváltján* az

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$$

polinomot értjük.

Láthatjuk, hogy immáron nem a polinomfüggvényeket, hanem magukat a polinomokat deriváljuk. A képletben szereplő együtthatókat, például na_n-et úgy kell érteni, hogy az a_n elemet n példányban önmagával összeadjuk (egy gyűrűelem egész számszorosát a 2.2.17. Definícióban, illetve az azt követő megjegyzésekben értelmeztük, amikor a hatvány, illetve többszörös általános fogalmáról volt szó).

3.6.2. Állítás. *Ha R szokásos gyűrű, akkor tetszőleges $f, g \in R[x]$ polinomokra érvényesek az alábbi deriválási szabályok.*

(1) $(f+g)' = f' + g'$.
(2) $(fg)' = f'g + fg'$, *speciálisan* $(cf)' = cf'$ *minden* $c \in R$ *esetén (hiszen* $c' = 0$*).*
(3) $f\big(g(x)\big)' = f'\big(g(x)\big)g'(x)$ *(láncszabály).*

Ezeknek a szabályoknak az igazolása úgy történhet, hogy az f és g polinomokat általános együtthatókkal írjuk fel, és a bizonyítandó azonosság mindkét oldalát kiszámoljuk. A számolásban néha segít, ha f vagy g foka szerinti indukciót alkalmazunk. A részletek kidolgozását az Olvasóra hagyjuk.

Az igazi matematikust nem elégíti ki, ha a fenti szabályokat számolással kihozza, tudni szeretné azt is, hogy ezek az analízisben tanult (és az ottani módszerekkel sokkal elegánsabban bizonyított) szabályok miért maradnak meg tetszőleges gyűrű fölött is. Egy lehetséges magyarázat szerepel Fried Ervin [**12**] könyvében (I. rész, 4.3. Fejezet). Röviden a következőről van szó.

Amikor a deriváltat képezzük, akkor az f függvény görbéjét egy rögzített b pont kis környezetében egy $y = cx + d$ egyenessel akarjuk közelíteni (és $f'(b)$ ennek az egyenesnek az iránytangense, vagyis c lesz). Azt akarjuk, hogy a kettő „egymáshoz simuljon". Ha például $b = 0$, akkor

$$f(x) - (cx + d)$$

kell, hogy „kis" x-ekre az x-hez képest „nagyon kicsi" legyen. Ha

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots ,$$

akkor

$$f(x) - (cx + d) = (a_0 - d) + (a_1 - c)x + a_2x^2 + \dots .$$

Ez akkor lesz „elég kicsi" x-hez képest, ha $a_0 = d$ és $a_1 = c$, vagyis ha ebben a különbségben már csak csupa x^2-tel osztható tag szerepel (ez az egyenessel elérhető legjobb közelítés). Ezért lesz tehát $f'(0) = a_1$.

Ha a b pont tetszőleges, akkor a változót $b + x$ alakban érdemes felírni, tehát a fenti képlet úgy módosul, hogy az

$$f(b + x) - \big(c(b + x) + d\big)$$

kifejezésről (mint x polinomjáról) követeljük meg, hogy „kis" x-ekre az x-hez képest „nagyon kicsi" legyen, azaz hogy ne legyen benne se konstans tag, se x-es tag, vagyis osztható legyen x^2-tel. Innen ismét kiszámítható az $f'(b) = c$ értéke. Ez már tisztán algebrai átfogalmazás, hiszen nincsen benne szó közelítésről, kicsi és nagy számokról, hanem csak polinomok oszthatóságáról, és így elmondható általános gyűrű fölött is. Az érdeklődő Olvasó Fried Ervin idézett könyvében elolvashatja, hogy ez az átfogalmazott definíció hogyan vezet el a deriválás tulajdonságainak elegáns bizonyításához.

3.6.3. Állítás. *Legyen R szokásos gyűrű, $b \in R$, és tegyük fel, hogy b az $f \in R[x]$ polinomnak legalább k-szoros gyöke. Ekkor b az f deriváltjának legalább $k - 1$-szeres gyöke.*

Bizonyítás. Ez a már bemutatott számolás könnyű általánosítása. Mivel b legalább k-szoros gyök, f felírható

$$f(x) = (x - b)^k q(x)$$

alakban, ahol $q \in R[x]$. Deriválva

$$f'(x) = \big((x - b)^k\big)' q(x) + (x - b)^k q'(x) .$$

A láncszabály szerint $(x - b)^k$ deriváltja $k(x - b)^{k-1}$ (hiszen a belső $x - b$ polinom deriváltja 1). Ezért $(x - b)^{k-1}$ tényleg osztója f deriváltjának. □

A számolást folytatva

$$f'(x) = (x - b)^{k-1}\big[kq(x) + (x - b)q'(x)\big] .$$

Tegyük föl, hogy b pontosan k-szoros gyöke f-nek, azaz $q(b) \neq 0$. A szögletes zárójelben lévő polinomba $x = b$-t helyettesítve a második tag eltűnik (azaz nullává válik), és az eredmény $kq(b)$ lesz. Azt gondolhatnánk, hogy $k \neq 0$ esetén $kq(b)$ sem lesz nulla, és így b pontosan $k - 1$-szeres gyöke f'-nek. A valós számok teste fölött ez biztosan így is van. A következő példa azonban óvatosságra int.

Kérdés. Legyen $f(x) = x^3 + x^2$ a $\mathbb{Z}_2$ fölött. Hányszoros gyöke ennek a nulla? És a deriváltjának hányszoros gyöke a nulla?

Válasz: mivel $x^3 + x^2 = x^2(x + 1)$ és itt 0 már nem gyöke az $x + 1$-nek, ezért a nulla pontosan kétszeres gyök. A polinom deriváltja $3x^2 + 2x$. Itt a 2 együtthatót úgy kell érteni, hogy az x^2 eredeti együtthatóját, ami 1, kétszer összeadjuk önmagával. De a $\mathbb{Z}_2$ testben $1 + 1 = 0$. Ezért f deriváltja $3x^2 = x^2$ lesz. Ennek pedig a nulla szintén kétszeres gyöke!

Érdemes összevetni a fentieket a 3.3.17. Gyakorlat megoldásában fellépő $(x+1)^2 = x^2+1$ összefüggéssel. Az $(x+1)^2$ kiszámításakor nem lép fel a 2 szám: az x-es tag együtthatója $1 +_2 1 = 0$ lesz. Ugyanakkor valakinek eszébe juthat, hogy az $(x+1)^2$ kiszámítására a 2.2.37. Gyakorlatban bizonyított binomiális tételt alkalmazza. Ekkor már a fent vizsgált jelenséggel szembesül, nevezetesen, hogy a $\mathbb{Z}_2[x]$ gyűrűben $2x = x + x = 0$.

A probléma oka tehát a következő: egy R nullosztómentes gyűrűben a $kq(b)$ igenis lehet nulla akkor is, ha sem k sem $q(b)$ nem nulla, hiszen k nem gyűrűelem, hanem egész szám! Például $\mathbb{Z}_2$-ben $2 \cdot 1 = 0$, noha a $2 = 1 + 1$ egész szám nem nulla, és az $1 \in \mathbb{Z}_2$ sem nulla (de természetesen $1 +_2 1 = 0$). Most már megfogalmazhatjuk azt a feltételt, ami biztosítja, hogy f'-nek a b pontosan $k-1$-szeres gyöke legyen.

3.6.4. Tétel. *Legyen R szokásos gyűrű, $b \in R$, és tegyük fel, hogy b az $f \in R[x]$ polinomnak pontosan k-szoros gyöke ($k \geq 1$ egész). Ekkor b az f deriváltjának legalább $k-1$-szeres gyöke. Ha az R gyűrű tetszőleges r elemére teljesül, hogy $kr = 0$-ból $r = 0$ következik, akkor b az f deriváltjának pontosan $k-1$-szeres gyöke.* □

A tételbeli feltétel teljesül, ha $k = 1$ (és az R gyűrű tetszőleges). Ebben az esetben arról van szó, hogy b a deriváltnak nullaszoros gyöke, vagyis nem gyöke. *Ha tehát egy elem egy polinomnak pontosan egyszeres gyöke, akkor a deriváltjának biztosan nem gyöke.* A feltétel akkor is teljesül, ha R az egész, a racionális, a valós, vagy a komplex számok gyűrűje (és k tetszőleges). Erre a furcsa feltételre vissza fogunk térni később, amikor gyűrűk *karakterisztikájáról* lesz szó.

3.6.5. Következmény. *Legyen R szokásos gyűrű, és $f \in R[x]$. Ekkor az f polinom többszörös gyökei pontosan az f és f' közös gyökei.*

Bizonyítás. Ha $b \in R$ legalább kétszeres gyöke f-nek, akkor gyöke f'-nek is, és így közös gyöke f-nek és f'-nek. Megfordítva, ha b közös gyöke f-nek és f'-nek, akkor f-nek legalább kétszeres gyöke, hiszen ha csak egyszeres gyöke lenne, akkor az előző állítás szerint f'-nek nullaszoros gyöke lenne. □

Ha tehát az az (f, f') kitüntetett közös osztó létezik, akkor (a 3.2.13. Állítás szerint) ennek gyökei pontosan f többszörös gyökei. Így például test fölött a többszörös gyököket kereshetjük úgy, hogy az euklideszi algoritmussal kiszámítjuk f és f' kitüntetett közös osztóját. Speciálisan ha (f, f') konstans, akkor f-nek nincs többszörös gyöke. Vizsgálhatjuk azt is, hogy van-e f-nek legalább háromszoros, négyszeres, stb. gyöke, ha a második, harmadik, stb. deriváltakat tekintjük (lásd a 3.6.10. Gyakorlatot, és a 3.6.11. Feladatot).

Gyakorlatok, feladatok

3.6.6. Gyakorlat. Határozzuk meg az $x^6+x^5+5x^4+4x^3+8x^2+4x+4$ polinom többszörös komplex gyökeit.

3.6.7. Gyakorlat. Miért igaz, hogy $\mathbb{Z}_2$ fölött $3x^2 = x^2$? Miért nem mondhatjuk ugyanilyen alapon a következőt: „$\mathbb{Z}_2$ fölött $x^2 = x$, hiszen $\mathbb{Z}_2$ bármelyik elemét, azaz akár 0-t, akár 1-et helyettesítünk, az x^2 és az x ugyanazt az értéket veszi föl”?

3.6.8. Gyakorlat. Adjunk meg egy olyan polinomot egy alkalmas test fölött, melynek egy nyolcszoros gyöke a polinom deriváltjának is (pontosan) nyolcszoros gyöke.

3.6.9. Gyakorlat. Legyen f egy $\mathbb{C}$ fölötti polinom, és tegyük fel, hogy f'-nek egy $b \in \mathbb{C}$ szám pontosan $k-1$-szeres gyöke (ahol $k \geq 1$ egész). Igazoljuk, hogy ha b gyöke f-nek, akkor pontosan k-szoros gyöke. Igaz-e ez az állítás tetszőleges test fölött?

3.6.10. Gyakorlat. Mutassuk meg, hogy egy f polinom legalább k-szoros gyökei az f-nek és a $k-1$-edik deriváltjának közös gyökei. Igaz-e az állítás megfordítása?

3.6.11. Feladat. Legyen $f \in \mathbb{Q}[x]$ normált polinom, és $k \geq 1$ egész. Jelölje $g_k(x)$ azoknak az $x-b$ gyöktényezőknek a szorzatát, amelyre $b \in \mathbb{C}$ az f-nek pontosan k-szoros gyöke. Mutassuk meg, hogy g_k is racionális együtthatós.

3.6.12. Gyakorlat. Igazoljuk tetszőleges test fölött, hogy ha egy f polinomnak van többszörös tényezője (azaz g^2 alakú osztója, ahol g nem konstans polinom), akkor $(f, f') \neq 1$. Mely p prímekre igaz, hogy $x^n - 1$-nek van többszörös tényezője $\mathbb{Z}_p$ fölött?

3.6.13. Feladat. Lehet-e egy $\mathbb{Q}$, illetve $\mathbb{Z}_2$ fölött irreducibilis polinomnak többszörös gyöke egy nagyobb testben?

3.6.14. Gyakorlat. Legyen $f(x) = c(x-b_1)\dots(x-b_n)$, ahol $c \neq 0, b_1, \dots, b_n$ egy T test elemei. Mutassuk meg, hogy

$$f'(x) = \frac{f(x)}{x-b_1} + \dots + \frac{f(x)}{x-b_n},$$

és hogy $f'(b_i) = c(b_i-b_1)\dots(b_i-b_{i-1})(b_i-b_{i+1})\dots(b_i-b_n)$.

3.6.15. Feladat. Mutassuk meg, hogy ha $f \in \mathbb{C}[x]$ legalább másodfokú polinom, akkor van olyan $c \in \mathbb{C}$, melyre $f(x)+c$-nek van többszörös komplex gyöke.

3.6.16. Feladat. Igazoljuk, hogy egy n-edfokú, $\mathbb{C}$ feletti polinom, legfeljebb $n-1$ kivételes értéktől eltekintve, az értékkészletének minden elemét n különböző helyen veszi fel.

3.7. A rezultáns és a diszkrimináns

Noha hasznos ismereteket tartalmaz, ez és a következő szakasz egy kitérő azon az úton, amit ebben a könyvben be szeretnénk járni, nevezetesen, hogy eljussunk az absztrakt algebrai fogalmak mély megértéséhez. Ezért ez a két szakasz vázlatosabb az eddigieknél, és a könyv későbbi részének megértéséhez nem szükséges elolvasni őket. Aki mégis rászánja magát, annak azt javasoljuk, hogy ismételje át a determinánsok alaptulajdonságait, például Freud Róbert [**10**] könyve, és a függelékben található lineáris algebrai összefoglaló alapján.

A 3.2.13. Állítás szerint az f és g polinomok közös gyökeit úgy kereshetjük meg, hogy (például az euklideszi algoritmussal) meghatározzuk a kitüntetett közös osztójukat. Képzeljük el azonban, hogy f és g együtthatói egy t paramétertől függenek, és azt szeretnénk tudni, hogy milyen t értékek azok, amelyekre f-nek és g-nek *van* közös gyöke. Az euklideszi algoritmust ezzel az általános paraméterrel végigszámolni reménytelennek tűnik, és ezért jó lenne, ha föl tudnánk írni egy képletet f és g együtthatói segítségével, amely pontosan akkor nulla, ha f-nek és g-nek van közös gyöke. Ilyen képlet az f és g *rezultánsa*. Ez arra is alkalmas, hogy többismeretlenes egyenletrendszereket egyismeretlenesre vezessünk vissza.

3.7.1. Definíció. Legyen T test, és $f, g \in T[x]$, mégpedig

$$f(x) = a_n x^n + \ldots + a_0 \quad \text{és} \quad g(x) = b_m x^m + \ldots + b_0\,.$$

Az f és g *rezultánsa* az az $R(f, g)$-vel jelölt $(m+n) \times (m+n)$-es determináns, amit a következőképpen készítünk el. Az első sorba az $a_n, a_{n-1}, \ldots, a_0$ együtthatókat írjuk, majd csupa nullákat. A második sor első eleme nulla, ezután jönnek sorban $a_n, a_{n-1}, \ldots, a_0$, majd ismét csupa nulla. A harmadik sor elején már két nulla van. Ezt a lépcsőt összesen m soron át folytatjuk, ekkor az m-edik sorban a_0 lesz a legutolsó elem. Ezután ugyanezt az eljárást a maradék n sorban elvégezzük a $b_m, b_{m-1}, \ldots, b_0$ együtthatókkal is.

Példaként lássuk ezt a determinánst, amikor $n = 4$ és $m = 3$:

$$R(f, g) = \begin{vmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & b_3 & b_2 & b_1 & b_0 \end{vmatrix}$$

Annak magyarázata, hogy hogyan jut eszünkbe pont ezt a determinánst felírni, megtalálható Fried Ervin [**12**] könyvében (II. rész, 9.3. Fejezet).

Fontos megjegyeznünk, hogy a rezultáns definíciójában megengedtük azt az esetet is, hogy a_n (vagy b_m) nulla legyen. A rezultáns tehát nemcsak az f és g polinomoktól függ, hanem az n és m számoktól is, azaz attól, hogy hány nulla együtthatót írunk ki a polinom „tetejére". Emiatt a rezultáns $a_n = b_m = 0$ esetén is nulla lesz, nemcsak akkor, amikor a két polinomnak van közös gyöke. Az Olvasó joggal kérdezheti: mi értelme van annak, hogy „felesleges" nulla együtthatókat írjunk a determinánsba?

A válasz a következő: elképzelhető, hogy az a_n és b_m együtthatókról *nem tudjuk*, hogy nullával egyenlőek-e! Ha mondjuk a_n egy t paramétertől függő kifejezés, akkor kényelmetlen (sőt néha kivitelezhetetlen) lenne előbb megvizsgálni, hogy mely t értékekre lesz ez nulla, és attól függően más és más rezultánst fölírni. Sokkal egyszerűbb ezt a determinánst csak egyszer kiszámítani. Erre a jelenségre példát fogunk mutatni, amikor a rezultánst egy egyenletrendszer megoldására alkalmazzuk.

A rezultáns fő tulajdonságát a 3.7.4. Tételben mondjuk ki. A több lehetséges bizonyítás közül azt mutatjuk be, amely nagyon tanulságos absztrakt algebrai szempontból is.

3.7.2. Állítás. *Legyen T test, $f(x) = a_n x^n + \ldots + a_0$ és $g(x) = b_m x^m + \ldots + b_0$ a T fölötti polinomok. Tegyük fel, hogy $a_n \neq 0$ (azaz f nem nulla és foka n), továbbá, hogy f gyöktényezőkre bomlik T fölött. Legyenek f gyökei $\alpha_1, \ldots, \alpha_n \in T$ (mindegyiket annyiszor felsorolva, amennyi a multiplicitása). Ekkor*

$$R(f, g) = a_n^m g(\alpha_1) \ldots g(\alpha_n) .$$

Mint láttuk, a rezultáns felírásakor nemcsak az f és g polinomokat, hanem az n és m számokat is meg kell adni. A fenti állítást úgy értjük, hogy a rezultánsban szereplő n és m ugyanaz, mint az állításban szereplő n és m. Az állítás tehát nem marad igaz, ha az f polinom „tetejére" nulla együtthatókat írunk (és ennek megfelelően növeljük a determinánst). Ugyanezt a g-vel azonban büntetlenül megtehetjük, vagyis $b_m = 0$ is megengedett.

Bizonyítás. A feltétel szerint

$$f(x) = a_n(x - \alpha_1) \ldots (x - \alpha_n) .$$

A számolást célszerű úgy elvégezni (a bizonyítás során meglátjuk majd, miért), hogy az α_i, b_j, a_n konkrét T-beli elemek helyett határozatlanokkal számolunk. Ezért tekintsük az $R = T[u, v_0, \ldots, v_m, x_1, \ldots, x_n, y_1, \ldots, y_m]$ polinomgyűrűt, és $R[x]$-ben az

$$F(x) = u(x - x_1) \ldots (x - x_n) ,$$

valamint a

$$G(x) = v_m x^m + \ldots + v_0$$

polinomokat. Ha belátjuk, hogy $R(F, G) = u^m G(x_1) \ldots G(x_n)$, akkor innen az $x_i \mapsto \alpha_i$, $v_j \mapsto b_j$, $u \mapsto a_n$ helyettesítéssel az állítást kapjuk. Az $y_1, \ldots, y_m$ a számolás során használt segédváltozók lesznek.

Az $R(F, G)$ rezultáns definíciójában szerepelő determinánst szorozzuk meg jobbról a $V(y_1, \ldots, y_m, x_1, \ldots, x_n)$ Vandermonde-determinánssal (lásd A.5.2). A fent bemutatott $n = 4$ és $m = 3$ esetben tehát a következő determinánsról van szó:

$$\begin{vmatrix} y_1^6 & y_2^6 & y_3^6 & x_1^6 & x_2^6 & x_3^6 & x_4^6 \\ y_1^5 & y_2^5 & y_3^5 & x_1^5 & x_2^5 & x_3^5 & x_4^5 \\ y_1^4 & y_2^4 & y_3^4 & x_1^4 & x_2^4 & x_3^4 & x_4^4 \\ y_1^3 & y_2^3 & y_3^3 & x_1^3 & x_2^3 & x_3^3 & x_4^3 \\ y_1^2 & y_2^2 & y_3^2 & x_1^2 & x_2^2 & x_3^2 & x_4^2 \\ y_1 & y_2 & y_3 & x_1 & x_2 & x_3 & x_4 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{vmatrix}$$

A determinánsok szorzástételét (A.5.3. Tétel) alkalmazzuk, és ezért számítsuk ki a két mátrix szorzatát. Eredményként egy olyan mátrixot kapunk, amely négy részmátrixból

tehető össze. A bal felső sarokban egy $m \times m$-es M mátrix áll, amelyben az i-edik sor j-edik eleme $F(y_j)y_j^{m-i}$. Mellette jobbra egy $m \times n$-es részmátrix áll, melynek elemei $F(x_j)x_j^{m-i}$. Ezek az elemek nullával egyenlőek, hiszen $F(x_j) = 0$ az F definíciója miatt. A bal alsó sarokban egy $n \times m$-es részmátrix áll, melynek elemei $G(y_j)y_j^{n-i}$. Végül a jobb alsó sarokban álló $n \times n$-es N részmátrix elemei $G(x_j)x_j^{n-i}$. Az $n = 4$ és $m = 3$ esetben tehát a következő determinánst kapjuk:

$$\left|\begin{array}{ccc|cccc} F(y_1)y_1^2 & F(y_2)y_2^2 & F(y_3)y_3^2 & F(x_1)x_1^2 & F(x_2)x_2^2 & F(x_3)x_3^2 & F(x_4)x_4^2 \\ F(y_1)y_1 & F(y_2)y_2 & F(y_3)y_3 & F(x_1)x_1 & F(x_2)x_2 & F(x_3)x_3 & F(x_4)x_4 \\ F(y_1) & F(y_2) & F(y_3) & F(x_1) & F(x_2) & F(x_3) & F(x_4) \\ \hline G(y_1)y_1^3 & G(y_2)y_2^3 & G(y_3)y_3^3 & G(x_1)x_1^3 & G(x_2)x_2^3 & G(x_3)x_3^3 & G(x_4)x_4^3 \\ G(y_1)y_1^2 & G(y_2)y_2^2 & G(y_3)y_3^2 & G(x_1)x_1^2 & G(x_2)x_2^2 & G(x_3)x_3^2 & G(x_4)x_4^2 \\ G(y_1)y_1 & G(y_2)y_2 & G(y_3)y_3 & G(x_1)x_1 & G(x_2)x_2 & G(x_3)x_3 & G(x_4)x_4 \\ G(y_1) & G(y_2) & G(y_3) & G(x_1) & G(x_2) & G(x_3) & G(x_4) \end{array}\right|$$

Mivel a jobb felső sarokban álló részmátrix mindegyik eleme nulla, ez a determináns az M és N részmátrixok determinánsainak a szorzata lesz (lásd A.5.4). Az M részmátrix oszlopaiból $F(y_j)$-t kiemelve a $V(y_1, \ldots, y_m)$ Vandermonde-determináns marad. Hasonlóan N oszlopaiból $G(x_j)$-t kiemelve $V(x_1, \ldots, x_n)$ marad. Mindezt összevetve

$$\begin{aligned} &R(F, G)V(y_1, \ldots, y_m, x_1, \ldots, x_n) = \\ &\quad = F(y_1) \ldots F(y_m)V(y_1, \ldots, y_m)G(x_1) \ldots G(x_n)V(x_1, \ldots, x_n)\,. \end{aligned}$$

Itt $F(y_i) = u(y_i - x_1) \ldots (y_i - x_n)$. A Vandermonde-determinánsok kifejtését beírva, és az $y_i - x_j$, $x_i - x_j$, $y_i - y_j$ nem nulla polinomokkal egyszerűsítve pontosan a bizonyítandó összefüggést kapjuk. Ez az egyszerűsítés megengedett, mert az R nullosztómentes (hiszen test fölötti polinomgyűrű). □

Most már világos, hogy miért kellett az α_i helyett határozatlanokkal számolni. Az ugyanis véletlenül megeshet, hogy f-nek van többszörös gyöke, és akkor $\alpha_i - \alpha_j$ nulla is lehet, amivel a fenti bizonyításban nem tudnánk egyszerűsíteni. A megfelelő $x_i - x_j$ polinom azonban nem a nulla polinom. A vele való egyszerűsítés ezért megengedett, és két egyenlő polinomot kapunk az egyszerűsítés után is. Ide helyettesítünk azután az x_i helyébe α_i-t. (Érdemes elolvasni mindezzel kapcsolatban a 2.5.15. Feladat (4)-es pontjának megoldását követő megjegyzéseket.)

3.7.3. Gyakorlat. Kihasználtuk-e valahol az előző bizonyításban, hogy $a_n \neq 0$? Adjunk példát arra, amikor az állítás $a_n = 0$ esetén nem marad igaz.

3.7.4. Tétel. *Legyenek $f(x) = a_nx^n + \ldots + a_0$, valamint $g(x) = b_mx^m + \ldots + b_0$ egy T test fölötti polinomok, melyek T fölött gyöktényezőkre bomlanak.*

(1) *Tegyük fel, hogy a_n és b_m egyike sem nulla, és így f és g gyöktényezős alakja felírható $f(x) = a_n(x-\alpha_1)\dots(x-\alpha_n)$ és $g(x) = b_m(x-\beta_1)\dots(x-\beta_n)$ alakban, ahol α_i, β_j a T test elemei. Ekkor*

$$R(f,g) = a_n^m g(\alpha_1)\dots g(\alpha_n) = a_n^m b_m^n \prod_{1\le i\le n}\prod_{1\le j\le m}(\alpha_i-\beta_j) = \\ = (-1)^{nm} b_m^n f(\beta_1)\dots f(\beta_m) = (-1)^{nm} R(g,f)\,.$$

(2) *Az $R(f,g)$ akkor és csak akkor nulla, ha vagy $a_n = b_m = 0$, vagy a két polinomnak van közös gyöke T-ben.*

Bizonyítás. Az (1) állítás első egyenlőségét már beláttuk az előző állításban. A második egyenlőség ebből azonnal látszik, ha g gyöktényezős alakjába behelyettesítünk. Ha mindegyik $\alpha_i - \beta_j$ szorzatot megfordítjuk, akkor összesen mn-szer váltottunk előjelet. Az f gyöktényezős alakjából tehát a harmadik egyenlőséget is megkapjuk. Innen az utolsó egyenlőség ismét az előző állításból következik, f és g szerepének megcserélésével.

Bizonyítsuk be most a (2) állítást. Három esetet különböztetünk meg.

Ha $a_n = b_m = 0$, akkor a rezultáns definíciójában a determináns első oszlopa nulla, és így a rezultáns is nulla. Ilyenkor tehát (2) igaz.

Ha $a_n \neq 0$, akkor alkalmazhatjuk a 3.7.2. Állítást, ami szerint

$$R(f,g) = a_n^m g(\alpha_1)\dots g(\alpha_n)\,.$$

Mivel $a_n \neq 0$, az $R(f,g)$ pontosan akkor lesz nulla, ha valamelyik α_i gyöke g-nek, tehát ha van közös gyök. Vagyis (2) ismét igaz.

Végül tegyük fel, hogy $b_m \neq 0$. Az f és g szerepének felcserélésével kapjuk, hogy $R(g,f)$ akkor és csak akkor nulla, ha a két polinomnak van közös gyöke. Vegyük észre azonban, hogy az $R(f,g) = (-1)^{nm}R(g,f)$ egyenlőség közvetlenül is világos, hiszen a determináns két sor cseréjekor előjelet vált. Ezért $R(f,g)$ és $R(g,f)$ ugyanakkor lesz nulla, és így (2) most is teljesül. □

A most bizonyított tétel akkor izgalmas, ha az f és g polinomoknak nem ismerjük a gyökeit. De mi a helyzet akkor, ha például racionális együtthatós polinomokról van szó, amelyeknek nincsen racionális gyöke? Mit mond róluk az, hogy a rezultánsuk nulla? Ebben az esetben a tételt a komplex számtestben érdemes alkalmazni (mert ott minden polinom gyöktényezős alakra bomlik), és azt kapjuk, hogy a két polinomnak van közös komplex gyöke. Később be fogjuk bizonyítani, hogy nemcsak a $\mathbb{Q}$, hanem minden test részteste egy olyan testnek, amelyben már minden polinomnak van gyöke. Ha a tételt erre a bővebb testre alkalmazzuk, akkor az alábbi következményt kapjuk.

3.7.5. Következmény. *Ha T test, akkor a T fölötti $a_nx^n+\dots+a_0$ és $b_mx^m+\dots+b_0$ polinomok rezultánsa akkor és csak akkor nulla, ha vagy $a_n = b_m = 0$, vagy a két polinomnak van közös gyöke egy alkalmas T-nél bővebb testben (aminek tehát T részteste).*

A rezultánsnak több alkalmazása is van. A szakasz végén megmutatjuk, hogyan lehet egyenletrendszereket megoldani a segítségével. Hasznos a rezultáns akkor is, ha egy polinom többszörös gyökeit akarjuk vizsgálni. Tudjuk, hogy egy f polinom többszörös gyökei az f-nek és a deriváltjának a közös gyökei, és így az $R(f, f')$ rezultáns akkor lesz nulla, ha a polinomnak van többszörös gyöke. Látni fogjuk azonban, hogy a következő eredmény akkor is hasznos információt nyújt a gyökökről, ha mindegyik csak egyszeres, például segít megállapítani egy valós együtthatós polinom valós gyökeinek a számát.

3.7.6. Tétel. *Legyen T test, és $f \in T[x]$. Tegyük fel, hogy $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$, ahol $c, \alpha_1, \dots, \alpha_n \in T$ és $c \neq 0$ az f főegyütthatója. Ekkor*

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} c^{2n-1} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 .$$

Bizonyítás. A 3.7.2. Állítás miatt

$$R(f, f') = c^{n-1} f'(\alpha_1) \dots f'(\alpha_n) .$$

A 3.6.14. Gyakorlat szerint

$$f'(\alpha_i) = c(\alpha_i - \alpha_1)\dots(\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1})\dots(\alpha_i - \alpha_n) .$$

Ezt az előző képletbe behelyettesítve, és az $\alpha_i - \alpha_j$ különbségek közül azokat megfordítva, ahol $i > j$, az állítást kapjuk. □

3.7.7. Definíció. Legyen T test, és az $f \in T[x]$ nem nulla polinom főegyütthatóját jelölje c. Ekkor a

$$\frac{(-1)^{\frac{n(n-1)}{2}} R(f, f')}{c}$$

kifejezést az *f diszkriminánsának* nevezzük.

Ha tehát f gyöktényezős alakja (akár egy bővebb testben) $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$, akkor diszkriminánsa a fenti tétel szerint

$$c^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 .$$

3.7.8. Következmény. *Ha T test, akkor egy T fölötti polinom diszkriminánsa akkor és csak akkor nulla, ha a polinomnak van többszörös gyöke egy alkalmas T-nél bővebb testben.*

Az $R(f, f')$ rezultánsnak vajon miért pont a $(-1)^{n(n-1)/2}/c$-szeresét választottuk f diszkriminánsának? A szakirodalom sem egységes ebben a tekintetben, a fenti választás mellett azonban több komoly érv szól. Egyrészt (az alábbi gyakorlat szerint) a másodfokú egyenlet esetében így vissza fogjuk kapni a megoldóképletbeli gyökjel alatti kifejezést, vagyis a diszkrimináns fogalma megegyezik a középiskolában megszokott szóhasználattal. Egy másik ok az, hogy a fenti szorzatformula szerint a diszkrimináns teljes négyzet (és így valós c és α_i esetén mindig nemnegatív), ennek jelentőségét az alább bizonyítandó állítás mutatja. Végül

nagyon fontos szempont, hogy a széles körben használt matematikai számítógépes programok (`Maple, Mathematica, Mupad`) szintén a fenti definíciót használják.

3.7.9. Állítás. *Ha f valós együtthatós nem nulla polinom, akkor a diszkriminánsa akkor és csak akkor pozitív, ha minden komplex gyöke egyszeres, és a nem valós komplex gyökeinek száma néggyel osztható.*

Bizonyítás. Legyenek $\alpha_1, \dots \alpha_n$ az f komplex gyökei, feltehetjük, hogy mindegyik egyszeres (különben a diszkrimináns nulla lesz, és az állítás igaz). Kiszámítjuk a rezultáns előjelét a fenti szorzatképlet alapján. Nyilván $c^{2n-2} > 0$. A szorzat további tagjai az $i < j$ számpárokhoz tartozó $(\alpha_i - \alpha_j)^2$ tényezők. Mivel f valós együtthatós, minden gyökének a konjugáltja is gyök. Ha tehát $\overline{\alpha_i} = \alpha_k$ és $\overline{\alpha_j} = \alpha_\ell$, akkor a szorzatban szerepel az $(\alpha_k - \alpha_\ell)^2$ tényező is ($k > \ell$ esetén $(\alpha_\ell - \alpha_k)^2$ formában). Ha az $\{i, j\}$ és $\{k, \ell\}$ számpárok különbözők, akkor ez két különböző tényező, és szorzatuk pozitív valós (hiszen egy számot a konjugáltjával szoroztunk össze). Ha viszont $\{i, j\} = \{k, \ell\}$, akkor vagy $i = k$ és $j = \ell$, vagy $i = \ell$ és $j = k$. Az első esetben α_i és α_j valós számok, és $(\alpha_i - \alpha_j)^2$ pozitív valós. A második esetben α_i és α_j egymás konjugáltjai. Ekkor $\alpha_i - \alpha_j$ tisztán képzetes szám, és így a négyzete negatív valós. A konjugált nem valós gyökpárok mindegyike tehát egy negatív valós számmal járul hozzá a fenti szorzathoz. Így a szorzat akkor és csak akkor lesz pozitív, ha ezeknek a gyökpároknak a száma páros. □

3.7.10. Gyakorlat. Legyen $f(x) = ax^2+bx+c$ másodfokú polinom. Mutassuk meg, hogy f diszkriminánsa $b^2 - 4ac$, vagyis a megoldóképletben a négyzetgyök alatt álló kifejezés. Az előző állítás alapján igazoljuk, hogy az f polinomnak akkor és csak akkor valósak a gyökei, ha a diszkriminánsa nemnegatív.

3.7.11. Gyakorlat. Legyen $f(x) = x^3 + px + q$. Mutassuk meg, hogy f diszkriminánsa $-27q^2 - 4p^3$, vagyis a Cardano-képletben a négyzetgyök alatt álló D kifejezés -108-szorosa.

3.7.12. Példa. Oldjuk meg az alábbi egyenletrendszert a rezultáns felhasználásával.

$$\left.\begin{aligned} yx^2 + y^2 - 2 = 0 \\ y^2x^2 + yx - 2 = 0 \end{aligned}\right\}$$

A megoldás során mindkét egyenlet bal oldalát x polinomjának képzeljük, és felírjuk a rezultánsukat. Az eredmény a következő lesz:

$$r(y) = \begin{vmatrix} y & 0 & y^2-2 & 0 \\ 0 & y & 0 & y^2-2 \\ y^2 & y & -2 & 0 \\ 0 & y^2 & y & -2 \end{vmatrix} = y^8 - 4y^6 + 5y^5 + 4y^4 - 10y^3 + 4y^2\,.$$

A rezultáns akkor és csak akkor nulla, ha vagy mindkét főegyüttható nulla, vagy a két polinomnak van közös gyöke. A két főegyüttható y, illetve y^2. Mindkettő akkor és csak akkor

nulla, ha $y = 0$. Az első egyenletből látszik, hogy erre az y-ra nincs megoldása az egyenletrendszernek. Tehát feltehetjük, hogy $y \neq 0$. Ebben az esetben az $r(y)$ polinom gyökei azok az y értékek, amelyekre az egyenletrendszer két egyenletének van (az x változóban) közös megoldása.

Normális körülmények között az $r(y)$ polinom gyökeit közelítő módszerekkel határoznánk meg. Most azonban szerencsénk van, mert ezt a polinomot viszonylag könnyű szorzattá alakítani. Az y^2 kiemelése után a racionális gyöktesztel megállapíthatjuk, hogy a racionális gyökei 1 és -2. A megfelelő gyöktényezők kiemelése után $y^4-y^3-y^2+4y-2$ marad, ami kis ügyeskedéssel két másodfokú polinom szorzatára bontható:

$$r(y) = y^2(y-1)(y+2)(y^2-2y+2)(y^2+y-1)\,.$$

Ha például $y = 1$, akkor az egyenletrendszer első egyenlete $x^2 - 1 = 0$, a második $x^2+x-2=0$ lesz. Ezek közös gyöke csak az $x = 1$. Ugyanilyen számolással kapjuk meg az $r(y)$ többi gyökéhez is a megfelelő x értékeket. Végeredményben az egyenletrendszer összes megoldása a következő hat (x, y) pár lesz:

$$(1,\,1)\,,\quad (1,\,-2)\,,\quad (-1+i,\,1+i)\,,\quad (-1-i,\,1-i)\,,$$
$$\left(\frac{\sqrt{5}+1}{2},\,\frac{\sqrt{5}-1}{2}\right),\quad \left(\frac{1-\sqrt{5}}{2},\,\frac{-1-\sqrt{5}}{2}\right). \quad \square$$

A rezultáns tehát alkalmas arra, hogy két egyenletből egy olyan csináljon, amelyben már eggyel kevesebb ismeretlen van. Ha kettőnél több ismeretlenünk vagy egyenletünk van, akkor a módszert többször egymás után kell alkalmazni.

Gyakorlatok, feladatok

3.7.13. Gyakorlat. A rezultáns módszerével vezessük vissza az alábbi három egyenletrendszert egyismeretlenes egyenletre, és oldjuk is meg őket $\mathbb{C}$ fölött.

$$\begin{cases} (x-1)\cdot y^2+(x+1)\cdot y-2=0 \\ (x-1)\cdot y^2+\qquad x\cdot y-1=0 \end{cases} \qquad \begin{cases} (x-1)\cdot y^2+(x+1)\cdot y-1=0 \\ (x-1)\cdot y^2+\qquad x\cdot y-1=0 \end{cases}$$

$$\begin{cases} x^2 = y+z+1 \\ y^2 = z+x+1 \\ z^2 = x+y+1 \end{cases}$$

3.8. A harmad- és negyedfokú egyenlet

A harmadfokú egyenlet megoldási ötletéről és a Cardano-képletről már volt szó a komplex számok bevezetése kapcsán, de számos kérdés nyitva maradt. Azóta felépítettük azokat az eszközöket, amelyekkel a témát lezárhatjuk (de a 6.10. Szakaszban, mélyebb eszközök

birtokában, még egyszer visszatérünk rá). A tárgyalás az előző szakaszhoz hasonlóan kissé vázlatos lesz, és csak arra az esetre szorítkozunk, amikor az egyenlet együtthatói komplex számok. Először röviden átismételjük, hogy meddig is jutottunk el az 1.2. Szakaszban.

Az általános harmadfokú egyenlet megoldásának kérdését visszavezettük arra az esetre, amikor az egyenlet

$$x^3 + px + q = 0$$

alakú. Megmutattuk, hogy ha u és v olyan számok, melyekre $uv = -p/3$ és $u^3+v^3 = -q$, akkor az $u + v$ szám biztosan megoldása az egyenletnek. Ezt az egyenletrendszert úgy próbáltuk megoldani, hogy az első egyenletet köbre emeltük. Ekkor az $s = u^3$ és $t = v^3$ értékekre

$$s = -\frac{q}{2} + \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \quad \text{és} \quad t = -\frac{q}{2} - \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

adódott. Ezekre az s és t számokra tehát $s + t = -q$ és $st = (-p/3)^3$ teljesül. Innen u-t és v-t köbgyökvonással akartuk meghatározni, és eredményül a Cardano-képletet kaptuk:

$$x = u + v = \sqrt[3]{s} + \sqrt[3]{t} = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\,.$$

Ezzel a képlettel több probléma is van. Nem mutattuk meg, hogy az egyenlet mindegyik megoldása megkapható ebből a képletből, és azt sem, hogy a képlet által adott szám megoldása az egyenletnek. Ennél súlyosabb probléma, hogy a képlet nem is egyértelmű, hiszen tudjuk, hogy egy nem nulla komplex számnak három különböző köbgyöke van. A képletet tehát elvileg $3 \cdot 3 = 9$-féle módon értékelhetjük ki.

Annyit azért tisztáztunk az 1.2.4 és az 1.2.10 gyakorlatok megoldása során, hogy a képletben (vagyis az s és t kifejezésekben) szereplő két négyzetgyököt úgy kell választani, hogy egymás ellentettjei legyenek. (Vigyázzunk, komplex számok esetén egy számnak két egyenrangú négyzetgyöke van, nincs közöttük kitüntetett, nem mondhatunk olyat, mint valósban, hogy a négyzetgyök mindig a nemnegatív értéket jelöli, lásd az 1.2.11. Gyakorlat megoldását). Ha ezt a két négyzetgyököt a képletben megcseréljük, akkor u és v kicserélődik, de $u+v$ nem változik meg.

3.8.1. Tétel. *Ha a Cardano-képletben szereplő u és v köbgyököket úgy választjuk, hogy szorzatuk $-p/3$ legyen, akkor a képlet az egyenlet megoldását szolgáltatja, és az egyenlet mindegyik megoldása megkapható ezen a módon.*

Bizonyítás. Bárhogyan is választjuk ki az u és v köbgyököket, $u^3 + v^3 = s + t = -q$ és $u^3v^3 = st = (-p/3)^3$ biztosan teljesülni fog. Ha $uv = -p/3$ is teljesül, akkor az imént felidézett állítás szerint $x = u + v$ tényleg megoldása az egyenletnek. Meg kell még mutatnunk, hogy az egyenlet mindegyik megoldása megkapható a képletből. Egyúttal gyakorlati útmutatót is adunk a képlet használatára.

Válasszuk külön azt az esetet, amikor $p = 0$. Ebben az esetben az egyenlet az $x^3+q = 0$ alakot ölti, megoldásai tehát a $-q$ szám köbgyökei, és ezért nem érdemes a képletet használni. Meg kell azonban mutatnunk, hogy a képlet ebben az esetben is kiadja az egyenlet megoldásait. Amikor behelyettesítünk, akkor a $(-q/2)^2$ számból kell négyzetgyököt vonni, ennek értékei $-q/2$ és $q/2$. Ha az s kifejezésben választjuk a $-q/2$, a t kifejezésben pedig a $q/2$ értéket, akkor $s = u^3 = -q$ és $t = v^3 = 0$ adódik. Így $v = 0$, és u a $-q$ szám valamelyik köbgyöke. Ezek szorzata tényleg $p/3 = 0$, és így a képlet tényleg kiadja az egyenlet megoldásait.

Tegyük most föl, hogy $p \neq 0$. Megmutatjuk, hogy u-nak szabad az s kifejezés *bármelyik* köbgyökét választani, a $v = -p/3u$ választás a t kifejezés egyik köbgyökét fogja eredményezni (és így az egyenletnek az egyik megoldását kapjuk). Tudjuk, hogy $st = (-p/3)^3$ (speciálisan s, és így u sem nulla). Ha tehát $u^3 = s$, akkor innen

$$v^3 = (-p/3u)^3 = (-p/3)^3/u^3 = st/s = t\,.$$

Tehát tényleg választhatjuk u-nak az s szám bármelyik köbgyökét.

Legyen az s három köbgyöke u_1, u_2, u_3, ekkor $v_i = -p/3u_i$ is kiadja a t szám három köbgyökét (hiszen három különböző számról van szó). Azt kell még megmutatni, hogy $u_i + v_i$ az egyenlet összes megoldása, azaz hogy

$$f(x) = x^3 + px + q = (x - u_1 - v_1)(x - u_2 - v_2)(x - u_3 - v_3)\,.$$

Ezzel valójában többet bizonyítunk: azt is megmutatjuk, hogy ha az f polinomnak vannak többszörös gyökei, akkor a Cardano-képletet az imént leírt módon használva minden gyököt annyiszor kapunk meg, amennyi a multiplicitása. A közvetlen beszorzás helyett rövidebb utat választunk.

Legyen $\alpha_i = u_i + v_i$, tudjuk, hogy ezek gyökei f-nek. Tegyük föl, hogy az α_i számok között van két különböző, mondjuk $\alpha_1 \neq \alpha_2$. Az f polinomban nem szerepel x^2-es tag, ezért gyökeinek összege nulla, és így harmadik gyöke csak $-\alpha_1 - \alpha_2$ lehet. Azt kell tehát belátni, hogy $-\alpha_1 - \alpha_2 = \alpha_3$. De ez igaz, mert egy komplex szám három köbgyökének az összege nulla, és így $u_1 + u_2 + u_3 = 0$, $v_1 + v_2 + v_3 = 0$, vagyis $\alpha_1 + \alpha_2 + \alpha_3 = 0$. Ebben az esetben tehát készen vagyunk.

Ha az α_i számok mindhárman egyenlők, akkor, mivel összegük nulla, mindegyik nulla kell, hogy legyen. Így $u_i = -v_i = p/3u_i$, azaz $u_i^2 = p/3$. Ez lehetetlen, mert a $p/3$-nak csak két négyzetgyöke lehet, az u_1, u_2, u_3 pedig (a most vizsgált $p \neq 0$ esetben) páronként különböző. Ez az ellentmondás bizonyítja az állítást. (Az Olvasó meggondolhatja, hogy a három α_i valójában csak a $p = q = 0$ esetben lehet egyenlő.) □

3.8.2. Tétel. *A komplex együtthatós $f(x) = x^3 + px + q$ polinomnak akkor és csak akkor van többszörös komplex gyöke, ha a Cardano-képletben a négyzetgyökjel alatt álló*

$$D = \left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$$

kifejezés nulla. Ha a p és q együtthatók valósak, akkor $D \leq 0$ esetén mindegyik gyök valós, $D > 0$ esetén pedig egy valós gyök van, a másik két komplex gyök pedig egymás konjugáltja.

Bizonyítás. A 3.7.11. Feladatban kiszámoltuk, hogy az f polinom diszkriminánsa $-108D$. Ez akkor és csak akkor nulla, ha $D = 0$, ami az első állítást bizonyítja (hiszen a diszkrimináns akkor tűnik el, ha van többszörös gyök).

Tegyük fel, hogy p és q valós. Ha a polinomnak van nem valós gyöke, akkor ennek konjugáltja is gyök, a harmadik gyök pedig valós, ebben az esetben tehát három különböző gyök van. A nem valós gyökök száma 2, ami nem osztható néggyel, tehát a 3.7.9. Állítás szerint ilyenkor f diszkriminánsa, azaz $-108D$ negatív, tehát $D > 0$. A másik lehetőség az, ha három valós gyök van. Ekkor a nem valós gyökök száma nulla, ami néggyel osztható szám, és így a 3.7.9. Állítás szerint f diszkriminánsa, azaz $-108D$ nulla vagy pozitív, vagyis $D \leq 0$. □

Ez az eredmény megerősíti azt az anomáliát, amit konkrét példákon már megismertünk az 1.2. Szakaszban. Ha $D > 0$, akkor az egyetlen valós gyököt csak valósban számolva megadja a Cardano-képlet. Ha azonban három valós gyök van, akkor a Cardano-képletben negatív számból kell négyzetgyököt vonni, tehát ha komplex számokat nem használhatunk, akkor a képlet az egyenlet egyik gyökét sem adja meg! A régiek, akik még nem ismerték a komplex számokat, ezt *Casus irreducibilisnek*, megoldhatatlan esetnek nevezték.

A helyzet valójában még rosszabb: nemcsak a Cardano-képlettel, hanem *semmilyen más, a négy alapműveletet és valósban maradó akárhányadik gyökvonásokat tartalmazó, akármilyen bonyolult képlettel sem lehet általában kiszámítani a harmadfokú egyenlet gyökeit akkor, ha három valós gyök van.* Ez a tétel a Galois-elmélet eszközeivel bizonyítható (lásd 6.10.2. Tétel). Az általános ötöd- (és magasabb) fokú egyenletet már komplex gyökvonások segítségével sem lehet általában megoldani, ezekre már nem létezik olyan megoldóképlet, amely az együtthatókból kiindulva a négy alapműveletet és az akárhányadik gyökvonásokat használja. Erről a 6.9. Szakaszban lesz szó.

Természetesen mérnöki számításokhoz már a harmadfokú egyenletet sem a megoldóképlettel érdemes megoldani, hanem közelítő módszerekkel. A közelítő módszerek azonban nem minden probléma megoldására alkalmasak. Ha például azt kell eldönteni, hogy van-e többszörös gyök, akkor a fenti elméletre, azaz a diszkrimináns vizsgálatára van szükség.

Ám egy olyan elméleti problémát, hogy létezik-e megoldóképlet, nem a gyakorlati alkalmazások miatt érdemes vizsgálni. Mint a könyv bevezetésében is írtuk, a matematikában általában nem lehet előre tudni, hogy mely kérdések a fontosak, mert ehhez nem vagyunk eléggé okosak. A gyökképletek vizsgálata elsősorban azért fontos, mert ez vezetett el az absztrakt algebra kifejlődéséhez.

3.8.3. Gyakorlat. Mutassuk meg, hogy a $px^2 + qx + r \in \mathbb{C}[x]$ polinom akkor és csak akkor négyzete egy $\mathbb{C}[x]$-beli polinomnak, ha $q^2 - 4pr = 0$ (itt $p = 0$ is megengedett, amikor $q^2 - 4pr = 0$ ekvivalens azzal, hogy $q = 0$). Mi a helyzet $\mathbb{Q}$ fölött?

3.8.4. Tétel. *Az általános negyedfokú komplex együtthatós polinomok gyökeit megkaphatjuk az együtthatókból a négy alapművelet és a gyökvonás segítségével.*

Bizonyítás. A negyedfokú egyenlet megoldóképlete annyira bonyolult, hogy nem szokás és érdemes felírni, hanem inkább egy módszert mutatunk a gyökök meghatározására. Csak a megoldás ötletét mutatjuk be, a diszkussziót a feladatokra és a 6.10. Szakaszra hagyjuk.

A főegyütthatóval leosztva az egyenlet a következő alakú lesz:

$$f(x) = x^4 + ax^3 + bx^2 + cx + d = 0\,.$$

A tervünk az, hogy f-et két másodfokú polinom szorzatára bontsuk, mert akkor már könnyű megkeresni a gyökeit. Ehhez egy harmadfokú egyenletet kell majd megoldanunk. A két másodfokú tényezőt $K+L$ és $K-L$ alakban keressük, az egyenletet tehát két négyzet különbségeként akarjuk felírni. A $K(x)$ polinomot

$$K(x) = x^2 + \frac{a}{2}x + u$$

alakban érdemes keresni (az x-es tag együtthatóját azért választjuk $a/2$-nek, hogy K^2-ben az x^3 együtthatója ugyanaz legyen, mint f-ben). Ekkor könnyű számolással adódik, hogy

$$f(x) = K(x)^2 - \left(\left(2u + \frac{a^2}{4} - b\right)x^2 + \left(au - c\right)x + \left(u^2 - d\right)\right)\,.$$

A zárójelben álló polinom akkor lesz egy $L(x)$ polinom négyzete, ha a diszkriminánsa nulla (3.8.3. Gyakorlat), azaz

$$(au - c)^2 - (8u + a^2 - 4b)(u^2 - d) = 0\,.$$

Ezt az u-ban harmadfokú g polinomot az f *harmadfokú rezolvensének* nevezzük. A kapott egyenletet u-ra megoldjuk, és így elvégezhetjük az f szorzatra bontását. □

Természetesen az f polinomban az $x = y - a/4$ helyettesítéssel eltűnik a harmadfokú tag (és ez a helyettesítés az irreducibilitást sem érinti a 3.5.5. Gyakorlat miatt). Vagyis feltehetjük, hogy $a = 0$, ekkor a harmadfokú rezolvens a

$$g(u) = 8u^3 - 4bu^2 - 8du + (4bd - c^2)$$

alakot ölti.

Gyakorlatok, feladatok

3.8.5. Gyakorlat. Oldjuk meg az alábbi egyenleteket a komplex számok között.

(1) $x^3 - 6ix - i + 8 = 0$.
(2) $x^3 + 12x - 16i = 0$.
(3) $x^3 - 21x + 20 = 0$.
(4) $x^4 + x^2 + 4x - 3 = 0$.

3.8.6. Gyakorlat. Keressük meg a 3.3.20. Feladatban vizsgált $f(x) = x^4 - 10x^2 + 1$ polinom harmadfokú rezolvensének mindhárom gyökét. Hogyan változik f felbontása két másodfokú szorzatára, ha a rezolvensnek más-más gyökét használjuk?

3.8.7. Feladat. Legyen $f(x) = x^4+ax^3+bx^2+cx+d = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$, ahol $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ komplex számok. Igazoljuk az alábbi állításokat.

(1) Az f harmadfokú rezolvense $g(x) = 8(x - u_1)(x - u_2)(x - u_3)$, ahol
$$u_1 = \frac{\alpha_1\alpha_2 + \alpha_3\alpha_4}{2}, \quad u_2 = \frac{\alpha_1\alpha_3 + \alpha_2\alpha_4}{2}, \quad u_3 = \frac{\alpha_1\alpha_4 + \alpha_2\alpha_3}{2}.$$
(2) Tegyük föl, hogy a 3.8.4. Tétel bizonyításában az $u = u_1$ gyököt használjuk. Ekkor az f polinom másodfokúakra történő felbontásának tényezői $(x - \alpha_1)(x - \alpha_2)$ és $(x - \alpha_3)(x - \alpha_4)$ lesznek.
(3) $2u_1 - b + a^2/4 = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2/4$.
(4) $c - au_1 = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)(\alpha_1\alpha_2 - \alpha_3\alpha_4)/2$.
(5) $u_1^2 - d = (\alpha_1\alpha_2 - \alpha_3\alpha_4)^2/4$.
(6) Ha $\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4 = 0$, akkor $u_1^2 - d = (\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2/4$.

3.8.8. Feladat. Egy negyedfokú polinomnak négy gyöke van, ezek háromféleképpen állíthatók párba, és így háromféle felbontása van két másodfokú szorzatára. Igazoljuk a 3.8.6. Gyakorlat általánosításaként, hogy ez a három párba állítás a harmadfokú rezolvens három gyökéből kapható, a negyedfokú egyenlet megoldásában leírt módszerrel.

3.8.9. Feladat. Legyen $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ és g az f harmadfokú rezolvense. Igazoljuk, hogy f pontosan akkor reducibilis $\mathbb{Q}$ fölött, ha az alábbi három eset valamelyike fennáll.

(1) Az f-nek van racionális gyöke.
(2) A g-nek van olyan u (racionális) gyöke, melyre $2u - b + a^2/4$ egy nem nulla racionális szám négyzete.
(3) Az $u = b/2-a^2/8$ számra $au = c$ teljesül, és u^2-d egy racionális szám négyzete.

Mutassuk meg, hogy a (2) és (3) esetben f felbomlik két másodfokú, racionális együtthatós polinom szorzatára. Igazoljuk azt is, hogy ha $a = 0$, akkor a (3) feltétel így fogalmazható: $c = 0$ és $\sqrt{b^2 - 4d} \in \mathbb{Q}$.

3.8.10. Gyakorlat. Legyen $f(x) = x^4 + bx^2 + d \in \mathbb{Q}[x]$. Mutassuk meg a következő állításokat.

(1) Az f harmadfokú rezolvensének gyökei $b/2$ és $\pm\sqrt{d}$.
(2) Az f pontosan akkor reducibilis $\mathbb{Q}$ fölött, ha a $b^2 - 4d$, $2\sqrt{d} - b$, $-2\sqrt{d} - b$ számok valamelyike egy racionális szám négyzete.

A (2) ponthoz tartozó mindhárom esetben adjuk is meg f felbontását két másodfokú polinom szorzatára.

3.8.11. Gyakorlat. Az előző gyakorlat mely esetébe tartozik az $x^4 - 2$, az $x^4 + 4$, és a 3.8.6. Gyakorlatban vizsgált $x^4 - 10x + 1$ polinom?

3.8.12. Feladat. Legyen $f(x)$ páratlan fokú reciprok polinom (lásd 3.5.9. Feladat). Mutassuk meg, hogy f-nek gyöke a -1. Vezessük vissza az $x^7 + 2x^6 - x^4 - x^3 + 2x + 1 = 0$ egyenletet legfeljebb negyedfokú egyenletre.

3.8.13. Feladat. Oldjuk meg az $x^8 + 2x^2 + 4x + 2 = 0$ egyenletet.

3.9. A körosztási polinom

Ebben a szakaszban speciális, konkrét polinomokról lesz szó: azokról, amelyeknek a gyökei pontosan az n-edik primitív egységgyökök. Ezek természetesen adódnak, amikor az $x^n - 1$ polinomot irreducibilisek szorzatára bontjuk $\mathbb{Z}$ fölött. Fel fogjuk őket használni a geometriai szerkeszthetőség elméletében is. Az alábbiak elolvasása előtt érdemes átismételni a komplex egységgyökökről és a rendjeikről tanult állításokat.

3.9.1. Definíció. Ha $n \geq 1$ egész, akkor Φ_n jelöli az *n-edik körosztási polinomot*, vagyis azt a normált polinomot, melynek gyökei pontosan a primitív n-edik egységgyökök (mindegyik egyszeres). Képletben:

$$\Phi_n(x) = (x - \xi_1) \dots (x - \xi_{\varphi(n)}) ,$$

ahol $\xi_1, \dots, \xi_{\varphi(n)}$ az összes primitív n-edik egységgyök, vagyis az összes n-edrendű komplex szám.

Látjuk, hogy Φ_n foka $\varphi(n)$. A definíciót kis n számok esetén közvetlenül felhasználhatjuk a körosztási polinomok kiszámítására. Nyilván

$$\Phi_1(x) = x - 1 \quad \text{és} \quad \Phi_2(x) = x - (-1) = x + 1 .$$

A negyedik egységgyökök (1, -1, i és $-i$) közül az i és a $-i$ negyedrendű, azaz primitív, és ezért

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1 .$$

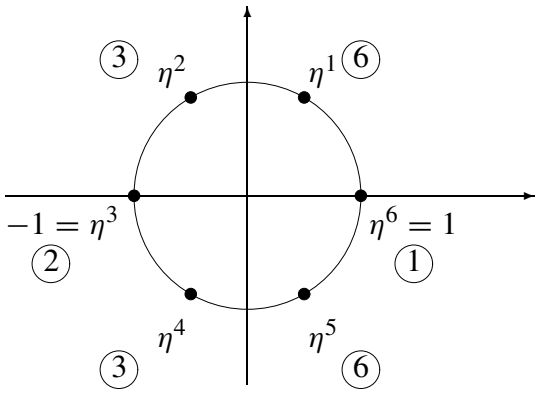
3.9.2. Gyakorlat. Mutassuk meg a megfelelő egységgyökök algebrai alakjának kiszámításával, hogy $\Phi_3(x) = x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$ és $\Phi_{12}(x) = x^4 - x^2 + 1$.

Ez a közvetlen módszer általában nem működik: nagyobb n-ekre már a $\sin(2\pi/n)$ és $\cos(2\pi/n)$ értékét is csak közelítőleg tudjuk kiszámolni, a beszorzás pedig végképp elbonyolítja a dolgot. Pedig az eredmény szép: az összes eddig tárgyalt esetben egész együtthatós polinom jött ki, és látni fogjuk, hogy meglepő módon ez általában is így van.

Hogyan határozhatnánk meg például a Φ_3 polinomot? Ennek gyökei harmadik egységgyökök. A három harmadik egységgyök az $x^3 - 1$ polinom három gyöke. Ezek közül az 1 nem jó, mert az nem primitív harmadik egységgyök, de a másik kettő igen. Ezért ez a másik két szám az $(x^3 - 1)/(x - 1) = x^2 + x + 1$ polinomnak lesz gyöke. Azaz $\Phi_3(x) = x^2 + x + 1$.

3.9.3. Gyakorlat. Általánosítsuk ezt a gondolatmenetet a 3 helyett tetszőleges prímszámra.

Ha a hatodik körosztási polinomot akarjuk kiszámítani, akkor a hatodik egységgyököket kell áttekintenünk. Legyen $\eta = \cos 60^\circ + i \sin 60^\circ$. Ez primitív hatodik egységgyök, ezért a hatodik egységgyökök ennek a hatványai. A hatvány rendjére vonatkozó képletből látjuk, hogy $o(\eta) = o(\eta^5) = 6$ (ezek a hatodik primitív egységgyökök), $o(\eta^2) = o(\eta^4) = 3$ (tehát η^2 és η^4 pont a két primitív harmadik egységgyök), $o(\eta^3) = 2$ (valójában $\eta^3 = -1$), végül $o(\eta^6) = 1$ (és $\eta^6 = 1$). Az alábbi ábrán feltüntettük a hatodik egységgyököket, a bekarikázott számok pedig a rendjeik.



3.1. Ábra. A hatodik egységgyökök rendjei.

Mivel $x^6 - 1$ gyökei pont a hat darab hatodik egységgyök, azt kapjuk, hogy

$$x^6 - 1 = (x - \eta)(x - \eta^2)(x - \eta^3)(x - \eta^4)(x - \eta^5)(x - \eta^6)\,.$$

Csoportosítsuk a gyöktényezőket az egységgyökök rendjei szerint.

$$\begin{aligned} x^6 - 1 = &\big[(x - \eta)(x - \eta^5)\big]\,\big[(x - \eta^2)(x - \eta^4)\big]\,(x - \eta^3)\,(x - \eta^6) = \\ = \quad &\Phi_6(x) \quad \cdot \quad \Phi_3(x) \quad \cdot\, \Phi_2(x) \,\cdot \Phi_1(x)\,. \end{aligned}$$

Innen

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)}\,.$$

Mivel a Φ_1, Φ_2 és Φ_3 polinomokat már kiszámoltuk, osztással megkapjuk a keresett Φ_6-ot is. A számolást lerövidíti, ha felhasználjuk a korábban már bebizonyított $\Phi_1(x)\Phi_3(x) = x^3 - 1$ összefüggést:

$$\Phi_6(x) = \frac{x^6 - 1}{(x^3 - 1)\Phi_2(x)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1\,.$$

3.9.4. Gyakorlat. Kövessük végig ezt a gondolatmenetet $n = 6$ helyett $n = 12$-re, és határozzuk meg a Φ_{12} polinomot ezzel a módszerrel is.

Az elhangzott gondolatmenetet most már könnyű általánosítani.

3.9.5. Lemma. *Ha $n \geq 1$, akkor $\prod_{d|n} \Phi_d(x) = x^n - 1$.*

Bizonyítás. Legyen $\eta = \cos(2\pi/n) + i\sin(2\pi/n)$. Ekkor η primitív n-edik egységgyök, és ezért hatványai az n-edik egységgyököket adják meg. Ezek éppen az $x^n - 1$ gyökei, és mivel n különböző számról van szó, az $x^n - 1$ gyöktényezős alakja

$$x^n - 1 = (x - \eta)(x - \eta^2)\dots(x - \eta^n)\,.$$

Ismét a megfelelő egységgyökök rendjei szerint csoportosítjuk a gyöktényezőket. Jelölje f_d a d rendű egységgyökökhöz tartozó gyöktényezők szorzatát. Így

$$x^n - 1 = \prod_d f_d(x)\,.$$

Elég belátni, hogy az itt fellépő d számok pontosan n osztói, és hogy ezekre $f_d = \Phi_d$.

Ha egy d szám fellép, vagyis ha $d = o(\eta^m)$ teljesül valamelyik m-re, akkor $(\eta^m)^n = (\eta^n)^m = 1^m = 1$ miatt n jó kitevője η^m-nek, és így $d \mid n$. Tehát a fellépő d számok tényleg csak n osztói lehetnek. Tegyük fel, hogy $d \mid n$. Ekkor Φ_d gyöktényezős felbontásában az *összes* d rendű komplex szám szerepel, f_d felbontásában pedig az olyan d rendű komplex számok szerepelnek, amik egyben n-edik egységgyökök is (mindegyik egyszer). De ezek ugyanazok a számok: mindegyik d-edik egységgyök egyben n-edik egységgyök is. Hiszen ha egy ξ számra $d = o(\xi) \mid n$, akkor $\xi^n = 1$, ezért ξ egy n-edik egységgyök. Beláttuk tehát, hogy $f_d = \Phi_d$. □

3.9.6. Gyakorlat. Igazoljuk, hogy tetszőleges $n \geq 1$ egészre $\sum_{d|n} \varphi(d) = n$.

3.9.7. Következmény. *Ha $n \geq 1$, akkor a Φ_n körosztási polinom egész együtthatós.*

Bizonyítás. Indirekt bizonyítunk, tegyük fel, hogy az állítás nem igaz, és legyen n a legkisebb olyan pozitív egész, melyre Φ_n nem egész együtthatós. Az előbbi lemma miatt

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d|n \\ d\neq n}} \Phi_d(x)}\,.$$

Az n minimalitása miatt a nevezőben csupa egész együtthatós polinom van, amik normáltak is. Ezért a nevező maga is normált, és egész együtthatós. Azt a gondolatot alkalmazzuk, amit már láttunk a 3.2.18. Gyakorlatban. Tudjuk, hogy minden olyan polinommal lehet maradékosan osztani, melynek a főegyütthatója invertálható. Ezért a számláló maradékosan eloszthető a nevezővel $\mathbb{Z}[x]$-ben. A maradékos osztás ($\mathbb{C}$ fölötti) egyértelműsége miatt a hányados és a maradék ugyanaz, mint ha az osztást $\mathbb{C}$ fölött végeznénk. De $\mathbb{C}$ fölött tudjuk, hogy a hányados Φ_n és a maradék nulla. Tehát $\mathbb{Z}$ fölött is Φ_n a hányados, vagyis Φ_n mégis egész együtthatós. Ez az ellentmondás bizonyítja az állítást. □

Ebben a bizonyításban a teljes indukciónak egy formáját használtuk, feltettük, hogy az állítás minden n-nél kisebb értékre igaz, és beláttuk ebből, hogy n-re is igaz (ennek egy változatát a számelméletben végtelen leszállásnak is nevezik). Noha a fenti fogalmazásból is látszik, hadd hangsúlyozzuk még egyszer, hogy ilyenkor az indukciónak nincs „kezdő esete". Például az $n = 1$-et nem kell külön megnézni: a fenti gondolatmenetnek ekkor is működnie

kell. Ha $n = 1$, akkor az, hogy minden n-nél kisebb értékre tudjuk az állítást, *üres feltétel*. A fenti képlet most így néz ki:

$$\Phi_1(x) = \frac{x^1 - 1}{\prod\limits_{\substack{d|1 \\ d\neq 1}} \Phi_d(x)}\,.$$

A nevező *üres szorzat* (ilyennel már találkoztunk a 2.2.43. Gyakorlatban), értéke tehát 1, és így a $\Phi_1(x) = x - 1$ összefüggést kapjuk, ami persze bizonyítja, hogy Φ_1 egész együtthatós.

A tanulság az, hogy miképpen egy programozónak figyelnie kell arra, hogy a programja akkor is jól működjön, ha mondjuk egy ciklus nullaszor fut le, *minden bizonyításban figyeljünk oda az „extrém" esetekre is, például arra, amikor egy halmaz, összeg, vagy szorzat üres, vagy valami nullával egyenlő, mert a bizonyításnak ilyenkor is működnie kell.*

Mint a Φ_6 példáján láttuk, az iménti bizonyítás egyben módot ad arra, hogy a körosztási polinomokat rekurzívan kiszámítsuk. A szakasz végén levő gyakorlatokban erre több példát is láthatunk. A 3.9.10. Gyakorlat, valamint a 3.9.14 és a 3.9.11. Feladatok lehetővé teszik, hogy az n-edik körosztási polinom kiszámítását visszavezessük arra az esetre, amikor az n páratlan, összetett, *négyzetmentes szám*, (vagyis minden prímosztója az első kitevőn szerepel).

A `Maple` program segítségével tetszőleges n esetén kiszámítható Φ_n (sőt, az eredményt a matematikai dokumentumok szedésére mindenki által használt, Donald Knuth által tervezett TEX nyelv formátumában is megkaphatjuk). Például a

```
with(numtheory):
for n from 3 by 2 to 105 do
  if issqrfree(n) and not isprime(n) then
    print(n, cyclotomic(n,x))
  fi
od;
```

parancssorozat kiírja páratlan, négyzetmentes, nem prím számokra a körosztási polinomokat 105-ig. Az eredmény az B.1. Függelékben olvasható. A listából megállapíthatjuk, hogy $n = 105$ a legkisebb olyan szám, melyre a Φ_n polinomnak van olyan együtthatója, ami nem a $0, 1, -1$ számok valamelyike. Ezt számítógép nélkül is megmutathatjuk, csak azt kell kiszámolni, hogy ha n két különböző páratlan prím szorzata, akkor Φ_n együtthatói csak a $0, 1, -1$ számok lehetnek.

Korábban azt állítottuk, hogy az $x^n - 1$ irreducibilis komponensei éppen a körosztási polinomok, más szóval, hogy a körosztási polinomok irreducibilisek $\mathbb{Z}$ fölött. Ezt most már be is tudjuk látni: a könyv első részének utolsó, és — véleményünk szerint — legszebb bizonyítása következik.

3.9.8. Tétel. *Mindegyik körosztási polinom irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ fölött.*

Bizonyítás. A 3.4.8. Tétel miatt a Φ_n körosztási polinom ugyanakkor irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ fölött, hiszen primitív (mert normált), és nem konstans. Bontsuk fel $\mathbb{Z}$ fölött irreducibilisek szorzatára: $\Phi_n(x) = f_1(x) \dots f_s(x)$. Az f_i tényezők főegyütthatója csak ± 1 lehet, tehát egyik sem konstans (hiszen akkor ± 1, vagyis egység lenne $\mathbb{Z}[x]$-ben), és így mindegyik f_i

irreducibilis $\mathbb{Q}[x]$ fölött is. Azt kell megmutatnunk, hogy ebben a felbontásban csak egy tényező szerepel.

3.9.9. Lemma. *Legyen $p \nmid n$ prím. Ha egy ε számra $f_1(\varepsilon) = 0$, akkor $f_1(\varepsilon^p) = 0$.*

A lemmából már következik a tétel. Valóban, mivel f_1 legalább elsőfokú, van egy $\varepsilon \in \mathbb{C}$ gyöke, ami Φ_n-nek is gyöke, azaz primitív n-edik egységgyök. Tehát az összes n-edik primitív egységgyök hatványa ε-nak (1.5.12. Tétel), méghozzá (a hatvány rendjének képlete miatt) n-hez relatív prím kitevőjű hatványa. Legyen ε^m ilyen szám, ahol $(m, n) = 1$. Az m felbontható prímek szorzatára: $m = p_1 \dots p_\ell$ (ezek között lehetnek egyenlők is), ahol persze egyik p_j sem osztója n-nek. A lemma miatt ε^{p_1} gyöke f_1-nek. Alkalmazzuk a lemmát az ε^{p_1} számra és a p_2 prímszámra. Azt kapjuk, hogy $(\varepsilon^{p_1})^{p_2} = \varepsilon^{p_1 p_2}$ is gyöke f_1-nek. A lemmát még $\ell - 2$-szer alkalmazva adódik, hogy $\varepsilon^{p_1 \cdots p_\ell} = \varepsilon^m$ is gyöke f_1-nek. Azaz f_1-nek gyöke az összes n-edik primitív egységgyök, és így Φ_n összes gyöktényezője már f_1-ben szerepel. Tehát f_1 a Φ_n felbontásának egyetlen tényezője. Így a 3.9.8. Tétel bizonyításához már csak a lemmát kell belátnunk, most ez következik.

Tegyük fel, hogy $f_1(\varepsilon) = 0$, de $f_1(\varepsilon^p) \neq 0$. Mivel $p \nmid n$, az ε^p is primitív n-edik egységgyök, azaz gyöke Φ_n-nek. Ezért ε^p gyöke valamelyik f_j polinomnak (ahol $j \neq 1$). Az indexek átszámozásával feltehetjük, hogy $j = 2$. Tehát $f_2(\varepsilon^p) = 0$.

Tekintsük az $f_1(x)$ és az $f_2(x^p)$ polinomok kitüntetett közös osztóját. Tudjuk, hogy ezt $\mathbb{Q}$ és $\mathbb{C}$ fölött kiszámítva ugyanazt a racionális együtthatós f polinomot kapjuk (3.2.5. Gyakorlat). Mivel a két polinomnak ε közös gyöke, az f polinom nem konstans (osztója $\mathbb{C}[x]$-ben $x - \varepsilon$). Ezért $f \mid f_1$-ből és f_1 irreducibilitásából az következik, hogy f az f_1 polinomnak asszociáltja, azaz nem nulla racionális konstansszorosa. Mivel $f(x) \mid f_2(x^p)$, ezért beláttuk, hogy $f_1(x)$ osztója az $f_2(x^p)$ polinomnak $\mathbb{Q}[x]$-ben. De akkor osztója $\mathbb{Z}[x]$-ben is, hiszen f_1 főegyütthatója ± 1, és így amikor a $g(x) = f_2(x^p)/f_1(x)$ osztást elvégezzük, akkor végig $\mathbb{Z}[x]$-ben maradunk (lásd 3.2.18. Gyakorlat, de hivatkozhatunk az első Gauss-lemma második következményére is.)

Vegyük a szereplő polinomok együtthatóit mod p, és jelölje felülvonás az így kapott polinomokat. Ekkor $\overline{f_1}(x)\overline{g}(x) = \overline{f_2}(x^p)$. A $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (3.3.18. Feladat), és ebben a feladatban azt is beláttuk, hogy $\overline{f_2}(x^p) = \overline{f_2}(x)^p$. Tehát $\overline{f_1} \mid \overline{f_2}^p$, ahol az oszthatóság $\mathbb{Z}_p[x]$-ben értendő. Mivel f_1 főegyütthatója ± 1, az $\overline{f_1}$ polinom sem konstans. Ez a polinom $\mathbb{Z}_p$ felett nem biztos, hogy irreducibilis, de mindenképpen van egy $\mathbb{Z}_p$ felett irreducibilis k osztója. Ekkor $k \mid \overline{f_1} \mid \overline{f_2}^p$, és mivel az irreducibilis polinomok $\mathbb{Z}_p[x]$-ben prímtulajdonságúak (hiszen $\mathbb{Z}_p$ test), azt kapjuk, hogy $k \mid \overline{f_2}$.

Találtunk tehát egy olyan $k \in \mathbb{Z}_p[x]$ nem konstans polinomot, ami $\overline{f_1}$-nak is és $\overline{f_2}$-nak is osztója. Ezért $k^2 \mid \overline{f_1 f_2}$. Viszont $f_1 f_2 \mid \Phi_n$, és $\Phi_n(x) \mid x^n - 1$. Ezért végülis $k^2 \mid \overline{x^n - 1}$. Ez azonban ellentmond a 3.6.12. Gyakorlat megoldásának, amely szerint $p \nmid n$ esetén az $x^n - 1$ polinomnak nincs többszörös tényezője mod p. Ezzel a lemma, és így a tétel bizonyítását is befejeztük. □

Gyakorlatok, feladatok

3.9.10. Gyakorlat. Számítsuk ki a prímhatvány-indexű körosztási polinomokat.

3.9.11. Feladat. Mutassuk meg, hogy ha $n > 1$ páratlan, akkor $\Phi_{2n}(x) = \Phi_n(-x)$.

3.9.12. Gyakorlat. Számítsuk ki az n-edik körosztási polinomot az összes $n \leq 20$ egészre.

3.9.13. Feladat. Bizonyítsuk be, hogy $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$, ahol μ az úgynevezett Möbius-függvény (A.4.5. Definíció).

3.9.14. Feladat. Legyenek $m \mid n$ pozitív egészek úgy, hogy n minden prímosztója osztja m-et is. Igazoljuk, hogy $\Phi_n(x) = \Phi_m(x^{n/m})$.

3.9.15. Gyakorlat. Számítsuk ki az előző feladat alapján a $\Phi_n(x)$ polinomokat abban az esetben, amikor $n = 36, 72, 144, 100$.

3.9.16. Feladat. Alkalmazzuk a gyökök és együtthatók összefüggését a 12-edik, 18-adik, illetve 24-edik primitív egységgyökök összegének és szorzatának kiszámítására. Általánosítsuk a feladatot n-edik primitív egységgyökökre.

3.9.17. Feladat. Határozzuk meg a Φ_n polinom együtthatóinak összegét.

3.9.18. Feladat. Határozzuk meg a $\Phi_n(-1)$ értékét.

3.9.19. Gyakorlat. Tegyük fel, hogy m és n relatív prímek. Mutassuk meg, hogy minden mn-edik primitív egységgyök egyértelműen előáll egy m-edik és egy n-edik primitív egységgyök szorzataként. Vezessük le ebből, hogy $\varphi(mn) = \varphi(m)\varphi(n)$.

3.9.20. Feladat. A 3.9.11. Feladat általánosításaként mutassuk meg, hogy ha m és n relatív prímek, akkor

$$\Phi_{mn}(x) = \prod_{o(\eta)=m} \Phi_n(\eta x)\,,$$

kivéve az $m = 2$, $n = 1$ esetben, amikor a két oldal egymás ellentettje.

3.9.21. Gyakorlat. Bontsuk az $x^{12} - 1$ polinomot irreducibilisek szorzatára $\mathbb{Z}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$ és $\mathbb{Z}_5$ fölött.

3.9.22. Feladat. Legyen p prímszám, és $n = p^k m$, ahol már $p \nmid m$. Mutassuk meg, hogy modulo p a Φ_n egyenlő a $\Phi_m^{\varphi(p^k)}$ polinommal.

3.9.23. Gyakorlat. Mutassuk meg a 3.5.6. Feladat általánosításaként, hogy a prímhatvány-indexű körosztási polinomok alkalmas eltoltjára teljesül a Schönemann-Eisenstein kritérium feltétele.

3.9.24. Feladat. Igazoljuk, hogy a Φ_n polinom egy alkalmas eltoltjára akkor és csak akkor teljesül a Schönemann-Eisenstein, ha n prímhatvány, vagy egy páratlan prímhatvány kétszerese.

3.9.25. Gyakorlat. Határozzuk meg a `Maple` program segítségével azt a legkisebb n értéket, melyre a Φ_n polinomnak van kettőnél, illetve háromnál nagyobb abszolút értékű együtthatója.

3.10. Összefoglaló

Ebben a fejezetben a polinomok számelméletével, és ennek alkalmazásaival foglalkoztunk. Először tetszőleges szokásos gyűrűben vizsgáltuk a számelméleti alapfogalmakat. Ezek: oszthatóság, asszociált, egység, triviális felbontás, felbonthatatlan, prím, kitüntetett közös osztó és közös többszörös. Megfogalmaztuk a számelmélet alaptételének megfelelő állítást, az ezt teljesítő gyűrűket alaptételes gyűrűknek neveztük. Definiáltuk a kanonikus alak fogalmát, és ennek segítségével képletet adtunk az oszthatóságra, a kitüntetett közös osztóra és közös többszörösre.

Megmutattuk, hogy alaptételes gyűrűben igaz a kitüntetett közös osztó kiemelési tulajdonsága. Megfordítva, beláttuk, hogy ha egy szokásos gyűrűben teljesül, hogy bármely két f és g elem kitüntetett közös osztója létezik, és felírható $fr + gs$ alakban, akkor igaz a kitüntetett közös osztó kiemelési tulajdonsága, ezért minden irreducibilis elem prím, és innen következik már az alaptétel egyértelműségi állítása is. Mindez a 3.1. Szakaszban, illetve az azt követő feladatokban történt.

Általános tudásunkat polinomgyűrűkre alkalmaztuk. Megmutattuk, hogy egy szokásos gyűrű fölött minden olyan polinommal lehet, méghozzá egyértelműen, maradékosan osztani, amelynek a főegyütthatója invertálható; speciálisan test fölött minden nem nulla polinommal lehet (3.2.1. Tétel). A maradékos osztás segítségével test fölött elvégezhető a kitüntetett közös osztó kiszámítására szolgáló euklideszi algoritmus, és kétféleképpen is beláttuk, hogy ilyenkor tetszőleges f és g polinomok kitüntetett közös osztója felírható $fp + gq$ alakban (3.2.6. Tétel). Ebből test fölötti polinomgyűrűben levezettük a számelmélet alaptételét (az egyértelműség az előző bekezdésben írottakból következik, a létezés bizonyításához a fokszám tulajdonságait használtuk).

Bebizonyítottuk a számelmélet alaptételét $\mathbb{Z}[x]$-ben is (3.4.10. Tétel). Ennek az eredménynek a kulcsa a 3.4.8. Tétel, amelyben a $\mathbb{Z}$ fölötti irreducibilitást sikerült visszavezetni a $\mathbb{Q}$ fölötti irreducibilitásra: egy $f \in \mathbb{Z}[x]$ polinom akkor és csak akkor irreducibilis, ha vagy konstans prímszám, vagy $\mathbb{Q}$ fölött irreducibilis, és primitív (azaz nem emelhető ki belőle egységtől különböző egész szám). A bizonyításban szereplő nagyon hasznos technikai segédeszköz a két Gauss-Lemma: az első szerint a $\mathbb{Z}$-beli prímek $\mathbb{Z}[x]$-ben is prímek maradnak, vagy ami ezzel ekvivalens: primitív polinomok szorzata is primitív (3.4.4. Következmény); a második Gauss-Lemma pedig azt teszi lehetővé, hogy egy egész együtthatós polinom $\mathbb{Q}$ fölötti felbontását racionális konstansokkal való szorzás segítségével $\mathbb{Z}$ fölötti felbontássá módosíthassuk (3.4.7. Lemma). Észrevettük, hogy bizonyításunk nemcsak $\mathbb{Z}[x]$-ben, hanem tetszőleges alaptételes gyűrű fölötti polinomgyűrűben is működik, és így például $\mathbb{Z}[x_1, \ldots, x_n]$, és tetszőleges T testre $T[x_1, \ldots, x_n]$ is alaptételes.

Az alaptétel birtokában figyelmünk az irreducibilis polinomok felé fordult, az előző bekezdésben írottak miatt test fölöttiekre. Egy test fölötti polinom akkor és csak akkor irreducibilis, ha nem konstans, és nem bontható alacsonyabb fokú polinomok szorzatára. Egy polinomnak akkor és csak akkor van elsőfokú tényezője, ha van gyöke az adott testben (3.3.3. Állítás). Ennek felhasználásával láttuk, hogy test fölött egy elsőfokú polinom mindig irreducibilis; egy másod- és harmadfokú akkor és csak akkor irreducibilis, ha nincs gyöke (3.3.4. Állítás); egy legalább negyedfokú polinom pedig nem lehet irreducibilis, ha van gyöke, de attól, hogy nincs gyöke, még nem biztos, hogy irreducibilis. Speciálisan $\mathbb{C}$ (illetve tetszőleges algebrailag zárt test) fölött az irreducibilis polinomok pontosan az elsőfokúak. A valós test fölött észrevettük, hogy egy polinom komplex gyökeinek konjugáltjai is ugyanannyiszoros gyökök (3.3.6. Lemma), ezért $\mathbb{R}$ fölött az elsőfokúakon kívül még azok a másodfokú polinomok irreducibilisek, amelyeknek nincs valós gyöke (és több irreducibilis polinom nincs). Következményként beláttuk, hogy páratlan fokú valós együtthatós polinomnak mindig van valós gyöke.

A racionális test fölött már nehezebb eldönteni az irreducibilitást. A gyökök meghatározása a racionális gyökteszt segítségével történhet (3.3.9. Tétel), így a legfeljebb harmadfokú polinomokkal nincs probléma. Ha szerencsénk van, használhatjuk az irreducibilitás eldöntésére a Schönemann-Eisenstein kritériumot (3.5.2. Tétel) a polinomra, vagy valamelyik eltoltjára. A polinomot felbonthatjuk $\mathbb{R}$ vagy $\mathbb{C}$ fölött, és ebből is következtethetünk néha arra, hogy irreducibilis-e $\mathbb{Q}$ fölött. Vizsgálhatjuk polinomunkat $\mathbb{Z}_p$ fölött alkalmas p prímszámra, ebben segít az az észrevétel, hogy itt tagonként lehet p-edik hatványra emelni (3.3.18. Feladat). Ezeket a módszereket a 104. oldal táblázatában foglaltuk össze.

Az n-edik körosztási polinom gyökei az n-edik primitív egységgyökök (3.9.1. Definíció), de ennek ellenére ez a polinom egész együtthatós, mert a 3.9.5. Lemma alapján rekurzívan is kiszámítható. A körosztási polinomok újabb példát szolgáltatnak a $\mathbb{Z}$ és a $\mathbb{Q}$ fölötti irreducibilitásra (3.9.8. Tétel).

Két polinom közös gyökei pontosan a kitüntetett közös osztójuknak a gyökei. Ez lehetővé teszi egy polinom többszörös gyökeinek meghatározását a formális deriválás módszerével (3.6.4. Tétel), mert egy k-szoros gyök a deriváltnak is legalább ($\mathbb{C}$ fölött pontosan) $k-1$-szeres gyöke. Így egy f polinom többszörös gyökei pontosan (f, f') gyökei lesznek. Azt, hogy két polinomnak van-e közös gyöke, a rezultáns módszerével is eldönthetjük (3.7.4. Tétel), ehhez egy speciális determinánst kell kiszámolni. A rezultáns segítségével egy többváltozós egyenletrendszert egyváltozós egyenletre vezethetünk vissza. Speciális esetként f és f' rezultánsának felírásával az f többszörös gyökeinek létezését is vizsgálhatjuk, így jutunk a diszkrimináns fogalmához (3.7.7. Definíció, 3.7.6. Tétel). A diszkrimináns előjele segít a konjugált komplex gyökpárok számának vizsgálatában is (3.7.9. Tétel).

Megmutattuk, hogy hogyan lehet a Cardano-képletből egy harmadfokú egyenlet összes gyökét megkapni (3.8.1. Tétel). Valós együtthatós egyenlet esetében a diszkrimináns akkor és csak akkor pozitív, ha az egyenletnek három valós gyöke van (3.8.2. Tétel). A diszkrimináns a négyzetgyökjel alatti kifejezés -108-szorosa, ezért amikor a gyökök mind valósak, akkor a Cardano-képletben negatív szám áll a négyzetgyökjel alatt, és így komplex számok

használatára kényszerülünk. Szó esett arról, hogy három valós gyök esetén más módszerrel sem lehet olyan megoldóképletet felírni, ami az egyenlet gyökeit komplex számok használata nélkül megadná (Casus irreducibilis). Végül röviden bemutattuk a negyedfokú egyenlet gyökjelekkel való megoldásának ötletét (3.8.4. Tétel).

II. rész

Klasszikus algebrai struktúrák

4. CSOPORTOK

Erre a tanácsos fejtegetni kezdte az anagrammák, permutációk, kódok, szimbólumok, jelek titkait, és az általános információelméletet, egyre bonyolultabban, és mind kevésbé érthetően, úgyhogy a királyt végülis elöntötte a pulykaméreg, és börtönbe vettette.

Stanisław Lem: *Kiberiáda*
(Murányi Beatrix fordítása)

A csoportelmélet (és az absztrakt algebra) oktatására általában a lineáris algebra után kerül sor. Ebben a fejezetben nem használunk több lineáris algebrai ismeretet, mint amire már a rezultáns vizsgálatához is szükségünk volt, azaz a mátrixok és determinánsok elemi tulajdonságait (sőt ezek is csak egy konkrét csoportfajta bevezetéséhez kellenek). Ugyanakkor néhány megjegyzésben, példában, feladatmegoldásban előjönnek a vektorterek és a lineáris leképezések alaptulajdonságai is (sőt, sok fontos csoportelméleti fogalmat ezek motiválnak, magyaráznak). A vektorterek valójában nagyon egyszerű szerkezetű struktúrák, igencsak hasznos (bár nem szükségszerű), ha az Olvasó megismerkedik velük, és ezzel némi absztrakt algebrai tapasztalatot is szerez, mielőtt a csoportok általános tanulmányozásába kezdene. Ehhez Freud Róbert [**10**] könyvét ajánljuk.

4.1. Bevezető példák

Egy idegen bolygó lakói üzenetet küldenek a többi civilizációnak, melyben be akarnak számolni kultúrájuk fejlettségéről. A prímszámokat persze mindenki ismeri, aki az adást fogni tudja, azokat kár elküldeni. Végülis az üzenet így kezdődik:

60, 168, 360, 504, 660, 1092, 2448, 2520, 3420, 4080, 5616, 6048, 6072,

7800, 9828, 12180, 14880, 20160, 20160, 25308, 25920, . . .

Meg tudja-e fejteni ezt az emberiség? A válasz az 1980-as évek óta igenlő. Ekkor bizonyították ugyanis be (több mint húszéves munka eredményeként) a híres *klasszifikáció* tételét. Az eredmény sok matematikus munkája, és a bizonyítás (melynek teljes publikációja most készül) durván tízezer oldal, tele nagyszerű ötletekkel. A klasszifikáció az úgynevezett véges egyszerű csoportokat írja le, ezekről részletesebben is beszélünk majd a fejezet végén.

A csoportelmélet a tizenkilencedik század első felében keletkezett Niels Henrik Abel és Evariste Galois munkássága nyomán. A kutatásokat eredetileg az a probléma inspirálta, hogy mely egyenleteket lehet gyökképlet segítségével megoldani. Ez vezetett el a *permutációcsoport* fogalmához, melynek elemei permutációk, a művelet pedig ezek kompozíciója. Általában egy alakzat (például egy négyzet vagy egy kocka) összes lehetséges szimmetriái alkotnak permutációcsoportot, és ennek vizsgálata sokat elárul magáról az alakzatról is. Később Felix Klein a geometriának is alapvető eszközévé tette a csoportokat, amelyek geometriai transzformációkból álltak, szintén a kompozíció műveletére.

A tizenkilencedik század végére kiderült, hogy a csoportokat egyszerre, egymáshoz való viszonyaikban hatékony vizsgálni. Megszületett az absztrakt csoport fogalma, melyek között a művelettartó leképezések (homomorfizmusok) létesítenek kapcsolatot. Az lett a feladat, hogy az általános csoportoknak minél jobban *feltárjuk a szerkezetét*, olyan struktúratételeket bizonyítsunk, amelyek alapján az alkalmazásokban felmerülő kérdésekre válaszolni lehet. Manapság a csoportelméletet (például a klasszifikáció tételét is) a legkülönbözőbb területeken alkalmazzák, a kombinatorikától kezdve az analízisen és a geometrián át a kristályok elméletéig.

A csoport általános fogalmát már ismerjük (2.2.13. Definíció). Láttuk, hogy ha R gyűrű, akkor R az összeadásra Abel-csoport lesz. Ezt R additív csoportjának neveztük, és R^+-szal jelöltük. Ha R egységelemes, akkor az invertálható elemei szintén csoportot alkotnak a szorzásra. Ez R multiplikatív csoportja, amelynek jele $R^\times$ (lásd 2.2.10. Feladat). Innen származtak a $\mathbb{C}^+$, $\mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{Z}^+$, $\mathbb{Z}_n^+$ és a $\mathbb{Z}_n^\times$ csoportok. A $\mathbb{Z}_n^\times$ csoporthoz nagyon hasonlít a számelméletből esetleg ismerős „redukált maradékosztályok csoportja a szorzásra”.

Ebből a sémából kiindulva más fontos konkrét csoportokhoz is eljuthatunk. Lineáris algebrából tudjuk, hogy egy T test fölötti $n \times n$-es mátrixok egységelemes gyűrűt alkotnak, melynek invertálható elemei a nem nulla determinánsú mátrixok (A.5.3. Tétel). Ennek a gyűrűnek a multiplikatív csoportja olyan fontos, hogy külön nevet és jelölést kapott.

4.1.1. Definíció. Legyen T test és $n \geq 1$ egész. Ekkor a T fölötti $n \times n$-es invertálható mátrixok csoportját a szorzásra *általános lineáris csoportnak* nevezzük, és $\mathrm{GL}(n, T)$-vel jelöljük (a G és L betűk a General Linear group angol elnevezésből származnak).

Szó esett már a részcsoport fogalmáról is (2.2.15. Definíció): részcsoportot akkor kapunk, ha egy csoport egy részhalmaza maga is csoport az eredeti műveletre nézve. Például a racionális számok részcsoportot alkotnak a komplex számok között az összeadásra, képletben $\mathbb{Q}^+ \leq \mathbb{C}^+$. A 2.2.16. Feladat megoldásában beláttuk azt is, hogy részcsoport egységeleme ugyanaz, mint a csoport egységeleme, és az inverzet is ugyanúgy kell képezni benne, továbbá hogy egy részhalmaz akkor és csak akkor részcsoport, ha nem üres, és zárt a G-beli szorzásra és inverzképzésre. Így minden részcsoport zárt az egész kitevőjű hatványozásra is (2.2.17. Definíció). A hatványozás azonosságait a 2.2.18. Gyakorlatban foglaltuk össze.

Vigyázzunk, hogy az inverzet ne felejtsük el megvizsgálni, például ha $G = \mathbb{Z}^+$ (az egész számok csoportja az összeadásra), akkor a nemnegatív egészek halmaza zárt az összeadásra

(sőt a neutrális elemet is tartalmazza), de mégsem részcsoport. A 4.3.4. Következményben belátjuk majd, hogy véges csoportok esetében nem kell az inverzzel bíbelődnünk, minden szorzásra zárt részhalmaz részcsoport lesz.

Minden csoportnak részcsoportja önmaga, valamint az egységelemből álló egyelemű $\{1\}$ részcsoport. Ezek a *triviális részcsoportok*. Szokás a G-től különböző részcsoportokat *valódi részcsoportoknak* nevezni.

4.1.2. Definíció. Legyen T test és $n \geq 1$ egész. Ekkor azok a T fölötti $n \times n$-es mátrixok, melyek determinánsa 1 (vagyis T egységeleme), részcsoportot alkotnak $\mathrm{GL}(n, T)$-ben. Ennek a csoportnak a neve *speciális lineáris csoport*, jele $\mathrm{SL}(n, T)$.

Az $\mathrm{SL}(n, T)$ tényleg részcsoport, hiszen az egységmátrix determinánsa 1, és a determinánsok szorzástétele miatt 1 determinánsú mátrixok szorzata és inverze is 1 determinánsú. Az S és L betűk a Special Linear group (speciális lineáris csoport) elnevezésből származnak.

Talán a legfontosabb csoportok azok, amelyek elemei egy halmaz permutációi. Először azt vizsgáljuk meg, hogyan alkothatnak a permutációk csoportot. Középiskolában permutációnak dolgok egy sorrendjét neveztük. Például az

$$\mathit{alma} \quad \mathit{szilva} \quad \mathit{barack}$$

e három gyümölcs nevének egy sorrendje. Ezt a három szót hatféleképpen tudjuk sorba rakni: az első helyre a három szó bármelyike kerülhet, ez eddig három lehetőség. Mindhárom esetben a második helyre a fennmaradó két szó bármelyikét tehetjük, ez tehát $2 \cdot 3 = 6$ lehetőség. Ezzel a harmadik szó helye is meg van határozva, tehát tényleg hatféle sorrend lehetséges. Általában n különböző tárgyat $n!$-féleképpen rakhatunk sorba (A.2.1. Tétel).

Kényelmesebb lesz, ha nem az elemek sorrendjére, hanem a sorba rakás vagy átrendezés aktusára koncentrálunk. Valaki például a fenti sorrendet átrendezheti úgy, hogy az első helyre a barack, a másodikra az alma kerüljön. Ezt a tevékenységet így írhatjuk le:

$$\begin{bmatrix} \mathit{alma} & \mathit{szilva} & \mathit{barack} \\ \mathit{barack} & \mathit{alma} & \mathit{szilva} \end{bmatrix}$$

(persze az eredetileg adott sorrendet hatféleképpen rendezhetjük át). Ezt az átrendezést egy f függvénynek is felfoghatjuk, amelyre

$$f(\mathit{alma}) = \mathit{barack}\,, \qquad f(\mathit{szilva}) = \mathit{alma}\,, \qquad f(\mathit{barack}) = \mathit{szilva}\,.$$

Nyilvánvaló, hogy f kölcsönösen egyértelmű megfeleltetése (más szóval bijekciója) az $X = \{\mathit{alma}, \mathit{szilva}, \mathit{barack}\}$ halmaznak önmagára. Megfordítva, e halmaz minden önmagára való kölcsönösen egyértelmű megfeleltetése „igazából” az elemek sorrendjének egy megváltoztatását jelenti. Vagyis az elemek különféle sorrendjeinek vizsgálata helyett tekinthetjük az adott elemek halmazának önmagára való bijekcióit is. Ezt a megközelítést általánosítja a következő definíció.

4.1.3. Definíció. Legyen X tetszőleges halmaz. Az X-et önmagára képező bijekciókat az X halmaz *permutációinak* nevezzük. Ezek halmazát S_X jelöli.

Egy X halmaz elemszámát általában $|X|$-szel jelöljük, így $|S_X| = |X|!$ tetszőleges véges X esetén. Ha $X = \{1, 2, \ldots, n\}$, akkor S_X helyett S_n-et írunk. Például S_4 egy eleme a fenti jelöléssel a következőképpen adható meg:

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}$$

Ez tehát azt jelenti, hogy $f(1) = 2,\ f(2) = 4,\ f(3) = 3,\ f(4) = 1$.

Leképezések kompozíciójával a 2.2.3. Definícióban találkoztunk: $(f \circ g)(x) = f(g(x))$. A kompozíció műveletét sokszor egyszerűen szorzásnak hívjuk majd, és egymás mellé írással jelöljük, vagyis $f \circ g$ helyett fg-t írunk. Vigyázzunk arra, hogy az $(f \circ g)(x) = f(g(x))$ képlet szerint az $f \circ g$ kiszámításakor először a g-t, azután az f-et kell végrehajtani.

Ezt azért érezzük furcsának, mert megszoktuk, hogy balról jobbra írunk, és ezért úgy képzelnénk, hogy az $f \circ g$ esetében „természetesebb" lenne, ha ez azt jelentené: hajtsd végre először f-et, utána g-t. Sok könyvben ezt a problémát úgy oldják meg, hogy a leképezés jelét a leképezett elem után írják, például $f(x)$ helyett xf vagy x^f szerepel. Könnyű meggondolni, hogy ez orvosolja a fenti természetellenességet. Mi mégsem alkalmazzuk ezt a trükköt, mert évek hosszú során át szoktattak bennünket például a $\sin(x)$ vagy $\log(x)$ jelölésre, és ezt nem könnyű újratanulni. Pedig a magyar nyelvben természetesebb lenne a fordított sorrend (hiszen míg az angol azt mondja: „sine of x", addig magyarul ez „x-nek a szinusza").

4.1.4. Gyakorlat. Számítsuk ki a fenti $f \in S_4$ esetén a $g = f \circ f$ kompozíciót, és írjuk fel ezt is a most tanult jelöléssel. Mutassuk meg, hogy g az f inverze lesz, vagyis $f \circ g = g \circ f$ az $\{1, 2, 3, 4\}$ halmaz identikus leképezése.

4.1.5. Gyakorlat. Igazoljuk, hogy S_X csoport a kompozíció műveletére nézve.

4.1.6. Definíció. Legyen X tetszőleges halmaz. Az S_X csoportot (a művelet a kompozíció) az X halmazon ható *szimmetrikus csoportnak* hívjuk. Ha $|X| = n$, akkor *n-edfokú* szimmetrikus csoportról beszélünk. Az S_X csoport egységelemét id_X, vagy egyszerűen csak id (sőt néha 1) jelöli, ez az identikus permutáció, amely minden elemet önmagába visz. Az $f \in S_X$ inverzét f^{-1}-gyel jelöljük.

A szimmetrikus csoport részcsoportjait permutációcsoportoknak hívjuk. Ezekkel részletesebben a 4.6. Szakaszban foglalkozunk majd. Általában úgy keletkeznek, hogy valamely alakzat összes szimmetriáit tekintjük. Fontos példaként most bemutatjuk a szabályos sokszögek szimmetriacsoportjait.

Legyen $n \geq 3$ egész. Egy szabályos n-szögnek $2n$ szimmetriája van (hogy nincsen több, azt majd a 4.6.8. Gyakorlatban látjuk be).

Szimmetria alatt olyan egybevágósági transzformációt értünk, ami a sokszöget önmagába viszi. Sokszor hasznos lesz ezeket úgy felfogni, mint a csúcsok permutációit. A két megközelítés lényegében ugyanaz, hiszen ha a csúcsok képeit megadjuk, akkor ($n \geq 3$ miatt) ez a transzformációt egyértelműen meghatározza.

Ezek a szimmetriák a középpont körüli n darab forgatás a $2\pi/n$ egész többszöröseivel, továbbá n tengelyes tükrözés. (Ha n páratlan, akkor mind az n tükrözés oldalfelező merőlegesre történik. Ha n páros, akkor a tükrözések fele történik oldalfelező merőlegesre, a másik fele pedig szemközti csúcsokon átmenő átlókra.)

4.1.7. Definíció. Egy szabályos n-szög szimmetriacsoportját n-edfokú *diédercsoportnak* nevezzük, és D_n-nel jelöljük.

Tudnánk-e kényelmesen, mechanikusan, gyorsan számolni e transzformációk kompozícióit? A rövidség kedvéért a kompozíciót egymás mellé írással jelöljük.

4.1.8. Állítás. *Jelöljön F a szabályos n-szög középpontja körüli $2\pi/n$ szögű forgatást, T pedig legyen a sokszög egyik (tetszőleges) tengelyes szimmetriája. Ekkor a D_n csoport összes eleme*

$$F^0 = 1,\ F,\ F^2,\ \dots,\ F^{n-1} \qquad \text{(a forgatások)},$$
$$T,\ TF,\ TF^2,\ \dots,\ TF^{n-1}, \qquad \text{(a tengelyes tükrözések)},$$

a szorzás szabálya pedig a következő:

$$F^iF^j = F^{i+j}, \qquad (TF^i)F^j = TF^{i+j},$$
$$F^i(TF^j) = TF^{j-i}, \qquad (TF^i)(TF^j) = F^{j-i},$$

ahol az F kitevőjében a $+$ és a $-$ jelek a mod n műveleteket jelentik. Speciálisan érvényesek az

$$F^n = 1, \qquad T^2 = 1, \qquad F^iT = TF^{-i}$$

összefüggések (ahol 1 az identitást jelöli).

A felsorolt állításokat ellenőrizhetnénk geometriai úton. Sokkal kényelmesebb és rövidebb lesz azonban a csoportelmélet fogalmait segítségül hívni a bizonyításhoz (lásd 4.9.8. és 4.9.9. Állítás). A következő szakaszban arról lesz szó, hogyan lehet a permutációkkal kényelmesen számolni.

Gyakorlatok, feladatok

4.1.9. Gyakorlat. Számítsuk ki az $f \circ g$ és $g \circ f$ kompozíciókat, ahol

$$f = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \quad \text{és} \quad g = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}.$$

Mely $n \geq 1$ egészekre lesz S_n kommutatív (vagyis Abel-csoport)?

4.1.10. Gyakorlat. Mely $n \geq 1$ egészekre lesz $\mathrm{GL}(n, T)$, illetve $\mathrm{SL}(n, T)$ Abel-csoport?

4.1.11. Gyakorlat. Mutassuk meg, hogy minden csoportban érvényes az *egyszerűsítési szabály*, vagyis az $ag = bg$, illetve $ga = gb$ egyenlőségek mindegyikéből $a = b$ következik.

4.1.12. Feladat. Tegyük fel, hogy S félcsoport (azaz van benne egy asszociatív művelet), amelyre nézve van egy bal oldali e egységelem, és S minden elemének van e-re nézve balinverze. Mutassuk meg, hogy akkor S csoport erre a műveletre (azaz e kétoldali egységelem, és minden elemnek van e-re nézve kétoldali inverze).

4.2. Permutációk előjele és ciklusfelbontása

Következő témánk a permutációk előjelének a vizsgálata lesz. Ezt általában kombinatorikai úton, az úgynevezett inverziók számának vizsgálatával szokás megközelíteni (lásd például Freud Róbert [**10**] könyvében az 1.1. Szakaszt). Mi ennek az útnak egy algebrai jellegű változatát járjuk végig.

4.2.1. Kérdés. Rendet lehet-e csinálni egy könyvespolcon úgy, hogy mindig csak két könyvet cserélünk meg?

Hát persze. Ha a legbaloldali helyen nem az a könyv van, ami odavaló, akkor odacseréljük azt, ami odavaló. Ezután a balról második helyre is odacseréljük azt, ami odavaló. Az eljárást folytatva minden könyv a helyére kerül (és a szükséges cserék száma a legrosszabb esetben is eggyel kevesebb, mint a könyvek száma).

4.2.2. Definíció. Legyen X halmaz. Azt a permutációt, amely az $x \neq y \in X$ elemeket cseréli ki, és X összes többi elemét fixen hagyja (vagyis önmagába viszi), az (x, y) szimbólummal fogjuk jelölni (az x és y közötti vesszőt néha elhagyva). Az így kapott permutációkat *cserének*, vagy *transzpozíciónak* nevezzük.

Az előző 4.2.1. Kérdésre adott válasz szerint S_n minden eleme felírható cserék szorzataként (és ehhez legfeljebb $n - 1$ csere mindig elegendő). Azt tervezzük, hogy azokat a permutációkat, amelyek páros sok csere szorzataként írhatók, páros permutációknak, azokat pedig, amelyek páratlan sok csere szorzataként írhatók, páratlan permutációknak nevezzük. Ezzel az elnevezéssel azonban probléma lehet, mert egy permutáció általában sokféleképpen áll elő cserék szorzataként.

4.2.3. Gyakorlat. Mutassuk meg, hogy

$$(12)(23)(31)(34) = (34)(24)$$

(az egymás mellé írás kompozíciót jelöl).

Ezek szerint nem lenne értelme beszélni a „néggyel osztható permutáció” fogalmáról, hiszen a fenti permutáció felírható néggyel osztható számú, és néggyel nem osztható számú transzpozíció szorzataként is. Ha lenne olyan permutáció, amely páros sok csere szorzataként is és páratlan sok csere szorzataként is előállna, akkor nem tudnánk, hogy most ezt párosnak, vagy páratlannak nevezzük. Szerencsére ez nem fordulhat elő, de ezt nem egészen triviális bebizonyítani. Most ez a bizonyítás következik.

Tekintsük az alábbi polinomot:

$$P(x_1, \ldots, x_n) = (x_1 - x_2) \cdot (x_1 - x_3) \cdot \ldots \cdot (x_1 - x_n) \cdot \\ \cdot (x_2 - x_3) \cdot \ldots \cdot (x_2 - x_n) \cdot \\ \ldots \\ \cdot (x_{n-1} - x_n) \,.$$

Vagyis összeszoroztuk az összes $x_i - x_j$ különbséget, ahol $i < j$.

Ha f permutáció az $\{1, 2, \ldots, n\}$ halmazon, akkor helyettesítsük P-be az $x_1, \ldots, x_n$ változókat az f által megadott sorrendben, azaz számítsuk ki a $P(x_{f(1)}, \ldots, x_{f(n)})$ kifejezést. Most is az $x_1, \ldots, x_n$ változók összes lehetséges különbségeit szorozzuk össze. Ha a P argumentumainak f szerinti új sorrendjében x_2 megelőzi x_1-et, akkor már nem az $x_1 - x_2$ különbség szerepel a szorzatban, hanem helyette az $x_2 - x_1$, vagyis a tényezők előjelei megváltozhatnak. Mindenesetre az eredmény csak előjelben különbözhet $P(x_1, \ldots, x_n)$-től. Ezt az előjelet (pontosabban a neki megfelelő $+1$ vagy -1 számot) az f permutáció előjelének fogjuk nevezni, és $\operatorname{sg}(f)$-fel jelöljük majd. Képletben:

$$P(x_{f(1)}, \ldots, x_{f(n)}) = \operatorname{sg}(f) P(x_1, \ldots, x_n) \,. \tag{4.1}$$

4.2.4. Gyakorlat. Határozzuk meg az (12) csere előjelét.

Természetesen roppant fáradságos lenne minden permutáció előjelét a P polinom segítségével kiszámítani. Ez nem is így fog történni! A P segítségével bebizonyítjuk az előjelképzés olyan tulajdonságait, amely már lehetővé teszi az előjel gyors, könnyű kiszámítását.

4.2.5. Lemma. *Ha $f, g \in S_n$, akkor* $\operatorname{sg}(f \circ g) = \operatorname{sg}(f)\operatorname{sg}(g)$.

Bizonyítás. A fenti (4.1) képletet az $f \circ g$ permutációra alkalmazva

$$P(x_{f\circ g(1)}, \ldots, x_{f\circ g(n)}) = \operatorname{sg}(f \circ g) P(x_1, \ldots, x_n) \,.$$

A bal oldalt máshogy is kiszámítjuk. Vezessük be az $y_j = x_{f(j)}$ segédváltozókat. Ekkor $x_{f\circ g(i)} = x_{f(g(i))} = y_{g(i)}$, és így

$$P(x_{f\circ g(1)}, \ldots, x_{f\circ g(n)}) = P(y_{g(1)}, \ldots, y_{g(n)}) = \operatorname{sg}(g) P(y_1, \ldots, y_n)$$

(az utolsó egyenlőség a (4.1) képlet következménye). Az x_i értékét visszaírva, és a (4.1) képletet harmadszor is alkalmazva

$$P(y_1, \ldots, y_n) = P(x_{f(1)}, \ldots, x_{f(n)}) = \operatorname{sg}(f) P(x_1, \ldots, x_n)$$

adódik. Így végülis

$$\operatorname{sg}(f \circ g) P(x_1, \ldots, x_n) = P(x_{f\circ g(1)}, \ldots, x_{f\circ g(n)}) = \operatorname{sg}(g)\operatorname{sg}(f) P(x_1, \ldots, x_n) \,.$$

A nem nulla P polinommal egyszerűsítve az állítást kapjuk. □

4.2.6. Gyakorlat. Nem baj-e, hogy az előző bizonyításban a $\mathrm{sg}(f \circ g) = \mathrm{sg}(g)\mathrm{sg}(f)$ összefüggés jött ki, és nem az, amit a lemmában állítottunk? Hiszen $f \circ g = g \circ f$ általában nem teljesül!

4.2.7. Következmény. *Az identikus permutáció előjele* $+1$. *Ha* $f, g \in S_n$ *egymás inverzei, akkor* f *és* g *előjelei egymásnak reciprokai, és így megegyeznek.*

Bizonyítás. Nyilván $id \circ id = id$, ezért az előző lemma miatt

$$\mathrm{sg}(id) = \mathrm{sg}(id \circ id) = \mathrm{sg}(id)\mathrm{sg}(id)\,.$$

A nem nulla $\mathrm{sg}(id)$ számmal egyszerűsítve $\mathrm{sg}(id) = 1$ adódik.

A második állítás bizonyításában azt használjuk ki, hogy $f \circ g = id$. Ismét az előző lemma miatt

$$1 = \mathrm{sg}(id) = \mathrm{sg}(f \circ g) = \mathrm{sg}(f)\mathrm{sg}(g)\,.$$

Ezért $\mathrm{sg}(g) = 1/\mathrm{sg}(f)$. De $\mathrm{sg}(f)$ értéke 1 vagy -1, és e két szám reciproka önmaga. □

A 4.2.5. Lemma igazából azt fejezi ki, hogy az $\mathrm{sg} : S_n \to \{1, -1\}$ leképezés művelettartó (lásd 2.2.32. Definíció), ahol az S_n-ben tekintett művelet a kompozíció, az $\{1, -1\}$ halmazon tekintett művelet pedig a számok közönséges szorzása (erre a műveletre $\{1, -1\}$ nyilván csoport). Ezért a fenti következmény bizonyításában a 2.2.41. Feladat állítására is hivatkozhattunk volna.

4.2.8. Lemma. *Minden csere előjele* -1.

Bizonyítás. A 4.2.4. Gyakorlat szerint az (12) csere előjele -1. Hasonlóan kiszámolhatnánk az (ij) csere előjelét is, elegánsabb azonban a következő gondolatmenet. Legyen g egy olyan permutáció, ami az 1-et i-be, a 2-t j-be viszi, a többi helyen pedig az értéke tetszőleges. Belátjuk, hogy

$$g \circ (12) \circ g^{-1} = (ij)\,.$$

Két függvény akkor egyenlő, ha minden helyen ugyanazt az értéket veszik fel, ezt kell ellenőrizni.

Az i helyen a jobb oldal értéke j. A bal oldalt kiértékelve először g inverzét kell alkalmaznunk, ez az i-t 1-be viszi. Ezután az (12) csere az 1-et elviszi 2-be, majd g a 2-t elviszi j-be. Tehát a bal oldal is j-be viszi az i-t.

A j helyen mind a bal, mind a jobb oldal értéke i lesz, a fentivel analóg gondolatmenet szerint.

Végül legyen k olyan hely, ami különbözik i-től is és j-től is. A jobb oldal k-t önmagába viszi. A bal oldalon először g inverzét alkalmazzuk k-ra, az eredményt jelölje ℓ (tehát akkor $g(\ell) = k$). Mivel g^{-1} bijekció, az ℓ szám különbözik 1-től és 2-től (hiszen az 1 és a 2 az i és a j képe g^{-1}-nél, és feltettük, hogy k különbözik i-től és j-től). Ezért (12) önmagába viszi ℓ-et, amelyet így g visszavisz k-ba. Tehát a bal és jobb oldal k-nál felvett értéke is egyenlő.

A fenti képletet tehát beláttuk, vegyük mindkét oldal előjelét. A 4.2.5. Lemmát ismételten alkalmazva

$$\mathrm{sg}\big((ij)\big) = \mathrm{sg}\big(g \circ (12) \circ g^{-1}\big) = \mathrm{sg}\big(g\big)\mathrm{sg}\big((12)\big)\mathrm{sg}\big(g^{-1}\big) = (-1)\mathrm{sg}\big(g\big)\mathrm{sg}\big(g^{-1}\big) = -1$$

a 4.2.4. Gyakorlat és a 4.2.7. Következmény miatt. □

Innen azonnal látszik, hogy ha egy permutáció páros sok csere szorzata, akkor előjele (a 4.2.5. Lemma szerint) $+1$, ha pedig páratlan sok csere szorzata, akkor előjele -1, és így két ilyen permutáció soha nem lehet egyenlő.

4.2.9. Definíció. Az $f \in S_n$ permutációt *párosnak* nevezzük, ha előáll páros sok csere szorzataként. Azt is mondjuk, hogy az ilyen permutációk *előjele* $+1$. A többi permutációt *páratlannak* mondjuk, ezek előjele -1. Az f permutáció előjelét $\mathrm{sg}(f)$ jelöli.

Foglaljuk össze most a permutációk előjelének eddig bizonyított tulajdonságait.

4.2.10. Tétel. *Legyen $n \geq 1$ egész és $f, g \in S_n$.*

(1) *Az S_n csoport egy eleme akkor és csak akkor páros permutáció, ha előáll páros sok csere szorzataként, és akkor és csak akkor páratlan permutáció, ha előáll páratlan sok csere szorzataként. Speciálisan minden csere páratlan permutáció, az identitás pedig páros permutáció (nulla darab csere szorzata).*
(2) $\mathrm{sg}(f \circ g) = \mathrm{sg}(f)\mathrm{sg}(g)$ *(ez a permutációk előjelének szorzástétele). Másképp fogalmazva: két páros, illetve két páratlan permutáció szorzata páros, egy páros és egy páratlan permutáció szorzata páratlan.*
(3) *Ha f és g egymás inverzei, akkor paritásuk és előjeleik egyenlők.*

Nagyon fontos megjegyzés, hogy ennek a tételnek a birtokában elfelejthetjük az előjel bonyolult, a P polinomot használó definícióját, ezt már soha nem fogjuk használni! A fenti tétel ugyanis egyértelműen meghatározza minden permutáció előjelét, és a lényeg az, hogy ilyen tulajdonságú sg függvény *létezik*. Ha ezt a létezést be tudnánk bizonyítani máshogy, egyszerűbben is, mint a P polinomra gondolva, akkor ezt a polinomot meg sem kellene említeni. Egy matematikai objektum tulajdonságai általában fontosabbak, mint az őt létrehozó konstrukció technikai részletei.

4.2.11. Definíció. Az S_n csoport páros permutációiból álló részcsoportot az n-edfokú *alternáló csoportnak* nevezzük, jele A_n.

Az előző tétel szerint a páros permutációk tényleg részcsoportot alkotnak. Most meghatározzuk az alternáló csoport elemeinek a számát.

4.2.12. Következmény. *Ha $n > 1$, akkor S_n-ben ugyanannyi páros és páratlan permutáció van. Az A_n alternáló csoport elemszáma tehát $n!/2$.*

Bizonyítás. Kölcsönösen egyértelmű megfeleltetést létesítünk a páratlan és a páros permutációk között. Ha f páros permutáció, akkor ehhez rendeljük hozzá az

$$F(f) = (12) \circ f$$

nyilván páratlan permutációt. Az F megfeleltetés azért lesz kölcsönösen egyértelmű, mert létezik inverze, ez tetszőleges g páratlan permutációhoz a

$$G(g) = (12) \circ g$$

páros permutációt rendeli. Az F és G tényleg egymás inverzei, hiszen ha egymás után alkalmazzuk őket, akkor

$$F\big(G(g)\big) = (12) \circ \big((12) \circ g\big) = \big((12) \circ (12)\big) \circ g = g\,,$$

és ugyanígy $G\big(F(f)\big) = f$. □

Ha X tetszőleges véges halmaz, amelynek n eleme van, akkor természetesen az S_X csoport esetében is beszélhetünk páros és páratlan permutációkról, valamint az A_X alternáló csoportról is, hiszen S_X-ben „ugyanúgy" kell a permutációkkal számolni, mint S_n-ben.

Egy permutáció előjelének megállapítása nem praktikus a P polinommal való számolással, de még a cserék szorzatára bontás is hosszadalmas lehet. Most egy olyan módszert mutatunk, amely ennél kényelmesebb és áttekinthetőbb. Ehhez először a csere fogalmát általánosítjuk.

4.2.13. Definíció. Legyen X halmaz, és $x_1, x_2, x_3, \ldots, x_{k-1}, x_k \in X$. Jelölje

$$(x_1, x_2, x_3, \ldots, x_{k-1}, x_k)$$

azt a permutációt, amelynél az x_1 képe x_2, az x_2 képe x_3, és így tovább, az x_{k-1} képe x_k, végül az x_k képe x_1, és X többi eleme a helyén marad. Az így kapott permutációkat *ciklusoknak* nevezzük. A k szám ennek a ciklusnak a *hossza*. A vesszőt a transzpozíciókhoz hasonlóan sokszor elhagyjuk majd a ciklus elemei közül.

A ciklus elnevezés magyarázata az, hogy a zárójelben a jelek *körbe*permutálódnak. Tipikus ciklus például, ha egy kártyacsomag lapjait úgy permutáljuk, hogy a felső lapot legalulra tesszük.

4.2.14. Gyakorlat. Mutassuk meg, hogy $(123) = (231)$, sőt tetszőleges $1 \le i \le k$ esetén

$$(x_1, \ldots, x_k) = (x_i, x_{i+1}, \ldots, x_k, x_1, x_2, \ldots, x_{i-1})\,,$$

vagyis egy ciklust bármelyik eleménél kezdve ugyanazt a permutációt kapjuk.

Nagyon fontos, hogy ne keverjük össze a permutációk kétféle jelölését. Az

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix} \quad \text{és} \quad g = (1342)$$

permutációk nem ugyanazok! Az f az 1-et 1-be, a g az 1-et 3-ba viszi. A g permutációt ciklus-jelöléssel négyféleképpen írhatjuk fel:

$$g = (1342) = (3421) = (4213) = (2134)\,.$$

Az f permutációnak a megadott felírásán nem lehet változtatni (mert akkor másik permutációt kapnánk). Ugyanakkor f is ciklus, és ezért három további módon felírható:

$$f = (234) = (342) = (423)\,.$$

A hagyományos jelölésnél tehát két sor van, a felső az alapsorrend. A ciklusos jelölésben viszont csak egy sor szerepel.

4.2.15. Definíció. Két ciklust *diszjunktnak* hívunk, ha nincs közös elemük.

4.2.16. Gyakorlat. Mutassuk meg, hogy ha f és g diszjunkt ciklusok, akkor felcserélhetők, azaz $f \circ g = g \circ f$.

A ciklusok jelentőségét a következő állítás világítja meg.

4.2.17. Tétel. *Tegyük fel, hogy X véges halmaz. Ekkor X minden permutációja felírható páronként diszjunkt ciklusok szorzataként.*

Bizonyítás. Egyben eljárást is adunk a ciklusfelbontás elkészítésére. Ehhez rajzolni fogunk, de kis gyakorlattal a rajz elhagyható, és az eljárás fejben elvégezhető.

Rajzoljuk le X elemeit egy papírra (vagyis minden $x \in X$ elemhez egy pont tartozzék). Rögzítsük az f permutációt, és minden $x \in X$ esetén húzzunk egy nyilat az x pontból az $f(x)$ pontba. Természetesen minden pontból pontosan egy nyíl indul, és minden pontba pontosan egy nyíl érkezik, hiszen f bijekció.

Vegyünk egy tetszőleges $x = x_1$ pontot, és kövessük sorban a belőle kiinduló nyilakat. Az x_1-ből induló nyíl x_2-be, az x_2-ből induló x_3-ba vezet, és így tovább. Mivel X véges, előbb-utóbb egy olyan pontba kell érkeznünk, ahol már jártunk. Megmutatjuk, hogy az *első* ilyen ismétlődő pont az $x = x_1$ kell, hogy legyen.

Legyen y az első olyan pont, ahol sétánk során kétszer járunk. Ebbe, mint az összes többi pontba is, csak egyetlenegy nyíl érkezik: $z \to y$. Tehát y-ba csakis z-ből érkezhetünk (mindkétszer). De z-ben nem jártunk kétszer, mert akkor z korábbi pont lenne a séta során, amit kétszer érintettünk. Ezért y a sétánk kiindulópontja, vagyis tényleg az x pont.

A sétánk során érintett pontok tehát egy $(x_1, x_2, \ldots, x_k)$ ciklust alkotnak, amit ebben a sorrendben járunk be, és utána visszatérünk x_1-be. Radírozzuk ki ezeket a pontokat, és a közéjük rajzolt k darab nyilat. A megmaradó rajzban újra minden pontból egy nyíl indul és egy nyíl érkezik, ezért megismételhetjük a gondolatmenetet. Így rajzunkat végülis diszjunkt „körökre” bontottuk. Megmutatjuk, hogy az így kapott diszjunkt ciklusok g szorzata (bármilyen sorrendben) az eredeti f permutáció.

Valóban: vegyünk egy tetszőleges x pontot, hová viszi ezt a g permutáció? Az x-et minden olyan ciklus fixálja, amelyben x nem szerepel. Az egyetlen olyan ciklusban, ahol x szerepel, az x-ből induló nyíl mentén mozdulunk el, amikor g-t alkalmazzuk, azaz $f(x)$-be jutunk. Az $f(x)$ pontot azonban a többi ciklus szintén fixálja, hiszen azokban sem szerepel. Ezért összegészében g az x-et tényleg $f(x)$-be viszi. □

Láttuk, hogy egy permutációt sokféleképpen írhatunk fel cserék szorzataként. A diszjunkt ciklusokra való felbontás ugyanakkor a sorrendtől eltekintve egyértelmű. Ennek pontos megfogalmazását és bizonyítását gyakorlatnak hagyjuk.

4.2.18. Gyakorlat. Fogalmazzuk meg, hogy a diszjunkt ciklusokra való felbontás milyen értelemben egyértelmű, és bizonyítsuk is be az állítást.

4.2.19. Gyakorlat. Igazoljuk, hogy

$$(x_1, \dots x_k) = (x_1x_2)(x_2x_3)\dots(x_{k-2}x_{k-1})(x_{k-1}x_k)\,.$$

Itt $k-1$ tényező szerepel, ezért *páratlan hosszú ciklus páros permutáció, páros hosszú ciklus pedig páratlan permutáció.* Így (a permutációk előjelének szorzástétele miatt) most már könnyű egy f permutáció előjelét meghatározni.

4.2.20. Következmény. *Bontsuk az f permutációt diszjunkt ciklusok szorzatára. Ha páratlan sok páros hosszú ciklus keletkezik, akkor f páratlan, egyébként pedig páros.*

Bizonyítás. Szorzat előjele az előjelek szorzata. A páratlan hosszú ciklusok párosak, tehát az előjel kiszámítása szempontjából nem számítanak. A páros hosszú ciklusok páratlanok, tehát ha m darab van belőlük, akkor az előjel $(-1)^m$. □

Természetesen ez az állítás akkor is igaz, ha a felbontásban szereplő ciklusok nem diszjunktak.

Gyakorlatok, feladatok

4.2.21. Gyakorlat. Adjuk meg az alábbi permutációk ciklusfelbontását és előjelét. Tegyük meg ugyanezt a „hátulról előre" permutációval is (amelynél az alsó sorban a felső sorrend fordítottja szerepel).

$$\begin{bmatrix}1&2&3&4&5&6&7&8\\2&5&6&1&4&3&8&7\end{bmatrix}\quad\begin{bmatrix}1&2&3&4&5&6&7&8\\5&7&6&4&8&3&2&1\end{bmatrix}\quad\begin{bmatrix}a&b&c&d&e\\c&a&e&b&d\end{bmatrix}$$

$$(1234)(35)(1432)(35)\,,\quad (12345)(234)(12345)^{-1}\,,\quad [(12)(23)(34)]^{1222}\,.$$

4.2.22. Gyakorlat. Legyen $f = (12)(345)$. Hány különböző hatványa van ennek a permutációnak a kompozíció műveletére nézve (lásd 2.2.17. Definíció)? Melyik a legkisebb hatványa, ami az egységelemet adja? Mely k és ℓ egészekre igaz, hogy $f^k = f^\ell$?

4.2.23. Gyakorlat. Rendezhetők-e a könyvek egy könyvespolcon, ha csak szomszédos (helyen lévő) könyvek cseréjét engedjük meg?

4.2.24. Gyakorlat. Mutassuk meg, hogy egy kártyacsomag lapjainak tetszőleges sorrendje megkapható a következő kétféle mozdulat véges sokszori alkalmazásával: a legfelső két lap cseréje, illetve a csomag elemelése (azaz a csomag tetejéről leveszünk egy kisebb csomagot, és azt változatlan sorrendben az aljára tesszük). Hogyan fogalmazható meg ez az állítás S_n permutációi segítségével? Milyen ciklusfelbontású permutációk felelnek meg ennek a két mozdulatnak?

4.2.25. Gyakorlat. Tegyük fel, hogy a kártyacsomagunk csak négy lapból áll, és az emeléseken kívül az első és a harmadik lapot szabad megcserélni. Megkaphatjuk-e a lapok összes lehetséges sorrendjét?

4.2.26. Feladat. Bizonyítsuk be, hogy ha $n \geq 3$, akkor A_n minden eleme (azaz minden páros permutáció) előáll hármasciklusok szorzataként.

4.2.27. Feladat. Keressük meg az összes olyan $f \in S_n$ permutációt, amely felcserélhető az $(1, 2, \ldots, n)$ ciklussal.

4.2.28. Feladat. Mutassuk meg, hogy egy permutáció akkor és csak akkor hatványa egy ciklusnak, ha ciklusfelbontásában a ciklusok hossza azonos (az egyelemű ciklusokat nem írjuk ki).

4.2.29. Feladat. Legyen adott S_n transzpozícióinak egy halmaza. Készítsünk egy G gráfot az $\{1, 2, \ldots, n\}$ csúcshalmazon úgy, hogy ha a halmazban benne van az (ab) transzpozíció, akkor behúzzuk az a-t b-vel összekötő élet. Bizonyítsuk be a következő állításokat.

(1) Ha a G gráf összefüggő, akkor az adott transzpozíciók alkalmas szorzataként minden permutáció előállítható (a szorzatban ugyanaz a transzpozíció többször is szerepelhet).
(2) Ha i és j a G gráf különböző komponenseiben vannak (vagyis nincs közöttük út), akkor az adott transzpozíciók szorzataként nem állítható elő egyetlen olyan permutáció sem, amely i-t j-be viszi.

4.2.30. Feladat. Mutassuk meg, hogy S_n valamennyi eleme előáll legfeljebb $n - 1$ darab transzpozíció szorzataként. Van-e olyan elem, amihez $n-1$ transzpozíciónál kevesebb nem elegendő?

4.2.31. Feladat. Legyenek k és t egynél nagyobb, relatív prím egészek. Az $1, 2, \ldots, n$ számok $1, 2, \ldots, n$ sorrendjéből kiindulva tetszőleges két olyan elemet felcserélhetünk, amelyek különbsége k vagy t. Bizonyítsuk be, hogy ilyen lépések egymásutánjával akkor és csak akkor juthatunk el minden lehetséges sorrendhez, ha $k + t - 1 \leq n$.

4.3. Elemrend, ciklikus csoportok

Ebben a szakaszban először a rend korábban komplex számokra már megismert tulajdonságait fogjuk általánosítani tetszőleges csoportra. Ez elvezet bennünket a ciklikus csoport fogalmához, melyeknek leírjuk a szerkezetét. Menet közben tisztázzuk azt a kérdést is, hogy mikor érdemes két csoportot „egyformának” tekinteni.

Az 1.5. Szakaszban megállapítottuk, hogy ha egy komplex számnak van két egyenlő hatványa, akkor a hatványai periodikusan ismétlődnek. A periódus hosszát a komplex szám rendjének neveztük. Megemlítettük, hogy ugyanez érvényes akkor is, ha egy n-hez relatív prím számot hatványozunk a mod n szorzásra nézve, így jutunk el a számelméletben tanult

rend fogalmához. A 4.2.22. Gyakorlat megoldásában pedig láttuk, hogy a permutációk hatványozásakor is hasonló dolgok történhetnek.

Ez a három példa azt sugallja, hogy általánosan is érvényesek hasonló összefüggések. A 2.2.18. Gyakorlatban már megtanultuk, hogy ha a művelet asszociatív, van egy e egységelem, és a hatványozandó elemnek létezik inverze, akkor a hatványozás szokásos azonosságai a pozitív és negatív kitevőkre is érvényben maradnak. Ezeket az azonosságokat használni szeretnénk, és így azt érdemes föltenni, hogy egy G csoportban vagyunk. Tehát:

- ha G a nem nulla komplex számok csoportja a szorzásra, azaz $G = \mathbb{C}^\times$, akkor vissza szeretnénk kapni a komplex számok rendjének tulajdonságait, ezért ez mintául szolgál az általánosítás elvégzéséhez;
- ha $G = \mathbb{Z}_n^\times$, akkor ingyen meg fogjuk kapni a számelméletben tanult elemrend tulajdonságait;
- ha $G = S_n$, akkor szintén ingyen a permutációk esetében is kiderül majd, hogy mik a hatványozás és az elemrend tulajdonságai;
- végül ha később új csoportokról hallunk, akkor az elemrend tulajdonságait ott is felhasználhatjuk majd (mondjuk az általános lineáris csoportban).

Az elvégzendő munka annyira hasonlít ahhoz, amin komplex számok esetében már átrágtuk magunkat, hogy az egészet gyakorlatnak hagyjuk.

4.3.1. Definíció. Legyen G csoport és $g \in G$. A g elem *rendje* a g különböző hatványainak a száma (ez tehát vagy egy pozitív egész szám, vagy pedig a ∞ szimbólum; az utóbbi esetben azt mondjuk, hogy g rendje végtelen). A g elem rendjének jele $o(g)$ (de csoportelméleti könyvekben gyakran alkalmazzák a $|g|$ jelölést is).

Azt mondjuk, hogy egy k egész szám *jó kitevője* a $g \in G$ csoportelemnek, ha $g^k = 1$ (azaz G egységeleme).

4.3.2. Gyakorlat. Legyen G csoport és $g \in G$. Mutassuk meg az alábbi állításokat.

(1) A g elemnek vagy bármely két egész kitevőjű hatványa különböző (ilyenkor a rendje végtelen), vagy pedig a hatványok a rend szerint periodikusan ismétlődnek.
(2) A rend a legkisebb pozitív jó kitevő.
(3) Tetszőleges k és ℓ egészekre

$$\boxed{\boxed{g^k = g^\ell \iff o(g) \mid k-\ell, \quad \text{speciálisan} \quad g^k = 1 \iff o(g) \mid k.}}$$

A jó kitevők tehát pontosan a rend többszörösei.
(4) A hatvány rendjének képlete:

$$\boxed{o(g^k) = \frac{o(g)}{(o(g), k)}\,.}$$

(5) Az egységelem az egyetlen olyan elem, melynek a rendje 1.

Egy permutáció ciklusfelbontása nemcsak az előjel, hanem a rend kiszámításához is komoly segítség. Azonban míg az előjelképzésnél nem volt lényeges, hogy a felbontásban szereplő ciklusok diszjunktak-e, a rend kiszámításánál ez alapvetően fontos.

4.3.3. Állítás. *Bontsuk az f permutációt diszjunkt ciklusok szorzatára. Ekkor f rendje a szereplő ciklusok hosszának legkisebb közös többszöröse.*

Bizonyítás. Elsőként azt mutatjuk meg, hogy minden k hosszú ciklus rendje k. Ha az $f = (x_1, \dots, x_k)$ ciklust $\ell < k$-adik hatványra emeljük, akkor az x_1-et $x_{\ell+1}$-be viszi. Ez nem az x_1, és így f^ℓ még nem az identikus permutáció. Viszont $f^k = id$, hiszen ekkor a ciklus minden x_i eleme egyszer „körbemegy". Vagyis k a legkisebb pozitív egész, amelyre f-et emelve az identitást kapjuk, és így k az f rendje.

Tekintsük most az $f = f_1 \dots f_m$ permutációt, ahol az $f_1, \dots, f_m$ diszjunkt ciklusok. Azt állítjuk, hogy $f^\ell = id$ akkor és csak akkor, ha minden j-re $f_j^\ell = id$. Ez azért igaz, mert ezek a ciklusok diszjunkt halmazokat mozgatnak. Ha például f_1 az $(x_1, \dots, x_k)$ ciklus, akkor az $f_2, \dots, f_n$ permutációk az $x_1, \dots, x_k$ mindegyikét fixen hagyják, és ezért f^ℓ ugyanoda viszi mindegyik x_i elemet, mint az f_1^ℓ. De f_j^ℓ akkor és csak akkor az identitás, ha f_j rendje (vagyis a hossza) osztója ℓ-nek. Tehát $f^\ell = id$ akkor és csak akkor, ha mindegyik f_j ciklus hossza osztója ℓ-nek. A legkisebb ilyen tulajdonságú pozitív egész pedig e ciklushosszak legkisebb közös többszöröse. □

Ha egy g csoportelem rendje $n < \infty$, akkor az előzőek szerint $g^{n-1} = g^{-1}$, vagyis g inverze megkapható úgy, hogy a g elemet néhány példányban önmagával összeszorozzuk.

4.3.4. Következmény. *Ha G olyan csoport, amelynek minden eleme véges rendű (például G véges csoport), akkor G minden nem üres, szorzásra zárt részhalmaza részcsoport.*

Egy G csoportot *torziócsoportnak* nevezünk, ha minden elemének véges a rendje. Ebből még nem következik, hogy a csoport maga is véges, például az összes komplex egységgyökök végtelen torziócsoportot alkotnak a szorzás műveletére. Egy G csoport *torziómentes*, ha az egységelemen kívül minden elem rendje végtelen. Ilyen például a komplex számok additív csoportja.

A csoportelméletben nemcsak egy csoportelem rendjéről, hanem magának a csoportnak a rendjéről is szokás beszélni.

4.3.5. Definíció. Egy G csoportnak a *rendje* a csoport elemeinek a száma. A halmazoknál megszokott jelöléssel a G csoport rendjét $|G|$ jelöli.

Fontos szerepet játszanak azok a csoportok, amelyek „olyan kicsik, hogy" egy elemük hatványaiból állnak. Ilyen csoport például az egész számok $\mathbb{Z}^+$ csoportja az összeadásra. Mivel a művelet az összeadás, itt hatvány helyett többszörösről kell beszélnünk. Az pedig világos, hogy az 1 szám összes egész számú többszöröse kiadja az összes egész számot.

4.3.6. Definíció. Egy G csoportot *ciklikusnak* nevezünk, ha egy alkalmas g elemének az egész kitevős hatványaiból áll. Az ilyen tulajdonságú g elemeket G *generátorelemének* (ritkán *primitív elemének*) nevezzük. Még máshogy fogalmazva: a g elem *generálja* a G csoportot.

Minden ciklikus csoport kommutatív, hiszen egy elem hatványai egymással felcserélhetők. További fontos példa ciklikus csoportra a $\mathbb{Z}_n^+$ csoport, ez is nyilván az 1 szám összes többszöröseiből áll.

4.3.7. Gyakorlat. Határozzuk meg a $\mathbb{Z}^+$ és a $\mathbb{Z}_{12}^+$ csoportok összes generátorelemét.

Nemsokára belátjuk első csoportelméleti struktúratételünket, ami azt mondja ki, hogy a felsoroltakon kívül nincs más ciklikus csoport. Mielőtt ezt megfogalmaznánk, tisztáznunk kell, mit értünk azalatt, hogy „nincs más"? Hiszen például az 1 és a -1 számok egy G csoportot alkotnak a szorzásra, ami nyilvánvalóan ciklikus: a -1 hatványaiból áll. Vegyük észre azonban, hogy ebben a G csoportban „ugyanúgy kell számolni", mint a $\mathbb{Z}_2^+$ csoportban. Hiszen ha valakinek el kellene mondanunk, hogy hogyan is kell számolni ezekben a csoportokban, akkor valahogy a következőképpen fogalmazhatnánk.

„Mindkét csoportnak két eleme van, a neutrális elem (ezt jelölje e), és ezen kívül még egy másik elem (ezt jelölje b). A neutrális elemmel nyilvánvaló, hogyan kell a műveletet végezni, ha meg a b elemet műveletezzük össze saját magával, akkor az e-t kapjuk (hiszen $(-1)(-1) = 1$, illetve $1 +_2 1 = 0$)."

Általában két csoportot akkor tekinthetünk „egyformának", ha „ugyanúgy kell számolni bennük", még ha mások is az elemeik vagy a művelet. Csak abban különbözhetnek, hogy az elemeket vagy a műveletet „máshogy hívják". A fenti példában a neutrális elem egyszer 0, egyszer meg 1 volt, a csoport „másik eleme" pedig egyszer 1, egyszer meg -1. Tekintsük azt a $\psi : \mathbb{Z}_2^+ \to G$ megfeleltetést, amelynél $\psi(0) = 1$ és $\psi(1) = -1$, ez kölcsönösen egyértelmű. Azt, hogy a két csoportban „ugyanúgy kell számolni", az fejezi ki, hogy a ψ leképezés *művelettartó* (erről már volt szó a 2.2.32. Definícióban is). Például a

$$\psi(1 +_2 1) = \psi(1)\psi(1)$$

képlet így olvasható: ha már a $\mathbb{Z}_2^+$ csoportban tudom, hogy az 1 elemet hogyan kell önmagával összeadni, akkor ez a képlet megadja, hogy a neki megfelelő $\psi(1) = -1$ elemet hogyan kell önmagával összeszorozni a G csoportban. Ha valaki az első csoportban ismeri az összes elempárra a művelet eredményét, akkor ψ segítségével a második csoportban is minden számítást el tud végezni.

4.3.8. Definíció. Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre. Azt mondjuk, hogy egy $\psi : G \to H$ leképezés *csoport-homomorfizmus*, ha művelettartó, vagyis ha tetszőleges $a, b \in G$ esetén

$$\psi(a * b) = \psi(a) \bullet \psi(b)\,.$$

Ha ψ kölcsönösen egyértelmű is a G és H halmazok között, akkor ψ *izomorfizmus*. A G és a H *izomorf csoportok*, ha létezik közöttük izomorfizmus. Ennek jele $G \cong H$.

4.3.9. Gyakorlat. Igazoljuk, hogy homomorfizmusok kompozíciója is homomorfizmus, és egy izomorfizmus inverze is izomorfizmus.

4.3.10. Gyakorlat. Mutassuk meg az izomorfia alábbi tulajdonságait.

(1) Minden csoport izomorf önmagával (az izomorfia *reflexív*).
(2) Ha $G \cong H$, akkor $H \cong G$ (az izomorfia *szimmetrikus*).
(3) Ha $G \cong H$ és $H \cong K$, akkor $G \cong K$ (az izomorfia *tranzitív*).

A 2.2.41. Feladatban beláttuk, hogy minden ψ csoport-homomorfizmus G egységelemét a H egységelemébe képzi, továbbá azt is, hogy $g \in G$ esetén

$$\psi(g^{-1}) = \psi(g)^{-1}$$

(a bal oldalon G-beli, a jobb oldalon H-beli inverzképzés szerepel). Vagyis minden homomorfizmus tartja az inverzképzés műveletét is.

4.3.11. Gyakorlat. Mutassuk meg, hogy minden homomorfizmus tartja az egész kitevős hatványozás műveletét is, vagyis ha $\psi : G \to H$ csoport-homomorfizmus, $g \in G$, és n egész szám, akkor $\psi(g^n) = \psi(g)^n$.

Az izomorfizmusok megőriznek minden olyan tulajdonságot, amely a csoport műveletének segítségével lett definiálva. Ilyen például a kommutativitás, a részcsoportok, az elemek rendje, és így tovább. Ezekre az állításokra az alábbi gyakorlatokban mutatunk mintabizonyításokat.

4.3.12. Gyakorlat. Legyen $\psi : G \to H$ csoport-homomorfizmus. Mi a kapcsolat $g \in G$ és $\psi(g) \in H$ rendje között? Mutassuk meg, hogy izomorfizmusnál az elemrend nem változik.

4.3.13. Gyakorlat. Legyen $\psi : G \to H$ szürjektív homomorfizmus. Mutassuk meg, hogy ha G kommutatív csoport, akkor H is az, és ha G ciklikus, akkor H is.

Folytassuk most a ciklikus csoportok analízisét. Először leírjuk őket izomorfia erejéig, majd meghatározzuk az elemeik rendjeit és a részcsoportjaikat.

4.3.14. Tétel. *Egy csoport akkor és csak akkor ciklikus, ha izomorf a $\mathbb{Z}^+$ vagy a $\mathbb{Z}_n^+$ csoportok valamelyikével (ahol $n \geq 1$ egész). Speciálisan minden ciklikus csoport kommutatív.*

Bizonyítás. Tegyük fel, hogy G ciklikus csoport, vagyis van olyan g eleme, hogy G a g elem egész kitevős hatványaiból áll. A G csoport műveletét szorzásnak nevezzük, és egymás mellé írással jelöljük majd.

Először azt az esetet vizsgáljuk, amikor g rendje végtelen. Tudjuk, hogy ekkor a g^k elemek páronként különbözők, és ezért a $\psi : k \to g^k$ leképezés $\mathbb{Z}$-ből G-be injektív (azaz különböző elemek képe is különböző). Mivel G a g hatványaiból áll, ez a leképezés szürjektív is, vagyis kölcsönösen egyértelmű. A művelettartás a hatványozás azonosságaiból következik: a 2.2.18. Gyakorlat szerint

$$\psi(k + \ell) = g^{k+\ell} = g^k g^\ell = \psi(k)\psi(\ell)\,.$$

Tehát G izomorf a $\mathbb{Z}^+$ csoporttal.

Ha a g elem rendje véges, mondjuk n, akkor azt mutatjuk meg, hogy G a $\mathbb{Z}_n^+$ csoporttal izomorf. Most is a $\psi(k) = g^k$ leképezést tekintjük. Az elemrendről tanultak miatt ez kölcsönösen egyértelmű $\mathbb{Z}_n$ és G között (hiszen g összes hatványa éppen $g^0, g^1, \ldots, g^{n-1}$). A művelettartáshoz azt kell megmutatni, hogy

$$g^{k+_n \ell} = g^k g^\ell \,.$$

Ez azonban teljesül: $g^k g^\ell = g^{k+\ell}$, a $k + \ell$ és $k +_n \ell$ számok különbsége a $+_n$ művelet definíciója szerint osztható n-nel, és így az n rendű g elem megfelelő két hatványa tényleg megegyezik.

Beláttuk tehát, hogy minden ciklikus csoport izomorf a $\mathbb{Z}^+$, illetve a $\mathbb{Z}_n^+$ csoportok valamelyikével. Még azt kell megmutatni, hogy megfordítva, ha egy G csoport izomorf a $\mathbb{Z}^+$, illetve a $\mathbb{Z}_n^+$ csoportok valamelyikével, akkor ciklikus. Azt már tudjuk, hogy $\mathbb{Z}^+$ és $\mathbb{Z}_n^+$ ciklikus csoportok. Ezért a 4.3.13. Gyakorlat miatt G is ciklikus. □

Egy csoportról sokszor egyáltalán nem könnyű eldönteni, hogy ciklikus-e, és ha a válasz igenlő, akkor ez rögtön nemtriviális alkalmazásokhoz vezethet.

4.3.15. Kérdés. Ciklikus-e a $\mathbb{Z}_{13}^\times$ csoport?

Némi keresgélés után rájöhetünk arra, hogy igen: ez a csoport a 2 hatványaiból áll. Általában is igaz az, hogy ha p prímszám, akkor a $\mathbb{Z}_p^\times$ csoport ciklikus. Ez nevezetes számelméleti tétel, amit ott úgy szokás fogalmazni, hogy „létezik primitív gyök modulo p".

4.3.16. Tétel. *Legyen T véges test. Ekkor T multiplikatív csoportja ciklikus. Speciálisan ha p prímszám, akkor a $\mathbb{Z}_p^\times$ csoport ciklikus, és így izomorf a $\mathbb{Z}_{p-1}^+$ csoporttal.*

Erre a tételre két bizonyítást is adunk a későbbiekben (lásd 4.4.36. Feladat és 4.8.31. Gyakorlat). Általában a k számot akkor nevezzük *primitív gyöknek* mod n, ha generálja a $\mathbb{Z}_n^\times$ csoportot.

Mi egy ilyen izomorfia haszna? Ha valaki megkérdezi tőlünk, hogy hány hatodrendű elem van a $\mathbb{Z}_{13}^\times$ csoportban, akkor a következőképpen válaszolhatunk. Ez a csoport ciklikus, tehát izomorf a $\mathbb{Z}_{12}^+$ csoporttal. Ebben már könnyebb számolni, azonnal látjuk, hogy két hatodrendű elem van, a 2 és a 10. Ezért két hatodrendű elem van a $\mathbb{Z}_{13}^\times$ csoportban is: a nekik megfelelő $2^2 = 4$ és $2^{10} = 10$. A $\mathbb{Z}_p^\times$ csoport ciklikus mivolta teszi lehetővé az úgynevezett binom kongruenciák megoldását a számelméletben.

4.3.17. Lemma. *Legyen G tetszőleges csoport, és g egy d (véges) rendű eleme. Ekkor g hatványainak rendje d-nek osztója, és g-nek pontosan $\varphi(d)$ darab d rendű hatványa van (itt φ az Euler-függvény).*

Bizonyítás. A hatvány rendjének képlete szerint

$$o(g^k) = \frac{o(g)}{(o(g), k)} = \frac{d}{(d, k)} \,.$$

Ez tényleg osztója d-nek, és pontosan akkor lesz d, ha $(d, k) = 1$. Mivel g rendje d, a k kitevő a $0, 1, \ldots, d-1$ értékeket veheti fel. A keresett d rendű elemek száma tehát azon $0 \leq k < d$ egészek számával egyenlő, amelyek d-hez relatív prímek, azaz $\varphi(d)$. □

4.3.18. Állítás. *Legyen G véges ciklikus csoport. Ha a d pozitív egész osztója G rendjének, akkor G-nek pontosan d darab olyan g eleme van, melyre $g^d = 1$, és ezek ciklikus részcsoportot alkotnak. A G csoportnak pontosan $\varphi(d)$ darab d rendű eleme van, amelyek egymás hatványai. Ha d nem osztója G rendjének, akkor G-ben nincs d rendű elem.*

Bizonyítás. Legyen $|G| = n$. Mivel G ciklikus, egy $g \in G$ elemének a hatványaiból áll. Így a g elemnek n különböző hatványa van, tehát a rendje n.

Tegyük fel, hogy $d \mid n$. A g^k elem d-edik hatványa akkor 1, ha $g^{kd} = 1$, vagyis ha $n \mid kd$, ami azzal ekvivalens, hogy $(n/d) \mid k$. Ha $h = g^{n/d}$, akkor ezek az elemek

$$h, h^2, \ldots, h^{d-1}, h^d = 1\,.$$

Tehát azok az elemek, amelyek d-edik hatványa 1, tényleg egy d rendű ciklikus részcsoportot alkotnak. Az előző lemma miatt így G-ben $\varphi(d)$ darab d rendű elem van (hiszen ha egy elem rendje d, akkor a d-edik hatványa 1, vagyis szerepel a felsoroltak között).

Ha h_1 egy másik d rendű eleme G-nek, akkor az előző lemma miatt ennek is $\varphi(d)$ darab d rendű hatványa van, vagyis G összes d rendű eleme hatványa lesz. Ezért a d rendű elemek tényleg egymás hatványai. Végül ha d nem osztója n-nek, akkor G-ben az előző lemma miatt nincs d rendű elem. □

4.3.19. Gyakorlat. Mutassuk meg, hogy a komplex n-edik egységgyökök csoportot alkotnak a szorzásra, és ez ciklikus csoport. Vezessük le az előző állításból, hogy a primitív n-edik egységgyökök száma $\varphi(n)$.

4.3.20. Lemma. *Ciklikus csoport minden részcsoportja is ciklikus.*

Bizonyítás. Az alábbiak megértéséhez érdemes átismételni a 3.2.6. Tétel bizonyítását és a 3.2.23. Feladat megoldását. Legyen G ciklikus csoport, amely a g elemének a hatványaiból áll, és H részcsoportja G-nek. Tekintsük azokat a k egészeket, melyekre $g^k \in H$:

$$I = \{k \in \mathbb{Z} : g^k \in H\}\,.$$

Megmutatjuk, hogy az I nem üres halmaz zárt az összeadásra, és minden elemének minden egész többszörösét tartalmazza. Valóban, nyilván $0 \in I$, hiszen g^0 a G és H közös egységeleme. Ha $k, \ell \in I$, akkor $g^k \in H$ és $g^\ell \in H$, és így $g^{k+\ell} = g^k g^\ell \in H$ (mert H zárt a szorzásra), vagyis $k + \ell \in I$. Ha pedig $k \in I$ és $m \in \mathbb{Z}$, akkor $g^k \in H$, vagyis $g^{km} = (g^k)^m \in H$ (hiszen H zárt a hatványozásra), vagyis $km \in I$. A 3.2.23. Feladat miatt van olyan j egész, hogy I éppen j többeseiből áll. Így $g^k \in H$ akkor és csak akkor, ha $j \mid k$, vagyis ha g^k hatványa g^j-nek. Tehát H pontosan g^j hatványaiból áll, és ezért ciklikus. □

A végtelen ciklikus csoport részcsoportjai tehát kölcsönösen egyértelmű megfeleltetésben állnak a nemnegatív egészekkel, hiszen minden részcsoportot egyértelműen generálhatunk egy nemnegatív egész számmal.

A fenti állítás már a 3.2.23. Feladatból is következik. Valóban, ha I részcsoportja $\mathbb{Z}^+$-nak, akkor bármely elemének az egész többszöröseit is tartalmazza, hiszen minden részcsoport zárt az egész kitevőjű hatványozásra, amely az additív írásmód esetén a többszörösnek felel meg.

4.3.21. Állítás. *Ha G egy n rendű (véges) ciklikus csoport, akkor annyi részcsoportja van, ahány pozitív osztója n-nek: minden d osztóhoz pontosan egy d rendű részcsoport létezik. Ez pontosan a generátorelem azon hatványaiból áll, ahol a kitevő n/d-nek többszöröse.*

Bizonyítás. Tegyük fel, hogy G véges, rendje n, és H egy d rendű részcsoportja G-nek. Az előző lemma miatt H ciklikus csoport, álljon a h elem hatványaiból. Ekkor h rendje d. Az előző 4.3.18. Állításban már megmutattuk, hogy h rendje osztója G rendjének, azaz $d \mid n$, továbbá hogy G minden d rendű eleme hatványa h-nak. Ha H_1 is egy d rendű részcsoport, akkor ez is ciklikus, és egy szintén d rendű h_1 elem hatványaiból áll. Ezért h és h_1 egymás hatványai, vagyis ugyanazok a hatványaik, és így $H = H_1$. Tehát G-nek legfeljebb egy darab d rendű részcsoportja lehet: az, amit az előző állításban megismertünk. □

Gyakorlatok, feladatok

4.3.22. Gyakorlat. Határozzuk meg a $\mathbb{Z}_m^+$, illetve $\mathbb{Z}_m^\times$ csoportok elemeinek a rendjeit, ahol $m = 7, 8, 12$.

4.3.23. Gyakorlat. Határozzuk meg a g elem rendjét a G csoportban az alábbi esetekben.

(1) $G = \mathbb{R}^+$, $g = -1$.
(2) $G = \mathbb{R}^\times$, $g = -1$.
(3) $G = \mathbb{Z}_{19}^+$, $g = 17$.
(4) $G = \mathbb{Z}_{19}^\times$, $g = 17$.
(5) $G = \mathbb{Z}_{32}^+$, $g = 3$.
(6) $G = \mathbb{Z}_{32}^\times$, $g = 3$.
(7) $G = \mathbb{Z}_{11}[x]^+$, $g = x + 1$.
(8) $G = \mathbb{Z}_{11}[x]^\times$, $g = 5$.

4.3.24. Gyakorlat. Határozzuk meg a 4.2.21. Gyakorlatban szereplő permutációk rendjeit.

4.3.25. Gyakorlat. Hány n hosszú ciklus van S_n-ben?

4.3.26. Gyakorlat. Hány másodrendű, harmadrendű, negyedrendű, ötödrendű, hatodrendű, illetve tizenkettedrendű elem van A_7-ben?

4.3.27. Gyakorlat. Legyen G csoport, amelynek elemszáma véges, és legalább kettő. Mutassuk meg, hogy G-ben van prímrendű elem.

4.3.28. Gyakorlat. Legyen G csoport és $g \in G$. Igazoljuk, hogy g akkor és csak akkor hatványa g^k-nak, ha $\big(o(g), k\big) = 1$.

4.3.29. Gyakorlat. Legyen g egy n-edrendű eleme a G csoportnak és $g = h^m$, ahol $m \mid n$. Határozzuk meg h rendjét.

4.3.30. Gyakorlat. Igaz-e tetszőleges G csoportban, hogy ha G-ben van d rendű elem, akkor ezek száma legalább $\varphi(d)$ (itt φ az Euler-függvény)? És az, hogy pontosan $\varphi(d)$?

4.3.31. Gyakorlat. Ciklikus-e a három-hatványadik komplex egységgyökök csoportja a szorzásra?

4.3.32. Gyakorlat. Mutassuk meg, hogy ha g és h relatív prím rendű felcserélhető elemei egy csoportnak, akkor $o(gh) = o(g)o(h)$. Elhagyható-e a két feltétel valamelyike?

4.3.33. Feladat. Igazoljuk, hogy ha a G csoport minden elemének a négyzete az egységelem, akkor G Abel. Igaz-e az állítás négyzet helyett negyedik hatványra?

4.3.34. Feladat. Mutassuk meg, hogy $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$ tetszőleges a, n, m pozitív egészekre.

A $\Phi_n(x)$ körosztási polinom gyökei a $\mathbb{C}$ test multiplikatív csoportjának n rendű elemei. A következő feladat azt mutatja, hogy ez igaz a $\mathbb{Z}_p$ testre is, ha $p \nmid n$.

4.3.35. Feladat. Tekintsük a $\Phi_n(x)$ körosztási polinomot $\mathbb{Z}_p$ fölött, ahol p olyan prímszám, amely nem osztója n-nek. Mutassuk meg, hogy ennek gyökei pontosan a $\mathbb{Z}_p^\times$ csoport n rendű elemei.

4.3.36. Feladat. Igazoljuk az előző feladat felhasználásával, hogy minden n pozitív egészre van $nk + 1$ alakú prímszám.

Ugyanezzel a technikával az is megmutatható, hogy végtelen sok $nk + 1$ alakú prímszám van. Általában Dirichlet nevezetes számelméleti tétele azt mondja ki, hogy ha a és b relatív prím pozitív egész számok, akkor végtelen sok $ak + b$ alakú prímszám van. Ezt eddig csak az analízis eszközeivel sikerült bebizonyítani.

4.4. Részcsoportok

Ebben a szakaszban a részcsoportokkal kapcsolatos elemi ismeretekről lesz szó. Megismerkedünk a mellékosztály fogalmával, és belátjuk Lagrange tételét, mely szerint minden csoportelemnek és részcsoportnak a rendje osztója a csoport rendjének (ezt ciklikus csoportok esetében már tudjuk). Ezután a generált részcsoport fogalmát vezetjük be.

A 2.2.16. Feladatban megmutattuk, hogy egy G csoport egy H részhalmaza akkor és csak akkor részcsoport (képletben $H \leq G$), ha tartalmazza az egységelemet, továbbá zárt a szorzásra és az inverzképzésre.

4.4.1. Gyakorlat. Igazoljuk, hogy egy G csoport egy nem üres H részhalmaza pontosan akkor részcsoport, ha tetszőleges $a, b \in H$ esetén $ab^{-1} \in H$ teljesül.

Ezt az állítást egy új jelöléssel átfogalmazzuk. Ez a jelölés, az úgynevezett komplexusszorzás azért hasznos, mert az elemekkel való számolásokat lerövidíti. Komplexusnak régebben egy csoport részhalmazait nevezték (ez az elnevezés a geometriából származik).

Vektorterek esetében az U és W alterek összegén az

$$U + W = \{u + w \,:\, u \in U, w \in W\}$$

halmazt értettük, ami maga is altér volt (sőt, az U és V által generált altér). Ennek analógiájára vezetjük be tetszőleges csoportban részhalmazok szorzatát.

4.4.2. Definíció. Legyenek X és Y tetszőleges részhalmazai egy G csoportnak. Ekkor

$$XY = \{xy \,:\, x \in X, y \in Y\}$$

az X és Y *komplexus-szorzata*, és

$$X^{-1} = \{x^{-1} \,:\, x \in X\}$$

az X *komplexus-inverze*. Ha speciálisan $X = \{a\}$ egy egyelemű halmaz, akkor $\{a\}Y$ és $Y\{a\}$ helyett egyszerűen aY-t, illetve Ya-t írunk.

4.4.3. Gyakorlat. Igazoljuk, hogy a komplexusszorzás asszociatív, és $(XY)^{-1} = Y^{-1}X^{-1}$.

4.4.4. Gyakorlat. Mutassuk meg, hogy egy G csoport egy H nem üres részhalmazára az alábbi három állítás ekvivalens.

(1) H részcsoport.
(2) $HH = H^{-1} = H$.
(3) $HH^{-1} \subseteq H$.

Igazoljuk azt is, hogy ha H részcsoport, és $h \in H$, akkor $hH = Hh = H$.

Lagrange tételének bizonyításához meg kell ismerkednünk a partíció és az ekvivalenciareláció fogalmával. Legyen X egy halmaz, és osszuk fel X-et nem üres, diszjunkt halmazok egyesítésére. Egy ilyen felosztást X egy *partíciójának* nevezünk, a benne szereplő halmazokat pedig a partíció *osztályainak*.

Egy X halmazon akkor értelmezünk egy *relációt*, ha X bármely két elemére megmondjuk, hogy azok relációban vannak-e, vagy sem. Ilyen reláció például az oszthatóság, vagy a $\leq$ reláció az egész számok halmazán. Azt, hogy a és b az R relációban áll, $a\ R\ b$ (vagy néha $(a, b) \in R$) jelöli.

Ha formalizálni akarnánk a reláció fogalmát, akkor a következőt kellene mondanunk. Tekintsük az összes (x, y) párok $X \times X$ halmazát, ahol $x, y \in X$ (vagyis az X halmaz *Descartes-szorzatát* önmagával). Egy R reláció az $X \times X$ egy tetszőleges részhalmaza: pontosan azokból a párokból áll, melyekre a reláció teljesül. Ez magyarázza a fenti $(a, b) \in R$ jelölést is.

Ha az X halmaznak adott egy partíciója, akkor készítsünk belőle egy R relációt a következőképpen: két elem akkor van relációban, ha azonos osztályhoz tartoznak. Ez a reláció nyilván teljesíti a következő definícióban megfogalmazott három tulajdonságot.

4.4.5. Definíció. Az R relációt *ekvivalencia-relációnak* nevezzük, ha bármely $x, y, z \in X$ esetén teljesül az alábbi három tulajdonság.

(1) R *reflexív*, azaz $x \ R \ x$ minden x-re.
(2) R *szimmetrikus*, azaz ha $x \ R \ y$, akkor $y \ R \ x$.
(3) R *tranzitív*, azaz ha $x \ R \ y$ és $y \ R \ z$, akkor $x \ R \ z$.

A 4.3.10. Gyakorlatban tehát azt láttuk be, hogy az izomorfia ekvivalencia-reláció a csoportok között. Az oszthatóság nem ekvivalencia-reláció, mert bár reflexív és tranzitív, de nem szimmetrikus. Az asszociáltság azonban ekvivalencia-reláció minden egységelemes, kommutatív gyűrűben, a 3.1.8. Gyakorlat pontosan ezt fogalmazza meg.

Láttuk, hogy minden partíció meghatároz egy ekvivalencia-relációt. A megfordítás is igaz: minden ekvivalencia-reláció meghatároz egy partíciót. Noha ez az állítás igen egyszerű, lépten-nyomon alkalmazzák, mert a matematikában igen gyakran fordulnak elő partíciók, és ezeket sokszor így érdemes megadni.

4.4.6. Tétel. *Legyen R ekvivalencia-reláció az X halmazon. Tetszőleges $a \in X$ esetén legyen R_a azoknak az X-beli x elemeknek a halmaza, melyekre $a \ R \ x$. Ekkor az R_a halmazok az X egy partícióját adják.*

Bizonyítás. Az R_a halmazok között lehetnek egyenlők; az állítást úgy kell érteni, hogy az R_a halmazok közül bármely kettő vagy egyenlő, vagy diszjunkt, és egyesítésük az egész X halmaz. Ez utóbbi állítás nyilván következik R reflexivitásából (hiszen $a \in R_a$ minden a-ra). Tegyük fel, hogy R_a és R_b nem diszjunkt, be kell látni, hogy egyenlőek. Legyen $c \in R_a \cap R_b$, megmutatjuk, hogy $R_a = R_c = R_b$. Valóban, $c \in R_a$ miatt $a \ R \ c$, és mivel R szimmetrikus és tranzitív, minden x-re igaz, hogy $a \ R \ x$ akkor és csak akkor, ha $c \ R \ x$. Ezért $R_a = R_c$. Az a és b szerepét felcserélve $R_b = R_c$ adódik. □

4.4.7. Állítás. *Legyen G csoport és $H \leq G$. Ekkor az*

$$a \ R \ b \iff a^{-1}b \in H$$

képlet ekvivalencia-relációt definiál G elemei között.

Bizonyítás. Valóban, R reflexív, hiszen $a^{-1}a = 1 \in H$. A 2.2.10. Feladatban igazoltuk az $(uv)^{-1} = v^{-1}u^{-1}$ összefüggést. Így ha $a^{-1}b \in H$, akkor $H \ni (a^{-1}b)^{-1} = b^{-1}a$, ezért R szimmetrikus. Végül ha $a^{-1}b \in H$ és $b^{-1}c \in H$, akkor $a^{-1}c = a^{-1}bb^{-1}c \in H$, vagyis R tranzitív. Tehát R ekvivalencia-reláció. □

4.4.8. Tétel [Lagrange-tétel]. *Véges csoport minden részcsoportjának rendje osztója a csoport rendjének.*

Bizonyítás. Legyen $H \leq G$, és tekintsük az imént vizsgált R ekvivalencia-relációt. Mik lesznek R osztályai? Ha $a \in G$, akkor a osztályát azon $x \in G$ elemek alkotják, melyekre $a \ R \ x$, azaz $a^{-1}x \in H$, vagyis $x \in aH$. Tehát beláttuk, hogy az aH halmazok, ahol a befutja G-t, a G egy partícióját adják.

Hány eleme van az aH halmaznak? Ugyanannyi, mint H-nak, hiszen a $h \leftrightarrow ah$ nyilván kölcsönösen egyértelmű megfeleltetés H és aH között (az egyszerűsítési szabály miatt). Ezért G elemszámát úgy kaphatjuk meg, hogy H elemszámát megszorozzuk az osztályok számával. Így $|H|$ osztója $|G|$-nek, és ezzel Lagrange tételét bebizonyítottuk. □

Az ebben a bizonyításban szereplő fogalmak annyira fontosak, hogy külön nevük is van.

4.4.9. Definíció. Legyen G csoport, $H \leq G$ és $a \in G$. Az aH halmazt (a H részcsoport szerinti) *bal oldali mellékosztálynak* nevezzük. Ugyanígy a Ha halmaz *jobb oldali mellékosztály*. A különböző H szerinti bal mellékosztályok számát a H részcsoport G-beli *indexének* nevezzük, és $|G : H|$-val jelöljük.

4.4.10. Következmény. *Bármely két H-szerinti bal oldali mellékosztály vagy megegyezik, vagy diszjunkt, és a bal oldali mellékosztályok uniója G. Ugyanez az állítás a jobb oldali mellékosztályokra is igaz. Ha G véges, akkor $|G| = |H| \cdot |G : H|$.*

4.4.11. Gyakorlat. Mutassuk meg, hogy ha H részcsoport a G csoportban, $a, b \in G$, és $a \in bH$, akkor $aH = bH$.

A bal és jobb oldali mellékosztályok általában különbözők lesznek.

4.4.12. Gyakorlat. Számítsuk ki az S_3 szimmetrikus csoportban a $H = \{id, (12)\}$ részcsoport szerinti bal és jobb mellékosztályokat, és mutassuk meg, hogy $(123)H \neq H(123)$.

Ezért tulajdonképpen a H szerinti bal, illetve jobb index fogalmát kellett volna definiálnunk. Ez a két szám azonban megegyezik. Ez véges csoportnál azonnal világos az imént bizonyított tételből (hiszen mindkettő $|G|/|H|$). Az index azonban lehet véges akkor is, ha a csoport maga végtelen!

4.4.13. Gyakorlat. Jelölje $n\,\mathbb{Z}^+$ az n-nel osztható egészekből álló részcsoportot $\mathbb{Z}^+$-ban. Igazoljuk, hogy $|\,\mathbb{Z}^+ : n\,\mathbb{Z}^+\,| = n$.

4.4.14. Feladat. Legyen H részcsoport a G csoportban. Mutassuk meg, hogy a H szerinti bal és jobb oldali mellékosztályok száma megegyezik.

4.4.15. Definíció. Legyen H részcsoport G-ben. Ha kiválasztunk minden H szerinti bal oldali mellékosztályból egy-egy elemet, akkor egy H szerinti bal oldali *reprezentánsrendszert* kapunk. Analóg módon definiáljuk a jobb oldali reprezentánsrendszer fogalmát is.

4.4.16. Következmény. *Véges csoport minden elemének rendje osztója a csoport rendjének. Minden csoportelemet a csoport rendjére, mint kitevőre emelve az egységelemet kapjuk.*

Bizonyítás. Legyen g eleme a G véges csoportnak, és tekintsük a g hatványaiból álló H részcsoportot. Ennek rendje ugyanaz, mint a g elem rendje. Lagrange tétele miatt viszont H rendje osztója G rendjének. Így $|G|$ jó kitevője g-nek, ahonnan $g^{|G|} = 1$. □

4.4.17. Gyakorlat. Az előző következményből vezessük le a számelméletből ismert Euler-féle kongruenciatételt: ha az a és n pozitív egészek relatív prímek, akkor $a^{\varphi(n)} \equiv 1\ (n)$.

Az előző bizonyítás utolsó mondatában szereplő ötletet érdemes külön is kiemelni.

4.4.18. Gyakorlat. Legyen G csoport, és $g \in G$. Mutassuk meg, hogy a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben.

4.4.19. Definíció. Legyen G csoport, és $g \in G$. Ekkor a g elem egész kitevőjű hatványaiból álló részcsoportot a g elem által *generált* részcsoportnak nevezzük, és $\langle g \rangle$-vel jelöljük.

Vegyük észre, hogy ha G csoport és $g \in G$, akkor $\langle g \rangle$ a *legszűkebb* olyan részcsoportja G-nek, amely a g elemet tartalmazza. Ez alatt azt értjük, hogy ha H tetszőleges részcsoportja G-nek, amely a g elemet tartalmazza, akkor $\langle g \rangle$ szűkebb H-nál, vagyis $\langle g \rangle \subseteq H$. Valóban, mivel H részcsoport, a $g \in H$ elem minden hatványát tartalmaznia kell.

A generálás szó, és a most említett „legszűkebb" tulajdonság is ismerős lineáris algebrából. Ha egy V vektortérben adottak a $v_1, \ldots, v_n$ vektorok, akkor olyan altereket szeretnénk keresni, amely ezeket mind tartalmazza. Az egyik véglet maga a V, ez a legbővebb ilyen altér. A másik véglet a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú lineáris kombinációk halmaza, ahol a λ_i tetszőleges skalárok. Ez a $\langle v_1, \ldots, v_n \rangle$ halmaz a $v_1, \ldots, v_n$ által generált altér, ami a legszűkebb azon alterek között, amelyek tartalmazzák vektorainkat. Ez azt jelenti, hogy ha W tetszőleges altere V-nek, ami a $v_1, \ldots, v_n$ vektorokat tartalmazza, akkor $\langle v_1, \ldots, v_n \rangle \subseteq W$.

Legyen G csoport, és $g_1, \ldots, g_n \in G$. Beszélhetünk-e ilyenkor is a legszűkebb olyan részcsoportról, amely ezeket az elemeket tartalmazza? Ha H részcsoportja G-nek, és $g_1, \ldots, g_n \in H$, akkor persze H-nak tartalmaznia kell a g_i elemek összes egész kitevős hatványait, és ezek szorzatait is. Első próbálkozásunk tehát az, hogy a $g_1^{m_1} \ldots g_n^{m_n}$ alakú elemek halmazát tekintsük. Ez Abel-csoportokra működik is, és ha a csoport elemeit additívan írjuk, akkor a lineáris kombinációkhoz hasonló képletet kapunk.

4.4.20. Állítás. *Legyen A Abel-csoport, melyben a művelet jele $+$, és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ alakú elemek L halmazát, ahol m_i egész számok. Ekkor L részcsoport, mégpedig A legszűkebb olyan részcsoportja, amely a $g_1, \ldots, g_n$ elemeket tartalmazza.*

Bizonyítás. Először azt látjuk be, hogy L részcsoportja A-nak, amely a g_i elemeket tartalmazza. Nyilván $0 = 0g_1 + \ldots + 0g_n \in L$. Az L zárt az összeadásra, mert ha a és b elemei L-nek, akkor

$$a = m_1 g_1 + \ldots + m_n g_n \quad \text{és} \quad b = k_1 g_1 + \ldots + k_n g_n$$

alkalmas n_i, k_i egészekre, de akkor

$$a + b = (m_1 + k_1) g_1 + \ldots + (m_n + k_n) g_n$$

szintén a kívánt alakú, tehát eleme L-nek. Hasonlóan látható be az inverzre (azaz ellentettre) való zártság is. Végül

$$g_i = 0g_1 + \ldots + 0g_{i-1} + 1g_i + 0g_{i+1} + \ldots + 0g_n$$

tényleg eleme L-nek.

Be kell még látnunk, hogy L a legszűkebb olyan részcsoport, amely a $g_1, \ldots, g_n$ elemeket tartalmazza. Tegyük fel, hogy H tetszőleges részcsoport, amelyre $g_1, \ldots, g_n \in H$. Meg kell mutatni, hogy $L \subseteq H$, azaz hogy minden $m_1g_1 + \ldots + m_ng_n$ alakú elem H-ban van. De ez világos, hiszen egy ilyen elem a $g_1, \ldots, g_n$ elemekből összeadással és kivonással keletkezik (kivonásra a negatív m_i számok esetén van szükség), ezekre a műveletekre pedig H zárt. □

A most kapott képlet nem véletlenül hasonlít a vektortereknél kapott lineáris kombinációs formulához. A modulusokról szóló fejezetben fogjuk majd látni, hogy valójában egy általánosabb fogalom két speciális esetéről van szó (7.1.5. Gyakorlat).

4.4.21. Gyakorlat. Legyen X végtelen részhalmaza az A Abel-csoportnak, és tekintsük az olyan (véges) $m_1g_1 + \ldots + m_ng_n$ összegek L halmazát, ahol $g_i \in X$ és $m_i \in \mathbb{Z}$. Mutassuk meg, hogy L az X elemeit tartalmazó legszűkebb részcsoport.

Ha a G csoport nem kommutatív, akkor a $g_1^{m_1} \ldots g_n^{m_n}$ képlet általában nem működik, hiszen semmi garancia nincs arra, hogy például g_2g_1 ilyen alakban felírható. Sőt, a generált részcsoportnak tartalmaznia kell az olyasfajta elemeket is, mint mondjuk

$$g_1^{-2}g_2^6g_1g_2^2g_1^{-1}g_2^2g_1g_2^{-3}\,.$$

Nagyon jól illusztrálja a problémát a 4.2.24. Gyakorlat, amelyben megmutattuk, hogy ha $G = S_n$, akkor G minden eleme felírható a $g_1 = (12)$ és $g_2 = (1, 2, \ldots, n)$ elemek alkalmas, sokténye zős szorzataként. Ha egy H részcsoport tartalmazza g_1-et és g_2-t, akkor ezeket a szorzatokat is, tehát csak G lehet. Új terminológiánkkal tehát azt mondhatjuk, hogy a g_1 és g_2 által generált részcsoport maga S_n. Szó sincs azonban arról, hogy S_n minden eleme $g_1^{m_1}g_2^{m_2}$ alakú lenne, hiszen ilyen alakú elemet összesen $2n$-et írhatunk fel, az S_n elemszáma (ami $n!$) pedig ennél sokkal nagyobb. Ez a nagyságrendi különbség mutatja, hogy nagyon egyszerű képletet semmiképpen sem várhatunk, amely G összes elemét megadja.

Van továbbá még egy probléma. Generálásról eddig két struktúrában hallottunk: vektortérben és csoportban. De nagyon természetes kérdés az is, hogy létezik-e egy gyűrűben (vagy testben) adott elemeket tartalmazó legszűkebb részgyűrű (vagy résztest), és ha igen, akkor hogyan adhatjuk meg az elemeit. Ugyanezt a kérdést feltehetjük minden további struktúrában (modulusban, hálóban), amelyről tanulni fogunk. A problémát teljes általánosságban a 8.1. Szakaszban oldjuk meg. Mindenesetre érdemes szétválasztani a létezés kérdését attól, hogy hogyan lehet leírni a generált részstruktúra elemeit.

4.4.22. Definíció. Tetszőleges G csoport esetén az $X \subseteq G$ által *generált részcsoport* a *legszűkebb* X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$. Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X összes elemét, tartalmazza az $\langle X \rangle$ részcsoportot is. Az X részhalmazt G *generátorrendszerének* nevezzük (illetve azt mondjuk, hogy X *generálja* G-t), ha $\langle X \rangle = G$.

A fenti definíció csak akkor értelmes, ha *egyértelműen létezik* ez a bizonyos legszűkebb részcsoport. Ezt most rögtön bebizonyítjuk, és látni fogjuk, hogy a bizonyítás nemcsak csoportra, hanem más struktúrákra, például gyűrűkre is szó szerint átvihető. Előbb azonban szeretnénk tisztázni precízen és általánosan a „legszűkebb" szó jelentését.

4.4.23. Definíció. Egy halmazrendszer *legszűkebb eleme* egy olyan halmaz (a halmazrendszerben), amely a halmazrendszer minden elemének részhalmaza. Egy halmazrendszer *minimális eleme* egy olyan halmaz, amelynél nincs szűkebb halmaz a rendszerben, vagyis amelynek a halmazrendszer egyetlen eleme sem valódi részhalmaza. Ugyanígy egy halmazrendszer *legbővebb eleme* egy olyan halmaz (a halmazrendszerben), amelynek a halmazrendszer minden eleme részhalmaza. Egy halmazrendszer *maximális eleme* egy olyan halmaz, amelynél nincs bővebb halmaz a rendszerben, azaz amely a halmazrendszer egyetlen elemének sem valódi részhalmaza.

4.4.24. Gyakorlat. Mutassuk meg, hogy egy halmazrendszernek legfeljebb egy legszűkebb, és legfeljebb egy legbővebb eleme lehet. Igazoljuk azt is, hogy a legszűkebb elem (ha létezik, akkor) minimális, és a legbővebb elem (ha létezik, akkor) maximális.

A generált részcsoport tehát egyértelműen meghatározott (vagyis nem lehet két különböző, X-et tartalmazó legszűkebb részcsoport). Most megmutatjuk, hogy létezik.

4.4.25. Gyakorlat. Mutassuk meg, hogy részcsoportok metszete is részcsoport (végtelen soké is).

4.4.26. Állítás. *Az X által generált részcsoport egyértelműen létezik, mint az összes X-et tartalmazó részcsoport metszete.*

Bizonyítás. Az X-et tartalmazó részcsoportok metszete is részcsoport, és ez a metszet részhalmaza minden tényezőjének, azaz tényleg a legszűkebb lesz az X-et tartalmazó részcsoportok között. □

4.4.27. Tétel. *Legyen G csoport és $X \subseteq G$. Ekkor $\langle X \rangle$ a G azon elemeiből áll, melyek felírhatók az X elemeiből és azok inverzeiből képzett soktényezős szorzatként (X minden eleme többször is felhasználható egy ilyen szorzatban).*

Bizonyítás. Legyen L a tételben leírt szorzatoknak a halmaza. Elegendő megmutatni, hogy L a legszűkebb X-et tartalmazó részcsoport, mert akkor a generált részcsoport egyértelműsége miatt $L = \langle X \rangle$.

Az X elemei, mint egytényezős szorzatok, elemei L-nek. Az egységelem benne van L-ben, mint üres szorzat. Nyilván L zárt a szorzásra, hiszen két bonyolult szorzatot egymás

mellé írva egy ugyanilyen fajta, csak még bonyolultabb szorzatot kapunk. Végül a szorzat inverzének képletét (2.2.10. Feladat) alkalmazva látjuk, hogy L az inverzképzésre is zárt.

Tegyük fel, hogy egy H részcsoport tartalmazza X elemeit. Ekkor tartalmazza az X elemeinek inverzeit, és az $X \cup X^{-1}$ elemeiből képzett szorzatokat is, azaz L valamennyi elemét. Tehát L tényleg a legszűkebb X-et tartalmazó részcsoport. □

4.4.28. Gyakorlat. Legyen $g_1, \ldots, g_n$ generátorrendszere a G csoportnak, és $h_1, \ldots, h_n$ egy H csoport tetszőleges elemei. Mutassuk meg, hogy legfeljebb egy olyan $\psi : G \to H$ homomorfizmus létezik, amelyre $\psi(g_i) = h_i$ minden i-re teljesül. Igaz-e az állítás végtelen generátorrendszerre is?

4.4.29. Gyakorlat. Legyenek A és B részcsoportok a G csoportban. Mutassuk meg, hogy az AB komplexusszorzat akkor és csak akkor részcsoport, ha $AB = BA$, és ekkor ez lesz az A és B (uniója) által generált részcsoport.

A csoportelmélet célja az, hogy a csoportok szerkezetét felderítse. Nem az a kérdés, hogy mik egy adott csoport elemei, hanem az, hogy a művelet hogyan működik rajtuk. Mivel az izomorf csoportok tulajdonságai ugyanazok, nem is érdemes megkülönböztetni őket egymástól. Ez a híres Steinitz-féle *izomorfia-elv*. Például az előző szakaszban már megértettük a ciklikus csoportok szerkezetét, és tudjuk, hogy az összes tízelemű ciklikus csoport egymással izomorf. Ezért ***a*** tízelemű ciklikus csoportról beszélhetünk (határozott névelővel). Mivel az izomorfia a csoportok között ekvivalencia-reláció, a tizedrendű ciklikus csoportok egy izomorfia-osztályt alkotnak.

> Van egy kivételes helyzet, amikor az izomorf csoportokat mégiscsak meg kell különböztetnünk, éspedig akkor, ha egy nagyobb csoportnak a részcsoportjairól van szó. Nyilvánvaló például, hogy az S_3 szimmetrikus csoportnak az (12) és az (13) által generált részcsoportjai izomorfak, hiszen mindkettő a kételemű ciklikus csoport. De két különböző részcsoportról van szó, nem azonosíthatjuk őket.

A cél az lenne, hogy az összes csoport szerkezetét feltérképezzük, izomorfia erejéig. Ez persze reménytelen feladat, de ahogy tételeket bizonyítunk, úgy egyre többet fogunk megtudni a csoportok szerkezetéről. Visszatérő témánk lesz, ahogy haladunk előre az anyagban, hogy a viszonylag kis elemszámú csoportokat fokozatosan felsoroljuk, lehetőleg olyan áttekinthető szerkezetű alakban, hogy a felmerülő kérdéseket könnyen megválaszolhassuk. Ennek a folyamatnak az összefoglalása a Függelékben olvasható (757. oldal).

Nyilván bármely két egyelemű csoport izomorf, tehát egyelemű csoportból (izomorfia erejéig) egyetlen darab van. A következő lépésben a prímrendű csoportokat értjük meg.

4.4.30. Következmény. *Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).*

Bizonyítás. Tegyük fel, hogy G-nek pontosan két részcsoportja van. Ekkor $|G| > 1$ és így G-nek létezik 1-től különböző eleme. Minden ilyen g elemre $\langle g \rangle \neq \{1\}$, azaz a feltétel miatt $\langle g \rangle = G$. Tehát G ciklikus. A g rendje nem lehet végtelen, mert egy ilyen elem

hatványai páronként különbözők, tehát $1 \neq g^2$ nem generálná G-t. Ha $o(g) = n(\neq 1)$, akkor legyen p prímosztója n-nek. A hatvány rendjének képlete miatt $h = g^{n/p}$ rendje p (ezt az ötletet használtuk már a 4.3.27. Gyakorlat megoldásában is). Így $1 \neq h$ is generálja G-t, azaz G prímrendű, és egyúttal ciklikus is. Megfordítva, ha G rendje egy p prím, és H részcsoportja G-nek, akkor H rendje csak 1 vagy p lehet, tehát $H = \{1\}$ vagy $H = G$. □

Tehát minden prímrendű csoport ciklikus, és mivel az azonos rendű ciklikus csoportok izomorfak, így izomorfia erejéig egyetlen prímrendű csoport létezik minden p prímszámra. Speciálisan a 2, 3, 5 és 7 rendű csoportokból is egy-egy van.

Gyakorlatok, feladatok

4.4.31. Gyakorlat. Az X halmazon alább megadott R relációk mindegyikéről döntsük el, hogy ekvivalencia-reláció-e. Ha igen, adjuk meg a hozzá tartozó partíció osztályait.

(1) $X = \mathbb{Z}$, $a \ R \ b \iff 1848 \mid b - a$.
(2) $X = \mathbb{R}$, $a \ R \ b \iff |b - a| \leq 1$.
(3) $X = \mathbb{C}$, $a \ R \ b \iff |a| = |b|$.
(4) X a sík pontjai, $(P, Q) \in R$ akkor és csak akkor, ha van olyan A egybevágósági transzformáció, mely fixálja az origót, és melyre $A(P) = Q$.
(5) X tetszőleges, f egy X-en értelmezett függvény, $a \ R \ b \iff f(a) = f(b)$.

4.4.32. Gyakorlat. Az alábbi halmazrendszerek közül melyeknek van legszűkebb és legbővebb eleme? Melyeknek van minimális illetve maximális eleme?

(1) A $\mathbb{Z}$ összes kételemű részhalmaza.
(2) A $\mathbb{Z}$ összes végtelen részhalmaza.
(3) A $\mathbb{Z}$ összes olyan valódi részhalmaza, amelynek komplementere véges.
(4) A $\mathbb{Z}$ összes olyan részhalmaza, amely tartalmazza a 7 vagy a 13 számokat.
(5) A $\mathbb{Z}$ összes olyan részhalmaza, amely tartalmazza a 7 és a 13 számokat.

4.4.33. Gyakorlat. Határozzuk meg Lagrange tételének felhasználásával az S_3, $\mathbb{Z}_{12}^{+}$ és a $\mathbb{Z}_{12}^{\times}$ csoportok összes részcsoportját, valamint az A_4 alternáló csoport összes negyedrendű részcsoportját.

4.4.34. Feladat. Mutassuk meg, hogy ha egy csoport két részcsoportjának uniója is részcsoport, akkor az egyik tartalmazza a másikat. Igaz ez három részcsoportra is?

4.4.35. Feladat. Igazoljuk, hogy egy G véges csoport rendje akkor és csak akkor páros, ha G-ben van másodrendű elem.

4.4.36. Feladat. Bizonyítsuk be, hogy ha T test, akkor T multiplikatív csoportjának minden véges részcsoportja ciklikus.

4.4.37. Gyakorlat. Határozzuk meg a G csoportban az X által generált részcsoportot az alábbi esetekben.

(1) $G = \mathbb{Z}^{+}$, $X = \{28, 34\}$.

(2) $G = \mathbb{R}^\times$, $X = \{2, 3\}$.
(3) $G = S_n$, $X = \{(12), (1, 2, \ldots, n)\}$.
(4) $G = S_4$, $X = \{(13), (1234)\}$.
(5) $G = S_4$, $X = \{(123), (12)(34)\}$.
(6) $G = \mathrm{GL}(n, \mathbb{R})$, X a 2 determinánsú mátrixok halmaza.

4.4.38. Gyakorlat. Mutassuk meg a 4.1.8. Állítás felhasználásával, hogy a D_n diédercsoportot generálják az F és T elemek. Határozzuk meg a D_5 és D_6 diédercsoportokban a $\langle T, F^2 \rangle$ részcsoportot.

4.4.39. Gyakorlat. Legyen G csoport, H részcsoportja G-nek és $g \in G$. Mutassuk meg, hogy a gHg^{-1} komplexusszorzat is részcsoport, melynek rendje ugyanaz, mint H rendje. Igaz-e, hogy a gH bal oldali mellékosztály G egy alkalmas részcsoportja szerinti jobb oldali mellékosztály is egyben?

4.4.40. Gyakorlat. Legyen G csoport és $H \leq K \leq G$. Igazoljuk, hogy $|G : H|$ akkor és csak akkor véges, ha $|G : K|$ és $|K : H|$ is véges, és ilyenkor $|G : H| = |G : K| \cdot |K : H|$.

4.4.41. Gyakorlat. Mutassuk meg, hogy két véges indexű részcsoport metszete is véges indexű. Mennyi lehet a metszet indexe legfeljebb?

4.4.42. Feladat. Legyenek a, b, c, d egész számok, melyekre $(a, b) = 1$ és $(c, d) = 1$. Mutassuk meg, hogy az a/b és c/d törtek által $\mathbb{Q}^+$-ban generált részcsoport ciklikus. Melyik elem generálja?

4.4.43. Feladat. Bizonyítsuk be, hogy a racionális számok additív csoportja nem végesen generált, sőt, minimális generátorrendszere sincs.

4.4.44. Feladat. Bizonyítsuk be, hogy végesen generált csoportnak minden véges indexű részcsoportja végesen generált.

4.4.45. Feladat. Legyen G véges csoport, és H részcsoportja G-nek. Mutassuk meg, hogy van olyan H szerinti bal oldali reprezentánsrendszer, ami egyúttal jobb oldali reprezentánsrendszer is H szerint.

4.5. Homomorfizmusok és normálosztók

Ebben a szakaszban áttekintjük az összes olyan homomorfizmust, ami egy G csoporton értelmezhető. Eljutunk a normálosztó és a faktorcsoport fogalmáig, és megvizsgáljuk ezek szerkezetét.

A homomorfizmus (a struktúrát megőrző leképezés) a matematika egyik legfontosabb fogalma. Nemcsak az algebrában van ez így: az analízisben (topológiában) például a folytonosság felel meg a művelettartásnak. Az izomorfizmusok azért voltak hasznosak, mert az egyformán viselkedő struktúrák közül csak egyet kellett megértenünk. Egy olyan homomorfizmus, amely nem izomorfizmus, viszont esetleg egy bonyolult struktúrát képez egy sokkal

egyszerűbbe. Az egyszerűbb struktúrában már tudunk dolgozni, és ezzel információt nyerünk a bonyolultabbról is. Ezt tesszük például az életben is, folyamatok modellezésekor. A lényeges dolgokat megragadjuk, és csak azokat vizsgáljuk, azaz „homomorfizmust" (a lényeget megtartó leképezést) készítünk egy már kezelhető struktúrába (a modellbe). Egy példa minderre a következő.

4.5.1. Kérdés. Előáll-e az (12) transzpozíció hármasciklusok szorzataként?

Nem akarjuk, talán nem is tudnánk áttekinteni a hármasciklusok összes lehetséges szorzatait. Ezt a kérdést úgy válaszolhatjuk meg, hogy tekintjük az előjelképzést, vagyis a sg homomorfizmust a kételemű $\{1, -1\}$ csoportba. Ebben már gond nélkül tudunk számolni, és ezt mondhatjuk: minden hármasciklus páros permutáció, előjele 1. Mivel az előjelképzés művelettartó, a hármasciklusok szorzatainak is 1 az előjele. De az (12) transzpozíció előjele -1, ezért a kívánt előállítás nem lehetséges.

A lineáris algebrában minden homomorfizmust egy mátrixszal adhatunk meg. A csoportoknál bonyolultabb a helyzet, mert általában nincs olyan „bázis", amin egy lineáris leképezést egyértelműen előírhatnánk. De egy analógia mégis érvényes. Ha egy $A : V \to W$ lineáris leképezésnek ismerjük a magterét, akkor a dimenziótétel miatt tudjuk $\mathrm{Im}(A)$ dimenzióját, és ezzel a kép, mint vektortér szerkezetét (hiszen egy vektorteret a dimenziója izomorfia erejéig meghatároz). Nézzük meg, hogy ha $\psi : G \to H$ csoport-homomorfizmus, akkor a „mag" ismerete meghatározza-e izomorfia erejéig a „képet".

4.5.2. Definíció. Ha $\varphi : G \to H$ egy csoport-homomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ *képe* (vagyis a φ függvény értékkészlete).

Ha φ szürjektív, vagyis ha $\mathrm{Im}(\varphi) = H$, és ezt hangsúlyozni akarjuk, akkor azt mondjuk, hogy φ a H-***ra*** (és nem a H-***ba***) képez.

4.5.3. Gyakorlat. Legyen $\varphi : G \to H$ tetszőleges csoport-homomorfizmus. Mutassuk meg, hogy $\mathrm{Im}(\varphi)$ részcsoport H-ban, továbbá φ akkor és csak akkor szürjektív, ha képe az egész H.

Az alábbi gyakorlat azt mutatja, hogy egy homomorfizmus képéről nem mondhatunk többet annál, mint hogy részcsoport.

4.5.4. Gyakorlat. Mutassuk meg, hogy egy H csoport minden részcsoportja előáll alkalmas H-ba vezető homomorfizmus képeként.

4.5.5. Definíció. Ha $\varphi : G \to H$ egy csoport-homomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G : \varphi(a) = 1_H\} \subseteq G$$

a φ *magja*. Itt 1_H a H csoport egységeleme.

4.5.6. Gyakorlat. Legyen $\varphi : G \to H$ tetszőleges csoport-homomorfizmus. Mutassuk meg, hogy φ magja részcsoport G-ben, továbbá hogy φ akkor és csak akkor injektív, ha magja csak az egységelemből áll.

Az injektív homomorfizmusokat szokás *beágyazásnak* is nevezni.

4.5.7. Gyakorlat. Tekintsük azt a $\varphi : \mathbb{Z}^+ \to \mathbb{Z}_n^+$ homomorfizmust, amely minden egész számhoz a mod n maradékát rendeli. Mutassuk meg, hogy φ magja az n-nel osztható számokból álló $n\,\mathbb{Z}$ részcsoport, és ha $\varphi(g) = h$ (ahol $g \in \mathbb{Z}$ és $h \in \mathbb{Z}_n$), akkor a h elemre φ-nél pontosan a $g + n\,\mathbb{Z}$ mellékosztály elemei képződnek (vö. 4.4.13. Gyakorlat).

Nézzük meg, hogy egy homomorfizmus magjáról sem mondhatunk-e többet annál, mint hogy részcsoport, azaz hogy magja lesz-e minden részcsoport egy alkalmas homomorfizmusnak. Tegyük fel, hogy $N \leq G$ a $\varphi : G \to H$ homomorfizmus magja. Ha $h \in \mathrm{Im}(\varphi)$, akkor G mely elemei képződnek h-ra? Legyen $\varphi(g) = h$, ekkor

$$\varphi(g') = h \iff \varphi(g') = \varphi(g) \iff \varphi(g^{-1}g') = 1_H \iff$$
$$\iff g^{-1}g' \in \mathrm{Ker}(\varphi) = N \iff g' \in gN\,.$$

Tehát h-ra épp a gN mellékosztály elemei képződnek.

Ez az eredmény gyanús! Mi okozza azt az aszimmetriát, hogy *bal* mellékosztály jött ki? A $\varphi(g') = \varphi(g)$ összefüggést ebben a számolásban balról szoroztuk $\varphi(g^{-1})$-gyel. Most szorozzuk jobbról.

$$\varphi(g') = h \iff \varphi(g') = \varphi(g) \iff \varphi(g'g^{-1}) = 1_H \iff$$
$$\iff g'g^{-1} \in \mathrm{Ker}(\varphi) = N \iff g' \in Ng\,.$$

Most az jött ki, hogy h-ra épp az Ng mellékosztály elemei képződnek. Tehát $gN = Ng$ minden $g \in G$ elemre. Így az N szerinti jobb- és bal oldali mellékosztályok megegyeznek. Ez a tulajdonság nem teljesül minden részcsoportra, például az S_3 csoport $\{id, (12)\}$ részcsoportjára sem (lásd 4.4.12. Gyakorlat). Tehát ez a részcsoport nem lesz homomorfizmusnak magja.

Vigyázzunk, $gN = Ng$ ***nem*** jelenti azt, hogy $gn = ng$ minden $n \in N$ esetén, hanem csak azt, hogy a gN és Ng halmazok megegyeznek! Ez az elemek nyelvén így mondható el: minden $n \in N$-hez van olyan $n' \in N$, hogy $gn = n'g$, és fordítva, minden n-hez van olyan n'', hogy $ng = gn''$. (Ennek az átfogalmazásnak a bonyolultságából látszik, hogy a komplexusműveletek mennyire kifejezőek.)

4.5.8. Gyakorlat. Ellenőrizzük, hogy az S_3 csoportban az $N = \{id, (123), (132)\}$ részcsoportra és a $g = (12)$ elemre teljesül a $gN = Ng$ összefüggés.

4.5.9. Gyakorlat. Legyen N részcsoport egy G csoportban, amely szerinti bal és jobb mellékosztályok megegyeznek, tehát minden gN bal oldali mellékosztály Ng' alakú alkalmas g'-re. Mutassuk meg, hogy akkor $gN = Ng$ minden $g \in G$-re.

4.5.10. Definíció. A G csoport egy N részcsoportját akkor nevezzük *normális részcsoportnak*, vagy *normálosztónak*, ha egy alkalmas, G-n értelmezett homomorfizmusnak a magja. Jelölés: $N \triangleleft G$.

4.5.11. Tétel. *A G csoport N részcsoportja akkor és csak akkor normálosztó, ha a szerinte vett bal és jobb oldali mellékosztályok megegyeznek, vagy ami ezzel ekvivalens, minden $g \in G$ elemre $gN = Ng$.*

Azt már megmutattuk, hogy a $gN = Ng$ feltétel teljesül minden olyan N részcsoportra, amely egy homomorfizmusnak magja. A tétel bizonyításához tehát azt kell belátni, hogy ha az $N \leq G$ részcsoportra $gN = Ng$ teljesül minden $g \in G$ esetén, akkor létezik olyan $\psi : G \to K$ homomorfizmus egy alkalmas K csoportba, melynek magja N.

Az ilyesfajta bizonyításoknál azonnal fel lehetne írni a K és a ψ konstrukcióját. De ez olyan lenne, mint a derült égből a villámcsapás: nem derülne ki, hogyan is lehet rájönni a bizonyításra. Ezért először tovább analizáljuk azt a helyzetet, amikor egy $\varphi : G \to H$ homomorfizmus magja N. Amíg ez a motiváció zajlik, addig tehát ebben az apróbetűs részben H és φ fog szerepelni, amikor meg elkezdjük az igazi bizonyítást, akkor K és ψ.

A H „felesleges”, azaz $\mathrm{Im}(\varphi)$-n kívüli elemeit nem akarjuk megkonstruálni, ezért ezeket elhagyva feltehetjük, hogy φ szürjektív. Láttuk, hogy ha $h \in H$, akkor pontosan egy N szerinti mellékosztály elemei képződnek h-ra. Azaz H elemei kölcsönösen egyértelmű megfeleltetésben állnak az N szerinti mellékosztályokkal. Így a tervünk az, hogy a keresett K csoport elemei az N szerinti mellékosztályok lesznek, a keresett ψ leképezés pedig a g elemhez az ő mellékosztályát, azaz a $gN = Ng$ halmazt fogja rendelni.

Hogyan kaphatjuk meg a G-beli szorzás ismeretében a $h_1, h_2 \in H$ elemek szorzatát? Ha $\varphi(g_1) = h_1$ és $\varphi(g_2) = h_2$, akkor

$$h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2)\,,$$

vagyis a $h_1 h_2$ szorzatnak a $g_1 g_2 N$ mellékosztály felel meg. Ezért a tervezett K csoportban két mellékosztály szorzatát a

$$(g_1 N) \cdot (g_2 N) = g_1 g_2 N$$

képlettel kell, hogy definiáljuk. Azt várjuk, hogy csoportot kapunk, és a $\psi(g) = gN$ leképezés csoport-homomorfizmus, melynek magja N.

4.5.12. Állítás. *Legyen G csoport, és $N \leq G$, melyre $gN = Ng$ minden $g \in G$-re. Álljon a K halmaz a G szerinti mellékosztályokból, és vezessünk be rajta szorzást a*

$$(g_1 N) \cdot (g_2 N) = g_1 g_2 N$$

képlettel. Ekkor K csoport lesz, melynek egységeleme az $N = 1 \cdot N$ mellékosztály, a gN inverze pedig $g^{-1}N$. Az a $\psi : G \to K$ leképezés, ami g-hez gN-et rendeli, homomorfizmus lesz, melynek képe K, magja N.

Bizonyítás. Még a csoportaxiómák ellenőrzése ***előtt*** van egy probléma. Ha a K csoport két elemét, mondjuk az M_1 és M_2 mellékosztályokat össze akarjuk szorozni, hogyan is kell eljárni? A fenti szabály azt mondja: írjuk fel az M_1-et $g_1 N$, az M_2-t $g_2 N$ alakban, és

akkor az eredmény g_1g_2N lesz. De itt a g_1 és a g_2 elemeket sokféleképpen választhatjuk! Márpedig egy művelet eredményének egyértelműen meghatározottnak kellene lennie.

A problémát a következő hasonlat világítja meg. A „narancsszín" egy értelmes fogalom: tetszőleges narancsnak a színét jelenti. Ez azért működik, mert minden narancsnak (lényegében) ugyanaz a színe. A narancsok halmazának tehát azért tudtuk értelmezni a színét, mert mindegy volt, melyik elemét választottuk, az eredmény ugyanaz lett. Hasonlóan azonban nem definiálhatjuk az „autószín" fogalmát, hiszen az autók színe nem egyforma.

Másik köznapi példa a következő. Ha adott a gyerekek halmazán egy kétváltozós reláció, és van két iskolai osztályunk, akkor megpróbálhatjuk értelmezni a relációt a két osztály között is a következő módon: kiveszünk egy-egy gyereket mindkét osztályból, és megnézzük, hogy ők ketten relációban vannak-e. Ha például X akkor van relációban Y-nal, ha X idősebb korosztályhoz tartozik, mint Y, akkor értelmes kijelentés az, hogy „a 7/B idősebb korosztályhoz tartozik, mint a 6/A", mert (normális esetben) a 7/B mindegyik tanulója idősebb a 6/A bármelyik tanulójánál (és ennek teszteléséhez elég egy-egy gyereket kiválasztani). De a fenti definíció alapján értelmetlen arról beszélni, hogy az egyik osztály „jobb tanuló", mint a másik, hiszen abból, hogy Juliska a 7/A-ból jobb tanuló, mint Jancsi a 6/B-ből, még nem következik, hogy a 7/A-ban mindenki jobb tanuló, mint a 6/B-ben.

Harmadik példánk már matematikai. Jelölje P_n az n-edfokú (mondjuk valós együtthatós) polinomok halmazát. Megpróbálhatjuk értelmezni a P_n és a P_m halmazok összegét és szorzatát a következőképpen. Kiveszünk egy $f \in P_n$ és egy $g \in P_m$ polinomot, és azt mondjuk: $P_n + P_m$ legyen az $f + g$ polinomot tartalmazó halmaz, vagyis $f + g \in P_k$ esetén P_k. Hasonlóan legyen $P_nP_m = P_\ell$, ha $fg \in P_\ell$. Jók ezek a definíciók?

A második definíció rendben van, mert bárhogyan is választjuk az $f \in P_n$ és $g \in P_m$ polinomokat, az fg biztosan a P_{n+m} eleme lesz (azaz $P_nP_m = P_{n+m}$). De az összeadással gond van. Például $P_2 + P_2$ összegét P_2-nek fogjuk találni akkor, ha az x^2, illetve $-2x^2$ polinomokat választjuk, viszont az $x^2 + x$ és a $-x^2$ polinomokat választva az eredmény P_1 lesz. Sőt, az x^2 és a $-x^2$ polinomok összege nulla, ami egyik P_k halmazba sem esik bele.

Ebből a példából már leszűrhetjük azt a szabályt, hogy mikor „jó" egy ilyen definíció. A szorzás definíciója azért volt rendben, mert az eredmény nem függött az f és g konkrét választásától. Ha f_1, f_2 ugyanannak a P_n halmaznak az eleme, és g_1, g_2 is ugyanannak a P_m halmaznak az eleme, akkor az f_1g_1, illetve az f_2g_2 szorzatok is ugyanannak a halmaznak (nevezetesen a P_{n+m}-nek) az elemei.

Ahhoz, hogy a K-beli szorzás *jóldefiniált*, azt kell tehát megmutatni, hogy az összeszorzandó M_1 és M_2 mellékosztályokat bármelyik elemükkel reprezentáljuk, az eredmény ugyanaz a mellékosztály lesz (tehát a szorzat csak a két mellékosztálytól függ, nem pedig a kiválasztott elemektől). Képletben:

$$\text{ha} \quad g_1N = M_1 = g_1'N \quad \text{és} \quad g_2N = M_2 = g_2'N\,, \quad \text{akkor} \quad g_1g_2N = g_1'g_2'N\,.$$

Ha ez igaz, akkor a szorzás definíciója értelmes.

A fenti következtetés nem igaz tetszőleges részcsoportra (például az S_3 csoport $\{id, (12)\}$ részcsoportjára sem). Most azonban tudjuk, hogy $gN = Ng$ minden $g \in G$-re. Ezért

$$g_1g_2N = g_1g_2'N = g_1Ng_2' = g_1'Ng_2' = g_1'g_2'N\,.$$

Tehát a szorzás a K halmazon tényleg jóldefiniált.

4.5.13. Gyakorlat. Mutassuk meg, hogy a K halmazon definiált művelet asszociatív, az N kétoldali neutrális elem, és a $\psi : g \to gN$ leképezés szürjektív homomorfizmus G-ből K-ra.

Azt, hogy a gN mellékosztálynak a $g^{-1}N$ mellékosztály inverze lesz, úgy ellenőrizhetjük, hogy szorzatuk kiszámításánál a g, illetve g^{-1} reprezentánselemeket választjuk. Ekkor $(gN) \cdot (g^{-1}N) = gg^{-1}N = N$, és ugyanígy $(g^{-1}N) \cdot (gN) = N$.

Egy mellékosztály inverze szintén nem függ a reprezentánselem választásától, vagyis ha $g_1N = g_2N$, akkor $g_1^{-1}N = g_2^{-1}N$. Ezt azonban nem kell ellenőriznünk, következik az inverz egyértelműségéből (2.2.10. Feladat).

Végül a ψ magjának kiszámításához vegyük észre, hogy $g \in \mathrm{Ker}(\psi)$ akkor és csak akkor, ha $\psi(g) = gN = N$ (a K egységeleme), vagyis ha $g \in N$. Tehát $\mathrm{Ker}(\psi) = N$. Ezzel az állítást, és így a 4.5.11. Tételt is beláttuk. □

4.5.14. Definíció. Legyen N normálosztó a G csoportban. Az előző 4.5.12. Állításban definiált K csoportot a G csoport N szerinti *faktorcsoportjának* nevezzük, és G/N-nel jelöljük. A $\psi : g \mapsto gN$ leképezés neve *természetes homomorfizmus*.

Ha G véges, akkor persze $|G/N| = |G : N| = |G|/|N|$. A fenti 4.5.11. Tétel utáni apróbetűs gondolatmenet során az is kiderült, hogy ha $\varphi : G \to H$ tetszőleges homomorfizmus, és $N = \mathrm{Ker}(\varphi)$, akkor $\mathrm{Im}(\varphi)$ elemei kölcsönösen egyértelmű, műveletartó megfeleltetésben állnak a $K = G/N$ csoport elemeivel (a $\varphi(g)$ elemnek a $gN = Ng$ felel meg), vagyis, hogy $\mathrm{Im}(\varphi) \cong K = G/N$. Ezzel megkaptuk a lineáris algebrai dimenziótétel csoportelméleti analogonját:

4.5.15. Tétel [Homomorfizmus-tétel]. *Ha G és H csoportok, és $\varphi : G \to H$ homomorfizmus, akkor* $\mathrm{Im}(\varphi) \cong G/\mathrm{Ker}(\varphi)$.

A faktorcsoportban a műveletet az osztályok elemeivel (reprezentánsokkal) végezzük el. Minél ügyesebben választjuk ezeket a reprezentánsokat, annál egyszerűbb a dolgunk. Így például a faktorcsoport elemeinek a rendjét is kiszámíthatjuk.

4.5.16. Állítás. *Legyen $N \triangleleft G$ és $g \in G$. Ekkor a $gN \in G/N$ elem rendje a legkisebb olyan pozitív n egész, melyre $g^n \in N$, és végtelen, ha ilyen n nem létezik.*

Bizonyítás. A k egész pontosan akkor jó kitevője a gN mellékosztálynak, ha $(gN)^k = N$ (a G/N csoport egységeleme). De $(gN)^k = g^kN$ (a szorzásnál minden tényezőből a g elemet választva reprezentánsként). Tehát k akkor és csak akkor jó kitevő, ha $g^kN = N$, azaz ha $g^k \in N$. Mivel a rend a legkisebb pozitív jó kitevő, az állítást beláttuk. □

A szakasz hátralévő részében megvizsgáljuk, mik lesznek faktorcsoport részcsoportjai, normálosztói, faktorcsoportjai. Ez a rész kicsit nehezebb az eddigieknél, ezért az Olvasó megteheti, hogy átugorja, és először minél több példát megismer normálosztóra és faktorcsoportra.

A G/N faktorcsoport a G csoport képe a természetes homomorfizmusnál. Sokszor kényelmesebb lesz a faktorcsoport helyett általában egy szürjektív homomorfizmusra gondolni.

4.5.17. Definíció. Legyen $\varphi : G \to H$ két halmaz közötti leképezés, és $L \subseteq H$. Ekkor az L részhalmaz *teljes inverz képe* azokból a G-beli elemekből áll, amelyek képe L-ben van. Képletben:

$$\varphi^{-1}(L) = \{g \in G \,:\, \varphi(g) \in L\}\,.$$

Ha $K \subseteq G$, akkor a φ függvény K-ra való *leszűkítése* (vagy *megszorítása*) az a $\psi : K \to H$ függvény, melynek értelmezési tartománya K, de különben ugyanúgy működik, mint a φ (azaz $\psi(k) = \varphi(k)$ minden $k \in K$-ra).

4.5.18. Gyakorlat. Mutassuk meg, hogy csoport-homomorfizmusnál részcsoport teljes inverz képe is részcsoport, ami a homomorfizmus magját tartalmazza.

4.5.19. Tétel. *Tegyük fel, hogy $\varphi : G \to H$ szürjektív csoport-homomorfizmus, melynek magja N. Ekkor a következő állítások teljesülnek.*

(1) *Ha K tetszőleges részcsoportja G-nek, akkor $\varphi(K)$ részcsoportja H-nak, melynek teljes inverz képe G-ben a $KN = NK$ részcsoport.*
(2) *A H részcsoportjai kölcsönösen egyértelmű megfeleltetésben állnak a G csoport azon részcsoportjaival, amelyek N-et tartalmazzák. Egy $L \leq H$ részcsoporthoz a $K = \varphi^{-1}(L)$ teljes inverz kép tartozik.*

Legyenek K és L ebben az értelemben egymásnak megfelelő részcsoportok.

(3) *Ha $g \in G$, és $\varphi(g) = h$, akkor a hL (illetve Lh) mellékosztály teljes inverz képe G-ben a gK (illetve a Kg) mellékosztály. Így a K szerinti bal (jobb) mellékosztályok pontosan az L szerinti bal (jobb) mellékosztályok teljes inverz képei.*
(4) *Az L indexe H-ban ugyanaz, mint a K indexe G-ben.*
(5) *Az L akkor és csak akkor normálosztó H-ban, ha K normálosztó G-ben. Ebben az esetben a G/K és a H/L faktorcsoportok izomorfak.*

Bizonyítás. Az (1) állítás igazolásához tegyük fel, hogy $K \leq G$. Ekkor $L = \varphi(K)$ nyilván részcsoport H-ban (ez megkapható a 4.5.3. Gyakorlatból is, ha azt a φ-nek a K-ra való leszűkítésére alkalmazzuk). Megfordítva, a 4.5.18. Gyakorlatban láttuk, hogy ha $L \leq H$, akkor $K = \varphi^{-1}(L)$ részcsoport G-ben, ami N-et tartalmazza. Azt kell megmutatnunk, hogy ha $L = \varphi(K)$, akkor $\varphi^{-1}(L) = KN$. Mivel $N \lhd G$, nyilván $KN = NK$.

Először a $KN \subseteq \varphi^{-1}(L)$ tartalmazást látjuk be. A KN elemei kn alakúak, ahol $k \in K$ és $n \in N$. De $\varphi(kn) = \varphi(k)\varphi(n) = \varphi(k) \in L$. A fordított tartalmazáshoz tegyük fel, hogy $g \in \varphi^{-1}(L)$, azaz hogy $h = \varphi(g) \in L$. Mivel $L = \varphi(K)$, van olyan $k \in K$, melyre $\varphi(k) = h$. Így $\varphi(g) = \varphi(k)$, vagyis $\varphi(k^{-1}g) = 1_H$, ahonnan $k^{-1}g \in \mathrm{Ker}(\varphi) = N$. Ezért $g \in kN \subseteq KN$, és így (1) igaz.

A (2) állítás megmutatásához két halmaz között kell kölcsönösen egyértelmű megfeleltetést létesíteni. Az első halmaz a H összes L részcsoportjainak a halmaza, ez legyen $\mathcal{H}$.

A másik a G csoport N-et tartalmazó K részcsoportjainak halmaza, ez legyen $\mathcal{G}$. Azt már láttuk, hogy $\varphi(K) \leq H$, ezért φ-t tekinthetjük egy $\mathcal{G}$-ből $\mathcal{H}$-ba képző függvénynek is. Megfordítva, φ^{-1} egy függvény $\mathcal{H}$-ból $\mathcal{G}$-be. Azt akarjuk megmutatni, hogy e két függvény egymás inverze, azaz mindkét sorrendben vett kompozíciójuk az identitás. Eszerint két dolgot kell megmutatni.

Az első dolog az, hogy ha $L \leq H$, és $K = \varphi^{-1}(L)$, akkor $\varphi(K) = L$. Mind a $\varphi(K) \subseteq L$, mind a $\varphi(K) \supseteq L$ tartalmazást a definíciókba való közvetlen behelyettesítéssel láthatjuk be (az utóbbi esetében ki kell használnunk azt, hogy φ szürjektív). Érdemes rajzot is készíteni.

A második dolog az, hogy ha $N \leq K \leq G$, és $L = \varphi(K)$, akkor $\varphi^{-1}(L) = K$. Ez következik az (1) állításból, hiszen K tartalmazza N-et, vagyis $KN = K$, és ezért L teljes inverz képe maga K lesz. A $K \longleftrightarrow L$ megfeleltetés tehát tényleg kölcsönösen egyértelmű, vagyis a (2) állítás is igaz.

A (3) megmutatásához a bal-jobb szimmetria miatt elég igazolni, hogy a hL teljes inverz képe gK. Nyilván tetszőleges $g' \in G$ esetén

$$g' \in \varphi^{-1}(hL) \iff \varphi(g') \in hL = \varphi(g)L \iff$$
$$\iff \varphi(g^{-1}g') \in L \iff g^{-1}g' \in K \iff g' \in gK\,.$$

Innen (4) és (5) már könnyen adódik, mert az index is és a „normálosztónak lenni” tulajdonság is megfogalmazható a mellékosztályok nyelvén. Például ha L normálosztó H-ban, akkor tetszőleges $g \in G$-re $\varphi(g)L = L\varphi(g)$. De akkor $gK = Kg$ is igaz, mert egyenlő halmazok teljes inverz képei. Tehát K is normálosztó.

Végül tegyük fel, hogy K és L normálosztók a G, illetve H csoportokban. Ekkor a (3)-beli megfeleltetés bijekciót létesít a G/K és az H/L faktorcsoportok elemei között. Megmutatjuk, hogy ez művelettartó is. Legyen h_1L és h_2L két L szerinti mellékosztály, meg kell mutatni, hogy a teljes inverz képeik szorzata ugyanaz, mint a szorzatuknak, azaz h_1h_2L-nek a teljes inverz képe. Válasszunk olyan g_1 és g_2 elemeket, melyekre $\varphi(g_1) = h_1$ és $\varphi(g_2) = h_2$. Ekkor h_1L, h_2L, h_1h_2L teljes inverz képe (3) szerint rendre g_1K, g_2K, g_1g_2K. Mivel g_1K és g_2K szorzata tényleg g_1g_2K, a tételt beláttuk. □

4.5.20. Következmény [Első izomorfizmus-tétel]. *Tegyük fel, hogy N normálosztó a G csoportban, és $K \leq G$. Ekkor KN részcsoport G-ben, $K \cap N$ normálosztó K-ban, és*

$$KN/N \cong K/(K \cap N)\,.$$

Ha $|G : N|$ véges, akkor $|K : (K \cap N)|$ osztója $|G : N|$-nek.

Bizonyítás. Legyen $\varphi : G \to G/N$ a természetes homomorfizmus, és φ_K a φ leszűkítése a K részcsoportra. Ez egy homomorfizmus K-ból G/N-be, és a magja nyilván $K \cap N$. Emiatt $K \cap N$ normálosztó K-ban, és a homomorfizmus-tétel miatt

$$K/(K \cap N) = K/\operatorname{Ker}(\varphi_K) \cong \operatorname{Im}(\varphi_K) = \varphi(K)\,.$$

Most legyen φ_{NK} a φ-nek az NK-ra való leszűkítése. Mivel $NK \supseteq N$, ennek a magja N. Ismét a homomorfizmus-tétel miatt

$$KN/N = KN/\operatorname{Ker}(\varphi_{KN}) \cong \operatorname{Im}(\varphi_{KN}) = \varphi(KN)\,.$$

De a 4.5.19. Tétel (1) állítása szerint $\varphi(K)$ és $\varphi(KN)$ egyenlő részcsoportjai G/N-nek, és így persze izomorfak.

Az utolsó állítás azért igaz, mert $|K : (K \cap N)|$ a $K/(K \cap N)$ csoport rendje, ami izomorf a $|G : N|$ rendű G/N egy részcsoportjával. □

4.5.21. Következmény [Második izomorfizmus-tétel]. *Tegyük fel, hogy N és K normálosztók a G csoportban és $N \subseteq K$. Ekkor*

$$(G/N)/(K/N) \cong G/K\,.$$

Az állításba beleértjük, hogy $N \lhd K$ és $(K/N) \lhd (G/N)$, vagyis hogy a felírt faktorcsoportok értelmesek.

Bizonyítás. Jelölje H a G/N faktorcsoportot, és legyen $\varphi : G \to G/N$ a természetes homomorfizmus. Nyilván $N \lhd K$, hiszen a φ homomorfizmus K-ra vett leszűkítésének is N a magja. A 4.5.19. Tétel (5) állítása szerint $L = \varphi(K) \lhd H$, és $H/L \cong G/K$. Így elég belátni, hogy $L = K/N$. De az $L = \varphi(K)$ csoport a $\varphi(k) = kN$ alakú elemek halmaza, ahol k befutja K-t, és ez definíció szerint K/N. □

Gyakorlatok, feladatok

4.5.22. Gyakorlat. Döntsük el az alább megadott $\varphi : G_1 \to G_2$ leképezésekről, hogy homomorfizmusok-e. Ha igen, határozzuk meg a magjukat és a képüket.

(1) $G_1 = \mathrm{GL}(n, T)$, $G_2 = T^\times$, $\varphi(A) = \det(A)$.
(2) $G_1 = S_n$, $G_2 = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).
(3) $G_1 = D_n$, $G_2 = \mathbb{Z}_2^+$, $\varphi(x) = 0$ ha x forgatás, 1 ha x tengelyes tükrözés.
(4) $G_1 = G_2 = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).
(5) $G_1 = \mathbb{R}[x]^+$, $G_2 = \mathbb{C}^+$, $\varphi(f) = f(i)$ (vagyis φ az i behelyettesítése).

4.5.23. Gyakorlat. Jelölje K a komplex egységkört, vagyis az egy abszolút értékű komplex számok halmazát, P pedig a pozitív valós számok halmazát, mindkettőt ellátva a szorzás műveletével. A homomorfizmus-tétel alapján igazoljuk a következő izomorfizmusokat.

(1) $\mathbb{C}^\times / K \cong P$. Milyen geometriai alakzatok ennek a faktorcsoportnak az elemei?
(2) $\mathbb{R}^+ / \mathbb{Z}^+ \cong K$.
(3) $S_n/A_n \cong \mathbb{Z}^\times$.
(4) $\mathbb{Z}^+ / n\,\mathbb{Z}^+ \cong \mathbb{Z}_n^+$.

4.5.24. Gyakorlat. Mivel lesznek izomorfak a $G/\{1\}$ és a G/G faktorcsoportok?

4.5.25. Gyakorlat. Ciklikus-e a $\mathbb{Z}_{16}^\times$ csoport, illetve az $\{1, 15\}$ és az $\{1, 9\}$ normálosztók szerinti faktorcsoportjai?

4.5.26. Gyakorlat. Legyenek $\varphi : G \to H$ és $\psi : G \to K$ homomorfizmusok, és tegyük fel, hogy φ szürjektív. Mutassuk meg, hogy pontosan akkor létezik olyan $\alpha : H \to K$ homomorfizmus, melyre $\psi = \alpha \circ \varphi$, ha $\mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\psi)$.

4.5.27. Gyakorlat. Legyen $\psi : G \to H$ szürjektív homomorfizmus. Mutassuk meg, hogy G bármelyik generátorrendszerének ψ-nél vett képe generátorrendszer lesz H-ban.

4.5.28. Gyakorlat. Legyen N normálosztó, H pedig részcsoport a G csoportban. Mutassuk meg, hogy az N és a H által generált részcsoport NH.

4.5.29. Gyakorlat. Legyenek $H \leq K$, továbbá N részcsoportok a G csoportban. Igazoljuk, hogy $HN \cap K = H(N \cap K)$. Ezt az összefüggést *moduláris szabálynak* hívjuk.

4.6. Permutációcsoportok

Ebben a szakaszban permutációkból álló csoportokról lesz szó. Az orbit és a stabilizátor fogalma segít majd egy alakzat szimmetriáinak megszámlálásában. Belátjuk Cayley tételét, miszerint minden csoport izomorf egy permutációcsoporttal. Végül a csoporthatás fogalmát vezetjük be.

4.6.1. Definíció. Legyen X halmaz. Az S_X szimmetrikus csoport részcsoportjait *permutációcsoportoknak* nevezzük. Az X halmaz elemeit néha *pontoknak* hívjuk.

Ez a szóhasználat a geometriából származik, hiszen például nagyon fontos permutációcsoport az, amit a sík egybevágósági (vagy hasonlósági) transzformációi alkotnak.

A 4.1.8. Állításban már megismerkedtünk a szabályos n-szög szimmetriacsoportjával, ezt diédercsoportnak neveztük, és D_n-nel jelöltük. Például egy négyzetnek négy szimmetriája van: négy tükrözés (az átlókra, illetve az oldalfelező merőlegesekre), és négy forgatás (a középpont körül rendre 0, 90, 180, 270 fokkal). Természetesen a 0 fokos forgatás az identitás, a 180 fokos pedig a középpontos tükrözés. Ez a nyolc transzformáció egy G részcsoportot alkot a sík összes permutációinak a csoportjában.

4.6.2. Kérdés. Hány helyre viheti a sík egy adott pontját ez a nyolc transzformáció?

Ezt könnyű végiggondolni. A négyzet középpontja csak önmagába mehet. A két átló többi pontja mind négy-négy helyre mehet. Ugyanez a helyzet az oldalfelező merőlegesek pontjaival is. A többi pontnak mind a nyolc képe különböző lesz.

4.6.3. Kérdés. A nyolc transzformáció közül hány hagyja helyben ezt a pontot?

A középpontot mind a nyolc. Azok a pontok, amelyeknek négy képe van, egy-egy szimmetriatengelyen helyezkednek el, ezeket két-két transzformáció hagyja helyben: a megfelelő tengelyes tükrözés, és a helybenhagyás. A többi pontot, amelynek tehát nyolc különböző képe van, csak a helybenhagyás viszi önmagába G elemei közül. Azt kaptuk tehát, hogy egy pont képeinek száma szorozva a pontot helyben hagyó transzformációk számával mindig nyolcat ad, tehát G elemszámát.

Most ezt az észrevételt fogjuk általánosítani. Tegyük fel, hogy G egy X halmaz permutációiból álló csoport, és válasszunk ki egy x pontot az X halmazból. Ha az x pontra a G összes elemét alkalmazzuk, akkor a kapott pontok X-nek egy részhalmazát alkotják. Ezt úgy hívjuk majd, hogy az x pont *orbitja* (pályája). Azok a G-beli permutációk, amelyek az x pontot önmagába viszik, könnyen láthatóan egy részcsoportot alkotnak, ennek neve x *stabilizátora*. Azt szeretnénk megmutatni, hogy az x orbitjának elemszáma szorozva az x stabilizátorának elemszámával mindig G elemeinek a számát adja.

Mielőtt ezt megtennénk, az előbbi példában érdemes észrevenni, hogy az orbitok a síknak egy partícióját alkotják. Ez talán még jobban látszik egy másik példán: legyen G most az origó körüli összes forgatásból álló részcsoport. Nyilvánvaló, hogy ekkor az orbitok az origó körüli körvonalak lesznek, továbbá még maga az origó is egy egypontú orbitot alkot. Így tényleg a sík egy partícióját kapjuk.

Annak belátásához, hogy az orbitok általában is egy partíciót alkotnak, kényelmesebb az orbit fogalmát egy ekvivalencia-reláció segítségével definiálni. Tegyük fel, hogy $G \leq S_X$, és definiáljunk egy $\sim_G$ relációt X-en a következőképpen: $x \sim_G y$ akkor és csak akkor, ha van olyan $g \in G$, melyre $g(x) = y$. Tehát két elem akkor áll relációban, ha az egyiket a másikba át lehet vinni G egy elemével. Azonnal látszik, hogy $\sim_G$ ekvivalencia-reláció. Valóban, $x \sim_G x$ (hiszen az egységelem x-et önmagába viszi); ha $x \sim_G y$, akkor $y \sim_G x$ (hiszen ha $g(x) = y$, akkor $g^{-1}(y) = x$); végül ha $x \sim_G y$ és $y \sim_G z$, akkor $x \sim_G z$ (hiszen ha $g(x) = y$ és $h(y) = z$, akkor $(hg)(x) = z$).

4.6.4. Definíció. A $\sim_G$ relációhoz tartozó partíció osztályait G *orbitjainak* nevezzük. Az $x \in X$ elemet tartalmazó orbitot szokás az x *pont orbitjának* is nevezni, jele $G(x)$, ez tehát a $g(x)$ pontok halmaza, ahol g befutja G-t. Egy-egy orbit elemszámát néha az orbit *hosszának* hívjuk. Ha X egyetlen orbitból áll, akkor azt mondjuk, hogy G *tranzitív* X-en.

4.6.5. Definíció. Ha $x \in X$ adott, akkor tekintsük azokat a $g \in G$ elemeket, melyek x-et *fixen hagyják*, azaz $g(x) = x$. Ezek nyilván részcsoportot alkotnak G-ben, melynek neve az x pont G-beli *stabilizátora*, jele G_x. Ha $g(x) = x$, akkor mondjuk majd azt is, hogy x *fixpontja* g-nek. Egy permutáció *fixpontmentes*, ha nincs egyetlen fixpontja sem.

4.6.6. Tétel. *Legyen $G \leq S_X$. Ekkor tetszőleges $x \in X$-re $|G(x)| = |G : G_x|$. Tehát egy pont orbitjának a hossza épp a pont stabilizátorának az indexe.*

Bizonyítás. Azt kell belátni, hogy $G(x)$ elemszáma ugyanaz, mint G_x indexe, vagyis a szerinte vett bal oldali mellékosztályok száma. Legyen gG_x egy bal oldali mellékosztály. Ennek elemei az x-et ugyanoda viszik, hiszen ha $h \in G_x$, akkor $h(x) = x$, és így

$$(gh)(x) = g\big(h(x)\big) = g(x)\,.$$

Ha viszont G két eleme különböző G_x szerinti mellékosztályban van, akkor x-et két különböző helyre viszik. Valóban, ha $g(x) = g'(x)$ lenne, akkor innen $g^{-1}g'(x) = x$, vagyis $g^{-1}g' \in G_x$, és ezért g és g' mégsincsenek különböző mellékosztályokban. Ez azt jelenti, hogy a G_x szerinti bal oldali mellékosztályok mindegyikéhez az orbitnak pontosan egy eleme tartozik: az, ahová ezek az elemek x-et elviszik. □

A fenti bizonyítás végtelen G-re vagy X-re is érvényes. Aki már hallott végtelen számosságokról, annak világos, hogy a következőt láttuk be: az orbit számossága, és a mellékosztályok halmazának számossága ugyanaz. Speciálisan egy pont orbitja akkor és csak akkor véges, ha a stabilizátora véges indexű részcsoport.

Most egy alkalmazást mutatunk be: kiszámoljuk, hány szimmetriája van a kockának. Legyen G azoknak az egybevágósági transzformációknak a halmaza, melyek a kockát önmagába képzik. Nyilván G részcsoportja a tér egybevágóságcsoportjának, de ha X jelöli a kocka csúcsainak halmazát, akkor G tekinthető az S_X részcsoportjának is, hiszen egybevágóság csúcsot csúcsba visz, és ha egy egybevágósági transzformációt a kocka csúcsain ismerünk, akkor már a tér minden pontjának a képét ki tudjuk számítani.

Legyen A a kocka egyik csúcsa. Egy egybevágósági transzformáció A-t csak a kocka valamelyik csúcsába viheti, azaz legfeljebb 8 helyre. Persze mind a nyolc csúcsba el is lehet vinni A-t a kocka egy-egy szimmetriájával: a szomszédos csúcsokba például egy síkra tükrözéssel, a többi csúcsba ilyenek egymásutánjával. Vagyis A orbitja nyolcelemű (és így G tranzitív a kocka csúcsain). Jelölje $H = G_A$ az A stabilizátorát G-ben. Tudjuk tehát, hogy G elemszáma a H elemszámának nyolcszorosa.

Legyen B, C, D az A csúcs három szomszédja. Mi lehet a B csúcs képe egy $g \in H$ transzformációnál? Mivel g egybevágóság, a $g(B)g(A)$ távolság meg kell hogy egyezzen az AB távolsággal. Tehát $g(B)$ élhossznyi távolságra van $g(A) = A$-tól. Ilyen csúcs három van: B, C és D. A testátló körüli két 120 fokos forgatás (mindkettő H-nak eleme) a B csúcsot elviszi C-be is és D-be is, ezért a B orbitja a H csoportnál $\{B, C, D\}$. Legyen K a B stabilizátora H-ban. Így H elemszáma a K elemszámának háromszorosa.

A C orbitja K-nál a C és D csúcsokból áll. Valóban: ha $g \in K$, akkor $g(C)$ az A-tól élnyi távolságra van, azaz B, C, D egyike, de $g(C)$ nem lehet B, hiszen B is fixen marad K elemeinél. Másrészt az AB-n átmenő átlósíkra való tükrözés fixen hagyja A-t és B-t, és kicseréli C-t D-vel. Ezért C orbitja K-nál tényleg a C és D csúcsokból áll, vagyis kételemű. Ha L jelöli a C stabilizátorát G-ben, akkor tehát K elemszáma az L elemszámának kétszerese.

Az L csoport elemei az A, B, C csúcsokat helyben hagyják, és a kockát is önmagába képzik, ilyen transzformáció már csak az identitás lehet. Tehát L elemszáma 1. Innen visszagöngyölítve $|K| = 2$, ezért $|H| = 2 \cdot 3 = 6$, és végül G elemszáma $6 \cdot 8 = 48$. A kockának tehát 48 szimmetriája van. Ha ezt „kézzel” akartuk volna meghatározni, jó eséllyel kifelejtettünk volna néhányat.

4.6.7. Állítás. *Összesen* 48 *olyan egybevágósági transzformáció van, amely egy adott kockát önmagába visz. A kocka csúcsait ezek tranzitívan permutálják.*

4.6.8. Gyakorlat. Mutassuk meg, hogy $n \geq 3$ esetén egy szabályos n-szögnek $2n$ szimmetriája van.

4.6.9. Gyakorlat. Igazoljuk, hogy a szabályos tetraédernek 24 szimmetriája van, vagyis a csúcsok bármely permutációja megvalósítható alkalmas egybevágósági transzformációval, és így ez a szimmetriacsoport S_4-gyel izomorf.

A permutációcsoportok olyan példákat szolgáltatnak, amelyek segítségével folytathatjuk a kis elemszámú csoportok felsorolását. Az egyelemű és a prímrendű csoportokat már megértettük. Az első két kimaradó szám a 4 és a 6. Vannak-e ilyen rendű csoportok? Természetesen igen, hiszen a $\mathbb{Z}_n^+$ csoport rendje n, azaz *minden pozitív n-re van n-edrendű csoport*. Vannak-e ezekkel nem izomorf, azaz nem ciklikus 4, illetve 6 rendű csoportok?

A válasz könnyebb 6-ra: az D_3 diédercsoportnak is 6 a rendje, de nem kommutatív, és ezért nem is lehet ciklikus. Később belátjuk majd, hogy hatelemű csoportból izomorfia erejéig csak kettő van: a $\mathbb{Z}_6^+$ ciklikus, és a D_3 diédercsoport.

4.6.10. Gyakorlat. Bizonyítsuk be, hogy a D_3 diédercsoport izomorf az S_3 szimmetrikus csoporttal.

4.6.11. Gyakorlat. Mutassuk meg, hogy egy téglalapnak, amely nem négyzet, pontosan négy szimmetriája van, az identitás kivételével ezek mindegyike másodrendű, és bármely két másodrendű elem szorzata a harmadik másodrendű elem.

Jelölje a téglalap szimmetriacsoportját K, ennek (és minden vele izomorf csoportnak) a neve *Klein-csoport*. Ez biztosan nem izomorf a $\mathbb{Z}_4^+$ ciklikus csoporttal, hiszen ez utóbbiban van negyedrendű elem, a Klein-csoportban pedig nincs. Ugyanakkor K izomorf a $\mathbb{Z}_8^\times$ csoporttal, mert abban minden egységtől különböző elem másodrendű. Ezt egyszerűbb általánosan bebizonyítani.

4.6.12. Tétel. *Minden négyelemű csoport izomorf vagy a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.*

Bizonyítás. Legyen G negyedrendű csoport. Ha G-nek van negyedrendű g eleme, akkor g-nek négy különböző hatványa van, ezért a G csoport a g hatványaiból áll, tehát ciklikus.

Tegyük fel, hogy G-ben nincs negyedrendű elem. Lagrange tétele miatt minden elemrend négynek osztója, és így csak 1 vagy 2 lehet. Nyilván az egységelem az egyetlen elsőrendű elem. Így a G csoport elemei $\{1, a, b, c\}$, ahol a, b, c mindegyike másodrendű. Próbáljuk meg kiszámítani az összes G-beli szorzatot.

Az áttekinthetőség kedvéért ezeket a szorzatokat egy táblázatba rendezzük. A táblázat minden sora és minden oszlopa G egy-egy elemének felel meg. A g-hez tartozó sor és a h-hoz tartozó oszlop metszéspontjába a gh szorzatot írjuk. Ezt a táblázatot a G csoport *Cayley-táblázatának* nevezzük. A $\mathbb{Z}_5^+$ csoport Cayley-táblázatát már kiszámítottuk a 9. oldalon. A G csoportban egyelőre a következő szorzatokat ismerjük:

G	1	a	b	c
1	1	a	b	c
a	a	1	?	?
b	b	?	1	?
c	c	?	?	1

Valóban, $1g = g1 = g$ minden g-re, az a, b, c elemek négyzete pedig 1, mert ezek az elemek másodrendűek.

Mennyi lehet az ab szorzat értéke? Négy lehetőségünk van: 1, a, b és c, vegyük őket sorra.

(1) Ha $ab = 1$, akkor b-vel szorozva $ab^2 = b$. Mivel $b^2 = 1$, innen $a = b$, ami lehetetlen.
(a) Ha $ab = a$, akkor a-val egyszerűsítve $b = 1$, ez is lehetetlen.
(b) Ugyanígy $ab = b$ sem lehetséges.
(c) Marad tehát egyedül az $ab = c$ lehetőség.

Mivel az a, b, c elemek szerepe teljesen szimmetrikus, ugyanez a gondolatmenet mutatja, hogy ezek közül bármely két elem bármely sorrendben vett szorzata a harmadik. Ezért a táblázatot teljesen kitölthetjük.

G	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Tehát minden szorzat ugyanaz, mint a Klein-csoportban, és ezzel az állítást beláttuk. □

Az eddig látott négyelemű példákat most már osztályozni tudjuk. A $\mathbb{Z}_8^\times$, a $\mathbb{Z}_{12}^\times$ és a $\mathbb{Z}_{16}^\times/\{1, 9\}$ csoportok, illetve az A_4 csoport egyetlen négyelemű részcsoportja a Klein-csoporttal izomorf, $\mathbb{Z}_{16}^\times/\{1, 15\}$ pedig a $\mathbb{Z}_n^+$ csoporttal (lásd 4.3.22, 4.4.33. és 4.5.25. Gyakorlatok).

Később belátjuk majd, hogy általában a prím-négyzet elemszámú csoportok száma is kettő, és mindketten kommutatívak. Megjegyezzük, hogy a Cayley-táblázat felírása csak kis csoportok esetében segít az izomorfizmus vizsgálatában, nagyobb csoportoknál már túl sok szorzatot kellene ellenőrizni. Ilyenkor az izomorfia bizonyításához inkább valamiféle elvet érdemes felhasználni, mint például a 4.6.9. Gyakorlatban, ahol megmutattuk, hogy a szabályos tetraéder szimmetriacsoportja S_4-gyel izomorf.

4.6.13. Gyakorlat. Írjuk fel a D_4 diédercsoport elemeit, mint a négyzet csúcsainak permutációit diszjunkt ciklusok segítségével, és készítsük el a Cayley-táblázatát.

Nyolcelemű csoport ötféle van, három kommutatív (ezek szerkezetéről később lesz szó), a D_4 diédercsoport, és az úgynevezett *Q kvaterniócsoport*. Ennek táblázata a következő:

Q	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

Szerencsére ezt a szorzást könnyen meg lehet jegyezni a következőképpen. Az 1 az egységelem, a -1-gyel való szorzás minden elemet az ellentettjére változtat. Az i, j, k mindegyike úgy viselkedik, mint a komplex i szám, azaz négyzetük -1. Egymással ezeket úgy szorozzuk, hogy az $\{i, j, k\}$ „körön" sorrendben haladva bármely kettő szorzata a harmadik, visszafelé haladva pedig bármely kettő szorzata a harmadik ellentettje. Természetesen ellenőrizni kellene az asszociativitást (ez elvileg 8^3 egyenlőség vizsgálatát jelentené). Ezt nem is így fogjuk elvégezni, hanem a következőképpen.

4.6.14. Gyakorlat. Tekintsük az alábbi $\mathbb{C}$ fölötti mátrixokat.

$$I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Mutassuk meg, hogy a $\pm I$, $\pm J$, $\pm K$ mátrixok az egységmátrixsszal és az ellentettjével együtt részcsoportot alkotnak $\mathrm{GL}(2, \mathbb{C})$-ben, mely teljesíti a kvaterniócsoport definíciójában megszabott szorzási szabályokat.

Ez a gyakorlat tehát bizonyítja, hogy a kvaterniócsoportban tényleg asszociatív a művelet (és azt is, hogy a $\mathrm{GL}(2, \mathbb{C})$ csoportban van Q-val izomorf részcsoport).

4.6.15. Feladat. Mutassuk meg, hogy a D_4 és a Q csoportok nem izomorfak.

Az egyszerűsítési szabály miatt egy G csoport Cayley-táblázatának minden sora (és minden oszlopa) a csoport elemeinek egy permutációja. A következő célunk annak megmutatása, hogy a sorok, mint permutációk, egy G-vel izomorf permutációcsoportot alkotnak.

4.6.16. Tétel [Cayley-tétel]. *Minden csoport izomorf egy permutációcsoporttal.*

Bizonyítás. Jelölje $\psi(g)$ a g elem sorához tartozó permutációt G szorzástáblájában. Ez a csoport egy x elemét gx-be viszi, képlettel $[\psi(g)](x) = gx$. Mivel a G csoport elemeinek egy permutációjáról van szó, a $\psi(g)$ permutáció az S_G szimmetrikus csoportnak eleme. Megmutatjuk, hogy $\psi : G \to S_G$ homomorfizmus, melynek $C = \mathrm{Im}(\psi)$ képe a G-vel izomorf részcsoport S_G-ben.

A ψ szorzattartása azt jelenti, hogy $\psi(g_1 g_2) = \psi(g_1) \circ \psi(g_2)$. Ez két függvény egyenlősége, azt kell megmutatni, hogy minden $x \in G$ helyen megegyeznek. De ez igaz, mert

$$[\psi(g_1 g_2)](x) = (g_1 g_2)x = g_1(g_2 x) = [\psi(g_1)](g_2 x) =$$
$$= [\psi(g_1)]\big([\psi(g_2)](x)\big) = [\psi(g_1) \circ \psi(g_2)](x)\,.$$

Tehát a $\psi : G \to S_G$ leképezés tényleg csoport-homomorfizmus.

A ψ leképezés nyilvánvalóan injektív. Ha ugyanis a g_1 és g_2 elemekre $\psi(g_1) = \psi(g_2)$, vagyis ha a Cayley-táblázat g_1-hez és g_2-höz tartozó sora megegyezik, akkor speciálisan az egységelem oszlopában is ugyanaz ennek a két sornak a megfelelő eleme. De az egységelem oszlopában g_1 sorában $g_1 \cdot 1 = g_1$ áll, a g_2 sorában pedig $g_2 \cdot 1 = g_2$. Tehát $g_1 = g_2$, és így ψ injektív. (Megjegyezzük, hogy $g_1 \neq g_2$ esetén a g_1 és g_2 sora minden egyes helyen eltér, hiszen a táblázat oszlopai is permutációk.)

Mivel a $C = \mathrm{Im}(\psi)$ részcsoportot a ψ értékkészleteként definiáltuk, ψ kölcsönösen egyértelmű a G csoport és a $C \leq S_G$ részcsoport között. Ezzel Cayley tételét beláttuk. □

Cayley tétele úgy is fogalmazható, hogy minden G csoport beágyazható az S_G szimmetrikus csoportba.

A bizonyításban a táblázatra való hivatkozás csak a jobb érthetőséget szolgálta, a tételt beláttuk végtelen csoportokra is, ahol a táblázatot nem is tudnánk felírni. A Cayley-tétel szerint elég lenne csak permutációcsoportokat vizsgálni (mint azt Galois korában tették). A Cayley-reprezentáció vizsgálata azonban csak ritkán segít a csoport szerkezetének feltárásában (a 4.11.40. Feladat egy ilyen alkalmazás).

Sokszor megtörténik az, hogy egy G csoport elemei maguk nem permutációi az X halmaznak, mégis G elemei „hatnak" az X halmazon. Például a kocka esetében beszélhetünk arról is, hogy az egybevágóságok a kocka éleit, lapjait, vagy testátlóit permutálják. Egy egybevágósági transzformáció a tér pontjain értelmezett függvény, tehát nem szakaszokat permutál. De mondhatjuk azt, hogy ha F egybevágóság, akkor az $\overline{AB}$ szakaszt F „vigye" az $\overline{F(A)F(B)}$ szakaszba. Ezt jelölhetjük a következőképpen: $F * \overline{AB} = \overline{F(A)F(B)}$.

4.6.17. Definíció. Azt mondjuk, hogy a G csoport az X halmazon *hat*, ha minden $g \in G$ és $x \in X$ esetén értelmezve van a $g * x \in X$ elem úgy, hogy bármely $g, h \in G$ és $x \in X$ esetén

$$g * (h * x) = (gh) * x$$

(azaz G elemeinek szorzata szorzatpermutációként hat), és ha 1 jelöli G egységelemét, akkor bármely $x \in X$ esetén

$$1 * x = x$$

(vagyis az egységelem identikusan hat X-en).

Ezek a szabályok hasonlítanak ahhoz, ahogy egy vektortér elemeit skalárokkal szorozzuk. Érdemes ellenőrizni, hogy a skalártest multiplikatív csoportja tényleg hat minden vektortéren a fenti értelemben.

4.6.18. Gyakorlat. Mutassuk meg, hogy a fenti hatásnál g^{-1} inverz leképezésként hat, azaz

$$g * x = y \iff g^{-1} * y = x\,.$$

Ezért minden $g \in G$ elemre az $x \mapsto g * x$ leképezés az X halmaz egy permutációja.

Az eddig tárgyaltakat speciális esetként kapjuk, ha $G \leq S_X$, azaz G maga permutációkból áll, és $g * x = g(x)$.

4.6.19. Definíció. Legyen G az X-en ható csoport. Ekkor az $x \in X$ *orbitja* a $g * x$ alakú pontokból áll ($g \in G$), vagyis azokból, ahová x-et G elemeivel el lehet vinni, jele $G(x)$. Az $x \in X$ *stabilizátora* azokból a $g \in G$ csoportelemekből áll, melyekre $g * x = x$, vagyis amelyek az x-et fixen hagyják, jele G_x. Azt mondjuk, hogy G hatása X-en *tranzitív*, ha csak egyetlen orbit van, azaz ha X bármely két eleme egymásba átvihető G egy alkalmas elemével.

4.6.20. Tétel. *Legyen G az X halmazon ható csoport. Ekkor G orbitjai X egy partícióját adják. Tetszőleges $x \in X$ pont orbitjának a hossza épp a pont stabilizátorának az indexe.*

Bizonyítás. Értelmezzük a $\sim_G$ ekvivalencia-relációt az X-en az X-en a következőképpen: $x \sim_G y$ akkor és csak akkor, ha van olyan $g \in G$, melyre $g * x = y$. Ennek osztályai nyilván az orbitok lesznek. A második állítás bizonyítása teljesen ugyanaz, mint a 4.6.6. Tételé: a G_x stabilizátor szerinti bal mellékosztályok elemei x-et ugyanoda, a különböző mellékosztályok elemei pedig különböző helyre viszik, hiszen

$$g' * x = g * x \iff (g^{-1}g') * x = x \iff g^{-1}g' \in G_x \iff g' \in gG_x\,.$$

Ezért az orbitnak ugyanannyi eleme van, mint ahány mellékosztály. □

Most két olyan fogalommal ismerkedünk meg, amelyek nem okvetlenül szükségesek a továbbiak megértéséhez, csak egy-két megjegyzésben és néhány feladatban használjuk majd őket. Az általános algebrákról szóló 8. Fejezetben is visszatérünk rájuk, mivel a hasonlóság a permutációcsoportok között fontos példát szolgáltat izomorfizmusra.

Ugyanaz a csoport sokféleképpen hathat egy halmazon. Legyen például $G = \{1, g\}$ a kételemű ciklikus csoport, és tekintsük a G-nek az alábbi ötféle hatását, az első hármat az $\{1, 2, 3, 4\}$, az utolsó kettőt az $\{a, b, c, d\}$ halmazon:

$$\begin{array}{llll} g *_1 1 = 1 & g *_1 2 = 3 & g *_1 3 = 2 & g *_1 4 = 4\,, \\ g *_2 1 = 1 & g *_2 2 = 2 & g *_2 3 = 3 & g *_2 4 = 4\,, \\ g *_3 1 = 4 & g *_3 2 = 2 & g *_3 3 = 3 & g *_3 4 = 1\,, \\ g *_4 a = b & g *_4 b = a & g *_4 c = d & g *_4 d = c\,, \\ g *_5 a = a & g *_5 b = b & g *_5 c = d & g *_5 d = c\,. \end{array}$$

Ezt úgy is fogalmazhatjuk, hogy a g elemhez tartozó permutáció az első esetben a (23), a második hatásnál az identitás, a harmadiknál az (14), a negyediknél az $(ab)(cd)$, az ötödiknél a (cd) permutáció. Ezek a példák két definícióra inspirálnak bennünket.

4.6.21. Definíció. Ha G hat az X halmazon, akkor legyen ψ az a leképezés, amely minden $g \in G$ elemhez a hozzá tartozó permutációt, vagyis az

$$x \mapsto g * x$$

permutációt rendeli. A kapott $\psi : G \to S_X$ homomorfizmus magját a *hatás magjának* nevezzük. A hatás *hű*, ha magja csak az egységelemből áll.

A fenti öt hatás közül tehát csak a második nem hű.

4.6.22. Gyakorlat. Mutassuk meg, hogy az előző definícióban szereplő ψ tényleg homomorfizmus, melynek N magja az összes pont stabilizátorainak a metszete. Igazoljuk, azt is, hogy G/N izomorf S_X egy alkalmas részcsoportjával, és ha a hatás hű, akkor G maga is beágyazható S_X-be.

Két hatást akkor szeretnénk egyformának nevezni, ha minden $g \in G$ elemhez „ugyanolyan" permutáció tartozik. Ennek akkor is van értelme, ha a két esetben a g elem más halmazokon hat, hiszen csak a g működése az érdekes, az nem, hogy a pontokat éppen hogyan hívják. Ilyen alapon tehát a fenti $*_1$ és $*_5$ hatásokat ekvivalensnek nevezhetjük, hiszen a pontokat átnevezhetjük így:

$$1 \leftrightarrow a \quad 2 \leftrightarrow c \quad 3 \leftrightarrow d \quad 4 \leftrightarrow b\,,$$

és akkor a két permutáció már ugyanaz lesz. Precízen ezt a következőképpen fogalmazhatjuk meg.

4.6.23. Definíció. Legyen $*_1$ és $*_2$ a G csoport hatása az X_1 és az X_2 halmazokon. Azt mondjuk, hogy ez a két hatás *ekvivalens*, ha létezik olyan $\alpha : X_1 \to X_2$ kölcsönösen egyértelmű leképezés, hogy tetszőleges $x \in X_1$ és $g \in G$ esetén

$$\alpha(g *_1 x) = g *_2 \alpha(x)\,.$$

A most elmondottak ugyanúgy hangzanak, mint amikor a csoportok közötti izomorfizmus fogalmát magyaráztuk: csak a műveletek számítanak, az elemeket bárhogyan átfesthetjük. Ezt az érzésünket csak megerősíti a formai hasonlóság a fenti képlet, és a lineáris algebrában tanult $A\lambda v) = \lambda A(v)$ összefüggés között, amely a lineáris leképezéseket jellemzi. Az általános algebrákról szóló részben fogjuk majd megmutatni mindennek az igazi hátterét.

4.6.24. Gyakorlat. Vizsgáljuk meg, hogy a fenti öt hatás közül melyek ekvivalensek, és melyek nem.

Végül egy olyan hatással ismerkedünk meg, amely a Cayley-tétel általánosításának tekinthető.

4.6.25. Definíció. Legyen G csoport, H részcsoportja G-nek, és X a H szerinti bal oldali mellékosztályok halmaza. Definiáljuk G hatását az X halmazon a $g * (aH) = gaH$ képlettel. Ezt a H részcsoport szerinti *mellékosztályokon való hatásnak* nevezzük.

4.6.26. Gyakorlat. Legyen $H \leq G$, és hasson G a H szerinti bal mellékosztályokon balszorzással az előző definíció szerint. Igazoljuk az alábbi állításokat.

(1) Tényleg hatást kaptunk.
(2) Ez a hatás tranzitív.
(3) Az aH pont stabilizátora az aHa^{-1} részcsoport.
(4) A hatás N magja az aHa^{-1} részcsoportok metszete, midőn a befutja G-t.
(5) A G/N faktorcsoport izomorf az S_k egy részcsoportjával, ahol $k = |G : H|$.
(6) Ha $H = \{1\}$, akkor ez a Cayley-tétel bizonyításában használt hatás.

Egy csoport tranzitív hatásai ekvivalensek egy stabilizátor mellékosztályain való hatással, mint azt az alábbi feladat mutatja.

4.6.27. Feladat. Tegyük fel, hogy G tranzitívan hat az X halmazon, és jelölje H az $x \in X$ pont stabilizátorát. Mutassuk meg, hogy G hatása X-en ekvivalens G hatásával a H szerinti bal mellékosztályokon.

Gyakorlatok, feladatok

4.6.28. Gyakorlat. Mik az alábbi $G \leq S_X$ permutációcsoportokban az orbitok és a stabilizátorok?

(1) X a sík pontjai, G az origó körüli forgatások csoportja.
(2) X a sík pontjai, G az x-tengellyel párhuzamos eltolások csoportja.
(3) X egy szabályos n-szög csúcsai, G ezt az n-szöget önmagába vivő egybevágóságok csoportjának egy adott csúcsot fixáló elemei.
(4) X egy kocka csúcsai, G a kocka szimmetriacsoportjában egy csúcs stabilizátora.
(5) $X = \{1, 2, 3, 4\}$, $G = A_4$.

4.6.29. Gyakorlat. Mely négyszögeknek van pontosan két szimmetriája? Melyeknek van ennél több?

4.6.30. Gyakorlat. Határozzuk meg az alábbi testek szimmetriáinak számát.

(1) Egy olyan téglatest, aminek mindhárom élhosszúsága különböző.
(2) Egy olyan négyzet alapú egyenes hasáb, ami nem kocka.
(3) Egy szabályos háromszög alapú egyenes hasáb.
(4) Egy szabályos háromszög alapú egyenes gúla, amely nem szabályos tetraéder.
(5) Egy oktaéder.

4.6.31. Feladat. Mutassuk meg, hogy a kocka G szimmetriacsoportja tranzitívan hat az élek halmazán, és minden él stabilizátora négyelemű. Igazoljuk azt is, hogy G a lapok halmazán is tranzitívan hat, és itt mindegyik stabilizátor a D_4 diédercsoporttal izomorf. Van-e G-nek 16 elemű részcsoportja?

4.6.32. Gyakorlat. Egy gráf szimmetriáján a csúcsainak egy olyan permutációját értjük, amely élt élbe visz. Rajzoljunk olyan nem egypontú gráfokat, melyeknek rendre pontosan 2, 4, 3, 1 szimmetriája van.

4.6.33. Feladat. Mutassuk meg, hogy minden véges csoport előáll egy alkalmas véges, irányítatlan (többszörös és hurokél nélküli) gráf szimmetriacsoportjaként.

4.6.34. Gyakorlat. Mutassuk meg, hogy ha $n \geq 3$, akkor az A_n alternáló csoportban minden pont stabilizátora A_{n-1}-gyel izomorf.

4.6.35. Gyakorlat. Legyen X véges halmaz, $Y \subseteq X$ és $G \leq S_X$. Mutassuk meg, hogy a G csoport azon g elemei, amelyek az Y halmazt önmagába képzik (azaz melyekre $g(Y) \subseteq Y$), részcsoportot alkotnak G-ben. Ezt szokás az Y részhalmaz stabilizátorának is nevezni.

4.6.36. Gyakorlat. Mutassuk meg, hogy ha X véges halmaz, és $g \in S_X$, akkor a g által generált részcsoport orbitjai épp a g ciklusfelbontását adják.

4.6.37. Gyakorlat. Tegyük fel, hogy G hat az X halmazon, legyen $x, y \in X$. Mutassuk meg, hogy ha $g * x = y$, és x stabilizátora H, akkor y stabilizátora gHg^{-1}.

4.6.38. Gyakorlat. Legyenek A és B részcsoportok a G csoportban. Legyen X a B szerinti bal oldali mellékosztályok halmaza, és hasson ezen A balszorzással, azaz legyen $a * (gB) = agB$. Határozzuk meg a B orbitját és stabilizátorát, majd igazoljuk, hogy $|AB| = |A||B|/|A \cap B|$.

4.6.39. Feladat. Hasson a G véges csoport az X véges halmazon. Bizonyítsuk be, hogy a G orbitjainak száma éppen a G elemei fixpontjainak átlagos száma.

Az előző feladat állítása *Burnside-lemma* néven ismeretes. Egyes leszámlálási feladatokban nagyon hasznos, ilyen például a következő.

4.6.40. Feladat. Bontsunk egy négyzetet 9 egybevágó kisebb négyzetre. Hányféleképpen lehet ezek közül négyet kiszínezni (egy színnel) úgy, hogy a négyzet szimmetriáival egymásba átvihető színezéseket nem tekintjük különbözőnek?

4.6.41. Gyakorlat. Legyen X legalább kételemű véges halmaz. Mutassuk meg, hogy S_X minden tranzitív részcsoportjában van fixpontmentes elem. Elhagyható-e a tranzitivitás feltétele?

4.6.42. Gyakorlat. Osztályozzuk az alábbi csoportokat aszerint, hogy melyek izomorfak közülük: $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$, $\mathbb{Z}_4^+$, $\mathbb{Z}_8^+$, $\mathbb{Z}_3^\times$, $\mathbb{Z}_5^\times$, $\mathbb{Z}_6^\times$, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, S_2, A_3, S_3, D_3, D_4, Q (a kvaterniócsoport), $\mathrm{GL}(2, \mathbb{Z}_2)$.

4.6.43. Gyakorlat. Keressük meg S_4-nek azt a részcsoportját, amit a Cayley-tétel bizonyítása a Klein-csoporthoz rendel. Tegyük meg ugyanezt S_6-ban a D_3 csoporttal is.

4.7. Hogyan keressünk normálosztót?

Egy G csoport szerkezetének megértése sokszor úgy történhet, hogy keresünk benne egy N normálosztót, és G-t az N és G/N csoportokból próbáljuk felépíteni. Ezért fontos olyan tételeket bizonyítani, amelyek normálosztók létezését biztosítják. Erre fokozatosan egyre komolyabb eszközöket dolgozunk majd ki. Elsőként a konjugálás fogalmát vezetjük be, amely nemcsak általában segít jellemezni egy csoport normálosztóit, hanem olyan konkrét, fontos normálosztókhoz is elvezet, mint a centrum és a kommutátor-részcsoport.

A normálosztót alkalmas homomorfizmus magjaként definiáltuk, beláttuk azonban, hogy N akkor és csak akkor normálosztó G-ben, ha $gN = Ng$ minden $g \in G$ elemre (4.5.11. Tétel). A kiindulópontunk az, hogy ezt a feltételt átfogalmazzuk.

4.7.1. Állítás. *A G csoport N részcsoportja akkor és csak akkor normálosztó, ha minden $a \in N$ és $g \in G$ esetén $gag^{-1} \in N$.*

Bizonyítás. Az állításban szereplő feltételt komplexusok segítségével úgy írhatjuk fel, hogy $gNg^{-1} \subseteq N$. Ha ez igaz minden g-re, akkor g^{-1}-re is, azaz $g^{-1}Ng \subseteq N$, ahonnan balról g-vel, jobbról g^{-1}-gyel szorozva $N \subseteq gNg^{-1}$ adódik. Tehát a lemma feltétele azzal ekvivalens, hogy $gNg^{-1} = N$ minden $g \in G$-re. Ez pedig pontosan akkor igaz, ha $gN = Ng$ (csak g-vel, illetve a megfordításhoz g^{-1}-gyel kell jobbról szorozni). □

4.7.2. Definíció. A gag^{-1} szorzatot *az a elem g-vel vett konjugáltjának* nevezzük. Az a $\varphi_g : G \to G$ leképezés, amely minden a elemhez gag^{-1}-et rendel, a g elemmel való *konjugálás*.

Az előző állítás tehát azt mondja, hogy a normálosztók pontosan a konjugálásra zárt részcsoportok. Emiatt minden G csoportban normálosztó az $\{1\}$ (hiszen az egységelem minden konjugáltja önmaga), és az egész G. (Megjegyezzük, hogy az $\{1\}$ a G identikus leképezésének, a G pedig az egyelemű csoportba képző homomorfizmusnak a magja.) Ezeket G *triviális normálosztóinak* nevezzük. Az N normálosztó *valódi*, ha $N \neq G$.

4.7.3. Definíció. A G csoportot *egyszerű csoportnak* nevezzük, ha pontosan két normálosztója van: a triviálisak.

Ez a kicsit furcsa fogalmazás arra hivatott, hogy az egyelemű csoportot kizárja az egyszerű csoportok közül, hasonlóan ahhoz, ahogy az 1 számot is kizártuk a prímszámok közül. A 4.4.30. Következményben megmutattuk, hogy egy csoportnak akkor van pontosan két részcsoportja, ha prímrendű ciklikus. Mivel egy Abel-csoportban minden részcsoport nyilván normálosztó, a következőt kapjuk.

4.7.4. Következmény. *A kommutatív egyszerű csoportok pontosan a prímrendű ciklikus csoportok, azaz $\mathbb{Z}_p^+$-szal izomorfak alkalmas p prímszámra.*

A nemkommutatív egyszerű csoportok sokkal bonyolultabbak, vizsgálatuk a csoportelmélet egyik legizgalmasabb területe. Később néhány példát és bizonyítási módszert is bemutatunk majd.

A konjugált gag^{-1} képlete nagyon sok helyen előjön a matematikában, általában olyankor, amikor egy dolgot más nézőpontból kezdünk megvizsgálni. Ekkor g adja meg azt a leképezést ami a nézőpontunkat módosítja. Például lineáris algebrában két mátrixot hasonlónak nevezünk, ha ugyanannak a lineáris transzformációnak a mátrixai, csak más bázisban. Ha a g adja meg az új bázist, akkor egy leképezés mátrixa az új bázisban (a bázistranszformáció ismert képlete szerint) a régi mátrixnak a g-vel való konjugáltja lesz.

A hasonlóság a mátrixok között ekvivalencia-reláció (és a cél az, hogy adott mátrixhoz megtaláljuk a hozzá hasonlók közül a legszebb, lehetőleg diagonális alakú mátrixot). Most ezt az észrevételt fogjuk általánosítani.

4.7.5. Definíció. Egy G csoportban az a és b elemeket akkor nevezzük *konjugáltaknak*, ha van olyan $g \in G$, melyre $gag^{-1} = b$, vagyis ha van olyan konjugálás, amely az a elemet a b elembe viszi. Ennek az ekvivalencia-relációnak az osztályait a csoport *konjugált osztályainak* nevezzük.

4.7.6. Gyakorlat. Ellenőrizzük, hogy a konjugáltság ekvivalencia-reláció.

Az új nyelvünkön a 4.7.1. Állítás a következőképpen fogalmazható át:

4.7.7. Következmény. *Egy N részcsoport akkor és csak akkor normálosztó G-ben, ha a G néhány konjugált osztályának egyesítése.*

Normálosztók kereséséhez tehát célszerű a csoportot konjugált osztályokra bontani. Ehhez viszont jó lenne tudni, hány eleme van egy adott elem konjugált osztályának. Ezt a problémát elemien is kezelhetnénk, sokkal elegánsabb és tanulságosabb azonban, ha a permutációcsoportokról tanultakat alkalmazzuk.

A szemünkről a fátylat az lebbentheti föl, ahogy a konjugált osztályokat definiáltuk, hiszen azt mondtuk: a és b egy osztályban van, ha G egy eleme konjugálással az egyiket a másikba *viszi*. A G elemei *hatnak* (konjugálással) a G alaphalmazán, a 4.6.17. Definíció értelmében.

4.7.8. Állítás. *Legyen G csoport, X a G alaphalmaza, és $g \in G$, $x \in X$ esetén*

$$g * x = gxg^{-1} .$$

Ekkor G hatását definiáltuk az $X = G$ halmazon, melynek orbitjai G konjugált osztályai.

Bizonyítás. A hatás axiómáit kell ellenőrizni. Ha a $g, h \in G$ és $x \in X$, akkor

$$(gh) * x = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g * (h * x) .$$

Legyen 1 a G egységeleme, akkor

$$1 * x = 1x1^{-1} = x .$$

Az ebből a hatásból keletkező orbitok G konjugált osztályai, hiszen két elem akkor van egy konjugált osztályban, ha G egy elemével egymásba átkonjugálhatók. □

Alkalmazzuk az orbit elemszámát megadó 4.6.20. Tételt erre a hatásra. Legyen $x \in X$, ekkor x orbitjának elemszáma az x stabilizátorának az indexe. Az x elem stabilizátora viszont azokból a $g \in G$ elemekből áll, melyekre $g * x = x$, vagyis $gxg^{-1} = x$. Ezt g-vel jobbról szorozva a vele ekvivalens $gx = xg$ alakot kapjuk. Vagyis x stabilizátora az x-szel felcserélhető elemekből áll.

4.7.9. Definíció. Legyen x eleme egy G csoportnak. Ekkor az x elem G-beli *centralizátora* az x-szel felcserélhető elemekből álló részcsoport, jele $C_G(x)$.

4.7.10. Következmény. *Az $x \in G$ elem konjugált osztályának elemszáma az x centralizátorának az indexe. Speciálisan minden konjugált osztály elemszáma osztója G rendjének.*

Természetesen minden elem benne van a saját centralizátorában, hiszen felcserélhető a hatványaival.

Külön figyelmet érdemelnek az egyelemű konjugált osztályok. Egy x elem osztálya akkor és csak akkor ilyen, ha x centralizátorának indexe 1, azaz ha ez a centralizátor az egész csoport, vagyis ha x felcserélhető G minden elemével.

4.7.11. Definíció. Egy G csoport *centrumának* azon $x \in G$ elemeinek halmazát nevezzük, amelyek G minden elemével felcserélhetők. Jele $Z(G)$.

4.7.12. Gyakorlat. Mutassuk meg, hogy G centruma kommutatív normálosztója G-nek, sőt minden részcsoportja is az.

A g elemmel való konjugálás tehát a G csoportnak önmagára való bijektív leképezése. Roppant hasznos tulajdonsága, hogy művelettartó is.

4.7.13. Gyakorlat. Mutassuk meg, hogy ha G csoport és $g \in G$, akkor a g-vel való konjugálás a G csoportot önmagára képző izomorfizmus.

4.7.14. Definíció. Egy G csoportot (vagy más struktúrát) önmagába képző homomorfizmust *endomorfizmusnak* nevezünk. Ha ez kölcsönösen egyértelmű is G-ből G-re, akkor a neve *automorfizmus*. Speciálisan egy csoport konjugálásait *belső automorfizmusoknak* nevezzük. Egy G csoport automorfizmusainak csoportját (a kompozíció műveletére) G *automorfizmus-csoportjának* hívjuk, és $\mathrm{Aut}(G)$-vel jelöljük. A belső automorfizmusok csoportját $\mathrm{Inn}(G)$ jelöli.

4.7.15. Gyakorlat. Mutassuk meg, hogy $\mathrm{Aut}(G)$ tényleg csoport, amelyben $\mathrm{Inn}(G)$ elemei (a belső automorfizmusok) normálosztót alkotnak.

Mivel a konjugálás automorfizmus, megőrzi a csoport szorzásának segítségével definiált tulajdonságokat. Például konjugáláskor az elemrend nem változik meg.

4.7.16. Gyakorlat. Alkalmazzuk a 4.6.22. Gyakorlatban leírtakat a G csoportnak az önmagán konjugálással való hatására. Mutassuk meg, hogy a $\varphi : g \mapsto \varphi_g$ homomorfizmus magja (vagyis a „hatás magja") pontosan G centruma, a φ képe pedig G belső automorfizmusainak csoportja, vagyis $\mathrm{Inn}(G)$. Vezessük le ebből, hogy $G/Z(G) \cong \mathrm{Inn}(G)$.

Az eddigiek alkalmazásaként meghatározzuk az S_3 és az S_4 szimmetrikus csoportok összes normálosztóit. Az S_3 csoport hatelemű. Az egységelem önmaga természetesen konjugált osztályt alkot (hiszen az egységelemet minden belső automorfizmus az egységelembe viszi). Az (123) elem centralizátora biztosan tartalmazza magát az (123) elemet, az egységelemet, és az $(123)^2 = (132)$ ciklust is, tehát legalább háromelemű. Mivel részcsoport, az elemszáma osztója S_3 rendjének, ami 6. Tehát $C_{S_3}\big((123)\big)$ rendje csak 3 vagy 6 lehet. Könnyű számolás mutatja, hogy az (123) és (12) elemek nem cserélhetők fel, és így ez a centralizátor nem az egész S_3. Ezért háromelemű, és akkor az (123) elemnek pontosan két konjugáltja van. Konjugált elemek rendje egyenlő, tehát csak az (132) jön szóba. Így {(123), (132)} egy konjugált elemosztály. Ugyanez a gondolatmenet az (12) centralizátorára alkalmazva azt adja, hogy a harmadik konjugált osztály {(12), (13), (23)}.

Ha N normálosztó S_3-ban, akkor rendje osztója a 6-nak, konjugált osztályok egyesítése, és tartalmazza az egységelemet. Azonnal látjuk, hogy a két triviális normálosztón kívül csak az {*id*, (123), (132)} jöhet szóba. Ez megfelelő is: részcsoport, mert ez az (123) által generált ciklikus részcsoport, és mivel konjugált osztályok egyesítése, normálosztó.

Az S_n csoportnak általában is kiszámíthatjuk a konjugált osztályait.

4.7.17. Gyakorlat. Mutassuk meg, hogy ha $(x_1 \dots x_k)$ egy tetszőleges ciklus az S_n csoportban, és $f \in S_n$, akkor

$$f \circ \big(x_1 \dots x_k\big) \circ f^{-1} = \big(f(x_1) \dots f(x_k)\big)\,.$$

Vezessük le ebből, hogy az S_n csoportban két elem akkor és csak akkor konjugált, ha ciklusfelbontásuk „egyforma”, azaz ugyanannyi, ugyanolyan hosszú ciklus szerepel bennük.

Ebből a gyakorlatból azonnal adódnak S_4 konjugált osztályai. A 4.3.26. Gyakorlatban már látott egyszerű kombinatorikai megfontolásokkal ezek elemszámát is megkaphatjuk. Az eredmény a következő:

6 darab $(abcd)$ alakú permutáció,
6 darab (ab) alakú permutáció,
3 darab $(ab)(cd)$ alakú permutáció,
8 darab (abc) alakú permutáció,
1 darab egységelem.

Ha $N \triangleleft S_4$, akkor konjugált osztályok egyesítése, rendje osztója a 24-nek, és tartalmazza az egységelemet. A két triviális normálosztón kívül csak az $1+3+8=12$ és az $1+3=4$ lehetséges. Az első esetben az A_4 alternáló csoportot kapjuk, amely persze normálosztó (hiszen az „előjelképzés” nevű homomorfizmus magja). A második esetben a

$$K = \{id, (12)(34), (13)(24), (14)(23)\}$$

részhalmaz adódik. A 4.4.33. Gyakorlatban már láttuk, hogy K részcsoport, és így tényleg normálosztó (amely a Klein-csoporttal izomorf).

4.7.18. Gyakorlat. Hogyan módosul az előző gondolatmenet, ha az A_4 csoport normálosztóit akarjuk meghatározni? Mutassuk meg, hogy A_n minden konjugált osztálya vagy konjugált osztálya S_n-nek is, vagy S_n egy konjugált osztályának két egyenlő elemszámú részre bontásából származik.

Fontos tudnunk, hogy egy normálosztó normálosztója nem feltétlenül normálosztó az egész csoportban (vagyis hogy a „normálosztójának lenni” reláció általában nem tranzitív). Például az S_4 csoport fenti K normálosztója Abel-féle, és így minden részcsoportja normálosztó. Ugyanakkor K-nak csak a két triviális részcsoportja lesz normálosztó G-ben is, a fennmaradó három kételemű részcsoport nem.

Ennek a jelenségnek könnyen megérthetjük az okát. Az N azért normálosztó G-ben, mert zárt a G-beli elemekkel való konjugálásra, vagyis a belső automorfizmusokra. Ha $K \triangleleft N$, akkor K zárt az N elemeivel való konjugálásra, de nem feltétlenül zárt a G elemeivel való konjugálásokra, hiszen ezek N-nek automorfizmusai, de általában nem belső automorfizmusok. Ha tehát K zárt az N összes automorfizmusára, akkor normálosztó lesz G-ben is. Ezt a fogalmat írja le a következő definíció.

4.7.19. Definíció. A G csoport egy N részcsoportját *karakterisztikus részcsoportnak* nevezzük, ha N invariáns G összes automorfizmusára, azaz $n \in N$ és $\alpha \in \mathrm{Aut}(G)$ esetén $\alpha(n) \in N$.

Karakterisztikus részcsoportokra a 4.7.47. Gyakorlatban láthatunk példákat.

4.7.20. Gyakorlat. Bizonyítsuk be a következő állításokat.

(1) Egy K részcsoport akkor és csak akkor karakterisztikus részcsoport G-ben, ha minden $\alpha \in \mathrm{Aut}(G)$ automorfizmusra $\alpha(K) = K$.
(2) Ha $N \triangleleft G$, akkor N minden karakterisztikus részcsoportja normálosztó G-ben.
(3) Karakterisztikus részcsoport karakterisztikus részcsoportja az egész csoportnak karakterisztikus részcsoportja.

Normálosztót a részcsoportoknál már tanult generálás segítségével is kereshetünk.

4.7.21. Gyakorlat. Mutassuk meg, hogy egy csoport tetszőleges normálosztóinak metszete is normálosztó.

Így a 4.4.26. Állítás bizonyításához hasonlóan minden $X \subseteq G$ halmazhoz (egyértelműen) létezik az X-et tartalmazó legszűkebb normálosztó (mint az X-et tartalmazó normálosztók metszete). Ezt az X által *generált normálosztónak* nevezzük.

4.7.22. Gyakorlat. Legyen X részhalmaza a G csoportnak, és álljon Y az X összes elemeinek összes konjugáltjaiból:

$$Y = \{gxg^{-1} \,:\, x \in X, g \in G\}\,.$$

Mutassuk meg, hogy G-ben az X által generált normálosztó pontosan az Y által generált részcsoport lesz. Tehát az X által generált normálosztó elemei az x elemeinek konjugáltjaiból és ezek inverzeiből készített tetszőleges szorzatok.

4.7.23. Állítás. *Ha N és K normálosztók a G csoportban, akkor NK is az, méghozzá ez az N és K (uniója) által generált normálosztó.*

Bizonyítás. A 4.5.28. Gyakorlat szerint $KN = NK$ a K és az N által generált részcsoport. Ha $g \in G$, akkor $gN = Ng$ és $gK = Kg$ miatt $gNK = NgK = NKg$, tehát NK normálosztó. Mivel részcsoport legalább annyi van, mint normálosztó, ha NK a legszűkebb N-et és K-t tartalmazó részcsoport, akkor nyilván a legszűkebb az N-et és K-t tartalmazó normálosztók között is. □

A centrum részcsoportjai mind kommutatív normálosztók. Most megkeressük egy csoport összes kommutatív faktorcsoportjait.

4.7.24. Definíció. Legyen G csoport és $a, b \in G$. Az $[a, b] = aba^{-1}b^{-1}$ elemet az a és b elemek *kommutátorának* nevezzük. A G csoport *kommutátor-részcsoportja* az összes kommutátorok által generált részcsoport, jele G'.

4.7.25. Állítás. *Tetszőleges G csoport kommutátor-részcsoportja normálosztó G-ben, sőt minden G'-t tartalmazó részcsoport is normálosztó. Ha $N \triangleleft G$, akkor G/N akkor és csak akkor kommutatív, ha $G' \subseteq N$.*

Bizonyítás. Jelölje φ_g a g elemmel való konjugálást. Ez szorzattartó, és ezért

$$\varphi_g([a,b]) = \varphi_g(aba^{-1}b^{-1}) = \varphi_g(a)\varphi_g(b)\varphi_g(a)^{-1}\varphi_g(b)^{-1} = [\varphi_g(a), \varphi_g(b)]\,.$$

Tehát ha X jelöli az összes kommutátorok halmazát, akkor az X elemeinek konjugáltjaiból készített Y halmaz megegyezik az X-szel. Így az X által generált részcsoport ugyanaz, mint az X által generált normálosztó (lásd 4.7.22. Gyakorlat). Ezért $G' \triangleleft G$.

Legyen most $N \triangleleft G$. Ekkor

$$aNbN = bNaN \iff abN = baN \iff aba^{-1}N = bN \iff$$
$$\iff aba^{-1}b^{-1}N = N \iff aba^{-1}b^{-1} \in N\,.$$

Vagyis G/N akkor és csak akkor kommutatív, ha az összes kommutátor benne van N-ben. Mivel G' a kommutátorok által generált részcsoport, ez azzal ekvivalens, hogy $G' \subseteq N$.

Végül legyen $G' \leq H \leq G$, be kell látnunk, hogy H normálosztó G-ben. Azt már láttuk, hogy a G/G' faktorcsoport kommutatív. De kommutatív csoport minden részcsoportja normálosztó. Speciálisan tehát a H/G' részcsoport is normálosztó, és ezért (a 4.5.19. Tétel (5) pontja miatt) $H \triangleleft G$. □

4.7.26. Definíció. Legyenek N és K részcsoportok a G csoportban. Ekkor az összes $[n,k]$ kommutátorok által generált részcsoportot (ahol $n \in N$ és $k \in K$) az N és K *kölcsönös kommutátor-részcsoportjának* nevezzük, jele $[N,K]$.

4.7.27. Gyakorlat. Legyenek N és K normálosztók a G csoportban. Mutassuk meg, hogy $[N,K] \subseteq N \cap K$. Speciálisan $[N,G] \subseteq N$, és ha $N \cap K = \{1\}$, akkor N minden eleme felcserélhető K minden elemével (azaz N *centralizálja* K-t).

Konjugáltja nemcsak elemnek, hanem részcsoportnak is van.

4.7.28. Definíció. Legyen H részcsoportja a G csoportnak és $g \in G$. A gHg^{-1} részcsoportot a H részcsoport g-vel való konjugáltjának nevezzük.

Mivel a g-vel való konjugálás automorfizmus, a H részcsoport képe, azaz gHg^{-1} szintén részcsoport. Legyen X a G részcsoportjainak a halmaza. Ekkor a

$$g * H = gHg^{-1}$$

képlet hatást definiál X-en. Ennek orbitjait a *részcsoportok konjugált osztályainak* nevezzük. Egy H részcsoport stabilizátora nyilván azokból a $g \in G$ elemekből áll, amelyekre $gHg^{-1} = H$, vagyis $gH = Hg$.

4.7.29. Definíció. Legyen H részcsoport a G csoportban. Ekkor azon $g \in G$ elemek halmazát, melyekre $gH = Hg$, a H részcsoport G-beli *normalizátorának* nevezzük, jele $N_G(H)$.

Az orbit elemszámáról szóló tétel most a következőt adja.

4.7.30. Következmény. *Tetszőleges $H \leq G$ részcsoport konjugáltjainak száma a H normalizátorának az indexe, vagyis $|G : N_G(H)|$.*

Nyilván $H \lhd G$ akkor és csak akkor, ha $N_G(H) = G$.

4.7.31. Gyakorlat. Igazoljuk, hogy a H részcsoport normalizátora a legbővebb olyan H-t tartalmazó részcsoportja G-nek, amelyben H normálosztó (speciálisan $H \subseteq N_G(H)$).

Általában tetszőleges részhalmaznak beszélhetünk a centralizátoráról és a normalizátoráról is.

4.7.32. Definíció. Legyen X részhalmaza egy G csoportnak. Ekkor X centralizátora azon $g \in G$ elemek halmaza, amelyek X minden elemével felcserélhetők (jele $C_G(X)$), az X normalizátora pedig azon $g \in G$ elemek halmaza, melyre $gX = Xg$ (jele $N_G(X)$).

4.7.33. Gyakorlat. Legyen X részhalmaza a G csoportnak. Bizonyítsuk be a következő állításokat.

(1) $C_G(X)$ részcsoport, méghozzá az $C_G(x)$ centralizátorok metszete, ahol $x \in X$.
(2) $N_G(X)$ részcsoport, méghozzá az X pont stabilizátora a G csoport egy alkalmas hatásánál.
(3) $C_G(X) \lhd N_G(X)$.
(4) Ha X részcsoport, akkor $C_G(X)/N_G(X)$ izomorf X automorfizmus-csoportjának egy alkalmas részcsoportjával.

Ha egy csoportban van „kis” indexű részcsoport, akkor „hajlamos” rá, hogy kis indexű normálosztót is tartalmazzon. Az alábbi állításon kívül a 4.7.45, a 4.12.21. és a 4.11.39. Feladatok is ezt fogják megerősíteni.

4.7.34. Állítás. *Tetszőleges csoportban minden kettő indexű részcsoport normálosztó.*

Bizonyítás. Ha $|G : N| = 2$, akkor G-nek két bal oldali mellékosztálya van N szerint. Az egyik N, a másik tehát N komplementuma, azaz $G - N$. Ugyanez azonban a jobb oldali mellékosztályokra is igaz. Tehát a bal oldali és a jobb oldali mellékosztályok halmaza is $\{N, G - N\}$. Ezért $N \lhd G$. □

Gyakorlatok, feladatok

4.7.35. Gyakorlat. Normálosztó-e a $H \leq G$ részcsoport a következő esetekben?

(1) $G = \mathbb{Z}^+$, $H = 3\,\mathbb{Z}^+$.
(2) $G = D_6$, $H = \{F^2, F^4, F^6 = 1\}$.
(3) $G = D_6$, $H = \{1, F^3, T, TF^3\}$.
(4) $G = \mathrm{GL}(n, \mathbb{R})$, H a diagonális mátrixok halmaza.
(5) $G = \mathrm{GL}(n, \mathbb{R})$, H az egységmátrix nem nulla skalárszorosainak a halmaza.
(6) $G = \mathrm{GL}(n, \mathbb{R})$, H a felső háromszögmátrixok halmaza.

4.7.36. Gyakorlat. Állapítsuk meg az alább felsorolt csoportok elemeinek konjugált osztályait és normálosztóit: D_3, D_4, Q (a kvaterniócsoport), D_5, S_5, A_5, $\mathrm{GL}(2, \mathbb{Z}_2)$.

4.7.37. Gyakorlat. A 4.2.27. Gyakorlatban már meghatároztuk az $(1, 2, \ldots, n)$ ciklus centralizátorát. Adjunk erre új bizonyítást annak birtokában, hogy már ismerjük S_n konjugált osztályait (4.7.17. Gyakorlat).

4.7.38. Gyakorlat. Határozzuk meg a $\mathbb{Z}_n^+$, Q, D_n, S_n, A_4 csoportok centrumát és kommutátor-részcsoportját.

4.7.39. Gyakorlat. Melyik korábbról már ismert csoporttal izomorfak az alábbi faktorok?

(1) $D_4/\{1, F^2\}$.
(2) $S_4/\{id, (12)(34), (13)(24), (14)(23)\}$.
(3) $D_8/\{1, F^2, F^4, F^6\}$.

4.7.40. Gyakorlat. Legyen G tizedrendű nemkommutatív csoport. Bizonyítsuk be a következő állításokat, majd általánosítsunk arra az esetre, ha G rendje egy prím kétszerese.

(1) G-ben nincs tizedrendű elem.
(2) Ötödrendű elem nem lehet felcserélhető másodrendű elemmel.
(3) G-ben nem lehet minden elem másodrendű.
(4) G-ben van másodrendű elem.
(5) Minden ötödrendű elem centralizátora ötelemű.
(6) Minden másodrendű elem centralizátora kételemű.
(7) G-ben öt darab másodrendű elem van, és ezek mind konjugáltak.
(8) G-ben négy darab ötödrendű elem van.
(9) Ha $o(f) = 5$ és $o(t) = 2$, akkor $tft^{-1} = f^{-1}$.
(10) $G \cong D_5$.

4.7.41. Gyakorlat. Legyen N kételemű normálosztó a G csoportban. Igazoljuk, hogy N része G centrumának.

4.7.42. Gyakorlat. Bizonyítsuk be, hogy egy G csoport egy X részhalmaza akkor és csak akkor generál kommutatív részcsoportot, ha X bármely két eleme egymással felcserélhető.

4.7.43. Feladat. Mi lesz egy ciklikus csoport, a Klein-csoport, illetve az S_3 szimmetrikus csoport automorfizmus-csoportja?

4.7.44. Feladat. Mely véges csoportoknak van olyan másodrendű automorfizmusa, amelynek egyetlen fixpontja az egységelem? (Az ilyen automorfizmust fixpontmentesnek szokás hívni, hiszen az egységelem amúgy is mindig fixpont, az „nem számít”.)

4.7.45. Feladat. Mutassuk meg, hogy páratlan rendű csoportban minden 3 indexű részcsoport normálosztó, de páros rendűben nem feltétlenül.

4.7.46. Gyakorlat. Mutassuk meg, hogy egy csoportban az n rendű elemek által generált részcsoport mindig normálosztó, sőt karakterisztikus részcsoport.

4.7.47. Gyakorlat. Igazoljuk az alábbi állításokat.

(1) Egy ciklikus csoport minden részcsoportja karakterisztikus.
(2) A centrum mindig karakterisztikus részcsoport.
(3) Ha ha N és K normálosztók G-ben, akkor $[N, K]$ is normálosztó G-ben, ha pedig N és K karakterisztikus részcsoportok, akkor $[N, K]$ is az. Speciálisan minden csoport kommutátor-részcsoportja karakterisztikus.
(4) Ha A (additívan írt) Abel-csoport, és n pozitív egész, akkor az $nA = \{na : a \in A\}$ és az $A[n] = \{a \in A : na = 0\}$ részcsoportok karakterisztikusak.

4.7.48. Feladat. Legyenek K, L, N normálosztók egy csoportban. Bizonyítsuk be, hogy $[K, N] = [N, K]$ és $[K, LN] = [K, L][K, N]$.

4.8. A direkt szorzat

A véges Abel-csoportokat sikerült izomorfia erejéig teljesen megérteni. Most ezt a tételt mutatjuk be, és majd a modulusokról szóló fejezetben, általánosabban igazoljuk (de a feladatokban szerepel egy alternatív bizonyítás is). Egy ilyen struktúratétel bizonyításakor két feladatunk van. Az első az, hogy a leírandó objektumokat (jelen esetben a véges Abel-csoportokat) össze tudjuk állítani egyszerűbb komponensekből (például ciklikus csoportokból), egy olyan konstrukció segítségével, amely lehetővé teszi a hatékony számolást, kérdések gyors megválaszolását. A másik feladat az, hogy valamiféle egyértelműséget bizonyítsunk (izomorfia erejéig). A legegyszerűbb példa ilyen struktúratételre a számelmélet alaptétele! Minden számot „egyszerűbb számokból", nevezetesen prímszámokból állítunk elő a „szorzás" nevű konstrukció segítségével, és ez az előállítás egy jól megfogalmazott értelemben egyértelmű is. Nem kell bizonygatni, hogy hasznos tételt kaptunk.

Második példaként adjunk struktúratételt a véges dimenziós vektorterekre. Lineáris algebrában minden vektortérben keresünk egy bázist, és ennek segítségével koordinátázzuk a vektorteret a T alaptest elemeinek, azaz a skalároknak a segítségével. Minden vektort egyértelműen megad a koordinátavektora, azaz egy n magas oszlopvektor, és ez a megfeleltetés tartja a műveleteket is. Vagyis minden véges dimenziós vektortér izomorfia erejéig megkonstruálható az alaptestből az „oszlopvektorok képzése" nevű konstrukcióval.

Az egyértelműség kérdése is tisztázott. Hogyan dönthetjük el, hogy a T^n és T^m vektorterek izomorfak-e? Vegyünk az első vektortérben egy (n elemű) bázist. Ha a két vektortér között van izomorfizmus, akkor a bázisunk képe bázis lesz T^m-ben is. Mivel a bázis elemszáma, azaz a dimenzió egyértelműen meghatározott, innen $m = n$ következik. Ennek a gondolatmenetnek a lényege az, hogy egy olyan tulajdonságot kerestünk (ez volt a dimenzió), amely az izomorfizmus során nem változik meg, *invariáns* marad.

Ha két csoportról akarjuk megmutatni, hogy nem izomorfak, akkor szintén olyan tulajdonságot (invariánst) érdemes keresni, ami az egyiknek megvan, a másiknak nincs. Például a 4.6.15. Gyakorlat megoldásában láttuk, hogy a D_4 és a Q csoportok nem izomorfak, mert más bennük a másodrendű elemek száma. Itt tehát az (izomorfizmusnál megőrződő) invariáns a másodrendű elemek száma volt. De ilyen invariáns a csoport rendje is például, vagy a kommutativitás, vagy a nyolcadrendű részcsoportok száma, és így tovább, általában minden olyan fogalom, amelyet a csoport szorzása segítségével definiálhatunk.

A fentiek szerint a vektortereket izomorfia erejéig egyetlen invariánssal, a dimenziójukkal jellemezhetjük. Ezért a vektortér a lehető legegyszerűbb algebrai struktúrák közé tartozik. Már a véges Abel-csoportoknál is bonyolultabb a helyzet, a nemkommutatív véges csoportok esetében pedig nem is ismerünk olyan invariánsrendszert, ami az izomorfiát eldöntené.

A véges Abel-csoportokat úgy fogjuk megkapni, hogy „oszlopvektorokat" képzünk, ezekbe azonban skalárok helyett prímhatványrendű ciklikus csoportok elemeit írjuk.

Az oszlopvektorokkal a műveleteket komponensenként végezzük. Ugyanezt akkor is megtehetjük, ha az egyes komponensek csoportokból valók. Legyenek $G_1, \ldots, G_n$ tetszőleges csoportok, és tekintsük a $(g_1, \ldots, g_n)$ sorozatokat, ahol $g_i \in G_i$ minden i-re. Ezeknek a sorozatoknak a halmazát $G_1 \times \ldots \times G_n$ jelöli. (A sorozatokat tipográfiai okokból nem oszlopba, mint a vektortereknél, hanem sorba írjuk.) A szorzást komponensenként definiáljuk:

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

(természetesen az i-edik komponensben a G_i csoport szorzását kell elvégezni).

4.8.1. Gyakorlat. Mutassuk meg, hogy csoportot kaptunk, melynek egységeleme az, ahol minden komponensbe a megfelelő csoport egységelemét tesszük, és az inverzet is komponensenként kell kiszámítani.

4.8.2. Definíció. A most kapott csoportot a $G_1, \ldots, G_n$ csoportok *direkt szorzatának* nevezzük, jele

$$G_1 \times \ldots \times G_n = \prod_{i=1}^{n} G_i \,.$$

Hasonlóan definiáljuk a direkt szorzatot végtelen sok komponens esetében is, végtelen sorozatok segítségével. Ha a tényezők egyenlők, akkor *direkt hatványról* beszélünk, és n tényező esetén a G^n jelölést alkalmazzuk.

4.8.3. Gyakorlat. Mutassuk meg, hogy a $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ csoport izomorf a $\mathbb{Z}_6^+$ csoporttal, de a $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$ csoport nem izomorf a $\mathbb{Z}_4^+$ csoporttal. A felsorolt csoportok közül izomorf-e valamelyik a Klein-csoporttal?

4.8.4. Állítás. *A direkt szorzat tetszőleges elemének rendje a komponensei rendjeinek legkisebb közös többszöröse, és végtelen, ha a komponensek között van végtelen rendű is.*

Bizonyítás. Az állítást az egyszerűbb jelölés kedvéért véges sok tényezős szorzatra bizonyítjuk. Legyen $(g_1, \ldots, g_n) = G_1 \times \ldots \times G_n$, határozzuk meg ennek az elemnek a jó kitevőit. Nyilván $(g_1, \ldots, g_n)^k = (g_1^k, \ldots, g_n^k)$ akkor és csak akkor az egységelem, ha minden i-re g_i^k a G_i egységeleme, azaz ha $o(g_i)$ osztója k-nak. A legkisebb ilyen pozitív k a rendek legkisebb közös többszöröse. □

Végtelen sok tényező esetén a direkt szorzat egy g elemének végtelen sok komponense van, és ezek rendjeinek legkisebb közös többszörösét kell kiszámítani. Ez nem mindig létezik (lásd a 3.1.20 Gyakorlat megoldását), ebben az esetben a g elemnek végtelen lesz a rendje.

4.8.5. Definíció. Egy csoport elemei rendjeinek a legkisebb közös többszörösét a csoport *exponensének* nevezzük. Az exponenst végtelennek tekintjük, ha a csoport elemeinek rendjei között van végtelen, vagy ha mind véges ugyan, de a legkisebb közös többszörösük nem létezik.

4.8.6. Következmény. *Egy direkt szorzat exponense a tényezők exponenseinek legkisebb közös többszöröse.*

4.8.7. Következmény. *A G és H véges csoportok direkt szorzata akkor és csak akkor ciklikus, ha G és H egymáshoz relatív prím rendű ciklikus csoportok.*

Bizonyítás. Legyen $|G| = n$ és $|H| = m$. Ha g generálja G-t és h generálja H-t, akkor a (g, h) rendje az $[n, m]$ legkisebb közös többszörös. Ha n és m relatív prímek, akkor ez egyenlő nm-el (lásd 3.1.29. Gyakorlat), tehát a $G \times H$ rendjével. Ezért ekkor (g, h) generálja a direkt szorzatot, és így az ciklikus.

Megfordítva, tegyük fel, hogy $G \times H$ ciklikus, és legyen (g, h) egy generátorelem, vagyis aminek a rendje mn. Lagrange tétele miatt g rendje osztója n-nek, h rendje pedig m-nek. Tehát (g, h) rendje $[o(g), o(h)] \mid [m, n]$. Innen $mn \mid [m, n]$, ami csak úgy lehetséges, hogy m és n relatív prímek. Ekkor $o(g)$ és $o(h)$ is azok, tehát (g, h) rendje $o(g)o(h) = mn$. Ezért $o(g) = n$ és $o(h) = m$, vagyis G és H is ciklikus csoportok. □

4.8.8. Következmény. *Ha m és n relatív prím pozitív egészek, akkor $\mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \cong \mathbb{Z}_{nm}^+$.*

Nevezetes számelméleti tény, hogy ennek a gyakorlatnak az állítása a multiplikatív csoportokra is igaz.

4.8.9. Következmény. *Ha m és n relatív prím pozitív egészek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.*

Bizonyítás. Az állítás az A.4.4. Tétel átfogalmazása, hiszen az ottani képlet azt fejezi ki, hogy a g megfeleltetés szorzattartó. □

Ennek az észrevételnek van egy nagyon érdekes számelméleti következménye. Emlékezzünk rá, hogy a $\mathbb{Z}_n^\times$ csoport generátorelemeit (ha van ilyen, azaz ha ez a csoport ciklikus, akkor) primitív gyöknek neveztük modulo n.

4.8.10. Gyakorlat. Mutassuk meg, hogy ha modulo k létezik primitív gyök, akkor k vagy prímhatvány, vagy egy prímhatvány kétszerese.

További vizsgálatokkal igazolható, hogy pontosan akkor létezik primitív gyök modulo n, ha $n = 1, 2, 4$, vagy egy páratlan prímhatvány, vagy annak kétszerese. Ez a 4.3.16. Tétel általánosítása.

Ha egy csoportról sikerül belátni, hogy direkt szorzat, akkor ez jó hír, mert a szerkezetét sikerült kisebb (és ezért remélhetőleg egyszerűbb) csoportokéra visszavezetni. Tehát szeretnénk tudni, hogyan lehet felismerni, hogy egy csoport izomorf-e egy direkt szorzattal.

Ehhez kanyarodjunk vissza a lineáris algebrához. A V vektorteret az U és W alterek direkt összegének neveztük, ha $U + W = V$ és $U \cap W = \{0\}$. Ezek a feltételek azt garantálják, hogy V minden v eleme egyértelműen felírható $u + w$ alakban, ahol $u \in U$ és $w \in W$. Azaz V elemei kölcsönösen egyértelmű megfeleltetésben állnak az (u, w) párokkal. Könnyű látni, hogy ha a vektortér-műveleteket ezekre a párokra komponensenként értelmezzük, akkor ez a megfeleltetés művelettartó is.

Legyen $G = A \times B$ direkt szorzat. Ekkor az a $\pi_1 : G \to A$ leképezés, amely az (a, b) párt a-ba viszi, nyilván szürjektív homomorfizmus, hiszen a műveleteket komponensenként végezzük. E homomorfizmus magja tehát normálosztó, amely azokból az (a, b) párokból áll, amelyre $a = 1_A$. Másképp fogalmazva a $B^* = \{(1_A, b) : b \in B\}$ normálosztóról van szó. Azért írtunk B^*-ot, mert ez a csoport nyilvánvalóan B-vel izomorf. A homomorfizmus-tétel miatt $G/B^* \cong A$.

A π_1 és π_2 homomorfizmusok neve *projekció*).

4.8.11. Állítás. *Tegyük fel, hogy $G = A \times B$, ahol A és B tetszőleges csoportok. Tekintsük az*

$$A^* = A \times \{1_B\} = \{(a, 1_B) : a \in A\}$$
$$B^* = \{1_A\} \times B = \{(1_A, b) : b \in B\}$$

halmazokat. Ekkor

$$G/B \cong A \cong A^* \lhd G, \quad G/A \cong B \cong B^* \lhd G,$$
$$A^* \cap B^* = \{1_G\}, \quad A^* B^* = G\,.$$

Bizonyítás. Csak annak a megmutatása maradt hátra, hogy $A^* \cap B^* = \{1_G\}$ és $A^* B^* = G$. Ha $(a, b) \in A^* \cap B^*$, akkor $(a, b) \in A^*$ miatt $b = 1_B$, és $(a, b) \in B^*$ miatt $a = 1_A$. Tehát $(a, b) = 1_G$. Ha $(a, b) \in G$ tetszőleges elem, akkor $(a, b) = (a, 1_B)(1_A, b) \in A^* B^*$. □

Miként lineáris algebrában is, a felsorolt tulajdonságoknak a megléte már elegendő ahhoz, hogy direkt szorzatot kapjunk.

4.8.12. Tétel. *Legyen G csoport, és tegyük fel, hogy G-ben van két normálosztó, A és B úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.*

Bizonyítás. A feltétel szerint G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$. Ez az előállítás egyértelmű is, ha ugyanis $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor átrendezéssel azt kapjuk, hogy

$$a'^{-1} a = b' b^{-1}\,.$$

Itt a bal oldal A-nak, a jobb oldal B-nek eleme. Tehát ez az elem $A \cap B$-ben van, vagyis a feltétel szerint az egységelem. De ha $a'^{-1}a = 1$, akkor, hogy $a = a'$, és hasonlóan kapjuk, hogy $b = b'$.

Ezzel beláttuk, hogy az a φ leképezés, melyet a $\varphi((a, b)) = ab$ képlet definiál, bijekció az $A \times B$ és G között. Még azt kell megmutatnunk, hogy φ szorzattartó. Ez a bizonyítás egyetlen nemtriviális lépése, de a munkát már elvégeztük a 4.7.27. Gyakorlatban, ahol beláttuk, hogy $A \cap B = \{1\}$ miatt A minden eleme felcserélhető B minden elemével. Ha tehát $a, a' \in A$ és $b, b' \in B$, akkor $a'b = ba'$, és ezért

$$\varphi((a, b)(a', b')) = \varphi((aa', bb')) = aa'bb' = aba'b' = \varphi((a, b))\varphi((a', b')) ,$$

amivel az állítást beláttuk. □

Ha az előző tételben nem tesszük fel, hogy $AB = G$, akkor a fenti bizonyításból az adódik, hogy AB (ami normálosztó, lásd 4.7.23. Állítás) izomorf A és B direkt szorzatával. Véges G csoport esetén az $AB = G$ feltételt helyettesíthetjük azzal, hogy $|A| \cdot |B| = |G|$ (a 4.6.38. Gyakorlat miatt).

Korábban már beszéltünk arról, hogy egy G csoportot megpróbálhatunk összerakni egy A normálosztóból és a G/A faktorcsoportból. A direkt szorzat a legegyszerűbb ilyen összerakási módszer, hiszen $G = A \times B$-ben van egy A-val izomorf normálosztó, amely szerinti faktor B-vel izomorf. Szó sincs azonban arról, hogy a G csoportot csak így lehetne összerakni A-ból és G/A-ból. Például ha $G = \mathbb{Z}_4^+$ és $A = \{0, 2\}$, akkor A is és G/A is a kételemű ciklikus csoport, de G nem izomorf ezek direkt szorzatával, mert G-ben csak egy darab kételemű részcsoport van. De ha van is G-ben olyan B részcsoport, melyre $AB = G$ és $A \cap B = \{1\}$, vagyis ha az előző tétel összes feltétele teljesül, kivéve hogy B normálosztó, abból még mindig nem következik, hogy $G \cong A \times B$. Erre a szakasz végén vizsgálunk meg egy példát, amely elvezet majd bennünket a direkt szorzat fogalmának egy általánosításához.

A több (de véges sok) tényezős direkt szorzatot is jellemezhetjük normálosztók segítségével a 4.8.12. Tétel általánosításaként.

4.8.13. Gyakorlat. Legyen G_i^* a $G = G_1 \times \ldots \times G_n$ direkt szorzat azon elemeinek a halmaza, melyek i-edik komponense tetszőleges eleme G_i-nek, a többi komponensben pedig a megfelelő csoport egységeleme áll. Igazoljuk, hogy G_i^* a G_i-vel izomorf normálosztója a G direkt szorzatnak, és hogy a G_i^* normálosztók teljesítik a következő tulajdonságokat:

(1) szorzatuk az egész G csoport;
(2) bárhogy is veszünk $n - 1$ darabot közülük, ezek szorzatának és a kimaradónak a metszete csak az egységelemből áll.

Megfordítva, mutassuk meg, hogy az ilyen tulajdonságú normálosztók direkt szorzatra való felbontást adnak.

Külön is felhívjuk a figyelmet arra, hogy a feltétel ***nem úgy szól***, hogy bármely két G_i^* metszete triviális. A vektorterekhez visszatérve, vegyünk a síkon három, origón átmenő egyenest. Ezek összege a sík, bármely kettő metszete nulla, mégsem igaz, hogy a sík ennek a

három egyenesnek a direkt összege lenne, hiszen három egyenes direkt összege biztosan háromdimenziós. A teret viszont felbonthatjuk három egyenes direkt összegére, például a három koordináta-tengely segítségével, és itt valóban igaz, hogy bármely két tengely által kifeszített sík nullában metszi a harmadik tengelyt.

4.8.14. Tétel [A véges Abel-csoportok alaptétele]. *Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A felbontásban szereplő tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Ez azt jelenti, hogy ha a G csoportot kétféleképpen felbontottuk prímhatványrendű ciklikus csoportok direkt szorzatára, akkor bárhogy is veszünk egy q prímhatványt, a q elemszámú tényezők száma mindkét felbontásban ugyanannyi lesz.*

Ezt a tételt csak később, és jóval általánosabban bizonyítjuk be (7.4.1. Tétel). A felbontás létezése a 4.8.33. Feladatból is következik.

Például legyen G rendje 24. Ekkor a lehetséges tényezők rendjei éppen a 24 szám prímhatvány-osztói, azaz $2, 4, 8, 3$. Ilyen elemszámú tényezőkből kell a 24-et kikombinálni. A lehetőségek tehát a következők:

$$\mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ , \quad \mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_4^+ , \quad \mathbb{Z}_3^+ \times \mathbb{Z}_8^+ .$$

Ezek szerint izomorfia erejéig 3 darab 24 rendű Abel-csoport van.

A fejezet zárásaként a direkt szorzat fogalmának egy általánosítását ismertetjük vázlatosan. A 4.8.12. Tétel bizonyításában nem hagyható el az a feltétel, hogy A és B mindketten normálosztók legyenek. Például legyen $G = S_3$, $A = \{id, (123), (132)\}$ és $B = \{id, (12)\}$. Ekkor $A \times B$ a hatodrendű ciklikus csoport lesz, és nem az S_3. A problémát az okozza, hogy bár az A normálosztó G-ben, a B nem az.

4.8.15. Definíció. Tegyük fel, hogy a G csoportban N normálosztó, H pedig részcsoport úgy, hogy $NH = G$ és $N \cap H = \{1\}$. Az ilyen H részcsoportot az N *komplementumának* nevezzük.

4.8.16. Gyakorlat. Mutassuk meg, hogy ha H komplementuma a G csoport N normálosztójának, akkor $H \cong G/N$.

Mi az a többletinformáció az N és H szerkezetén kívül, ami a G csoportot már meghatározza? Mivel $G = NH$, a G elemei nh alakban írhatók, ahol $n \in N$ és $h \in H$. Két ilyen elem szorzatát a következőképpen számíthatjuk ki:

$$(n_1h_1)(n_2h_2) = \big(n_1(h_1n_2h_1^{-1})\big)(h_1h_2) .$$

A $h_1n_2h_1^{-1}$ elem az n_2-nek a h_1-gyel vett konjugáltja, vagyis N-beli. Ezért az N és H szorzástábláján kívül még azt kell tudnunk, hogy hogyan hat konjugálással a H részcsoport az N normálosztón. A $h_1n_2h_1^{-1}$ elemek táblázatos felsorolása helyett érdemes észrevenni a következőket.

4.8.17. Gyakorlat. Legyen N normálosztó, H részcsoport a G csoportban, és jelölje

$$\varphi_h : n \mapsto hnh^{-1}$$

a h elemmel való konjugálást N-en. Igazoljuk, hogy φ_h egy (nem feltétlenül belső) automorfizmusa N-nek, és a $\varphi : h \mapsto \varphi_h$ leképezés homomorfizmus H-ból N automorfizmuscsoportjába.

Most már nincs más dolgunk, mint megfordítani az eddigieket: N-ből, H-ból és φ-ből megkonstruálni G elemeit és szorzását. Technikai megjegyzés, hogy az nh elem helyett (n, h)-t fogunk írni, hasonlóan ahhoz, ahogy a komplex számok precíz bevezetésénél $a+bi$ helyett (a, b)-t írtunk.

4.8.18. Definíció. Legyenek N, H csoportok, és $\psi : H \to \mathrm{Aut}(N)$ tetszőleges homomorfizmus. Definiáljuk a G csoportot úgy, hogy elemei az (n, h) rendezett párok ($n \in N$, $h \in H$), a szorzás pedig

$$(n_1, h_1)(n_2, h_2) = \big(n_1\big(\psi(h_1)\big)(n_2), h_1h_2\big)\,.$$

Az így kapott csoportot N és H *szemidirekt szorzatának* nevezzük, és $N \rtimes_\psi H$-val jelöljük (az indexben lévő ψ-t néha elhagyva).

4.8.19. Gyakorlat. Legyen G a most definiált szemidirekt szorzat, továbbá

$$N^* = \{(n, 1) : n \in N\} \quad \text{és} \quad H^* = \{(1, h) : h \in H\}\,.$$

Igazoljuk az alábbiakat.

(1) G tényleg csoport a megadott szorzásra.
(2) Az N^* az N-nel izomorf normálosztó G-ben.
(3) A H^* a H-val izomorf részcsoport G-ben.
(4) $G = N^*H^*$, és $N^* \cap H^* = \{(1, 1)\}$.
(5) A H^* konjugálással úgy hat N^*-on, ahogy a ψ leképezés előírja, azaz

$$(1, h)(n, 1)(1, h)^{-1} = \big(\big(\psi(h)\big)(n), 1\big)\,.$$

Gyakorlatok, feladatok

4.8.20. Gyakorlat. Adjuk meg a $\mathbb{Z}_2^+ \times \mathbb{Z}_4^+$ csoport összes negyedrendű elemét.

4.8.21. Gyakorlat. Mutassuk meg az elemrendek kiszámításával, hogy a $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_4^+$ és a $\mathbb{Z}_4^+ \times \mathbb{Z}_4^+$ csoportok nem izomorfak.

4.8.22. Gyakorlat. A véges Abel-csoportok alaptételének segítségével döntsük el, hogy izomorfia erejéig hány 6, 8, 16, 32, 48 rendű Abel-csoport van.

4.8.23. Gyakorlat. Döntsük el, hogy az alábbi csoportok közül melyek bonthatók fel két valódi normálosztójuk direkt szorzatára, és igenlő válasz esetén adjunk is meg egy-egy ilyen felbontást: $\mathbb{Z}_6^+$, $\mathbb{Z}_8^+$, $\mathbb{Z}^+$, $\mathbb{Q}^+$, $\mathbb{C}^+$, $\mathbb{Z}_{15}^\times$, $\mathbb{Z}_{16}^\times$, D_3, D_4, D_6, Q, A_4, S_5.

4.8.24. Gyakorlat. Hányféleképpen bontható direkt szorzatra $\mathbb{Z}_5^+ \times \mathbb{Z}_5^+$?

4.8.25. Gyakorlat. Tegyük fel, hogy C normálosztó az A és D normálosztó a B csoportban. Mutassuk meg, hogy $(C \times D) \lhd (A \times B)$ és $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$.

4.8.26. Gyakorlat. Igazoljuk, hogy $Z(G \times H) = Z(G) \times Z(H)$ és $(G \times H)' = G' \times H'$ (G és H tetszőleges csoportok, a vessző kommutátor-részcsoportot jelöl).

4.8.27. Gyakorlat. Álljon G az S_8 azon elemeiből, melyek az $\{1, 2, 3, 4\}$ részhalmazt önmagába képzik. Mutassuk meg, hogy ez részcsoport, de nem normálosztó S_8-ban. Igaz-e, hogy $G \cong S_4 \times S_4$?

4.8.28. Feladat. Bizonyítsuk be, hogy a kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-szal.

4.8.29. Feladat. Legyen A Abel-csoport és p prímszám. Tegyük fel, hogy $pa = 0$ minden $a \in A$ esetén. Definiáljuk $\lambda \in \mathbb{Z}_p$ esetén a λa szorzatot, mint egész többszöröst. Igazoljuk, hogy ezzel a szorzással A vektortérré válik $\mathbb{Z}_p$ fölött. Hol romlik el ez a gondolatmenet, ha A a negyedrendű ciklikus csoport és $p = 2$?

4.8.30. Gyakorlat. Igazoljuk, hogy $\mathrm{Aut}\big((\mathbb{Z}_p^+)^n\big) \cong \mathrm{GL}(n, \mathbb{Z}_p)$. Itt a $(\mathbb{Z}_p^+)^n$ egy n tényezős direkt szorzatot, azaz direkt hatványt jelöl.

4.8.31. Feladat. Bizonyítsuk be, hogy egy véges Abel-csoportban mindig van olyan elem, amelynek a rendje a csoport exponense, és így a csoport akkor és csak akkor ciklikus, ha exponense megegyezik a rendjével. Adjunk ennek felhasználásával új bizonyítást arra a tényre, hogy egy test multiplikatív csoportjának minden véges részcsoportja ciklikus (4.4.36. Feladat).

4.8.32. Gyakorlat. Izomorfak-e egy korábbról már ismert csoporttal az alábbi szemidirekt szorzatok? Ha nem, mennyi a rendjük?

(1) $H = \mathbb{Z}_2^+$, $N = \mathbb{Z}_n^+$, $\psi(1)$ minden elemet invertál.
(2) $H = \mathbb{Z}_3^+$, $N = \mathbb{Z}_7^+$, $\psi(1)$ minden elemet megkétszerez.
(3) $H = \mathbb{Z}_2^+$, $N = \{1, a, b, c\}$ a Klein-csoport, $\psi(1)$ az (ab) transzpozíció.
(4) $H = \mathbb{Z}_3^+$, $N = \{1, a, b, c\}$ a Klein-csoport, $\psi(1)$ az (abc) ciklus.
(5) $H = S_3$, $N = \{1, a, b, c\}$ a Klein-csoport, $\psi\big((12)\big) = (ab)$, $\psi\big((123)\big) = (abc)$.
(6) $H = \mathbb{Z}_4^+$, $N = \mathbb{Z}_3^+$, $\big(\psi(1)\big)(x) = -x$.

4.8.33. Feladat. Legyen A véges Abel-csoport, és p prímosztója A rendjének. Mutassuk meg, hogy ha $a \in A$ maximális rendű az A csoport p-hatványrendű elemei között, akkor A felbomlik a $\langle a \rangle$ részcsoport, és egy másik alkalmas részcsoport direkt szorzatára.

4.9. Szabad csoportok és definiáló relációk

Az eddigiek során számos példát láttunk csoportra. Eleinte konkrét csoportokat vizsgáltunk, amelyek számokból, permutációkból, mátrixokból álltak. Ezután előtérbe kerültek olyan konstrukciók, amelyek csoportokból újabb csoportokat állítanak elő. Szó volt direkt szorzatról, faktorcsoportról, de ide sorolhatjuk a generált részcsoport fogalmát is. Ebben a szakaszban egy újabb csoportkonstrukciót ismertetünk. A most készítendő csoportok homomorf képeként minden más csoport előáll majd.

Lineáris algebrában a független generátorrendszereket neveztük bázisnak. A bázis jelentősége nemcsak az, hogy a vektorteret koordinátázhatjuk a segítségével, hanem az is, hogy lehetővé teszi a vektortéren értelmezett lineáris leképezések áttekintését. Az előírhatósági tétel szerint egy bázis elemein bárhogy is adunk meg egy függvényt egy másik vektortérbe, az egyértelműen kiterjeszthető egy lineáris leképezéssé. Így a lineáris leképezéseket mátrixokkal jellemezhetjük, és ezért könnyebb számolni velük.

Egy φ csoport-homomorfizmust is egyértelműen meghatároz az, ha ismerjük egy generátorrendszeren felvett értékeit (lásd 4.4.28. Gyakorlat). Az azonban nem igaz általában, hogy ezeket az értékeket tetszőlegesen írhatnánk elő. Például ha a g_1 generátorelem négyzete az egységelem, akkor ennek a feltételnek a $\varphi(g_1)$ elemre is teljesülnie kell. Ugyanígy, ha $g_1g_2 = g_2g_1$, akkor $\varphi(g_1)$ és $\varphi(g_2)$ is felcserélhető lesz. Ezek a generátorelemek közötti összefüggések a lineáris összefüggés általánosításainak tekinthetők. A $g_1, \ldots, g_n$ generátorrendszert szabad generátorrendszernek szeretnénk nevezni, ha nincs az elemei között ilyen rejtett összefüggés. Nem könnyű azonban megfogalmazni, hogy milyen összefüggéseket zárjunk ki. Például a $g_1g_1^{-1} = g_2^{-1}g_2$ összefüggést meg kell, hogy engedjük, hiszen ez a csoportaxiómák miatt mindig teljesül. Egy összefüggést akkor kell megengednünk (akkor nem rontja el a szabadságot), ha az minden csoportban igaz. Az ilyen megengedett összefüggések technikai leírása helyett sokkal kényelmesebb ezt a tulajdonságot a homomorfizmusok nyelvén megfogalmazni. Például a $g_1g_2 = g_2g_1$ nem megengedett összefüggés, mert nem teljesül mondjuk az S_3 csoport (12) és (23) elemeire. Vagyis nincs olyan homomorfizmus, ami g_1-et (12)-be, g_3-at (23)-ba vinné. Ezek szerint a szabadság feltétele az, hogy az előírhatósági tétel teljesüljön az adott generátorrendszerre.

4.9.1. Definíció. A G csoport egy $g_1, \ldots, g_n$ generátorrendszerét *szabad generátorrendszernek* nevezzük, ha bárhogyan is választunk egy H csoportot, és benne $h_1, \ldots, h_n$ elemeket, (egyértelműen) létezik olyan $\varphi : G \to H$ homomorfizmus, melyre $\varphi(g_i) = h_i$ minden $1 \leq i \leq n$ esetén. Átfogalmazva: az $X \subseteq G$ (esetleg végtelen) generátorrendszer akkor szabad, ha bárhogyan is veszünk egy H csoportot és egy $\varphi : X \to H$ tetszőleges függvényt, ez kiterjeszthető egy $G \to H$ homomorfizmussá. A G csoport *szabad*, ha van szabad generátorrendszere.

4.9.2. Tétel. *Minden X halmazhoz létezik egy olyan csoport, amelyet X szabadon generál, és ez a csoport izomorfia erejéig egyértelműen meghatározott. Az X által generált szabad csoportot $F(X)$-szel fogjuk jelölni.*

Ezt a tételt (általánosabban, nemcsak csoportokra) belátjuk majd 8.3. Szakaszban. Most egy másik bizonyítást adunk, aminek az az előnye, hogy leírja az X által generált szabad csoport elemeit (lásd 4.9.4. Következmény). Azt javasoljuk az Olvasónak, hogy mindenképpen

eméssze meg ennek a következménynek az állítását akkor is, ha a most következő bizonyítást a könyv első olvasásakor átugorja.

Bizonyítás. Elsőként az egyértelműséget látjuk be, mert ahhoz nem kell ismerni a szabad csoportok szerkezetét. Tegyük fel, hogy a G és a H csoportokat is szabadon generálja az X generátorrendszer. Mivel G szabad, az X identikus leképezése kiterjeszthető egy $\varphi : G \to H$ homomorfizmussá. Ugyanígy, mivel H szabad, van olyan $\psi : H \to G$ homomorfizmus, ami X elemeit fixen hagyja. Megmutatjuk, hogy φ és ψ egymás inverzei. Ehhez elég belátni, hogy $\psi \circ \varphi$ a G identikus leképezése, és $\varphi \circ \psi$ a H identikus leképezése. Az elsőt mutatjuk meg, a második ugyanúgy megy.

A G csoportból önmagába két homomorfizmusunk van: $\psi \circ \varphi$ és az identitás. Az X generátorrendszeren megegyeznek (mert ott mindkettő az identitás). A 4.4.28. Gyakorlat miatt tehát a két homomorfizmus az egész G-n megegyezik.

Térjünk most rá a szabad csoport létezésének bizonyítására. Az X halmaz minden x eleméhez készítsünk el egy x^{-1} elemet is (úgy, hogy ezek az X elemeitől és egymástól is különbözzenek). Jelölje S az így kapott x és x^{-1} „betűkből" álló „szavak" halmazát, vagyis az olyan véges sorozatokét, amelyek minden eleme x vagy x^{-1} alakú. Ha $X = \{x, y\}$, akkor egy ilyen „szó" például a következő lehet:

$$x^{-1}x^{-1}yyyyyyxyyx^{-1}yyxy^{-1}y^{-1}y^{-1}\,.$$

Ezt a szót az összevonásokat elvégezve így írhatjuk fel:

$$x^{-2}y^6xy^2x^{-1}y^2xy^{-3}\,.$$

Az üres szót is bevesszük, aminek egyetlen betűje sincs. Értelmezzük az s és t szavak szorzatát st-nek, azaz úgy, hogy a szavakat ebben a sorrendben egymás után írjuk (betűköz nélkül). Az nyilvánvaló, hogy ez egy asszociatív művelet, amelyre nézve az üres szó kétoldali neutrális elem. Ezért az üres szót a továbbiakban 1-gyel jelöljük.

Azt szeretnénk, hogy x és x^{-1} egymás inverzei legyenek. Ez most nem áll, mert xx^{-1} nem az egységelem (nem az üres szó). Ezért xx^{-1}-et (és $x^{-1}x$-et) azonosítani szeretnénk 1-gyel. Ez persze további azonosításokat von maga után. Például az $xyy^{-1}x^{-1}x$, és az $y^{-1}yx$ szavak is egyenlővé válnak, hiszen ha mindkettőből kihúzzuk az egymás melletti „inverzeket", akkor mindkettő az x szóvá egyszerűsödik. Azt szeretnénk belátni, hogy az azonosítás után már csoportot kapunk, mégpedig az X által generált szabad csoportot.

Technikailag az azonosítást a következőképpen kezelhetjük. Nevezzük elemi átalakításnak azt a lépést, amikor egy szóból kihúzunk (vagy betoldunk) xx^{-1}-et vagy $x^{-1}x$-et. Képletben:

$$sxx^{-1}t \sim st \quad \text{és} \quad sx^{-1}xt \sim st$$

tetszőleges s, t szavak és $x \in X$ esetén. Azt mondjuk, hogy az s és t szavak ekvivalensek, képletben $s \sim t$, ha véges sok elemi átalakítás segítségével s-ből megkaphatjuk t-t.

Nagyon könnyű ellenőrizni, hogy a $\sim$ ekvivalencia-reláció az S halmazon. A reflexivitás teljesül, hiszen minden szó önmagába alakítható nulla lépésben. A szimmetria is igaz,

hiszen az elemi átalakítások is szimmetrikusak: oda-vissza alkalmazhatók. Végül a tranzitivitást az biztosítja, hogy két véges átalakítás-sorozatot egymás után fűzve szintén véges átalakítás-sorozatot kapunk.

A G csoport elemei legyenek a $\sim$ ekvivalencia-relációhoz tartozó partíció osztályai. A bizonyítás első lépése az, hogy könnyen megjegyezhető és alkalmazható szabályt adunk arra, mikor ekvivalens két szó. Vegyünk egy s szót, és kezdjük kihuzigálni belőle az egymás melletti xx^{-1} és $x^{-1}x$ alakú betűpárokat. Ezt esetleg sokféleképpen tehetjük, hiszen az s szóban több ilyen betűpár is lehet. A végeredmény egy olyan szó lesz, amiben már nincs kihúzható betűpár. Az ilyen szavakat egyszerűsíthetetlennek hívjuk majd.

4.9.3. Állítás. *Az s szót bárhogyan is egyszerűsítjük kihúzásokkal, a kapott egyszerűsíthetetlen szó mindig ugyanaz lesz. Az s és t szavak akkor és csak akkor ekvivalensek, ha őket kihúzásokkal leegyszerűsítve ugyanazt az egyszerűsíthetetlen szót kapjuk.*

Ez az állítás tehát azt fejezi ki, hogy ha az s és t szavakat nagyon trükkösen, például sok betoldással és kihúzással egymásba tudjuk alakítani, akkor ezt megtehetjük azzal az egyszerű módszerrel is, hogy mindkettőt a lehető legprimitívebben egyenlővé egyszerűsítjük.

Bizonyítás. A kulcs a következő észrevétel. Tegyük fel, hogy egy u szóba egy elemi átalakítással betoldunk, a következő lépésben pedig kihúzunk belőle, és így egy w szóhoz jutunk. Megmutatjuk, hogy ekkor vagy $u = w$ (azaz a két lépés teljesen fölösleges), vagy pedig u-ból w-be eljuthatunk úgy is, hogy először u-ból kihúzunk egy párt, majd az eredménybe betoldunk egy párt.

Ahhoz, hogy ezt belássuk, legyen a kiinduló szó $u = st$, amibe betoldunk s és t közé xx^{-1}-et (ha $x^{-1}x$-et toldunk be, a gondolatmenet ugyanaz lesz), majd a kapott $sxx^{-1}t$ szóból kihúzunk egy betűpárt, és eredményül az w szót kapjuk.

Ha a kihúzás az s vagy a t szóból történt, akkor nyilván megtehetjük, hogy először ezt a kihúzást végezzük el, és utána toldunk be xx^{-1}-et. Akkor sincs gond, ha a most betoldott xx^{-1}-et húzzuk ki, mert akkor $u = st = w$. A harmadik lehetőség az, ha a most betoldott xx^{-1} betűk valamelyikét húzzuk ki. Ez vagy úgy történhet, hogy s utolsó betűje x^{-1}, vagy úgy, hogy t első betűje x. Az első esetben $s = s_1x$ és a kihúzás után $w = s_1xt$. Vagyis ismét $u = w$. Ugyanígy $u = w$ adódik a másik esetben is, (amikor t első betűje x). Észrevételünket tehát beláttuk.

Az észrevételnek az a következménye, hogy ha az s és t szavak között van egy akármilyen hosszú átalakítás-sorozat, akkor ezt módosíthatjuk úgy, hogy először a kihúzások, és azután a betoldások következzenek. (Valóban, ha betoldás megelőz kihúzást, akkor van olyan betoldás is, ami után közvetlenül kihúzás következik, és akkor egy kihúzást mindig eggyel előbbre hozhatunk.) Legyen r a kihúzások után következő szó az átalakításban. Ekkor tehát s-ből kihúzásokkal r, innen betoldásokkal t adódik.

Ha tehát s és t ekvivalens szavak, akkor mindkettőből alkalmas kihúzásokkal elérhető ugyanaz a szó (nevezetesen az r). Még azt kell megmutatni, hogy ha egy szót többféleképpen egyszerűsítünk, akkor ugyanazt az eredményt kapjuk. Valóban, tegyük fel, hogy egy u szónak s és t is egyszerűsíthetetlen alakja. Ekkor s és t ekvivalensek, és ezért a már

bizonyítottak szerint van közös r egyszerűsítésük. De mindketten egyszerűsíthetetlenek, tehát csak $s = r = t$ lehetséges. Ezzel a 4.9.3. Állítást beláttuk. A továbbiakban egy s szó (egyértelműen meghatározott) egyszerűsíthetetlen alakját s'-vel fogjuk jelölni. □

Megértettük tehát, hogy az s és t szavak akkor és csak akkor vannak egy $\sim$-osztályban, ha az (egyértelműen meghatározott) egyszerűsíthetetlen alakjuk egyenlő, azaz $s' = t'$. Ennek birtokában definiálhatjuk az osztályok között (azaz a G csoportban) a szorzást. Két osztályt úgy akarunk összeszorozni, ahogy a faktorcsoportban szorzunk: kiveszünk belőlük egy-egy szót, megnézzük, hogy a szorzatuk melyik osztályba esik, és ez az osztály lesz az eredmény. A faktorcsoportnál tanultakhoz hasonlóan most is meg kell mutatni, hogy ez a művelet jóldefiniált, ami a következőt jelenti: ha $s_1 \sim t_1$ és $s_2 \sim t_2$, akkor be kell látni, hogy $s_1 s_2 \sim t_1 t_2$.

Az $s_1 s_2$ szorzat egyszerűsítését kezdhetjük úgy, hogy először külön-külön s_1-et, illetve s_2-t egyszerűsítjük le. Ekkor $s_1' s_2'$-höz jutunk, és így $s_1 s_2 \sim s_1' s_2'$. Ugyanígy $t_1 t_2 \sim t_1' t_2'$. De tudjuk, hogy $s_1 \sim t_1$ miatt $s_1' = t_1'$, és $s_2 \sim t_2$ miatt $s_2' = t_2'$, ezért $s_1' s_2' = t_1' t_2'$. Így

$$s_1 s_2 \sim s_1' s_2' = t_1' t_2' \sim t_1 t_2 \,.$$

A $\sim$-osztályok között most definiált szorzás tehát tényleg jóldefiniált.

Az a leképezés, ami minden szóhoz a $\sim$-osztályát rendeli, nyilván szorzattartó. Emiatt S szorzásának asszociativitása öröklődik az osztályok szorzására is. Az is nyilvánvaló, hogy az üres szó osztálya egységelem lesz. Végül belátjuk, hogy minden osztálynak van inverze. Az x és x^{-1} osztályai inverzek, mert az xx^{-1} és az $x^{-1}x$ szorzatok 1-re egyszerűsödnek. De minden szó ilyen elemek szorzata, és ezért minden osztály $x_1 \dots x_n$ alakban írható, ahol az x_i valamelyik x-nek vagy x^{-1}-nek az osztálya alkalmas $x \in X$-re. Ekkor pedig ennek az osztálynak inverze lesz $x_n^{-1} \dots x_1^{-1}$. Így beláttuk, hogy a $\sim$-osztályok G halmaza csoport, amelyben az $x \in X$ elemek osztályai generátorrendszert alkotnak. Meg kell még mutatnunk, hogy ez a generátorrendszer szabad.

Legyen H tetszőleges csoport, és $\varphi : X \to H$ egy függvény. Ekkor φ megadható minden $s \in S$ szón is: ha $x \in X$, és $\varphi(x) = h$, akkor legyen $\varphi(x^{-1}) = h^{-1}$, ha pedig $s = x_1 \dots x_n$, ahol $x_i \in X \cup X^{-1}$, akkor legyen $\varphi(s) = \varphi(x_1) \dots \varphi(x_n)$. Nyilván φ egy szorzattartó leképezés S-ből H-ba.

Mi azonban nem S-en, hanem a G csoporton szeretnénk a φ leképezést értelmezni. Ehhez belátjuk, hogy φ minden $\sim$-osztályon konstans. Nyilván $\varphi(xx^{-1}) = \varphi(x^{-1}x) = 1_H$. Emiatt elemi átalakítások során sem változik meg φ értéke, de akkor ilyenek sorozatánál sem. Értelmezzük φ-t az s szó osztályán $\varphi(s)$-nek. Ekkor egy G-ből H-ba vezető homomorfizmust kaptunk, ami az $x \in X$ elemek osztályain a φ által előírt értékeket veszi fel. Ezzel a 4.9.2. Tétel bizonyítását befejeztük. □

Az előző bizonyításban kapott G csoportnak valójában nem részhalmaza X, hanem az $x \in X$ elemek $\sim$-osztályai lesznek G elemei. Ezek azonban páronként különböző osztályok (hiszen az egybetűs szavakat nem lehet egyszerűsíteni). Ezért azonosíthatjuk az x

elemet az x osztályával. Ekkor G-nek X részhalmazává válik. Természetesen az x^{-1} szimbólumot is azonosítjuk az x osztályának inverzével. Ez azzal jár, hogy xx^{-1} és $x^{-1}x$ az egységelemmel lesz azonos, vagyis a $\sim$-osztályok egy elemre esnek össze. Ezt az elemet természetesen az osztály egyetlen egyszerűsíthetetlen elemének érdemes választani, amikor a csoport elemeit leírjuk. A 4.9.3. Állítás miatt a szabad csoport elemeiről a következőket állíthatjuk.

4.9.4. Következmény. *Legyen G az X halmaz által generált szabad csoport. Ekkor X és X^{-1} diszjunktak, és G az $X \cup X^{-1}$ elemeiből készített szorzatokból áll. Ha*

$$x_1 \dots x_n \quad \text{és} \quad y_1 \dots y_k$$

két ilyen szorzat, melyek egyszerűsíthetetlenek, vagyis egyikben sem áll közvetlenül egymás mellett egy X-beli elem és az inverze, akkor e két szorzat csak akkor egyenlő, ha tényezőről tényezőre megegyeznek (vagyis $n = k$, és $x_1 = y_1, \dots, x_n = y_n$).

A szabad csoportokkal kapcsolatban bizonyítás nélkül megemlítünk egy nevezetes tételt.

4.9.5. Tétel [Nielsen–Schreier-tétel]. *Szabad csoport minden részcsoportja is szabad.*

4.9.6. Feladat. Mutassuk meg, hogy ha egy szabad csoportban X és Y is szabad generátorrendszer, akkor X és Y elemszáma megegyezik.

4.9.7. Feladat. Bizonyítsuk be, hogy a két elemmel generált szabad csoportnak van olyan részcsoportja, amelynek a szabad generátorrendszere végtelen.

Csoportokat úgy is konstruálhatunk, hogy megmondjuk, milyen tulajdonságú elemek generálják, és ezek között milyen összefüggések teljesüljenek. Technikailag ezt úgy valósítjuk meg, hogy a csoportot egy szabad csoport faktoraként definiáljuk. A módszert először konkrét példákon mutatjuk be, az elméleti részt a szakasz végére hagyjuk.

Egy szabályos n-szög szimmetriacsoportját diédercsoportnak neveztük, és D_n-nel jelöltük. A 4.6.8. Gyakorlatban beláttuk, hogy a csoportnak $2n$ eleme van: n forgatás, és n tükrözés. A 4.1.8. Állításban pedig kimondtuk, de nem láttuk be, hogy hogyan lehet a diédercsoport elemeivel kényelmesen számolni. Most ezt az állítást igazoljuk, de úgy, hogy egyben a definiáló relációk fogalmához is eljussunk.

4.9.8. Állítás. *Jelöljön F egy szabályos n-szög középpontja körüli $2\pi/n$ szögű forgatást, T pedig legyen a sokszög egyik (tetszőleges) tengelyes szimmetriája. Ekkor a D_n csoportot generálják az F és T elemek, és érvényesek az*

$$F^n = 1\,, \qquad T^2 = 1\,, \qquad FT = TF^{-1}$$

összefüggések (ahol 1 az identitást jelöli).

Bizonyítás. Nyilvánvaló, hogy F hatványai kiadják az összes forgatásokat, így F rendje n. Ez összesen n darab elem, ami a csoport elemszámának a fele. Az F és T által generált részcsoport ennél több elemű, és Lagrange tétele miatt rendje osztja D_n rendjét, vagyis $2n$-et. Ezért ez a részcsoport csak maga D_n lehet. Nyilván $T^2 = 1$ (az identitás), hiszen T

tükrözés. Végül az FT elem is tengelyes tükrözés (mert ha forgatás lenne, azaz $FT = F^i$, akkor innen $T = F^{i-1}$ következne, márpedig T nem forgatás). Ezért $(FT)^2 = 1$, ahonnan TF^{-1}-zel szorozva $FT = TF^{-1}$ adódik. □

Most felejtsük el a geometriai hátteret, és vizsgáljuk meg, hogy a felsorolt szabályok elegendőek-e ahhoz, hogy a csoportban számolni tudjunk.

4.9.9. Állítás. *Tegyük fel, hogy a G csoportot generálják az f és t elemek, melyekre teljesülnek az $f^n = t^2 = 1$, $ft = tf^{-1}$ összefüggések. Ekkor G összes eleme*

$$\{f^0 = 1, f, f^2, \ldots, f^{n-1}, t, tf, tf^2, \ldots, tf^{n-1}\},$$

és a szorzás szabálya a következő:

$$f^i f^j = f^{i+j}, \qquad (tf^i) f^j = tf^{i+j},$$
$$f^i (tf^j) = tf^{j-i}, \qquad (tf^i)(tf^j) = f^{j-i},$$

ahol az f kitevőjében a $+$ és a $-$ jelek a mod n műveleteket jelentik.

Bizonyítás. A felsorolt szorzatok nyilván G elemei. Az $ft = tf^{-1}$ összefüggést többször egymás után alkalmazva $f^i t = tf^{-i}$ adódik, ahonnan a fenti négy szorzási szabály azonnal következik (felhasználva a $t^2 = 1 = f^n$ összefüggéseket is). Emiatt az

$$\{f^0, f, f^2, \ldots, f^{n-1}, t, tf, tf^2, \ldots, tf^{n-1}\}$$

halmaz zárt a szorzásra. Zárt az inverzképzésre is, hiszen $(f^i)^{-1} = f^{-i} = f^{n-i}$, és

$$(tf^i)^{-1} = f^{-i}t = tf^i.$$

Ezért ez a halmaz részcsoport. Mivel tartalmazza a t és f elemeket, tartalmazza az általuk generált részcsoportot is, ami a feltételünk szerint G. Ezzel a 4.1.8. Állítást is beláttuk. □

Ha G a D_n diédercsoport, akkor a felsorolt $2n$ elem mind különböző (hiszen tudjuk, hogy D_n rendje $2n$). Ne higgyük azonban, hogy csak a D_n csoport tesz eleget a feltételeknek. Egészen triviális példaként megfelel például az egyelemű csoport is, ahol $f = t = 1$. De kielégíti a feltételeket az n-edrendű ciklikus csoport is, ahol f az egyik generátorelem, és $t = 1$. Ugyanígy a kételemű ciklikus csoport is jó lesz, ahol t a generátorelem és $f = 1$. Sőt, megfelel a D_k diédercsoport is $k \mid n$ esetén, ha f-et egy $2\pi/k$ szögű forgatásnak, t-t pedig tetszőleges tengelyes tükrözésnek választjuk. A felsorolt esetek mindegyikében valamiféle összeesés van az eredetileg felsorolt $2n$ elem között. Ez az összeesés valójában egy homomorfizmus!

4.9.10. Állítás. *Egy G csoport akkor és csak akkor elégíti ki az előző állítás feltételeit, ha van olyan $\varphi : D_n \to G$ szürjektív homomorfizmus, melyre $\varphi(F) = f$ és $\varphi(T) = t$.*

Bizonyítás. A 4.9.9. Állításban leírt szorzási táblázat természetesen a D_n diédercsoportra is érvényes. Ezért ha egy G csoport eleget tesz ezeknek az összefüggéseknek, akkor a $\varphi : T^i F^j \mapsto t^i f^j$ szürjektív homomorfizmus (hiszen a D_n és a G csoportokban ugyanazok a képletek adják meg a szorzástáblát). Megfordítva, ha $\varphi : D_n \to G$ egy szürjektív

homomorfizmus, akkor $f = \varphi(F)$ és $t = \varphi(T)$ nyilván generátorrendszert alkot G-ben (lásd 4.5.27. Gyakorlat), amely teljesíti az $f^n = 1$, $t^2 = 1$, $ft = tf^{-1}$ egyenlőségeket, hiszen ezek F-re és T-re is teljesülnek. □

A D_n diédercsoport tehát a „legnagyobb" olyan csoport, ami a felírt három feltételt teljesíti, abban az értelemben, hogy minden más ilyen csoport D_n-nek homomorf képe. Sokszor előfordul, hogy a fordított feladatot kell megoldanunk: olyan csoportokat keresünk, amelynek bizonyos generátorelemei között bizonyos összefüggéseket ismerünk.

4.9.11. Gyakorlat. Legyenek $n > 0$, $m > 0$ és k egész számok. Mutassuk meg, hogy ha a G csoportot generálják az f és t elemek, melyekre $f^n = t^m = 1$ és $ft = tf^k$ teljesül, akkor G elemszáma legfeljebb nm, és minden eleme $t^i f^j$ alakban is, $f^k t^\ell$ alakban is felírható alkalmas i, j, k, ℓ egészekre.

Például melyek azok a csoportok, amelyek az f és t elemekkel generálhatók, de most azt tudjuk, hogy

$$f^4 = t^4 = 1\,, \qquad f^2 = t^2\,, \qquad ft = tf^{-1}\,?$$

Az egyelemű csoport persze most is kielégíti a feltételeket, de esetleg más csoportok is. Van-e ezek között legnagyobb? A megoldást most is kezdhetjük úgy, hogy megpróbáljuk a csoport összes elemét felírni. A 4.9.11. Gyakorlat szerint a csoport minden eleme $t^i f^j$ alakú lesz, ahol $0 \le i, j < 4$. Látszólag ez 16 elemet enged meg, de $f^2 = t^2$ miatt f^2 helyébe t^2-et, f^3 helyébe $t^2 f$-et írhatunk. Tehát a j értéke csak 0 vagy 1 lehet. Így a csoportnak legfeljebb 8 eleme van.

Abból azonban, hogy ezt a nyolc szót felírjuk, és össze is tudjuk szorozni őket az adott szabályok szerint, még nem következik, hogy ***van*** ilyen nyolcelemű csoport. Hiszen nem tudhatjuk, hogy ha még tovább ügyeskednénk és alakítgatnánk a fenti elemeket, akkor a most kapott nyolc elem között nem fedezhetnénk-e fel további összeeséseket.

Például tekintsük az alábbi összefüggésrendszert:

$$f^3 = t^3 = 1\,, \qquad ft = tf^{-1}\,.$$

Ugyanúgy, mint az előző két példában, itt is minden elemet $f^i t^j$ alakra hozhatunk, ahol $0 \le i, j < 3$, vagyis a csoportnak legfeljebb kilenc eleme lehet. De ezek között további, rejtett egyenlőségek vannak! Hogy ezeket felfedezzük, próbáljuk meg az $ft = tf^{-1} = tf^2$ összefüggéssel „előreszállítani" az $f = ft^3$ elem három t betűjét:

$$f = ft^3 = (ft)t^2 = tf^2t^2 = tf(ft)t = tftf^2t =$$
$$= t(ft)f^2t = t^2f^2f^2t = t^2f^4t = t^2(ft) = t^3f^2 = f^2.$$

Innen pedig $f = 1$, vagyis ez a csoport maximum háromelemű, és így a legnagyobb ilyen csoport a harmadrendű ciklikus csoport, ahol f az egységelem, t pedig az egyik generátor.

Azt, hogy ebből a számolásból $f = 1$ jött ki, a következő magyarázza. Folytassuk a 4.9.11. Gyakorlat megoldásában elkezdett gondolatmenetet. Láttuk, hogy a t elemmel való φ_t konjugálás az invertálás az $N = \langle f \rangle$ normálosztón. A t^3-nel való konjugálás a φ_t^3 lesz (a 4.8.17. Gyakorlat szerint), vagyis az invertálás (kompozícióra vett) köbe, ami szintén az

invertálás, hiszen az invertálás az N csoportnak másodrendű automorfizmusa. A t elemnek viszont a köbe az egységelem, és így a vele való konjugálás az identitás. Az jött tehát ki, hogy az N-en az invertálás az identitással egyenlő, vagyis $f = f^{-1}$. Innen $f^3 = 1$ miatt tényleg $f = 1$ adódik.

Térjünk most vissza az imént vizsgált

$$f^4 = t^4 = 1\,, \qquad f^2 = t^2\,, \qquad ft = tf^{-1}\,.$$

feltételrendszerhez. Ha azt akarjuk bizonyítani, hogy a kapott nyolc elem között már nincs összeesés, akkor elvileg megtehetnénk, hogy felírjuk a szorzástáblát, és ellenőrizzük az asszociativitást. Ez óriási munka lenne, és gyorsabban is célt érhetünk, ha találunk egy olyan nyolcelemű csoportot, ami ezeket az összefüggéseket teljesíti. Ilyen a kvaterniócsoport, ahol $f = i$ és $t = j$ megfelelő lesz. Az összefüggéseinket kielégítő többi csoport pedig a kvaterniócsoport homomorf képe.

Bárhogyan is írunk fel generátorokat és összefüggéseket, az egyelemű csoport mindig kielégíti őket. Általában igen nehéz, sőt sokszor megoldhatatlan feladat adott összefüggések esetében megállapítani, hogy melyik az a legnagyobb csoport, ami ezeket kielégíti. Erről részletesebben a szakasz végén mesélünk majd. Most belátjuk, hogy ez a legnagyobb csoport mindig létezik.

Fogalmazzuk meg pontosan, hogy mit is értünk „generátorelemek közötti összefüggés" alatt. Egy ilyen összefüggés, például az $ft = tf^{-1}$, valójában két „szó" egyenlősége, amelyek „betűi" a generátorelemekből és inverzeikből kerülnek ki. Tehát itt a szabad csoport elemeiről van szó.

4.9.12. Definíció. Tegyük fel, hogy adottak az $x_1, \ldots, x_n$ úgynevezett „generátorok", és az $u_1 = v_1, \ldots, u_k = v_k$ úgynevezett „(definiáló) relációk", ahol $u_1, v_1, \ldots, u_k, v_k$ az $X = \{x_1, \ldots, x_n\}$ halmaz által generált szabad csoport elemei (vagyis az x_i és x_i^{-1} „betűkből" képzett „szavak"). Azt mondjuk, hogy egy G csoport $g_1, \ldots, g_n$ generátorrendszere teljesíti ezeket a relációkat, ha az u_i és v_i szavakban x_i helyébe mindenütt g_i-t írva mindegyik $u_i = v_i$ „reláció" a G csoportban egyenlőséggé válik.

Az előző definíció a könnyebb érthetőség kedvéért szemléletes, fogalmazzuk meg precízen is. Megjegyezzük, hogy mind a generátorok, mind a relációk száma végtelen is lehet. Adott tehát egy X halmaz által generált F szabad csoport, és egy $u = v$ reláció ($u, v \in F$). Ha G tetszőleges csoport, amelyben X minden elemének megfelel egy elem, akkor ezt egy $\varphi : X \to G$ függvénnyel adhatjuk meg. Tudjuk, hogy ez egyértelműen kiterjeszthető egy $\varphi : F \to G$ homomorfizmussá. Az, hogy az $u = v$ reláció G ezen elemeire teljesül, precízen úgy fogalmazható, hogy $\varphi(u) = \varphi(v)$.

4.9.13. Tétel. *Tegyük fel, hogy tetszőlegesen adottak x_i generátorok, és $u_j = v_j$ definiáló relációk. Ekkor létezik egy olyan G csoport, amely a homomorf kép értelmében a legnagyobb az e relációkat teljesítő csoportok között. Vagyis G alkalmas g_i generátorrendszere teljesíti az adott relációkat, és ha egy H csoport egy h_i generátorrendszere is teljesíti ezeket a relációkat, akkor van olyan $\alpha : G \to H$ szürjektív homomorfizmus, amelyre $\alpha(g_i) = h_i$ minden i-re. A G csoport izomorfia erejéig egyértelműen meghatározott.*

Bizonyítás. Jelölje X az x_i generátorok halmazát, és F az $F(X)$ szabad csoportot. Tekintsük az $u_j^{-1}v_j$ elemeket F-ben, ahol $u_j = v_j$ befutja az összes relációt, és legyen N a legszűkebb normálosztója F-nek, amely ezeket az elemeket tartalmazza (4.7.22. Gyakorlat). Megmutatjuk, hogy a $G = F/N$ és $g_i = x_iN$ választás kielégíti a feltételeket.

Jelölje $\varphi : F \to G$ a természetes homomorfizmust, amelyre tehát $\varphi(w) = wN$. Ekkor $\varphi(x_i) = x_iN = g_i$, továbbá $u_j^{-1}v_j \in N$ miatt $u_jN = v_jN$, vagyis $\varphi(u_j) = \varphi(v_j)$. Ez azt jelenti, hogy a G csoport g_i elemei teljesítik az $u_j = v_j$ relációkat.

Legyen most H egy csoport, amelynek a h_i generátorrendszere szintén kielégíti az adott relációkat. Tekintsük azt a $\psi : F \to H$ homomorfizmust, amely mindegyik x_i-t h_i-be viszi. Mivel a h_i elemek teljesítik a relációkat, $\psi(u_j) = \psi(v_j)$ minden j-re. Emiatt a ψ leképezés M magja tartalmazza az $u_j^{-1}v_j$ elemeket. De N a legszűkebb normálosztó, ami ezeket az elemeket tartalmazza, és így $N \subseteq M$. A 4.5.26. Gyakorlat szerint tehát van olyan $\alpha : G \to H$ homomorfizmus, amelyre $\psi = \alpha \circ \varphi$. Erre

$$\alpha(g_i) = \alpha(x_iN) = \alpha\varphi(x_i) = \psi(x_i) = h_i\,.$$

Innen az is látszik, hogy α szürjektív (mert generátorrendszert generátorrendszerbe visz). A G csoport tehát megfelel a feltételeknek.

Végül tegyük fel, hogy egy másik, K csoport alkalmas k_i generátorrendszere is teljesíti a tétel feltételeit. Ekkor a már bizonyított állítás miatt létezik olyan $\alpha : G \to K$ homomorfizmus, melyre $\alpha(g_i) = k_i$ minden i-re. Mivel K is teljesíti a tétel feltételeit, G pedig az adott relációkat, létezik egy olyan $\beta : K \to G$ homomorfizmus is, amelyre $\beta(k_i) = g_i$ minden i-re. Ez a két homomorfizmus egymás inverze a két generátorrendszeren, és ezért egymás inverzei a G és a H csoportokon is (ezt ugyanaz a gondolatmenet bizonyítja, mint amit a 4.9.2. Tétel bizonyításának legelején használtunk). Ezzel a tételt beláttuk. □

4.9.14. Definíció. Az előző tételben meghatározott G csoportot a következőképpen jelöljük:

$$\langle \ldots, x_i, \ldots \mid \ldots, u_j = v_j, \ldots \rangle\,.$$

Azt is mondjuk, hogy a G csoportot az x_i generátorok és az $u_j = v_j$ *definiáló relációk* határozzák meg.

Az eddig szerepelt három konkrét számolás eredménye tehát az új jelöléssel a következőképpen írható:

4.9.15. Példa. Az n-edfokú diédercsoport az

$$\langle f, t \mid f^n = t^2 = 1,\ ft = tf^{-1} \rangle \cong D_n\,;$$

a nyolcelemű kvaterniócsoport az

$$\langle f, t \mid f^4 = t^4 = 1,\ f^2 = t^2,\ ft = tf^{-1} \rangle \cong Q\,;$$

a harmadrendű ciklikus csoport az

$$\langle f, t \mid f^3 = t^3 = 1,\ ft = tf^{-1} \rangle \cong \mathbb{Z}_3^+$$

definiáló relációkkal adható meg.

Természetesen a harmadrendű ciklikus csoportot egyszerűbb az $\langle f \mid f^3 = 1 \rangle$ definiáló relációval megadni.

4.9.16. Következmény [Dyck-tétel]. *Ha egy definiáló relációkkal megadott csoporthoz további relációkat veszünk hozzá, akkor az eredeti csoportnak egy homomorf képét kapjuk.*

Bizonyítás. Ha új relációkat veszünk be, akkor a régi relációk továbbra is fennállnak, tehát egy olyan csoportot kapunk, ami az adott relációkat teljesíti. Az előző tétel szerint ez homomorf képe az eredeti csoportnak. □

A szakasz hátralévő részében azt érzékeltetjük, hogy egy definiáló relációkkal megadott csoport elemeinek (vagy akár csak a rendjének) kiszámítása mennyire nehéz feladat. Természetes kérdés, hogy mit mondhatunk azokról a csoportokról, melyekben minden elem N-edik hatványa az egységelem.

4.9.17. Definíció. Jelölje $B(k, N)$ azt a csoportot, amelynek k generátora van, a definiáló relációi pedig $w^N = 1$, ahol w befutja az összes lehetséges szót. Ezeket a csoportokat *Burnside-csoportoknak* hívjuk.

A $B(n, k)$ Burnside-csoport tehát a (homomorf értelemben) legnagyobb olyan k elemmel generálható csoport, ahol minden elem rendje N-nek osztója. Ezeknek a csoportoknak annyira nem ismerjük a szerkezetét, hogy még az is megoldatlan probléma, melyek végesek közülük.

4.9.18. Feladat. Mutassuk meg, hogy $B(k, 2) \cong (\mathbb{Z}_2^+)^k$.

4.9.19. Feladat. Bizonyítsuk be, hogy $B(k, 3)$ véges csoport.

A $B(k, 4)$ és a $B(k, 6)$ csoportok is végesek. Híres megoldatlan probléma, hogy $B(2, 5)$ véges csoport-e. A 4.10.10. Gyakorlatban fogunk példát látni olyan 125 elemű csoportra, amely két elemmel generálható, minden elemének az ötödik hatványa az egységelem, de nem kommutatív. Ez tehát homomorf képe $B(2, 5)$-nek, így a $B(2, 5)$ csoport sem kommutatív, és legalább 125 eleme van.

Ugyanakkor Novikov és Adjan bonyolult és hosszú bizonyítással megmutatta, hogy ha N páratlan és legalább 665, akkor már $B(2, N)$ is végtelen. Olsanszkij pedig minden 10^{75}-nél nagyobb p prímszámra olyan végtelen csoportot (úgynevezett *Tarski-monstrumot*) konstruált, amelynek a triviális részcsoportokon kívül csakis p rendű részcsoportjai vannak. Hogy ez mennyire furcsa csoport, azt igazán a p-csoportokról szóló fejezetben értjük majd meg.

Mindenesetre egy Tarski-monstrum erős ellenpélda arra a korábbi sejtésre, hogy egy végtelen csoportnak mindig van végtelen valódi részcsoportja.

Ahhoz, hogy az ilyen problémákon gondolkozni tudjunk, le kellene tudni írni egy definiáló relációkkal megadott csoport elemeit. Ez azt jelenti, hogy a generátorok segítségével felírt bármely két szóról gyorsan el kellene tudni döntenünk, hogy az adott relációk segítségével egymásba alakíthatóak-e, vagy sem. Ahelyett, hogy minden szópár esetében külön trükköt keresgélnénk, jó lenne írni erre egy számítógépes programot. Döbbenetes felfedezés, hogy ***ilyen program nem írható***! Sőt nemcsak általában nincs olyan program, ami beolvassa a relációkat, és utána tetszőleges általunk megadott szópárról eldönti, hogy egymásba alakíthatóak-e. Meg lehet adni egy konkrét csoportot, amelyben ez a szóprobléma nem oldható meg. Egy híres ilyen példát mutatunk a B.2.1. Tételben. A csoportnak tíz generátora van $(a, b, c, d, e, p, q, r, t, k)$, és 27 relációval adtuk meg.

Mit jelent az, hogy a szóprobléma erre a konkrét csoportra nem oldható meg? Valaki hoz két szót (például $pacqar$ és $rpcaqa$), és megkérdezi, hogy ezek egymásba alakíthatóak-e. A világ matematikusai összeülnek, és egyiküknek sikerül megoldania a problémát: megadja az átalakítást. Ezután jön másvalaki két újabb szóval (mondjuk p^9a és ap). Egy másik matematikus idővel felfedezi azt a trükköt, ami mutatja, hogy ezek nem alakíthatók egymásba (például megmutatja, hogy a $\mathbb{Z}_9^+$ csoport alkalmas elemei teljesítik mind a 27 relációt, és az p^9a és az ap szavak képe mégis különböző lesz). De ha valaki egy harmadik szópárral rukkol elő, akkor jó eséllyel megint újra kell kezdeni a gondolkodást, soha nem lesz olyan ötlet, ami az összes szópárt egyszerre elintézi. (A kép azért nem teljesen fekete: vannak híres eljárások, például a Knuth-Bendix algoritmus, amik intelligensen keresnek, és sok szópár esetében sikeresen eldöntik a problémát.)

Annak a precíz bizonyításához, hogy ilyen program nem létezik, elvileg az összes lehetséges (végtelen sok) programot át kellene tudnunk tekinteni. Ehhez pontosan meg kell fogalmazni azt, hogy mit is értünk programon, ami már a matematikai logikához tartozó kérdés.

Gyakorlatok, feladatok

4.9.20. Feladat. Az alább felsorolt, definiáló relációkkal megadott csoportoknak határozzuk meg a rendjeit, és döntsük el, izomorfak-e valamelyik korábbról már ismert csoporttal.

(1) $\langle a \mid a^2 = 1\rangle$.
(2) $\langle a \mid a^3 = 1\rangle$.
(3) $\langle a \mid a^5 = 1,\ a^7 = 1\rangle$.
(4) $\langle a, b \mid a^2 = 1,\ b^2 = 1,\ ab = ba\rangle$.
(5) $\langle a, b \mid a^2 = 1,\ b^3 = 1,\ ab = ba\rangle$.
(6) $\langle a, b \mid a^2 = 1,\ b^7 = 1,\ aba^{-1} = b^{-1}\rangle$.
(7) $\langle a, b \mid a^2 = 1,\ b^7 = 1,\ aba^{-1} = b^2\rangle$.
(8) $\langle a, b \mid a^3 = 1,\ b^7 = 1,\ aba^{-1} = b^2\rangle$.
(9) $\langle a, b \mid a^6 = 1,\ b^2 = a^3,\ bab^{-1} = a^{-1}\rangle$.
(10) $\langle a, b \mid a^2 = 1,\ b^2 = 1,\ (ab)^3 = 1\rangle$.
(11) $\langle a, b \mid a^2 = 1,\ b^2 = 1,\ (ab)^n = 1\rangle$ (ahol $n \geq 3$).
(12) $\langle a, b \mid a^3 = b^2 = (ab)^3 = 1\rangle$.
(13) $\langle a, b \mid a^3 = b^2 = (ab)^4 = 1\rangle$.

(14) $\langle a, b, c \mid a^2 = b^2 = c^3 = 1,\ ab = ba,\ cac^{-1} = b\rangle$.

4.9.21. Feladat. Bizonyítsuk be, hogy ha F szabad csoport, akkor bárhogy is veszünk egy $\alpha : G \to H$ szürjektív csoport-homomorfizmust, az F csoport minden H-ba menő φ homomorfizmusa „keresztülvezethető" az α leképezésen, azaz van olyan $\psi : F \to G$ homomorfizmus, hogy $\varphi = \alpha \circ \psi$.

4.9.22. Feladat. Nevezzük egy szabad csoport egy elemét nullösszegűnek, ha bármelyik generátort is vesszük, azoknak a kitevőknek az összege, amin ez a generátor ebben a szóban szerepel, nullával egyenlő. (Például $x^2y^{-3}x^{-1}zx^{-1}y^2z^{-1}y$ nullösszegű szó, mert az x kitevőire $2-1-1=0$, az y kitevőire $-3+2+1=0$, a z kitevőire $1-1=0$.) Igazoljuk, hogy a nullösszegű szavak pontosan F kommutátor-részcsoportjának elemei.

4.10. Prímhatványrendű csoportok, Sylow tételei

Ha egy csoport rendje prímhatvány, akkor a szerkezete sokkal szebb, mint az általános csoportoké. Ugyanakkor Sylow tételei szerint minden csoport felépítésében alapvető szerepet játszanak a prímhatványrendű csoportok. Ezért e csoportok vizsgálata külön figyelmet érdemel. A szakasz elolvasása előtt érdemes átismételni a konjugált osztályokról és a centrumról tanultakat.

4.10.1. Definíció. Legyen p prímszám. Azt mondjuk, hogy a G véges csoport *p-csoport*, ha G rendje p-nek hatványa. Az egyelemű csoportot minden p-re p-csoportnak tekintjük.

Amikor végtelen csoportokat is vizsgálnak, akkor a fenti definíció nem alkalmazható. Helyette azt szokás föltenni, hogy a csoport minden elemének a rendje p-hatvány. Lagrange tétele miatt egy p-hatvány rendű csoport minden elemének a rendje p-hatvány. Megfordítva, ebben a szakaszban belátjuk majd, hogy ha egy véges csoport minden elemének rendje p-hatvány, akkor a csoport rendje szintén p-nek hatványa. Így véges csoport esetében mindegy lesz, hogy melyik definíciót alkalmazzuk. Mi csak véges p-csoportokat vizsgálunk, ezért a fenti definícióval dolgozunk.

4.10.2. Tétel. *Legyen p prímszám. Ha P (véges) nem egyelemű p-csoport, akkor $Z(P)$ sem egyelemű.*

Bizonyítás. Bontsuk fel P-t konjugált osztályainak uniójára. Vonjuk egybe az egyelemű osztályokat, ezek P centrumát alkotják. Ha $K_1, \ldots, K_m$ a többi konjugált osztály, akkor tehát

$$|P| = |Z(P)| + |K_1| + \ldots + |K_m|$$

(ezt *P osztályegyenletének* nevezzük).

Tudjuk, hogy K_i elemszáma (ami tetszőleges eleme centralizátorának az indexe) osztója P rendjének, ami a p prímszámnak hatványa. Ezért K_i elemszáma is p-hatvány. Mivel $|K_i| > 1$, azt kapjuk, hogy $|K_i|$ osztható p-vel. De $|P|$ is osztható p-vel, hiszen P nem az

egyelemű csoport. Az osztályegyenletből az adódik, hogy $|Z(P)|$ is osztható p-vel. Ekkor pedig $Z(P)$ nem lehet egyelemű. □

4.10.3. Következmény. *Minden prímnégyzet rendű csoport kommutatív.*

Bizonyítás. Legyen P egy p^2 rendű csoport, ahol p prím. Ekkor $Z(P)$ elemszáma az előző tétel és Lagrange tétele szerint vagy p, vagy p^2. Az utóbbi esetben készen vagyunk, hiszen $Z(P)$ kommutatív, az előbbit kell kizárnunk. Legyen $1 \neq g \in Z(P)$, és $h \in G$, $h \notin Z(P)$. Ekkor $gh = hg$, hiszen g a centrumban van. Ezért a

$$H = \langle g, h \rangle = \{g^n h^m \,:\, n, m \in \mathbb{Z}\}$$

halmaz egy kommutatív részcsoportja P-nek (4.7.42. Gyakorlat). A H részcsoport tartalmazza $Z(P)$-t (hiszen a prímrendű $Z(P)$-t már g hatványai is kiadják), sőt, a h elem miatt bővebb $Z(P)$-nél. Így H rendje csakis p^2 lehet. Ezért $H = P$, vagyis P Abel. Ekkor azonban $Z(P) = P$, azaz a centrum mégsem p rendű. Ez az ellentmondás bizonyítja az állítást. □

Ha G egy p^2 rendű csoport, akkor tehát kommutatív, és így a véges Abel-csoportok alaptétele miatt kétféle lehet: $\mathbb{Z}^+_{p^2}$ és $(\mathbb{Z}^+_p)^2$. Az előző bizonyítás fő gondolatát érdemes külön is megfogalmazni.

4.10.4. Gyakorlat. Igazoljuk, hogy ha egy G csoportban $G/Z(G)$ ciklikus, akkor G Abel (és így $G/Z(G)$ az egyelemű csoport).

4.10.5. Következmény. *Ha p prím, akkor a véges egyszerű p-csoportok éppen a prímrendű csoportok.*

Bizonyítás. Legyen P egy egyszerű p-csoport. Ekkor a 4.10.2. Tétel miatt $|Z(P)| > 1$. Mivel $Z(P) \triangleleft P$, és P egyszerű, ezért $Z(P) = P$, vagyis P kommutatív. A 4.7.4. Következmény miatt így P prímrendű ciklikus csoport. □

Megmutatjuk még, hogy egy p-csoportnak mindig „nagyon sok” nagy részcsoportja van (ellentétben a véges egyszerű csoportokkal, amelyeknek bizonyos értelemben „nagyon kevés” nagy részcsoportja is lehet, vö. 4.11.8. Tétel).

4.10.6. Definíció. Egy G csoport egy H valódi részcsoportját *maximális részcsoportnak* nevezzük, ha nincs G-nek H-t tartalmazó, valódi részcsoportja (a H-n kívül).

4.10.7. Gyakorlat. Mutassuk meg, hogy minden prímindexű részcsoport maximális.

4.10.8. Tétel. *Legyen p prím, és P egy véges p-csoport. Ekkor P minden maximális részcsoportja normálosztó, és az indexe p.*

Bizonyítás. Indukcióval bizonyítunk P rendje szerint. Ha P az egyelemű csoport, akkor egyáltalán nincs maximális részcsoportja, és az állítás ezért igaz.

Tegyük fel, hogy a P rendjénél kisebb rendű csoportokra már igaz az állítás, és legyen M maximális részcsoport P-ben. Tudjuk, hogy $Z(P)$ normálosztó P-ben, ami nemcsak az egységelemből áll. Két esetet különböztetünk meg.

Az első eset az, hogy $Z(P)$ nem része M-nek. Tekintsük az M részcsoport $N_G(M)$ normalizátorát (4.7.29. Definíció). Ez tartalmazza $Z(P)$-t hiszen $Z(P)$ minden eleme felcserélhető M elemeivel. Tartalmazza továbbá M-et is, és így M-nél bővebb. Ezért ez a normalizátor M maximalitása miatt az egész G, vagyis M normálosztó G-ben.

A második eset az, ha $Z(P) \subseteq G$. Ebben az esetben a 4.5.19. Tételt alkalmazzuk a $P/Z(P)$ faktorcsoportra. Tudjuk, hogy ennek részcsoportjai kölcsönösen egyértelmű megfeleltetésben állnak a P csoport $Z(P)$-t tartalmazó részcsoportjaival, és normálosztónak normálosztó felel meg. Ezért $M/Z(P)$ maximális részcsoportja $P/Z(P)$-nek. Az indukciós feltevést $P/Z(P)$-re alkalmazva azt kapjuk, hogy $M/Z(P)$ normálosztó $P/Z(P)$-ben. Ezért a neki megfelelő M is normálosztó lesz P-ben.

Beláttuk tehát, hogy $M \lhd P$. Ismét a 4.5.19. Tétel miatt az M/P csoportnak csak triviális részcsoportjai vannak, és így prímrendű ciklikus csoport (4.4.30. Következmény). Ezért $|G : M| = p$. □

Az eddig bizonyított tételek alapján valamit mondhatunk a p^3 rendű csoportok szerkezetéről is. Legyen $|P| = p^3$. Ha P kommutatív, akkor a véges Abel-csoportok alaptétele miatt P háromféle lehet: $(\mathbb{Z}_p^+)^3$, $(\mathbb{Z}_{p^2}^+)^2 \times \mathbb{Z}_p^+$ és $\mathbb{Z}_{p^3}^+$. Tegyük fel, hogy P nem kommutatív. Ekkor a 4.10.4. Gyakorlat miatt $P/Z(P)$ nem lehet ciklikus. Speciálisan nem lehet p rendű. Nem lehet p^3 rendű sem, mert akkor $Z(P)$ egyelemű volna. Ezért $P/Z(P)$ rendje p^2, és nem ciklikus. Ilyen csoport a most bizonyítottak miatt csak egyetlen van: $(\mathbb{Z}_p^+)^2$. A P csoport P' kommutátor-részcsoportja $Z(P)$-vel egyenlő. Valóban, $P/Z(P)$ kommutatív, ezért $P' \subseteq Z(P)$ (a 4.7.25. Állítás miatt). Másfelől $P' < Z(P)$ sem lehetséges, mert akkor P' az egyelemű csoport lenne, ahonnan az következne, hogy G kommutatív.

A P szerkezetét tovább analizálva pontosan meg tudnánk határozni izomorfia erejéig. Ha $p = 2$, akkor a Q kvaterniócsoport és a D_4 diédercsoport is eleget tesz a feltételeknek, és meg lehet mutatni, hogy izomorfia erejéig nincs más nyolcelemű nemkommutatív csoport. Ha $p > 2$, akkor is két nemkommutatív nyolcelemű csoport van, de ezek másmilyenek, mint a $p = 2$ esetben. A legfontosabb különbség, hogy az egyikükben nincsen p^2 rendű elem. Ezt a legegyszerűbben mátrixok segítségével lehet megadni.

4.10.9. Definíció. Legyen T test, és álljon G azokból az $n \times n$-es mátrixokból, amelyek főátlója alatt csupa nulla, a főátlójában pedig csupa nem nulla elem áll. E mátrixok csoportját a szorzásra $\mathrm{T}(n, T)$-vel fogjuk jelölni. A $\mathrm{T}(n, T)$ azon elemeinek halmazát, amelyben a főátlóban végig 1-esek állnak, $\mathrm{U}(n, T)$ jelöli.

Nyilvánvaló, hogy ha T véges test, akkor $\mathrm{U}(n, T)$ elemszáma $|T|^{n(n-1)/2}$, hiszen a főátló fölötti elemek mindegyikét tetszőlegesen választhatjuk T-ből. A $\mathrm{T}(n, T)$ csoportban a főátlóbeli elemeket a nulla kivételével szintén tetszőlegesen választhatjuk, ezért $\mathrm{T}(n, T)$ elemszáma $\mathrm{U}(n, T)$ elemszámának $(|T| - 1)^n$-szerese.

4.10.10. Gyakorlat. Mutassuk meg, hogy ha $p > 2$ prím, akkor az $\mathrm{U}(3, \mathbb{Z}_p)$ csoport egy p^3 rendű, nemkommutatív, két elemmel generálható csoport, melyben minden elem rendje 1 vagy p. Melyik csoportot kapjuk $p = 2$ esetén?

A másik p^3 rendű nemkommutatív csoportot definiáló relációkkal (de igazándiból szemidirekt szorzatként) adjuk meg. Ez a definíció $p = 2$ esetén szintén a D_4 csoportot adja.

4.10.11. Feladat. Legyen p prímszám, és

$$G = \langle a, b \mid a^{p^2} = 1, b^p = 1, bab^{-1} = a^{p+1} \rangle.$$

Mutassuk meg, hogy G nemkommutatív p^3 rendű csoport, amelyben van p^2 rendű elem.

A Lagrange-tétel megfordítása általában nem igaz. Ha G véges csoport, és d osztója G rendjének, akkor nem feltétlenül van G-ben sem d rendű elem, sem d rendű részcsoport. Például az A_5 csoportban nincsen 30 rendű részcsoport, és így 30 rendű elem sem, hiszen minden kettő indexű részcsoport normálosztó (4.7.34. Állítás), márpedig az A_5 egyszerű csoport. Ha azonban d egy p prím hatványa, akkor mindig van d rendű részcsoport, sőt ezek száma kongruens 1-gyel modulo p. Ez Sylow nevezetes tétele, melyet most bebizonyítunk.

4.10.12. Lemma. *Legyenek G és H egyforma rendű véges csoportok, és q egy p prím hatványa, mely osztja ezt a közös rendet. Jelölje n_G, illetve n_H a G, illetve H azon részcsoportjainak számát, melyek rendje q. Ekkor $n_G \equiv n_H (p)$.*

Ez a lemma azért hasznos, mert ha speciálisan H a ciklikus csoport, akkor az n_H értékét ismerjük: a 4.3.21. Állítás szerint $n_H = 1$ (tetszőleges q esetén). Ezért a következő állítást kapjuk:

4.10.13. Tétel. *Ha a p prím egy q hatványa osztja a G véges csoport rendjét, akkor van G-ben q rendű részcsoport, sőt ezek száma kongruens 1-gyel modulo p.*

Természetesen ha tudjuk, hogy n_G kongruens 1-gyel modulo p, akkor n_G nem lehet nulla, tehát nem kell külön bebizonyítani, hogy van q rendű részcsoport.

Bizonyítás. A 4.10.12. Lemmát kell belátni. Jelölje X a G összes q-elemű részhalmazaiból álló halmazt. Hasson G az X-en balszorzással:

$$g * A = gA \quad (= \{ga : a \in A\})$$

(itt $g \in G$, $A \in X$). A „pontok” tehát halmazok, és könnyen ellenőrizhetjük, hogy ez tényleg hatás.

Először vizsgáljuk azokat az orbitokat, amelyek valamelyik eleme egy K részcsoport (még nem tudjuk, van-e ilyen orbit). Ekkor az orbit többi eleme gK alakú, azaz ennek az orbitnak az elemei éppen a K szerinti bal mellékosztályok. Ezért ennek az orbitnak az elemszáma $|G : K| = |G|/q$, és az orbitban az egyetlen részcsoport a K, vagyis az ilyen orbitok száma n_G.

Most tegyük fel, hogy az $A = \{a_1, \ldots, a_q\} \in X$ elem orbitjának egyetlen eleme sem részcsoport. Tekintsük az A „pont” G_A stabilizátorát. Ez azokból a $g \in G$ elemekből áll, melyekre $gA = A$. Ezért

$$A = G_A A = G_A a_1 \cup \ldots \cup G_A a_q \,,$$

vagyis az A halmaz G_A szerinti jobb mellékosztályok egyesítése. Jelölje az ebben az unióban szereplő *különböző* mellékosztályok számát m_A, akkor tehát $q = |A| = m_A \cdot |G_A|$. Ha $m_A = 1$ lenne, azaz ha $A = G_A a$ alkalmas $a \in A$ esetén, akkor az $a^{-1}A = a^{-1}G_A a$ halmaz benne van A orbitjában, és részcsoport. Ez ellentmondás, tehát $m_A > 1$, és így $m_A \mid q$ miatt m_A osztható p-vel. Az A orbitjának elemszáma pedig

$$|G(A)| = |G : G_A| = \frac{|G|}{|G_A|} = \frac{|G| m_A}{q} .$$

Tudjuk, hogy az orbitok elemszámának összege kiadja az alaphalmaz, azaz X elemszámát. Jelöljük a $|G|/q$ számot t-vel, akkor tehát minden részcsoportot tartalmazó orbit elemszáma t, és ezeknek az összhossza $n_G t$. A többi orbit hossza $t m_A$ alakú, ahol m_A egy p-vel osztható szám. Ezért

$$|X| = t n_G + t p x_G ,$$

ahol x_G valamilyen egész szám (ami a G csoporttól függ).

Ugyanez a gondolatmenet a H csoportra is elmondható:

$$|X| = t n_H + t p x_H ,$$

ahol x_H valamilyen egész szám. A két egyenlőséget összevetve és t-vel osztva éppen a 4.10.12. Lemma állítása adódik. □

4.10.14. Definíció. Legyen G véges csoport, és a rendjének a prímtényezős felbontása $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. A $p_i^{\alpha_i}$ rendű részcsoportokat a G csoport *p_i-Sylow részcsoportjainak* nevezzük. Egy részcsoport tehát akkor p-Sylow részcsoport, ha rendje p-hatvány, indexe pedig p-vel nem osztható.

4.10.15. Lemma. *Legyen G véges csoport, $Q \leq G$ egy p-hatványrendű részcsoport, P pedig egy p-Sylow részcsoport. Ekkor van olyan $g \in G$, melyre $Q \leq gPg^{-1}$.*

Bizonyítás. Legyen X a P részcsoport G-beli konjugáltjainak a halmaza:

$$X = \{gPg^{-1} \,:\, g \in G\} .$$

A 4.7.30. Következmény miatt az X halmaz elemszáma $|G : N_G(P)|$. Ez a szám osztója $|G : P|$-nek (hiszen $|G : P| = |G : N_G(P)| \cdot |N_G(P) : P|$). Mivel P egy p-Sylow részcsoport, $|G : P|$ nem osztható p-vel. Ezért X elemszáma sem osztható p-vel.

Hasson a Q részcsoport az X halmazon konjugálással, azaz $h \in Q$, $P' \in X$ esetén legyen

$$h * P' = hP'h^{-1} .$$

Mivel Q rendje p-hatvány, minden stabilizátor indexe (azaz minden orbit elemszáma) szintén p-hatvány, tehát vagy p-vel osztható, vagy 1. De $|X|$ nem osztható p-vel, így van olyan orbit, amelynek elemszáma 1, azaz amelynek a stabilizátora a teljes Q. Ha ennek az orbitnak az egyetlen eleme $P' = gPg^{-1}$, akkor tehát azt kaptuk, hogy bármely $h \in Q$ esetén $hP'h^{-1} = P'$, azaz $Q \leq N_G(P')$.

Meg szeretnénk mutatni, hogy valójában $Q \leq P'$ (ezzel készen is lennénk). Az $N_G(P')$ csoportban P' normálosztó, Q részcsoport. Ezért az első izomorfizmus-tétel szerint $P'Q$ is részcsoport, és rendje $|P'||Q|/|P' \cap Q|$. Ez p-hatvány, és így legfeljebb $|P'|$ lehet, hiszen P' egy p-Sylow részcsoport. Tehát $P' = P'Q \supseteq Q$. □

Foglaljuk össze az eddig bizonyítottakat.

4.10.16. Tétel [Sylow tételei]. *Legyen G véges csoport, és p a G rendjének tetszőleges prímosztója. Ekkor igazak a következő állítások.*

(1) *Van G-ben p-Sylow részcsoport.*
(2) *G minden p-hatványrendű részcsoportja része G egy p-Sylow részcsoportjának.*
(3) *Bármely két p-Sylow részcsoport konjugált G-ben.*
(4) *Ha q egy G rendjét osztó p-hatvány, akkor a q-rendű G-beli részcsoportok száma kongruens 1-gyel modulo p.*
(5) *A p-Sylow részcsoportok száma osztója $|G : P|$-nek.*

Bizonyítás. A (4) állítás éppen a 4.10.13. Tétel, amiből (1) is következik. A (2) és (3) állítások az előző lemmából adódnak, hiszen p-Sylow részcsoport minden konjugáltja is p-Sylow részcsoport. Végül (5) következik (3)-ból, hiszen tudjuk, hogy egy részcsoport konjugáltjainak száma a normalizátorának indexe, márpedig ha P egy p-Sylow, akkor $|N_G(P) : P|$ osztója $|G : P|$-nek. □

4.10.17. Következmény [Cauchy-tétel]. *Ha a G véges csoport rendje osztható a p prímszámmal, akkor G-ben van p rendű elem.*

Bizonyítás. A Sylow-tételek miatt van p rendű részcsoport, amit csak p rendű elem generálhat. □

A most bizonyított tétel feltételei harmonikusan együttműködnek. Mintaként megmutatjuk, hogy nincs 100 rendű egyszerű csoport. Valóban, legyen G egy 100 rendű csoport, és jelölje n az 5-Sylow részcsoportok számát G-ben. Ekkor az előző tétel szerint $n \equiv 1$ (5), másrészt pedig n osztója minden 5-Sylow indexének. Az 5-Sylowok rendje 25, és így indexük $100/25 = 4$. Ennek osztói 1, 2, 4, és ezek közül csak az 1 kongruens 1-gyel modulo 5. Ezért G-ben egyetlen 5-Sylow van. Ez tehát az összes konjugáltjaival megegyezik (mert egy 5-Sylow részcsoport minden konjugáltja nyilván 5-Sylow részcsoport), azaz normálosztó. Vagyis egy 100 rendű csoportban mindig van 25 rendű normálosztó, és ezért egy ilyen csoport nem lehet egyszerű.

4.10.18. Következmény. *Legyenek $p > q$ prímek, és G egy pq rendű csoport. Ekkor G-ben a p-Sylow részcsoport normálosztó. Ha $p-1$ nem osztható q-val, akkor G ciklikus.*

Bizonyítás. A p-Sylowok száma osztója q-nak, és így csak 1 vagy q lehet, továbbá kongruens 1-gyel modulo p. De q nem kongruens 1-gyel modulo p, hiszen $q < p$. Ezért a p-Sylowok száma 1, és így ez az egyetlen p-Sylow részcsoport normálosztó. Ha $p-1$ nem osztható q-val, akkor ugyanez a gondolatmenet a q-Sylowokra is elmondható. Tehát

ilyenkor az egyetlen q-Sylow is normálosztó. Jelölje ezeket P, illetve Q, ekkor $P \cap Q$ egyelemű (hiszen rendje osztója a p-nek is és a q-nak is). Ezért a 4.8.12. Tétel miatt a PQ részcsoport izomorf $P \times Q$-val, azaz a $\mathbb{Z}_p^+ \times \mathbb{Z}_q^+ \cong \mathbb{Z}_{pq}^+$ csoporttal (lásd 4.8.8. Következmény). Mivel G rendje pq, a PQ részcsoport az egész G, tehát G ciklikus. □

Ha $p \equiv 1\ (q)$, akkor pq rendű csoportból összesen két darab van, a ciklikus, és egy nemkommutatív (amely $q = 2$ esetén a D_p diédercsoport). Valóban, $\mathbb{Z}_p^+$ automorfizmuscsoportja a 4.7.43. Feladat szerint $\mathbb{Z}_p^\times$, aminek a rendje $p - 1$, és feltettük, hogy ez q-val osztható. Ezért (például a Sylow-tétel miatt, vagy mert ez ciklikus csoport) van q rendű eleme. Így a 4.8.32. Feladat (2) pontjának általánosításaként elkészíthető egy nemkommutatív $\mathbb{Z}_p^+ \rtimes \mathbb{Z}_q^+$ szemidirekt szorzat. Az, hogy csak egy ilyen csoport van, a 4.10.35. Feladat állítása.

Ezzel (és a korábban már elhangzott eredményekkel) áttekintettük az összes olyan véges csoportokat, melyek rendje legfeljebb 15, a 12 rendűek kivételével. Meg lehet mutatni, hogy három nemkommutatív 12 rendű csoport van, az A_4 és a $D_6 \cong S_3 \times \mathbb{Z}_2^+$ mellett még az, ami a 4.8.32. Feladat (6) pontjában szerepel. A legfeljebb 30 rendű csoportokat a 757. oldalon foglaltuk össze.

Gyakorlatok, feladatok

4.10.19. Gyakorlat. Mutassuk meg, hogy ha P véges p-csoport valamilyen p prímre, és N nemtriviális normálosztó P-ben, akkor $|N \cap Z(P)| > 1$.

4.10.20. Gyakorlat. Mutassuk meg, hogy ha H valódi részcsoportja egy prímhatványrendű P csoportnak, akkor van olyan H-t valódi módon tartalmazó részcsoportja P-nek, amelyben H normálosztó.

4.10.21. Gyakorlat. Legyen P egy p-Sylow G-ben, és $N \lhd G$. Igazoljuk, hogy $P \cap N$ egy p-Sylowja N-nek, és $(PN)/N$ egy p-Sylowja G/N-nek.

4.10.22. Gyakorlat. Ha p prím, és a G nemkommutatív csoport rendje p^3, akkor mutassuk meg, hogy G nem bontható fel két valódi részcsoportjának direkt szorzatára.

4.10.23. Gyakorlat. Mutassuk meg, hogy az $\mathrm{U}(n, T)$ csoport normálosztó a $\mathrm{T}(n, T)$ csoportban, és a rá vett faktor a $T^\times$ csoport n tényezős direkt hatványával izomorf.

4.10.24. Feladat. Mely véges csoportoknak van csak egy maximális részcsoportja?

4.10.25. Gyakorlat. Melyik csoporttal izomorf az S_4 csoport 2-Sylow részcsoportja?

4.10.26. Gyakorlat. Tegyük fel, hogy a G csoport rendjében a p prím az első hatványon szerepel. Mutassuk meg, hogy a p-Sylow részcsoportok száma a p rendű elemek számának $p - 1$-ed része.

4.10.27. Gyakorlat. Mutassuk meg, hogy ha egy G csoportban egy Sylow-részcsoport normálosztó, akkor karakterisztikus is.

4.10.28. Feladat. Határozzuk meg az alábbi csoportok Sylow-részcsoportjainak a számát: S_3, S_4, A_5, D_n.

4.10.29. Gyakorlat. Igazoljuk, hogy nincs 200, 204, 260, 56, 616 rendű egyszerű csoport.

4.10.30. Feladat. Igazoljuk, hogy ha p, q, r páronként különböző prímek, akkor nincs pqr rendű egyszerű csoport.

4.10.31. Feladat. Mutassuk meg, hogy ha p és q különböző prímek, akkor nincs p^2q rendű egyszerű csoport.

4.10.32. Feladat. Igazoljuk, hogy ha $p \neq q$ prímek és $\alpha > 0$, akkor nincs $p^\alpha q$ rendű egyszerű csoport.

4.10.33. Feladat [Frattini-elv]. Legyen $N \lhd G$ és P egy p-Sylowja N-nek. Igazoljuk, hogy $G = NN_G(P)$, és hogy $N_G(P)$ tartalmazza G egy p-Sylow részcsoportját.

4.10.34. Feladat. Tegyük fel, hogy a $K \leq G$ részcsoport tartalmazza G egy p-Sylowjának normalizátorát. Mutassuk meg, hogy $N_G(K) = K$, és hogy $|G : K| \equiv 1\ (p)$.

4.10.35. Feladat. Bizonyítsuk be, hogy ha $p \neq q$ prímek, akkor bármely két nemkommutatív pq rendű csoport izomorf.

4.11. Primitív és többszörösen tranzitív csoportok

A 4.7.36. Gyakorlatban megmutattuk, hogy az A_5 alternáló csoport egyszerű. Ebben a szakaszban megismerkedünk néhány alapvető fogalommal a permutációcsoportok elméletéből, majd ezeket felhasználjuk annak bizonyítására, hogy az A_n csoport egyszerű, ha $n \geq 5$ egész szám.

Egy X halmazon ható G permutációcsoportot tranzitívnak neveztünk, ha X bármely elemét X bármely elemébe el lehet vinni G egy alkalmas elemével. Ilyen volt például a kocka szimmetriacsoportjának hatása a kocka csúcsainak a halmazán. Ez azt fejezi ki, hogy a kocka csúcsai egyenrangúak, semelyik sincs kitüntetve a másikhoz képest.

Ennél magasabb szintű szimmetria lenne az, ha a kocka bármely két különböző csúcsát bármely két másik csúcsba át tudnánk vinni egy alkalmas egybevágóság segítségével. Ez már nem teljesül, hiszen ha a kiinduló két csúcs élnyi távolságban volt, akkor ezeket nem lehet átvinni két olyan csúcsba, melyek lapátlónyi (vagy testátlónyi) távolságra vannak egymástól. Ugyanakkor legyen G a sík összes hasonlósági transzformációiból álló csoport. Bármely $P_1 \neq P_2$ és $Q_1 \neq Q_2$ pontokhoz van olyan eleme G-nek, amely P_1-et Q_1-be, P_2-t pedig Q_2-be viszi. Ugyanez ponthármasokra már nem igaz, hiszen ha például $P_1P_2P_3$ egy szabályos háromszög, akkor minden hasonlósági transzformációnál vett képe is az, vagyis a kép nem lehet tetszőleges ponthármas.

4.11.1. Definíció. Legyen G az X halmazon ható permutációcsoport. Azt mondjuk, hogy ez *k-szorosan tranzitív* ($k \geq 1$ egész), ha bármely páronként különböző $x_1, \ldots, x_k \in X$ és szintén páronként különböző $y_1, \ldots, y_k \in X$ pontokhoz van olyan $g \in G$, hogy $g * x_i = y_i$ minden $1 \leq i \leq k$ esetén.

Szokás *szigorú k*-tranzitivitásról is beszélni, ha ez a g elem mindig egyértelműen meghatározott. A szigorú tranzitivitás fogalmát csak akkor fogjuk használni, ha G az S_X részcsoportja.

Általános hatás esetén a hatás magjának elemei az egész X-en identikusan hatnak, és ezek elrontanák az egyértelműséget. Ezért ilyenkor úgy módosítják a szigorú tranzitivitás definícióját, hogy a mag elemeit nem veszik figyelembe, vagyis G helyett a hatás magja szerinti faktorcsoporttal dolgoznak.

Nyilvánvaló, hogy az S_n csoport szigorúan n-tranzitív az $\{1, 2, \ldots, n\}$ halmazon.

4.11.2. Gyakorlat. Igazoljuk, hogy $n \geq 3$ esetén az A_n-csoport szigorúan $n-2$-tranzitív az $\{1, 2, \ldots, n\}$ halmazon.

Szeretnénk kevésbé triviális példát mutatni sokszorosan tranzitív permutációcsoportra. E tulajdonság ellenőrzése a stabilizátorok vizsgálatával lehetséges.

4.11.3. Állítás. *Ha a G csoport k-tranzitívan hat az X halmazon, akkor minden $x \in X$ pont stabilizátora $k-1$-tranzitívan hat az X-ből az x pont kihagyásával kapott $X-\{x\}$ halmazon. Megfordítva, ha G tranzitívan hat az X halmazon, és valamely $x \in X$ pont stabilizátora $k-1$-tranzitív az $X-\{x\}$ halmazon, akkor G hatása az X halmazon k-tranzitív.*

Bizonyítás. Ha G hatása k-tranzitív, és $x \in X$, akkor legyen $x_2, \ldots, x_k$, illetve $y_2, \ldots, y_k$ páronként különböző pontokból álló két pontrendszere az $X-\{x\}$ halmaznak. Mivel G az X-en k-tranzitív, van olyan $g \in G$, ami az $(x, x_1, \ldots, x_k)$ pontrendszert az $(x, y_1, \ldots, y_k)$ pontrendszerbe viszi, azaz amelyre igaz, hogy $g * x = x$ és $g * x_i = y_i$ ha $2 \leq i \leq k$. Ez a g elem benne van x stabilizátorában, és így ez a stabilizátor tényleg $k-1$-tranzitív az $X-\{x\}$ halmazon.

Megfordítva, tegyük fel, hogy G tranzitív az X halmazon, és egy $x \in X$ pont H stabilizátora $k-1$-tranzitív $X-\{x\}$-en. Meg kell mutatnunk, hogy ha $x_1, \ldots, x_k$, illetve $y_1, \ldots, y_k$ páronként különböző pontokból álló két pontrendszer az X halmazon, akkor van olyan $g \in G$ elem, amelyre $g * x_i = y_i$ minden $1 \leq i \leq k$-ra.

A G tranzitivitása miatt van olyan $u \in G$ elem, amelyre $u * x_1 = x$, továbbá olyan $v \in G$ is, amelyre $v * x = y_1$. Az u elem permutációként hat az X halmazon, és ezért

$$u * x_2, \ldots, u * x_k$$

páronként különböző elemei $X-\{x\}$-nek. Ugyanez mondható a

$$v^{-1} * y_2, \ldots, v^{-1} * y_k$$

pontrendszerről is. Mivel az x elem H stabilizátora $k-1$-tranzitív $X-\{x\}$-en, van olyan $h \in H$, melyre

$$h * (u * x_i) = v^{-1} * y_i$$

minden $2 \leq i \leq k$ esetén. Ekkor a $g = vhu$ elem nyilván megfelel a feltételeknek. □

4.11.4. Gyakorlat. Jellemezzük a szigorú tranzitivitást is a stabilizátorok segítségével.

Többszörösen tranzitív csoportra az egyik legfontosabb példa a következő.

4.11.5. Definíció. Legyen T test, $n \geq 1$ egész, és tekintsük a

$$\mathrm{Aff}(n, T) = \{v \mapsto Mv + b \,:\, b \in T^n, M \in \mathrm{GL}(n, T)\}$$

leképezéseket a T^n halmazon (az M tehát tetszőleges, $n \times n$-es invertálható mátrix). Ezek csoportját a kompozícióra az n-dimenziós, T fölötti *affin csoportnak* hívjuk.

Speciálisan az $\mathrm{Aff}(1, T)$ csoport az $x \mapsto ax + b$ leképezésekből áll, ahol $a \neq 0$ és b a T test elemei (vagyis ezek pontosan az elsőfokú polinomokhoz tartozó polinomfüggvények). Megmutatjuk, hogy ez a csoport 2-tranzitív a T halmazon. Már az $x \mapsto x + b$ alakú leképezések mutatják, hogy a csoport tranzitív: ha $u, v \in T$, akkor az $x \mapsto x + (v - u)$ leképezés u-t elviszi v-be. Ezért az előző állítás miatt elegendő megmutatni, hogy a $0 \in T$ elem stabilizátora tranzitív a $T - \{0\}$ halmazon.

Nyilván az $x \mapsto ax + b$ leképezés akkor és csak akkor viszi a nullát önmagába, ha $b = 0$. Ha u és v nem nulla elemei T-nek, akkor az $x \mapsto (vu^{-1})x$ leképezés a nullát nullába, u-t pedig v-be viszi. Így az $\mathrm{Aff}(1, T)$ csoport tényleg 2-tranzitív. Könnyű meggondolni, hogy szigorúan 2-tranzitív csoportot kaptunk.

4.11.6. Gyakorlat. Igazoljuk, hogy az $\mathrm{Aff}(n, T)$ csoport egy $(T^+)^n$-nel izomorf normálosztó, és egy $\mathrm{GL}(n, T)$-vel izomorf részcsoport szemidirekt szorzata.

4.11.7. Gyakorlat. Mutassuk meg, hogy az $\mathrm{Aff}(n, T)$ csoport 2-tranzitív a T^n halmazon. Mikor lesz szigorúan 2-tranzitív? Lehet-e 3-tranzitív, illetve szigorúan 3-tranzitív?

A most vizsgált $\mathrm{Aff}(1, T)$ csoportot 3-tranzitív permutációcsoporttá bővíthetjük a következőképpen. Egészítsük ki a T testet egy ∞ nevű elemmel, és tekintsük az

$$f(x) = \frac{ax + b}{cx + d}$$

úgynevezett *törtlineáris* leképezéseket, ahol $a, b, c, d \in T$, és $ad - bc \neq 0$. Ezeket a leképezéseket az $X = T \cup \{\infty\}$ halmazon értelmezzük úgy, hogy a ∞ szimbólummal a határértékszámításban megszokott módon bánunk. Például ha $c \neq 0$, akkor $f(x)$ határértékét $x \to \infty$ esetén úgy számítanánk ki, hogy x-szel elosztanánk a számlálót és a nevezőt is. Ekkor b/x és d/x nullához tartana, így az eredmény a/c lenne. A T testben ugyan nem létezik általában a határérték fogalma (ez a test például véges is lehet), de azt megtehetjük, hogy

$$\frac{a\infty + b}{c\infty + d}$$

értékét $c \neq 0$ esetén a/c-nek definiáljuk. Hasonlóképpen $x = -d/c$ esetén $f(x)$ értékét ∞-nek célszerű definiálni (a számláló $x = -d/c$-re nem lesz nulla, mert $ad \neq bc$).

Az eseteket végiggondolva láthatjuk, hogy egy permutációcsoportot kaptunk, amit $K(T)$-vel jelölünk (az $ad \neq bc$ feltételre az inverz létezéséhez is szükség van). Ebben a ∞ stabilizátora pontosan az $x \mapsto ax + b$ alakú leképezésekből fog állni (vagyis ahol $c = 0$). Mivel ezek csoportjáról már beláttuk, hogy 2-tranzitív, a $K(T)$ már 3-tranzitív (sőt szigorúan 3-tranzitív) a $T \cup \{\infty\}$ halmazon.

A $K(T)$ csoport a projektív geometriában és a komplex függvénytanban játszik szerepet (úgy is nevezik néha, hogy a projektív egyenes kollineáció-csoportja). A 4.13.11. Gyakorlatban megmutatjuk, hogy hogyan lehet ezt a csoportot mátrixok segítségével származtatni.

A most látott bővítési procedúrát azonban nem folytathatjuk vég nélkül. Ennek illusztrálására két olyan eredményt mutatunk, amelyek bizonyítása nagyon nehéz, mert felhasználja a véges egyszerű csoportok klasszifikációját (osztályozását), amelyről a 4.13. Szakaszban részletesebben is szó lesz.

Az $\mathrm{Aff}(1, \mathbb{Z}_p)$ csoport rendje nyilván $p(p-1)$ (hiszen az $x \mapsto ax + b$ leképezésben az a-t $p-1$-féleképpen, a b-t p-féleképpen választhatjuk). Ez a csoport a $\{0, 1, \ldots, p-1\}$ halmaz permutációiból áll, és így a p-edfokú szimmetrikus csoport egy részcsoportjáról van szó, amelyről láttuk, hogy 2-tranzitív. Az $\mathrm{Aff}(1, \mathbb{Z}_p)$ rendkívül kicsi részcsoport, hiszen az indexe, ami $(p-2)!$, nagyon nagy a rendjéhez képest. Ezért úgy gondolhatnánk, hogy bőségesen lenne hely arra, hogy ehhez a részcsoporthoz még további elemeket hozzávegyünk, abban reménykedve, hogy sokszorosan tranzitív csoportot kapunk. De ezt nem lehet megcsinálni! Akárhogy is veszünk hozzá akár egyetlen új permutációt is, az összes többi permutáció ki fog generálódni.

4.11.8. Tétel. *Legyen $p > 3$ prímszám. Ekkor az $\mathrm{Aff}(1, \mathbb{Z}_p)$ csoport maximális részcsoportja a p-edfokú szimmetrikus csoportnak.*

A permutációcsoportok elmélete a kombinatorikával függ szorosan össze. Rendkívül szimmetrikus véges halmazrendszerek (úgynevezett blokkrendszerek) vizsgálatával öt egyszerű csoportra bukkantak, amelyeket felfedezőjükről Mathieu-csoportoknak neveztek el. Jelük M_{11}, M_{12}, M_{22}, M_{23} és M_{24}. Az index azt fejezi ki, hogy ezek az adott elemszámú halmazon ható permutációcsoportok. Az M_{24} csoport 5-tranzitív, és M_{23} (ami M_{24}-ben egy pont stabilizátora) 4-tranzitív. Ugyanígy 4-tranzitív az M_{12} is. Nevezetes, és szintén a klasszifikációból következő tétel, hogy más sokszorosan tranzitív véges csoport nem létezik!

4.11.9. Tétel. *Ha az S_n szimmetrikus és az A_n alternáló csoportoktól eltekintünk, akkor az M_{24}, M_{23} és M_{12} Mathieu-csoportokon kívül minden véges permutációcsoport legfeljebb 3-tranzitív lehet.*

A klasszifikációból még erősebb eredmények is következnek: a véges 2-tranzitív csoportok szerkezetét is sikerült megérteni. Ide kapcsolódó eredmény Burnside híres tétele, amely szerint egy ilyen csoport vagy egy véges „majdnem” egyszerű csoportból származtatható (ezekről mesélünk kicsit a 4.13. Szakaszban), vagy pedig a foka prímhatvány, és a csoport része a 4.11.5. Gyakorlatban leírt affin csoportnak (tehát lineáris algebrai eszközökkel vizsgálható).

Az Olvasó joggal kérdezheti azonban a következőt. Ha ismerünk is egy egyszerű csoportot izomorfia erejéig, hogyan tudjuk eldönteni, hogy van-e S_X-nek ezzel izomorf, sokszorosan tranzitív részcsoportja? Tegyük fel, hogy a G csoport 2-tranzitív részcsoportja S_X-nek. Ekkor minden pont stabilizátora maximális részcsoport G-ben (ezt a szakasz hátralévő részében be fogjuk bizonyítani), és ha ez a maximális M részcsoport adott, akkor a csoport hatása ekvivalens az M szerinti bal mellékosztályokon való hatással (lásd 4.6.27. Feladat). Ezért ha a majdnem egyszerű csoportoknak ismerjük a maximális részcsoportjait, akkor ebből a 2-tranzitív csoportok is megkaphatók.

Az 1-tranzitív csoportok pontosan a tranzitívak. A szigorúan 1-tranzitív csoportokat regulárisnak nevezzük.

4.11.10. Gyakorlat. Mutassuk meg, hogy egy permutációcsoport akkor és csak akkor szigorúan 1-tranzitív, ha tranzitív, és valamelyik pont stabilizátora egyelemű. Igazoljuk azt is, hogy ilyenkor a csoport elemszáma ugyanannyi, mint a foka.

Mivel a 4.6.37. Gyakorlat szerint tranzitív csoportban a stabilizátorok konjugáltak, ha az egyik stabilizátor egyelemű, akkor valamennyi az.

4.11.11. Definíció. Legyen G részcsoportja az S_X csoportnak. Azt mondjuk, hogy G *reguláris*, ha tranzitív, és minden pont stabilizátora az egyelemű részcsoport.

4.11.12. Gyakorlat. Mutassuk meg, hogy a Cayley-tételben (4.6.16. Tétel) minden G csoporthoz egy olyan vele izomorf részcsoportot rendeltünk S_G-ben, amely reguláris.

Eszerint minden csoport izomorf egy reguláris permutációcsoporttal. Ugyanakkor láttuk, hogy a 2-tranzitivitás már igen erős megszorítás a csoport szerkezetére. Most egy olyan fogalmat vezetünk be, amely a tranzitivitás és a 2-tranzitivitás között helyezkedik el.

4.11.13. Definíció. Legyen G az X halmazon ható permutációcsoport. Az X halmaz egy $\sim$ ekvivalencia-relációját (vagyis partícióját) *G-invariáns partíciónak* vagy *kongruenciának* nevezzük, ha tetszőleges $x \sim y$ és $g \in G$ esetén $g * x \sim g * y$.

A kongruencia fogalmát (a fentinél általánosabb formában) a 8.2. Szakaszban próbáljuk majd megérteni. Ott azt is elmagyarázzuk, mi köze a most bevezetett fogalomnak a számelméletben tanult kongruenciákhoz (8.2.25. Állítás).

Bármi az X és a G, két kongruencia mindig létezik. Az első az, ahol X mindegyik eleme egyedül, egyelemű osztályban van, ennek neve 0_X. A másik az ellenkező véglet, amikor az egész X halmaz egyetlen osztály, ennek jele 1_X. Ezt a két partíciót az X halmaz *triviális partícióinak* (illetve triviális kongruenciáinak) nevezzük. Partíciókról többet a 8.1. Szakasz végén olvashatunk.

4.11.14. Gyakorlat. Mutassuk meg, hogy ha G hat X-en, akkor az orbitok kongruenciát alkotnak, amely pontosan akkor lesz 1_X, ha ez a hatás tranzitív.

4.11.15. Gyakorlat. Legyenek X elemei egy szabályos hatszög csúcsai, és hasson ezeken a D_6 diédercsoport a szokásos módon. Tekintsük X-nek azt a partícióját, amelynek három kételemű osztálya van: az átellenes csúcspárok. Mutassuk meg, hogy ez kongruencia. Van még más nemtriviális kongruencia is?

4.11.16. Gyakorlat. Mutassuk meg, hogy egy véges halmazon ható tranzitív permutációcsoport esetében egy kongruencia minden osztálya ugyanannyi elemből áll.

Most megvizsgáljuk, hogy egy tranzitív permutációcsoportban miként kaphatjuk meg az összes kongruenciát. Hasson G tranzitívan az X halmazon, legyen $x \in X$ egy rögzített pont, és H az x stabilizátora.

Ha $\sim$ egy kongruencia, akkor belátjuk, hogy

$$K = \{g \in G \,:\, g * x \sim x\}$$

egy H-t tartalmazó részcsoportja G-nek. Valóban, ha $g \in H$, akkor $g * x = x$, tehát $g \in K$. Tegyük fel, hogy $k_1, k_2 \in K$. Ez azt jelenti, hogy $k_1 * x \sim x$ és $k_2 * x \sim x$. Mivel $\sim$ kongruencia, innen $k_1 * (k_2 * x) \sim k_1 * x$, ahonnan $(k_1 k_2) * x = k_1 * (k_2 * x) \sim x$ (hiszen $\sim$ tranzitív). Tehát K szorzásra zárt. A $k_1 * x \sim x$ összefüggésre k_1 inverzét alkalmazva azt kapjuk, hogy $x = k_1^{-1} * (k_1 * x) \sim k_1^{-1} * x$, tehát K zárt az inverzképzésre is, és így részcsoport.

Megfordítva, tegyük fel, hogy $H \leq K \leq G$. Egy $\sim$ kongruenciát fogunk készíteni a K részcsoportból. Tegyük fel, hogy $x_1, x_2 \in X$. Mivel G tranzitív, léteznek (nem feltétlenül egyértelműen) olyan g_1, g_2 elemek G-ben, melyekre $x_1 = g_1 * x$ és $x_2 = g_2 * x$. Legyen

$$x_1 \sim x_2 \iff g_1^{-1} g_2 \in K\,.$$

Megmutatjuk, hogy $\sim$ jóldefiniált (vagyis $x_1 \sim x_2$ csak az x_1 és x_2 pontoktól függ, nem pedig a g_1 és g_2 választásától). Tegyük fel, hogy $x_1 = g_1' * x$ és $x_2 = g_2' * x$. Ekkor $(g_1^{-1} g_1') * x = x$, így $h_1 = g_1^{-1} g_1'$ és ugyanúgy $h_2 = g_2^{-1} g_2'$ elemei H-nak. Nyilván

$$g_1'^{-1} g_2' = h_1^{-1} g_1^{-1} g_2 h_2\,.$$

Mivel $H \subseteq K$, ez pontosan akkor van K-ban, ha $g_1^{-1} g_2 \in K$ (hiszen $h_1^{-1} K h_2 = K$). Tehát $\sim$ tényleg jóldefiniált. Kongruencia is: ha $g_1 * x \sim g_2 * x$, akkor $g * (g_1 * x) \sim g * (g_2 * x)$, mert

$$(g g_1)^{-1} g g_2 = g_1^{-1} g^{-1} g g_2 = g_1^{-1} g_2 \in K\,.$$

A H részcsoporthoz nyilván a 0_X, a G-hez pedig az 1_X kongruencia tartozik.

4.11.17. Gyakorlat. Mutassuk meg, hogy a most kapott megfeleltetés az X kongruenciái és a G csoportnak a H stabilizátort tartalmazó részcsoportjai között kölcsönösen egyértelmű.

Arra biztatjuk az Olvasót, hogy a most vizsgált megfeleltetést a kongruenciák és a részcsoportok között vizsgálja meg abban a speciális esetben, amikor a G csoport egy H részcsoportjának bal mellékosztályain hat balszorzással. (A 4.6.27. Feladat miatt ez igazából az általános eset.) Az állítás bizonyítása ebben az esetben egyszerűbb: egy $K \geq H$ részcsoporthoz tartozó

kongruenciánál ugyanis két H szerinti mellékosztály akkor lesz relációban, ha ugyanannak a K szerinti bal mellékosztálynak a részhalmazai.

4.11.18. Definíció. Azt mondjuk, hogy a G csoport *primitíven* hat az X halmazon, ha tranzitív, és az X halmaznak pontosan két kongruenciája van: a triviálisak.

Ha az X legalább háromelemű, akkor abból, hogy nincs nemtriviális kongruencia, következik, hogy a csoport tranzitív (lásd 4.11.35. Gyakorlat). Egy kételemű halmazon azonban csak triviális partíciók vannak, és így a fenti definícióban a tranzitivitás feltétele csupán ebben az esetben nem fölösleges.

Az egyszerű csoport definíciójához hasonlóan itt is két különböző kongruenciáról beszélünk, azaz kizárjuk azt az esetet, amikor az X halmaz egyelemű. Az előbbi gyakorlat szerint a primitív csoportokat a következőképpen jellemezhetjük.

4.11.19. Következmény. *Egy tranzitív permutációcsoport pontosan akkor primitív, ha valamelyik (vagy ami ezzel ekvivalens: mindegyik) pont stabilizátora maximális részcsoport.*

Ha tehát H maximális részcsoportja G-nek, akkor G primitíven hat a H szerinti bal mellékosztályok halmazán Emiatt a primitív permutációcsoportok is elég nagy számban fordulnak elő: ha az M maximális részcsoportja G-nek, amelynek konjugáltjai csak az egységelemben metszik egymást, akkor a 4.6.26. Gyakorlat miatt G izomorf az S_n egy primitív részcsoportjával, ahol $n = |G : M|$.

4.11.20. Állítás. *Minden 2-tranzitív permutációcsoport primitív.*

Bizonyítás. Tegyük fel, hogy a G csoport 2-tranzitívan hat az X halmazon. Legyen $\sim$ egy kongruencia X-en, ami nem a 0_X. Ez azt jelenti, hogy van olyan $x_1 \neq x_2 \in X$, melyre $x_1 \sim x_2$. A 2-tranzitivitás miatt tetszőleges $y_1 \neq y_2$ elemekhez létezik olyan $g \in G$, melyre $g * x_1 = y_1$ és $g * x_2 = y_2$. Mivel $\sim$ kongruencia, $y_1 \sim y_2$. Ezért $\sim$ az 1_X partíció. □

4.11.21. Állítás. *Egy primitív permutációcsoport minden normálosztója tranzitív, kivéve azokat a normálosztókat, amelyek minden eleme identikusan hat (vagyis amelyek részei a hatás magjának).*

Bizonyítás. Legyen G primitív permutációcsoport X-en, $N \triangleleft G$, és $\sim$ az N orbitjaiból álló partíció. Megmutatjuk, hogy $\sim$ kongruencia. Valóban, tegyük fel, hogy $x \sim y$. Ez azt jelenti, hogy van olyan $n \in N$, melyre $n * x = y$. De akkor

$$(gng^{-1}) * (g * x) = g * (n * x) = g * y\,.$$

Mivel N normálosztó, $gng^{-1} \in N$, ami azt jelenti, hogy $g*x \sim g*y$. Tehát $\sim$ kongruencia, és mivel G primitív, ez valamelyik triviális kongruencia. Ha N-nek van olyan eleme, ami nem hat identikusan, akkor $\sim$ nem a 0_X partíció, tehát akkor az 1_X partíció. Ez pedig azt jelenti, hogy N tranzitív. □

4.11.22. Tétel. *Az A_n alternáló csoport $n \geq 5$ esetén nemkommutatív egyszerű csoport.*

Bizonyítás. Az állítást n szerinti indukcióval bizonyítjuk. Az $n = 5$ kiinduló esetet már elintéztük a 4.7.36. Gyakorlatban.

4.11.23. Gyakorlat. Vizsgáljuk meg a most következő bizonyítást abból a szempontból, hogy a szereplő ötletek felhasználhatók-e az $n = 5$ esetben is.

Tegyük fel, hogy $n \geq 6$, és hogy A_{n-1} egyszerű csoport. Legyen N egy nemtriviális normálosztó A_n-ben. Mivel $n \geq 6$, az A_n csoport 2-tranzitív (sőt, $n - 2 \geq 4$-tranzitív). Ezért A_n primitív (4.11.20. Állítás), és így az N normálosztó tranzitív (4.11.21. Állítás).

Jelölje H az 1 pont stabilizátorát A_n-ben. Ez a $\{2, 3, \ldots, n\}$ halmaz páros permutációiból áll, vagyis egyrészt $n - 3 \geq 3$-tranzitív ezen a halmazon, másrészt izomorf A_{n-1}-gyel, amiről feltettük, hogy egyszerű csoport. De $N \cap H$ normálosztó H-ban. Ezért két lehetőség van: vagy $N \cap H$ csak az identitásból áll, vagy pedig $N \cap H = H$, vagyis $H \subseteq N$. Ez a második eset azonban nem lehetséges. Ugyanis A_n primitív, és így H maximális részcsoport (4.11.19. Következmény). Mivel N nemtriviális normálosztó, így $N \neq G$, vagyis H maximalitása miatt $N = H$, ami ellentmond annak, hogy N tranzitív (hiszen H nem tranzitív: az 1 pontot H elemei fixen hagyják).

Beláttuk tehát, hogy $N \cap H$ egyelemű. Ebből következik, hogy N elemszáma pontosan n. Valóban, tekintsük azt a megfeleltetést, amely a $g \in N$ elemhez a $g(1)$ pontot rendeli. Mivel N tranzitív, $\{1, 2, \ldots, n\}$ minden eleme előáll $g(1)$ alakban. Másfelől ha $g_1, g_2 \in N$, és $g_1(1) = g_2(1)$, akkor $g_1^{-1} g_2 \in H \cap N = \{1\}$, vagyis $g_1 = g_2$. Jelöljük n_i-vel azt az egyértelműen meghatározott N-beli elemet, melyre $n_i(1) = i$.

Az N normálosztó reguláris, hiszen az $N \cap H$ nem egyéb, mint az 1 pont N-beli stabilizátora. Ezért a 4.11.10. Gyakorlat miatt N elemszáma n. Számunkra azonban fontos lesz a most megadott $i \mapsto n_i$ megfeleltetés.

A H részcsoport konjugálással hat az N normálosztó egységelemtől különböző elemeinek $N - \{1\}$ halmazán. Megmutatjuk, hogy ennek a halmaznak pontosan a páros permutációit kapjuk meg így. Valóban, ha $h \in H$, és mondjuk $h(i) = j$, akkor

$$h n_i h^{-1}(1) = h n_i(1) = h(i) = j = n_j(1) .$$

Mivel $h n_i h^{-1} \in N$, ezért $h n_i h^{-1} = n_j$. Tehát H elemei konjugálással ugyanúgy hatnak N elemein, mind ahogy h permutálja a nekik megfelelő pontokat.

Igazából azt láttuk be, hogy H hatása az $\{1, 2, \ldots, n\}$ halmazon ekvivalens azzal, ahogyan a H konjugálással hat az N normálosztón (lásd 4.6.23. Definíció).

Ez azonban ellentmondásra vezet, mert a H elemeivel való konjugálások N-nek automorfizmusai, és így N automorfizmusai 3-tranzitívan hatnak az N egységtől különböző elemeinek a halmazán (hiszen $|N| = n \geq 6$, és a teljes alternáló csoportot megkapjuk ezen a legalább ötelemű halmazon). Ilyen sok automorfizmusa azonban csak nagyon kevés csoportnak lehet! Hiszen a $(g_1, g_2, g_1 g_2)$ hármast biztosan nem lehet elvinni a (g_1, g_2, x) hármasba, kivéve ha $x = g_1 g_2$.

Pontosan a gondolatmenet a következő. Legyen $g_1 \in N$ tetszőleges egységtől különböző elem, $g_2 \in N$ olyan, ami az egységelemtől, g_1-től és g_1^{-1}-től különbözik, végül $g_3 \in N$

olyan, amely az egységtől, g_1-től, g_2-től és g_1g_2-től is különböző. Ilyen elemek léteznek, hiszen N elemszáma $n \geq 6$. Mivel g_1, g_2, g_1g_2 az $N - \{1\}$-nek páronként különböző elemei, a 3-tranzitivitás miatt van olyan α automorfizmusa N-nek, hogy

$$\alpha(g_1) = g_1\,, \quad \alpha(g_2) = g_2\,, \quad \alpha(g_1g_2) = g_3 \neq g_1g_2\,.$$

Ez lehetetlen, mert α szorzattartó, és így

$$\alpha(g_1g_2) = \alpha(g_1)\alpha(g_2) = g_1g_2\,.$$

Ezzel a bizonyítást befejeztük. □

Még egy fontos permutációcsoport-típussal ismerkedünk meg.

4.11.24. Definíció. A $G \leq S_X$ csoportot *Frobenius-csoportnak* nevezzük, ha tranzitív, de nem reguláris, és minden $g \in G$ permutációnak legfeljebb egy fixpontja van. Egy G Frobenius-csoport *magja* az egységelemből, továbbá a fixpontmentes elemekből álló részhalmaz. Az X-beli pontok stabilizátorait Frobenius-*komplementumnak* hívjuk.

4.11.25. Tétel [Frobenius-tétel]. *Minden véges Frobenius-csoport magja normálosztó.*

Ez nehéz tétel, nem bizonyítjuk. Azt könnyű megmutatni, hogy a mag konjugáltságra zárt, a nehéz állítás az, hogy ez részcsoport.

4.11.26. Gyakorlat. Igazoljuk, hogy ha $G \leq S_X$ Frobenius-csoport, és H egy $x \in X$ pont stabilizátora, akkor H nemtriviális részcsoport, és $g \in G - H$ esetén $H \cap gHg^{-1} = \{1\}$. Megfordítva, tegyük fel, hogy a G véges csoportnak H ilyen tulajdonságú részcsoportja. Mutassuk meg, hogy akkor G hatása H bal mellékosztályain Frobenius-csoportot ad, melynek magja az egységelemen kívül azokból az elemekből áll, melyek H egyetlen konjugáltjában sincsenek benne, a komplementumok pedig pontosan H konjugáltjai lesznek. Igazoljuk, hogy a mag elemszáma $|G : H|$, és hogy ha a mag részcsoport, akkor normálosztó, amelynek H tényleg komplementuma.

4.11.27. Gyakorlat. Tekintsük az S_3, D_{2n+1}, A_4, $\mathrm{Aff}(1, T)$ csoportokat a szokásos módon permutációcsoportoknak. Mutassuk meg, hogy ezek Frobenius-csoportok. Mi lesz a magjuk?

4.11.28. Gyakorlat. Mutassuk meg, hogy ha egy véges csoportban van olyan prímrendű részcsoport, amelynek normalizátora önmaga, akkor ez Frobenius-csoport. Vezessük le ebből, hogy ha $p > q$ prímek, akkor minden pq rendű nemkommutatív csoport Frobenius-csoport.

Gyakorlatok, feladatok

4.11.29. Gyakorlat. Határozzuk meg $n \geq 5$ esetén az S_n csoport összes normálosztóját.

4.11.30. Gyakorlat. Bizonyítsuk be, hogy ha a $G \leq S_n$ csoport k-tranzitív, akkor rendje osztható $n(n-1)\dots(n-k+1)$-gyel, és itt oszthatóság helyett akkor és csak akkor áll egyenlőség, ha a hatás szigorúan k-tranzitív.

4.11.31. Gyakorlat. Igazoljuk, hogy ha $A \leq S_n$ Abel-féle és tranzitív, akkor reguláris, és így $|A| = n$.

4.11.32. Gyakorlat. Mutassuk meg, hogy minden prímfokú tranzitív permutációcsoport primitív.

4.11.33. Gyakorlat. Az alábbi permutációcsoportokról döntsük el, hogy primitívek-e (illetve mikor azok): A_3, A_4, az A_4 csoport négyelemű normálosztója, a D_n csoport a szabályos n-szög csúcsain, a kocka szimmetriacsoportja a kocka csúcsain, élein és lapjain.

4.11.34. Feladat. Mikor hat primitíven egy véges csoport automorfizmus-csoportja a csoport egységtől különböző elemeinek a halmazán?

4.11.35. Gyakorlat. Bizonyítsuk be, hogy ha G egy legalább háromelemű halmazon hat, és csak triviális kongruenciája van, akkor tranzitív.

4.11.36. Feladat. Mutassuk meg, hogy ha egy véges $G \leq S_X$ csoportban van Abel-féle, tranzitív, minimális normálosztó, akkor G primitív. (Az $1 < N \triangleleft G$ *minimális normálosztó*, ha $K < N$ és $K \triangleleft G$ esetén $K = \{1\}$).

4.11.37. Feladat. Bizonyítsuk be, hogy ha p prím, és G tranzitív részcsoportja S_p-nek, mely tartalmaz transzpozíciót, akkor $G = S_p$.

4.11.38. Feladat. Milyen n-ekre van S_n-ben Q-val izomorf részcsoport?

4.11.39. Feladat. Tegyük fel, hogy a G egyszerű csoportban van n-indexű részcsoport (ahol $n > 1$ egész). Bizonyítsuk be, hogy G izomorf az S_n egy alkalmas részcsoportjával.

4.11.40. Feladat. Egy véges G csoport Cayley-reprezentációjában mely elemeknek lesz páratlan permutáció a képe? Igazoljuk, hogy ha a 2-Sylow részcsoport ciklikus (speciálisan ha G rendje $4k+2$ alakú), akkor G nem lehet nemkommutatív egyszerű csoport.

4.11.41. Feladat. Igazoljuk, hogy nincs 1960, 120, 180 rendű egyszerű csoport.

4.11.42. Feladat. Bizonyítsuk be, hogy ha G primitív permutációcsoport egy legalább háromelemű, páros elemszámú halmazon, akkor G rendje osztható néggyel.

4.11.43. Feladat. Igazoljuk, hogy ha H és K részcsoportok egy G csoportban, akkor a G hatása a H szerinti bal mellékosztályokon akkor és csak akkor ekvivalens a K szerinti bal mellékosztályokon való hatással, ha H és K konjugáltak G-ben.

4.11.44. Gyakorlat. Mi a szükséges és elégséges feltétele annak, hogy az $N \rtimes_\psi H$ véges szemidirekt szorzat olyan Frobenius-csoport legyen, melynek magja N, egyik komplementuma pedig H?

4.12. Feloldható csoportok

Ha adott egy G csoport, ami nem egyszerű, akkor vegyünk egy nemtriviális N normálosztót, és tekintsük az N és G/N csoportokat. Ha még ezek sem egyszerűek, folytassuk az eljárást N-nel és G/N-nel is. Ha G véges, akkor előbb-utóbb már csupa egyszerű csoporthoz jutunk. A kapott egyszerű csoportok sokat elárulnak G szerkezetéről.

4.12.1. Definíció. Legyen G csoport, ekkor G *normálláncának* nevezzük G részcsoportjainak egy olyan sorozatát, melyre

$$\{1\} = N_n \lhd N_{n-1} \lhd \ldots \lhd N_2 \lhd N_1 \lhd N_0 = G\,.$$

Az itt szereplő n szám a normállánc *hossza*. Ha az összes N_i/N_{i+1} faktorcsoport egyszerű, akkor az ilyen láncot G *kompozícióláncának* nevezzük, az N_i/N_{i+1} egyszerű faktorcsoportokat pedig G *kompozíció-faktorainak*.

Minden csoportnak van normállánca (például $\{1\} \lhd G$), és ha G véges, akkor biztosan van kompozíciólánca is. Például az A_4 alternáló csoport esetén a következő kompozícióláncot kaphatjuk:

$$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4\,.$$

Tudjuk, hogy $\{id, (12)(34)\}$ nem lesz normálosztó A_4-ben (lásd 4.7.18. Gyakorlat), vagyis egy normállánc elemei általában nem lesznek a G normálosztói. A fenti lánc kompozíció-faktorai

$$\mathbb{Z}_2^+\,, \quad \mathbb{Z}_2^+\,, \quad \mathbb{Z}_3^+\,.$$

Természetesen számít a multiplicitás, egy faktorcsoport többször is szerepelhet (ugyanígy, ahogy a 12 szám prímtényezős felbontásában is kétszer szerepel a 2 prímszám).

A kompozíció-faktorok sok információt szolgáltatnak a csoportról, de nem határozzák meg a szerkezetét. Például az S_3 csoport esetén

$$\{1\} \lhd \{id, (123), (132)\} \lhd S_3$$

kompozíciólánc, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$. Ugyanezek lesznek az S_3-mal nem izomorf $\mathbb{Z}_6^+$ csoport kompozíció-faktorai is, amit az alábbi lánc bizonyít:

$$\{0\} \lhd \{0, 3\} \lhd \mathbb{Z}_6^+\,.$$

A $\mathbb{Z}_6^+$ csoportnak van egy másik kompozíciólánca is:

$$\{0\} \lhd \{0, 2, 4\} \lhd \mathbb{Z}_6^+\,.$$

A kompozíció-faktorok most is $\mathbb{Z}_2^+$ és $\mathbb{Z}_3^+$, csak más sorrendben. Jordan és Hölder nevezetes tétele azt mondja ki, hogy ez általában is így van. Bárhogyan is vesszük egy G

csoport két kompozícióláncát, a kapott kompozíció-faktorok (a multiplicitásokkal együtt) ugyanazok lesznek a két láncban.

4.12.2. Definíció. Tegyük fel, hogy a G csoportnak

$$\{1\} = N_n \lhd N_{n-1} \lhd \ldots \lhd N_2 \lhd N_1 \lhd N_0 = G$$

és

$$\{1\} = M_m \lhd M_{m-1} \lhd \ldots \lhd M_2 \lhd M_1 \lhd M_0 = G$$

normálláncai. Azt mondjuk, hogy ezek *izomorfak*, ha ($n = m$, vagyis a két lánc hossza egyenlő, és) az első lánc, illetve a második lánc faktorai, vagyis az

$$\{N_{n-1}/N_n, \ldots, N_1/N_2, N_0/N_1\},$$

illetve az

$$\{M_{m-1}/M_m, \ldots, M_1/M_2, M_0/M_1\}$$

csoport-rendszerek között van olyan kölcsönösen egyértelmű megfeleltetés, hogy az egymásnak megfelelő csoportok izomorfak.

A fenti csoport-rendszerek elemei között lehetnek egyformák (izomorfak) is. A megfeleltetést úgy kell érteni, hogy ha mondjuk az első rendszerben háromszor szerepel a $\mathbb{Z}_3^+$ csoport, akkor a másodikban is pontosan háromszor kell, hogy szerepeljen.

4.12.3. Tétel [Jordan–Hölder-tétel]. *Tetszőleges csoport bármely két kompozíciólánca izomorf.*

Bizonyítás. Mivel nem minden csoportnak van kompozíciólánca, a bizonyításban hasznos lesz a következő segédállítás.

4.12.4. Lemma. *Ha egy G csoportnak van kompozíciólánca, akkor minden normálosztójának is van, és ennek kompozíció-faktorai az eredeti csoport kompozíció-faktorai közül kerülnek ki.*

Bizonyítás. Tegyük fel, hogy

$$\{1\} = N_n \lhd N_{n-1} \lhd \ldots \lhd N_2 \lhd N_1 \lhd N_0 = G \tag{4.2}$$

kompozíciólánca, K pedig normálosztója a G csoportnak. Tekintsük a K csoport

$$\{1\} = (N_n \cap K) \lhd (N_{n-1} \cap K) \lhd \ldots \lhd (N_1 \cap K) \lhd (N_0 \cap K) = K$$

normálláncát. Belátjuk, hogy tetszőleges $0 \leq i < n$ esetén az $(N_i \cap K)/(N_{i+1} \cap K)$ faktorcsoport vagy egyelemű, vagy egyszerű csoport, amely N_i/N_{i+1}-gyel izomorf. Ezzel kész is leszünk, hiszen a láncból az ismétlődéseket elhagyva ezek szerint kompozícióláncot kapunk, melynek faktorai a (4.2)-beli lánc faktorai közül valók.

Alkalmazzuk az első izomorfizmus-tételt (4.5.20. Következmény) a $H = N_i \cap K$ részcsoportra és az N_{i+1} normálosztóra:

$$H/(H \cap N_{i+1}) \cong HN_{i+1}/N_{i+1}\,.$$

A bal oldalon $(N_i \cap K)/(N_i \cap K \cap N_{i+1})$ áll. De $N_i \cap K \cap N_{i+1} = N_{i+1} \cap K$, hiszen $N_{i+1} \subseteq N_i$. A jobb oldalon szereplő HN_{i+1} viszont normálosztója N_i-nek, mert N_i-ben $H = N_i \cap K$ és N_{i+1} is normálosztó. Ezért a fenti izomorfia így alakul:

$$(N_i \cap K)/(N_{i+1} \cap K) \cong HN_{i+1}/N_{i+1} \lhd N_i/N_{i+1}$$

(itt felhasználtuk, hogy a 4.5.19. Tétel szerint a faktorcsoport normálosztói az eredeti csoport magot tartalmazó normálosztóinak felelnek meg). De N_i/N_{i+1} egyszerű csoport, amelynek csak a két triviális normálosztója van. Ezért $(N_i \cap K)/(N_{i+1} \cap K)$ vagy tényleg egyszerű csoport, ami N_i/N_{i+1}-gyel izomorf, vagy az egyelemű csoport, amikor $N_i \cap K = N_{i+1} \cap K$, és így a láncból e két normálosztó egyike elhagyható. □

A Jordan–Hölder-tételt a kompozíciólánc hossza szerinti indukcióval látjuk be. Ha a G csoportnak van 1 hosszú kompozíciólánca, akkor ez $\{1\} \lhd G$ alakú, és ilyenkor ez az egyetlen kompozíciólánc, tehát a tétel igaz. Most tegyük fel, hogy a tétel igaz minden olyan csoportra, amelynek van n-nél rövidebb kompozíciólánca (és akkor a tétel állítása szerint minden kompozíciólánca egyforma hosszúságú). Legyenek

$$\{1\} = N_n \lhd N_{n-1} \lhd \ldots \lhd N_2 \lhd N_1 \lhd N_0 = G$$

és

$$\{1\} = M_m \lhd M_{m-1} \lhd \ldots \lhd M_2 \lhd M_1 \lhd M_0 = G$$

a G csoport kompozícióláncai. Meg kell mutatnunk, hogy ezek izomorfak.

Ha a két lánc legfelső szeme egyenlő, azaz ha $N_1 = M_1$, akkor készen vagyunk. Az indukciós feltevést ugyanis alkalmazhatjuk az N_1 normálosztóra, amelynek van $n-1$ hosszú kompozíciólánca, $N_n \lhd \ldots \lhd N_1$. Mivel $M_m \lhd \ldots \lhd M_1 = N_1$ egy másik kompozíciólánca N_1-nek, az indukciós feltevés szerint $n-1 = m-1$, és ez a két lánc izomorf. Ekkor pedig az eredeti két lánc is izomorf, hiszen a kompozíció-faktorok rendszeréhez mindkét esetben a $G/N_1 = G/M_1$ csoportot kell hozzávenni.

Tegyük fel most, hogy $N_1 \neq M_1$. Mivel G/N_1 egyszerű csoport, a G csoportnak nincsen N_1-et tartalmazó más normálosztója, mint N_1 és G. Ugyanígy M_1-et tartalmazó normálosztó is csak M_1 vagy G lehet. Az N_1M_1 normálosztó mind N_1-et, mind M_1-et tartalmazza, és ha nem G lenne, akkor $N_1 = N_1M_1 = M_1$ teljesülne, amiről most feltettük, hogy nem igaz. Ezért $N_1M_1 = M_1N_1 = G$. Az első izomorfizmus-tétel miatt így

$$G/N_1 = M_1N_1/N_1 \cong M_1/(M_1 \cap N_1) \quad \text{és} \quad G/M_1 = N_1M_1/M_1 \cong N_1/(N_1 \cap M_1)\,.$$

Legyen $K = M_1 \cap N_1$. Ez normálosztó G-ben, ezért az előző lemma szerint van kompozíciólánca:

$$\{1\} = K_k \lhd K_{k-1} \lhd \ldots \lhd K_1 \lhd K_0 = K\,.$$

Ehhez a lánchoz vegyük hozzá N_1-et. Ekkor az N_1 csoport egy kompozícióláncát kapjuk, mert láttuk, hogy $N_1/K \cong G/M_1$, és G/M_1 egyszerű csoport. Az N_1 csoportnak van n-nél rövidebb kompozíciólánca, ezért az indukciós feltevés miatt az $N_n \lhd \ldots \lhd N_2 \lhd N_1$ és a $K_k \lhd \ldots \lhd K \lhd N_1$ láncok izomorfak, speciálisan $k = n-2$. Most vegyük hozzá a $K_k \lhd \ldots \lhd K$ lánchoz az M_1 normálosztót. Ekkor M_1 egy kompozícióláncát kapjuk (hiszen

$M_1/K \cong G/N_1$ is egyszerű csoport), melynek hossza $k+1 = n-1$. Tehát az M_1 csoportnak is van n-nél rövidebb kompozíciólánca, így alkalmazható az indukciós feltevés, amely szerint a $K_k \lhd \ldots \lhd K \lhd M_1$ és az $M_m \lhd \ldots \lhd M_1$ láncok izomorfak. De akkor készen vagyunk, mert ezek szerint a két eredeti $N_n \lhd \ldots \lhd N_0$ és $M_m \lhd \ldots \lhd M_0$ lánc kompozíciófaktorait úgy kaphatjuk meg, hogy a $K_k \lhd \ldots \lhd K$ lánc faktoraihoz még hozzátesszük a $G/N_1 \cong M_1/K$ és a $G/M_1 \cong N_1/K$ faktorokat (csak más sorrendben). Ezzel a Jordan–Hölder-tétel bizonyítását befejeztük. □

4.12.5. Definíció. Egy G csoportot *feloldhatónak* nevezünk, ha van olyan normállánca, amelynek minden faktora Abel-csoport.

4.12.6. Gyakorlat. Mutassuk meg, hogy egy véges csoport akkor és csak akkor feloldható, ha a kompozíció-faktorai mind prímrendű ciklikus csoportok (vagyis nincs közöttük nemkommutatív egyszerű csoport). Speciálisan egy véges egyszerű csoport akkor és csak akkor feloldható, ha prímrendű ciklikus.

4.12.7. Gyakorlat. Igazoljuk, hogy az S_2, S_3 és S_4 csoportok feloldhatók.

A feloldható csoportok fontos szerephez jutnak az egyenletek gyökképleteinek vizsgálatában (és a geometriai szerkesztések elméletében is). Az, hogy pontosan a legfeljebb negyedfokú egyenletekre van általános megoldóképlet (6.9.7. Tétel), az alábbi állításnak a következménye.

4.12.8. Tétel. *Az S_n szimmetrikus csoport akkor és csak akkor feloldható, ha $n \leq 4$.*

Bizonyítás. A 4.12.7. Gyakorlat miatt csak azt kell igazolni, hogy $n \geq 5$ esetén S_n nem feloldható. De ilyenkor A_n egyszerű (4.11.22. Tétel), és ezért S_n-nek kompozíciólánca lesz $\{1\} \lhd A_n \lhd S_n$. Tehát S_n-nek kompozíció-faktora a nemkommutatív egyszerű A_n csoport, és így nem feloldható. □

Minden A Abel-csoport feloldható, hiszen $\{0\} \lhd A$ olyan normállánc, amelynek a faktorai Abel-félék.

4.12.9. Következmény. *Minden véges prímhatványrendű csoport feloldható.*

Bizonyítás. Legyen p prím és P tetszőleges p-csoport. Készítsük el P egy kompozícióláncát. Ebben a faktorok rendje osztója $|P|$-nek, azaz mindegyik ilyen F faktorcsoport egyszerű p-csoport. A 4.10.5. Állítás miatt F rendje p. Ez a P kompozícióláncának minden faktorára igaz, tehát P feloldható. □

4.12.10. Tétel [Burnside „kétprímes" tétele]. *Ha a G véges csoport rendjének legfeljebb két prímosztója van, akkor G feloldható.*

Ez már jóval nehezebb tétel, nem is bizonyítjuk. Még ennél is sokkal-sokkal nehezebb azt megmutatni, hogy minden páratlan rendű véges csoport feloldható.

4.12.11. Tétel [Feit–Thompson-tétel]. *A nemkommutatív véges egyszerű csoportok rendje páros.*

4.12.12. Következmény. *Minden páratlan rendű véges csoport feloldható.*

Bizonyítás. Legyen G tetszőleges páratlan rendű csoport, és F egy kompozíció-faktora. Ekkor F rendje osztója G rendjének, azaz páratlan. Így a Feit–Thompson-tétel miatt F csakis kommutatív egyszerű csoport, tehát prímrendű lehet. □

Feloldható csoportokra a Sylow-tételek erősebb formában igazak.

4.12.13. Tétel [Hall-tétel]. *Tegyük fel, hogy az n pozitív egész szám osztója a G véges feloldható csoport rendjének. Ha n és $|G|/n$ relatív prímek, akkor G-ben van n-edrendű részcsoport, és az összes n-edrendű részcsoport egymás konjugáltja.*

Megfordítva, megmutatható, hogy ha G rendjének minden olyan n osztójára, melyre n és $|G|/n$ relatív prímek, van n rendű részcsoport G-ben, akkor G feloldható. A tételben szereplő részcsoportokat, tehát azokat, amelyek rendje és indexe relatív prím, *Hall-részcsoportoknak* nevezzük. A Hall-tétel bizonyításában alapvető szerepet játszik az alábbi, önmagában is fontos tétel.

4.12.14. Tétel [Schur–Zassenhaus-tétel]. *Tegyük fel, hogy a G véges csoport egy N normálosztójának rendje és indexe relatív prím. Ekkor van olyan H részcsoportja G-nek, melyre $NH = G$ és $N \cap H = \{1\}$ (vagyis az N normálosztónak van komplementuma G-ben), és ezek a H komplementumok egymás konjugáltjai.*

A Schur–Zassenhaus-tétel viszonylag egyszerűen bebizonyítható abban az esetben, ha N és G/N egyike feloldható. De ez a feltétel mindig teljesül! Ugyanis N és G/N rendjei relatív prímek, ezért valamelyikük rendje páratlan, és az feloldható a Feit–Thompson-tétel miatt.

Gyakorlatok, feladatok

4.12.15. Gyakorlat. Adjuk meg az $S_4 \times \mathbb{Z}_3^+ \times \mathbb{Z}_2^+$ csoport egy kompozícióláncát, és kompozíciófaktorait. Mutassuk meg, hogy két feloldható csoport direkt szorzata is feloldható.

4.12.16. Gyakorlat. Mutassuk meg, hogy egy Abel-csoportnak akkor és csak akkor van kompozíciólánca, ha véges.

4.12.17. Gyakorlat. Igazoljuk Burnside tételének felhasználása nélkül, hogy ha egy véges csoport rendje két prím szorzata, akkor a csoport feloldható.

4.12.18. Feladat. Legyen G tetszőleges csoport. Képezzük G kommutátor-részcsoportját, azaz G'-t, ennek a kommutátor-részcsoportját, azaz G''-t, és így tovább (ezt a *G kommutátorláncának* nevezzük). Mutassuk meg, hogy G akkor és csak akkor feloldható, ha ez a lánc véges sok lépésben leér az $\{1\}$ részcsoportig. Igazoljuk azt is, hogy a kommutátorlánc minden eleme normálosztó G-ben.

4.12.19. Feladat. Bizonyítsuk be, hogy a feloldható csoportok osztálya zárt a részcsoportképzésre és a faktorcsoport képzésére.

4.12.20. Feladat. Legyen G tetszőleges csoport, mutassuk meg az alábbiakat.

(1) Ha N normálosztó G-ben, melyre N és G/N is feloldható, akkor G is feloldható.
(2) Ha N és K normálosztók G-ben, melyek feloldhatók, akkor NK is feloldható.

4.12.21. Feladat. Mutassuk meg Burnside kétprímes tételének felhasználása nélkül, hogy ha p páratlan prím, akkor minden $4p^\alpha$ rendű csoport feloldható.

4.12.22. Feladat. Mutassuk meg, hogy tetszőleges T test felett a $\mathrm{T}(n, T)$ csoport feloldható.

4.12.23. Feladat. Bizonyítsuk be, hogy egy véges feloldható csoportban minden minimális normálosztó úgynevezett *elemi Abel-féle p-csoport*, azaz izomorf $(\mathbb{Z}_p^+)^n$-nel valamilyen p prímre és n egészre.

4.12.24. Feladat. Igazoljuk, hogy véges feloldható csoport maximális részcsoportjának indexe prímhatvány, vagy másképp fogalmazva: egy feloldható primitív permutációcsoport foka mindig prímhatvány.

4.13. Véges egyszerű csoportok

A csoportelmélet befejezéseképpen, a teljesség bármiféle igénye nélkül, a véges egyszerű csoportok klasszifikációjával kapcsolatos eredményekről mesélünk egy kicsit. Nemkommutatív egyszerű csoportot nem is olyan könnyű találni. Egy ilyen csoport rendjének Burnside kétprímes tétele miatt legalább három különböző prímosztója kell, hogy legyen, és ez a rend a Feit–Thompson-tétel szerint biztosan páros szám. A 4.10. Szakasz végén megállapítottuk, hogy a legfeljebb 15 rendű csoportokat már mind ismerjük. Ezek mind feloldhatók, sőt az eddig tanult eszközökkel megmutatható, hogy minden 60-nál kisebb rendű csoport feloldható. Ekkor érjük el az A_5 alternáló csoportot, amely a legkisebb elemszámú nemkommutatív egyszerű csoport.

4.13.1. Gyakorlat. Bizonyítsuk be az eddig már igazolt tételekre, gyakorlatokra és feladatokra hivatkozva, hogy minden 60-nál kisebb rendű csoport feloldható. (Ne használjunk nem bizonyított tételt, például Burnside tételét.)

Az, hogy A_n egyszerű csoport ha $n \geq 5$, már Galois számára is ismeretes volt. Ugyancsak régről (geometriából és analízisből) ismeretesek az úgynevezett klasszikus egyszerű csoportok, melyek több végtelen sorozatot alkotnak. Ezek talán legfontosabb családjával most megismerkedünk.

Egy T test fölötti, $n \times n$-es invertálható mátrixok csoportját a szorzásra általános lineáris csoportnak neveztük, és $\mathrm{GL}(n, T)$-vel jelöltük. A determinánsképzés homomorfizmusa ennek a csoportnak a T test multiplikatív csoportjába. E homomorfizmus magja, vagyis az 1 determinánsú mátrixokból álló normálosztó a speciális lineáris csoport, azaz $\mathrm{SL}(n, T)$. Így $\mathrm{GL}(n, T)$ általában nem egyszerű csoport. Találhatunk azonban másképp is normálosztót $\mathrm{GL}(n, T)$-ben.

4.13.2. Gyakorlat. Igazoljuk, hogy a $\mathrm{GL}(n, T)$ csoport Z centruma az E egységmátrix nem nulla skalárszorosaiból áll, az $\mathrm{SL}(n, T)$ centruma pedig azon λE mátrixokból ($\lambda \in T$), melyekre $\lambda^n = 1$.

A $\mathrm{GL}(n, T)/Z$ csoportnak geometriai jelentése van, ahonnan a neve is származik.

4.13.3. Definíció. A $\mathrm{GL}(n, T)$ csoport centruma szerinti faktorcsoportját *projektív általános lineáris csoportnak* nevezzük, jele $\mathrm{PGL}(n, T)$. Végül $\mathrm{PSL}(n, T)$ (vagy $L_n(T)$) jelöli az $\mathrm{SL}(n, T)$ csoportnak a centruma szerinti faktorcsoportját, ez a *projektív speciális lineáris csoport*.

Ha $n = 1$, akkor csoportjaink mindegyike kommutatív, ezért a továbbiakban feltesszük, hogy $n \geq 2$. Mivel véges csoportokat szeretnénk kapni, célszerű a T testet is végesnek választani. Ha a T test véges, és elemszáma q, akkor szokás $\mathrm{GL}(n, T)$ helyett $\mathrm{GL}(n, q)$-t írni. Ez a jelölés zavart okozhatna, ha többféle olyan test is létezne, aminek az elemszáma q. A Galois-elmélet keretében azonban be fogjuk látni, hogy izomorfia erejéig minden q prímhatványhoz pontosan egy q elemű test létezik. Ugyanilyen értelemben szokás használni az $\mathrm{SL}(n, q)$, $\mathrm{PGL}(n, q)$, $\mathrm{PSL}(n, q)$, $\mathrm{Aff}(n, q)$, $\mathrm{T}(n, q)$, $\mathrm{U}(n, q)$ jelöléseket is.

4.13.4. Tétel. *A* $\mathrm{PSL}(n, T)$ *csoport egyszerű, kivéve* $\mathrm{PSL}(2, 2)$ *és* $\mathrm{PSL}(2, 3)$.

A tételt nem bizonyítjuk. A projektív lineáris csoportok között több korábbról már ismert csoport fordul elő, mint azt a 4.13.11. Gyakorlat, és az alábbi állítás is mutatja.

4.13.5. Állítás. *Az alábbi izomorfizmusok teljesülnek.*

(1) $\mathrm{PSL}(2, 2) \cong \mathrm{SL}(2, 2) = \mathrm{GL}(2, 2) \cong S_3$.
(2) $\mathrm{PSL}(2, 3) \cong A_4$.
(3) $\mathrm{PSL}(2, 4) \cong \mathrm{PSL}(2, 5) \cong A_5$.
(4) $\mathrm{PSL}(2, 7) \cong \mathrm{PSL}(3, 2)$ *(rendjük* 168*).*
(5) $\mathrm{PSL}(2, 9) \cong A_6$.
(6) $\mathrm{PSL}(4, 2) \cong A_8$.

4.13.6. Feladat. Legyen

$$M = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}) \quad \text{és} \quad d = (q - 1, n)\,.$$

Mutassuk meg, hogy

$$|\mathrm{GL}(n, q)| = M\,; \quad |\mathrm{SL}(n, q)| = |\mathrm{PGL}(n, q)| = \frac{M}{q - 1}\,; \quad |\mathrm{PSL}(n, q)| = \frac{M}{(q - 1)d}\,.$$

Hasonlóan kaphatunk egyszerű csoportokat egybevágósági transzformációk segítségével is. A mátrixokból származtatott egyszerű csoportokon kívül beszéltünk már a Mathieu-csoportokról is (4.11.9. Tétel). Ezeket a tizenkilencedik század végén fedezték fel. Segítségükkel hatékony kódolási eljárás készíthető, és így az M_{11} csoportot egy űrszonda is magával vitte már.

A csoportelmélet első igazán mély eredményei a huszadik század elején keletkeztek Burnside és Frobenius munkássága nyomán. Kialakult az úgynevezett *reprezentációelmélet*, amely lineáris algebrai eszközöket használ: a vizsgált csoport elemeit mátrixokkal reprezentáljuk (vagyis egy homomorfizmust készítünk az általános lineáris csoportba). Burnside és Frobenius ennek az elméletnek a segítségével bizonyította be a 4.12.10. Tételt, illetve a 4.11.25. Tételt. A reprezentációelmélet fontos szerepet játszik a kémiában és a részecskefizikában is. A reprezentációelmélet kiindulópontját a 5.12. Szakaszban mutatjuk be.

Burnside már akkoriban azt sejtette, hogy a véges nemkommutatív egyszerű csoportok rendje páros kell, hogy legyen. A kor eszközei azonban elégtelennek bizonyultak a sejtés bizonyításához. Az 1950-es években Suzuki meghatározta az összes olyan egyszerű csoportot, melyben minden egységtől különböző elem centralizátora Abel-féle. Suzuki gondolataiból kiindulva 1963-ban sikerült bebizonyítani Burnside sejtését, vagyis a Feit–Thompson-tételt. A több, mint 250 oldalas bizonyítás felhasználja a csoportelmélet korábbi eredményeit, például a reprezentációelméletet is (lásd [**9**]). Ezután Thompson egy újabb 600 oldalas cikkben meghatározta azokat az egyszerű csoportokat, melyek minden valódi részcsoportja már feloldható, ez utóbbi munkájáért Fields-Medalt (matematikai Nobel-díjat) kapott.

A klasszifikáció az 1980-as évek elején vált teljessé. A véges, nemkommutatív, egyszerű csoportok 17 végtelen sorozatba tartoznak (az A_n, illetve a $\mathrm{PSL}(n,q)$ két ilyen sorozat), és ezen kívül van még 26 egyszerű csoport, melyek egyik sorozatnak sem tagjai. Ezeket *sporadikus* egyszerű csoportoknak nevezzük. A végtelen sorozatokat Chevalley foglalta egységes rendszerbe. A sporadikus egyszerű csoportok listája a 758. oldalon található. Ide tartoznak például a már említett Mathieu-csoportok is.

Érdemes elidőzni kicsit a legnagyobb sporadikus csoportnál, mely a Monster (azaz Szörnyeteg) névre hallgat. Rendje

$$808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000\,,$$

azaz $8.08 \cdot 10^{53}$. Összehasonlításképpen néhány adat: a világegyetem nukleonjainak (protonok és neutronok) száma $3 \cdot 10^{77}$, térfogata (jelenleg) 10^{85} köbcenti, a Föld tömege $3.5 \cdot 10^{51}$-szerese egy proton tömegének (tehát a Monsternek sokkal több eleme van, mint ahány atomból a Föld áll), végül az ősrobbanás (azaz a világ kezdete) óta „mindössze” $4.7 \cdot 10^{17}$ másodperc telt el.

Ebből láthatjuk, hogy egy ekkora csoportot egyáltalán nem triviális megkonstruálni. Semmiféle számítógép nem tárolhatja például a szorzástábláját. A klasszifikációnak ez a konstrukció volt az utolsó lépése. Már tudták, hogy a Monster elemszáma csak a fenti lehet, azt is, hogy 194 konjugált osztálya kell, hogy legyen, csak azt nem tudták, hogy ilyen csoport létezik-e. Végül Griess talált egy 196884-dimenziós vektorteret, melynek bizonyos szimmetriái a Monsterrel izomorf csoportot alkotnak.

Érdekes észrevenni, hogy a konjugált osztályok száma milyen kicsi a csoport rendjéhez képest. Az M_{24} Mathieu-csoportnak például mindössze 26 konjugált osztálya van. Ez a

csoport alapvető szerepet játszik a Monster, és sok más sporadikus egyszerű csoport szerkezetében is.

Összesen 56 darab olyan nemkommutatív egyszerű csoport van, melynek rendje egymilliónál kisebb. Ezek közül 39 izomorf a $\mathrm{PSL}(2, q)$ csoporttal alkalmas q prímhatványra (lásd 759. oldal). A többi 17 csoportot a 760. oldalon soroltuk fel, ezek közül három izomorf $\mathrm{PSL}(3, q)$-val ($q = 3, 4, 5$), és egy, $A_8 \cong \mathrm{PSL}(4, 2)$. Szerepel még két alternáló csoport (A_7, A_9), öt sporadikus csoport (az első három Mathieu és az első két Janko), a maradék hat csoport pedig további végtelen sorozatoknak elemei (ezeket nem definiáljuk). Megjegyezzük, hogy két nemizomorf 20160 rendű egyszerű csoport van. További érdekes információk találhatók a Véges Egyszerű Csoportok Atlaszában [**5**].

A klasszifikáció alkalmazásai közül már beszéltünk két olyanról, amely permutációcsoportokkal kapcsolatos (a 4.11.8. Tétel, illetve a 4.11.9. Tétel). A 2-tranzitív csoportok leírása kapcsán előjöttek a „majdnem" egyszerű csoportok is. Miféle csoportok ezek?

Tudjuk, hogy egy G csoport belső automorfizmusainak $\mathrm{Inn}(G)$ csoportja $G/Z(G)$-vel izomorf (4.7.16. Gyakorlat). Ha G nemkommutatív egyszerű csoport, akkor $Z(G) = \{1\}$, és így $\mathrm{Inn}(G) \cong G$, más szóval G automorfizmus-csoportjában a belső automorfizmusok egy G-vel izomorf normálosztót alkotnak (4.7.15. Gyakorlat). De mennyivel lehet ennél nagyobb az egész automorfizmus-csoport?

4.13.7. Tétel. *Ha $n > 3$, és $n \neq 6$, akkor az A_n alternáló csoport automorfizmus-csoportja S_n-nel izomorf.*

Ez nem nehéz tétel, és mutatja, hogy az S_n mennyire természetes módon származtatható az A_n-ből. Ha $n \geq 5$, akkor az S_n szimmetrikus csoportot az A_n egyszerű csoporthoz tartozó majdnem egyszerű csoportnak nevezzük. Általában ha G nemkommutatív egyszerű csoport, akkor az ebből származtatott *majdnem egyszerű csoportok* azok, amelyek részei G automorfizmus-csoportjának, de tartalmazzák a belső automorfizmusok G-vel izomorf $\mathrm{Inn}(G)$ normálosztóját.

Ha meg akarjuk érteni a majdnem egyszerű csoportokat (és ezzel a 2-tranzitív permutációcsoportokat), akkor tehát le kell írni a véges egyszerű csoportok automorfizmuscsoportjait. Még a klasszifikáció bizonyítása előtt Schreier azt sejtette, hogy ez nem lehet sokkal nagyobb, mint az $\mathrm{Inn}(G)$ normálosztó, vagyis hogy az $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ faktorcsoport feloldható (e faktorcsoport neve *G külső automorfizmus-csoportja*). Utóbb, már a klasszifikáció ismeretében be is bizonyosodott Schreier sejtése: a külső automorfizmuscsoport nemcsak feloldható, de az esetek többségében kicsi Abel-csoport, maximum egy diédercsoport fordulhat elő. Azt mondhatjuk tehát, hogy a véges egyszerű csoportok bonyolultak, de az automorfizmus-csoportjaik viszonylag egyszerűek!

Megemlítjük a klasszifikáció még egy érdekes következményét. Nyilvánvaló, hogy egy csoport pontosan akkor kommutatív, ha bármely két elemmel generált részcsoportja az. Ugyanezt feloldható csoportokra csak a klasszifikáció felhasználásával sikerült belátni.

4.13.8. Tétel. *Minden véges egyszerű csoport generálható két elemmel.*

4.13.9. Gyakorlat. Mutassuk meg az előző tétel felhasználásával, hogy ha egy G véges csoport bármely két elemmel generálható részcsoportja feloldható, akkor G is feloldható.

Gyakorlatok, feladatok

4.13.10. Gyakorlat. Igazoljuk a véges egyszerű csoportok táblázatainak (B.2. Függelék) felhasználásával, hogy minden 200 elemű csoport feloldható.

4.13.11. Gyakorlat. Mutassuk meg, hogy ha T test, akkor a 219. oldalon definiált $K(T)$ csoport (vagyis a $T \cup \infty$ halmazon értelmezett törtlineáris leképezések csoportja) izomorf a $\mathrm{PGL}(2, T)$ csoporttal.

4.13.12. Gyakorlat. Igazoljuk az alábbi izomorfizmusokat.

(1) $\mathrm{PSL}(2, 2) \cong \mathrm{SL}(2, 2) = \mathrm{GL}(2, 2) \cong S_3$.
(2) $\mathrm{PSL}(2, 3) \cong A_4$.

4.13.13. Feladat. Bizonyítsuk be, hogy csak egy 60 rendű egyszerű csoport van, és ezért $\mathrm{PSL}(2, 4) \cong \mathrm{PSL}(2, 5) \cong A_5$.

4.13.14. Gyakorlat. Igazoljuk, hogy a $\mathrm{GL}(n, p)$ csoport p-Sylowja izomorf $\mathrm{U}(n, p)$-vel.

4.13.15. Gyakorlat. Bizonyítsuk be, hogy ha G egy n elemű csoport, akkor G beágyazható a $\mathrm{GL}(n, p)$ csoportba tetszőleges p esetén, és ha G egy p-csoport, akkor beágyazható $\mathrm{U}(n, p)$-be is.

4.14. Összefoglaló

A csoportok tanulmányozását konkrét példák vizsgálatával kezdtük. A gyűrűk additív és multiplikatív csoportjain kívül megismerkedtünk a D_n diédercsoporttal, amely a szabályos n-szög szimmetriacsoportja, és az S_X szimmetrikus csoporttal, amely az X halmaz permutációiból (azaz önmagára való bijekcióiból) áll, és a művelet a kompozíció. Ezeket a permutációkat diszjunkt ciklusok szorzataként írtuk fel. Bevezettük a permutációk előjelének a fogalmát. Ez egy szorzattartó leképezés, amely minden permutációhoz a $+1$ és -1 számok egyikét rendeli úgy, hogy minden csere előjele -1. Megállapítottuk, hogy diszjunkt ciklusok szorzatának előjele pontosan akkor páros, ha a szorzatban páros sok páros hosszú ciklus szerepel. A páros permutációk száma fele az összes permutációkénak, ezek az A_X alternáló csoportot alkotják.

A komplex egységgyököknél már megismert rend fogalmát tetszőleges csoportra általánosítottuk. Egy g csoportelem rendje a különböző hatványainak a száma. Ha ez végtelen, akkor g bármely két egész kitevőjű hatványa különböző. Ha egy véges d szám, akkor g hatványai d szerint periodikusan ismétlődnek. Egy diszjunkt ciklusokra bontott permutáció rendje a benne szereplő ciklusok hosszainak legkisebb közös többszöröse.

Egy csoportot ciklikusnak neveztünk, ha egy elemének hatványaiból áll. Leírtuk a ciklikus csoportok elemeinek rendjeit, és összes részcsoportjaikat, amelyek mind ciklikusak. Megmutattuk, hogy minden ciklikus csoport kölcsönösen egyértelmű, művelettartó megfeleltetésben áll (azaz *izomorf*) a $\mathbb{Z}^+$ és a $\mathbb{Z}_n^+$ csoportok valamelyikével. Beláttuk, hogy minden véges test multiplikatív csoportja ciklikus.

Ezután a részcsoportok általános tanulmányozásába kezdtünk. Bevezettük a komplexusszorzás fogalmát, amely többek között az elemekkel való számolások lerövidítésére, tömör megfogalmazására alkalmas. Egy H részcsoport szerinti bal oldali mellékosztály az aH halmaz, megmutattuk, hogy két ilyen vagy diszjunkt, vagy egyenlő, és ezért ezek a halmazok a csoport egy partícióját adják. E mellékosztályok száma a H részcsoport indexe. Következményként kaptuk Lagrange tételét, amely szerint egy véges csoportban minden részcsoport és minden elem rendje osztója a csoport rendjének. A bizonyításban felhasznált technikai segédeszköz az ekvivalencia-reláció fogalma volt.

Ha adott egy csoport egy X részhalmaza, akkor az X-et tartalmazó legszűkebb részcsoportot az X által generált részcsoportnak neveztük. Ez mindig létezik, mint az X-et tartalmazó részcsoportok metszete. Elemei az X elemeiből és ezek inverzeiből készített szorzatok. Ha a csoport kommutatív, akkor minden ilyen szorzat egy egész együtthatós „lineáris kombinációvá" egyszerűsödik.

Két csoport között a művelettartó leképezéseket homomorfizmusoknak hívjuk. Ezek képe, vagyis értékkészlete mindig részcsoport, magja azokból az elemekből áll, amelyek az egységelembe képződnek. A homomorfizmusok magjai a normálosztók. Ezek pontosan azok a részcsoportok, amelyek szerinti bal és jobb oldali mellékosztályok megegyeznek. Ezek a mellékosztályok maguk is csoportot alkotnak, amelyben a szorzást reprezentánselemek segítségével végezhetjük el. Ahhoz, hogy ez a definíció helyes legyen, meg kellett mutatni, hogy a szorzat nem függ a reprezentánselemek választásától. Így kaptuk a normálosztó szerinti faktorcsoportot, amely az eredeti csoportnak homomorf képe a természetes homomorfizmusnál. A faktorcsoportok részcsoportjait és normálosztóit leírtuk az eredeti csoport részcsoportjai és normálosztói segítségével (4.5.19. Tétel). Következményként adódott az első és második izomorfizmus-tétel.

Az S_X szimmetrikus csoport részcsoportjait permutációcsoportnak neveztük. Ennek általánosításaként definiáltuk egy G csoport hatását egy X halmazon. Az $x \in X$ orbitja azokból az X-beli pontokból áll, ahová x elvihető G egy elemével, az x stabilizátora pedig azon G-beli elemekből álló részcsoport, amelyek az x elemet önmagába viszik. Az orbit elemszáma (hossza) pontosan a stabilizátor indexe lesz. Ez az észrevétel lehetővé teszi alakzatok, például a kocka szimmetriáinak megszámolását. Az orbitok az X halmaz egy partícióját alkotják. Röviden megemlítettük a hatás magjának, és az ekvivalens hatásnak a fogalmát is.

A csoportok szerkezetét le szeretnénk írni izomorfia erejéig. Megállapítottuk, hogy a prímrendű csoportok pontosan azok, amelyeknek nincs nemtriviális részcsoportja (egyben a kommutatív egyszerű csoportok), és mind ciklikusak. Osztályoztuk a négyelemű csoportokat is, ebből kétféle van, a ciklikuson kívül az úgynevezett Klein-csoport, amelynek

felírtuk a szorzástábláját (az úgynevezett Cayley-táblázatot). Ez a táblázat azonban már kis elemszámú csoportok, például a nyolcelemű kvaterniócsoport bevezetésére sem igazán alkalmas a hatalmas számolási igény miatt. A Cayley-táblázat sorai permutációk, és ebből beláttuk Cayley tételét, miszerint minden véges csoport izomorf egy permutációcsoporttal. Általánosításként megvizsgáltuk egy csoport hatását egy részcsoport szerinti bal mellékosztályok halmazán.

Következő célunk az volt, hogy eszközöket találjunk normálosztók keresésére. A legfontosabb ezek között a csoport önmagán való hatása konjugálás segítségével: a g-vel való konjugálás az x elemet gxg^{-1}-be viszi. Ezek a leképezések a csoportnak önmagával való izomorfizmusai, azaz (belső) automorfizmusok. Az orbitok a csoport konjugált osztályai. Nevezetes tény, hogy egy részcsoport akkor és csak akkor normálosztó, ha konjugált osztályok egyesítése. Az x elem stabilizátora ennél a hatásnál az x-szel felcserélhető elemekből áll, neve az x centralizátora. Így egy konjugált osztály elemszáma az elemei centralizátorainak indexe. Alkalmazásként leírtuk az S_4 és A_4 csoportok normálosztóit, és megállapítottuk, hogy A_5 egyszerű csoport, vagyis csak a két triviális normálosztója van.

Egy G csoport automorfizmusai csoportot alkotnak a kompozícióra, amelyben a belső automorfizmusok csoportja normálosztó. Karakterisztikusnak neveztük azokat a részcsoportokat, amelyek minden automorfizmusra zártak. Egy normálosztó normálosztója általában nem normálosztó az eredeti csoportban, de egy normálosztó karakterisztikus részcsoportja már igen.

Speciális normálosztó, sőt karakterisztikus részcsoport a csoport centruma, amely az összes elemmel felcserélhető elemekből áll, másképp fogalmazva az egyelemű konjugált osztályok egyesítése. Ennek minden részcsoportja is kommutatív normálosztó. Ugyancsak karakterisztikus részcsoport a csoport kommutátor-részcsoportja: a legszűkebb olyan normálosztó, amely szerinti faktor kommutatív. Egy H részcsoport normalizátora a legbővebb olyan részcsoport, amelyben H normálosztó, és azokból az elemekből áll, amelyek H-t önmagába konjugálják. Így H konjugáltjainak száma a normalizátorának az indexe. Hasznos észrevétel, hogy minden kettő indexű részcsoport normálosztó.

Az egyik legfontosabb mód, ahogyan csoportokból újabb csoportot tudunk készíteni, a direkt szorzat, amelynek alaphalmaza a csoportok Descartes-szorzata, a műveletet pedig komponensenként végezzük. Azt, hogy egy csoportot direkt szorzatra lehet-e bontani, speciális normálosztók létezésének vizsgálatával dönthetjük el. Például a két tényezős direkt felbontásoknak olyan A és B normálosztók felelnek meg, ahol AB az egész csoport, $A \cap B$ pedig csak az egységelemből áll. Ha itt B-ről csak annyit teszünk fel, hogy részcsoport, akkor A és B nem határozza meg az egész csoport szerkezetét, mint a direkt szorzat esetében, hanem azt is meg kell mondanunk, hogy hogyan hat B konjugálással az A normálosztón. Ebből származik a szemidirekt szorzat fogalma. A direkt szorzat legfontosabb alkalmazása a véges Abel-csoportok alaptétele, miszerint minden véges Abel-csoport felbontható prímhatvány rendű ciklikus csoportok direkt szorzatára, és a felbontásban szereplő tényezők rendjei egyértelműen meghatározottak. A direkt szorzatban könnyű számolni, például az elemek rendjei a tényezők rendjeinek legkisebb közös többszörösei. Ez az észrevétel,

és a $\mathbb{Z}_n^\times$ csoport direkt felbontásainak vizsgálata számelméleti szempontból is fontos, mert lehetővé teszi annak eldöntését, hogy van-e primitív gyök egy adott modulusra nézve.

A szabad csoport a legáltalánosabb csoport abban az értelemben, hogy minden más csoport ennek homomorf képeként kapható (ugyanakkor a Nielsen–Schreier-tétel szerint egy szabad csoport minden részcsoportja szintén szabad). Úgy konstruálhatjuk, hogy veszünk egy X halmazt, a szabad generátorok halmazát, és ezekből, valamint inverzeikből egymás mellé írással szavakat képezünk. Ezek között a szavak között további összefüggéseket is megkövetelhetünk, úgynevezett definiáló relációkat. Ekkor a szabad csoportnak egy faktorcsoportját kapjuk. Az így megadott csoportokban szerencsés esetben könnyű számolni, de még ekkor is vigyáznunk kell arra, hogy nincsenek-e a generátorokból készített szavak között „rejtett" összefüggések. Általában azonban megoldhatatlan probléma két szóról eldönteni, hogy az adott relációk segítségével egymásba alakíthatók-e.

A konstrukciós módszerek tárgyalásának lezárása után visszatértünk a csoportok szerkezetének felderítésére. Ha p prím, akkor a p-hatvány rendű csoportokat p-csoportnak neveztük. Ezek szerkezete lényegesen szebb, mint az általános csoportoké. A konjugált osztályok vizsgálatával kiderült, hogy egy véges, nem egyelemű p-csoport centruma sem állhat csak az egységelemből, és a rá vett faktor csak akkor lehet ciklikus, ha a csoport kommutatív. Ebből adódott, hogy prímnégyzet rendű csoport mindig kommutatív, és izomorfia erejéig csak két ilyen csoport van. Beláttuk azt is, hogy egy p-csoportban minden valódi részcsoport normalizátora nagyobb önmagánál, és minden maximális részcsoport egy prímindexű normálosztó. Megkonstruáltuk a két nemkommutatív, p^3 rendű csoportot is.

A Lagrange-tételt nem lehet úgy általánosítani, hogy ha d osztja a G csoport rendjét, akkor G-ben van d rendű részcsoport. Igaz ez az állítás azonban akkor, ha d prímhatvány. Egy G csoport p-Sylow részcsoportjai azok a részcsoportok, amelyek rendje p-hatvány, indexe pedig nem osztható p-vel. Sylow tétele azt mondja ki, hogy adott p mellett ezek száma kongruens 1-gyel modulo p (tehát van ilyen rendű részcsoport), továbbá hogy a p-Sylow részcsoportok egymás konjugáltjai. Speciálisan ha egy p prím osztja egy csoport rendjét, akkor abban van p rendű elem.

Mivel egy p-Sylow részcsoport konjugáltjainak száma a normalizátorának az indexe, ez számelméleti összefüggéseket ad a p-Sylow részcsoportok számára. Ennek alkalmazásaként sok adott rendű csoportról eldönthető, hogy nem lehet egyszerű. Ilyenek például azok a csoportok, amelyek rendje két prím szorzata. Áttekintettük a legfeljebb 15 elemű csoportok szerkezetét, és kimondtuk, hogy a legkisebb nemkommutatív egyszerű csoport az A_5. A kis elemszámú csoportokat a 757. oldalon foglaltuk össze.

Hogy további egyszerű csoportokat találjunk, a permutációcsoportok elméletét fejlesztettük tovább. Egy permutációcsoportot k-tranzitívnak hívunk, ha bármely k különböző pontot bármely k különböző pontba el tud vinni a csoport egy alkalmas eleme. Az S_n és A_n csoportokon kívül ezek igen ritkák: a véges egyszerű csoportok klasszifikációjából következik, hogy nincs más 6-tranzitív permutációcsoport. Példát mutattunk 3-tranzitív csoportra törtlineáris leképezések, illetve egy kételemű test feletti vektortéren ható affin transzformációk segítségével.

A 2-tranzitivitásnál kicsit gyengébb feltevés az, hogy a csoport primitív legyen. Ez azt jelenti, hogy a hatás tranzitív, és nincs nemtriviális kongruenciája. A primitív csoportok azok a tranzitív csoportok, amelyekben minden stabilizátor maximális részcsoport. Ezt a fogalmat felhasználtuk annak bizonyítására, hogy az A_n alternáló csoport egyszerű, ha $n \geq 5$. Röviden szó esett Frobenius-csoportokról és Frobenius tételéről is.

A Galois-elméletről szóló fejezetben fontos szerepet kapnak majd a feloldható csoportok, vagyis azok, amelyek kommutatív csoportokból bővítések egymásutánjával kaphatók (másképp fogalmazva nem tartalmaznak nemkommutatív egyszerű csoportot egy részcsoport homomorf képeként sem). Technikailag ezt a fogalmat a normálláncok vizsgálatával kezeltük. Beláttuk Jordan és Hölder tételét, miszerint egy véges csoportot bárhogyan is bontunk le egyszerű csoportok bővítéseire, a kapott egyszerű csoportok mindig ugyanazok lesznek. Az S_n szimmetrikus csoport akkor és csak akkor feloldható, ha $n \leq 4$. Minden véges Abel-csoport és véges p-csoport feloldható. Ennél nehezebb Burnside tétele, miszerint egy nem feloldható véges csoport rendjének legalább három különböző prímosztója van. Még sokkal nehezebb belátni a Feit–Thompson-tételt, ami azt állítja, hogy minden páratlan rendű véges csoport feloldható. A feloldható csoportok körében érvényesek a Hall-tételek, amelyek a Sylow-tételeket általánosítják. Bizonyításuk eszköze a Schur–Zassenhaus-tétel.

Végezetül meséltünk kicsit a véges egyszerű csoportok klasszifikációjával kapcsolatos eredményekről (melyek bizonyítása az emberiség egyik csúcsteljesítménye). Szó esett a projektív speciális lineáris csoportokról, amelyek az alternáló csoportok sorozatához hasonlóan szintén véges sok kivétellel egyszerűek. Ilyen sorozatból összesen 17 van, és ezen kívül még van 26 úgynevezett sporadikus egyszerű csoport. Megemlítettünk néhány nevezetes problémát, amit csak a klasszifikáció segítségével sikerült megoldani.

A 8.12. Ábrán (473. oldal) néhány csoportelméleti fogalom egymáshoz való viszonyát ábrázoltuk, konkrét példákkal illusztrálva.

5. GYŰRŰK

Ti víz lakói, bölcs leányok,
kik búsan éltek a mélyben,
most újra vigadjatok.
Hő vágyatok ím teljesül:
tisztuljon meg a vértől a gyűrű. [...]
Ti odalenn oldjátok fel,
hogy újból a Rajna kincse legyen.

Richard Wagner: *A Nibelung gyűrűje*
(Blum Tamás fordítása)

A gyűrűelmélet az algebrának a csoportelmélettel egyenrangúan fontos ága. Olyan területeken alkalmazzák, mint a geometria (ahol görbék, felületek viselkedését értik meg az *algebrai geometria* keretében), és a számelmélet (az *algebrai számelmélet* elsősorban bizonyos komplex számok szerkezetét, és ezzel diofantoszi egyenletek megoldhatóságát vizsgálja). Wiles híres bizonyítása, amit a Fermat-sejtésre adott, gyűrűelméleti eszközöket is használ. A nemkommutatív gyűrűk elméletének fontos alkalmazásai vannak a csoportelméletben (a már említett reprezentációelmélet ezeken alapszik). Vizsgálnak nem asszociatív gyűrűket is: a Lie-algebrák elmélete szorosan kapcsolódik a differenciálgeometriához.

A gyűrűkről mindennek ellenére kevesebbet fogunk beszélni, mint korábban a csoportokról. Ennek okai sokrétűek. Egyrészt az alapvető fogalmakat már megtanultuk, részben a polinomok elméleténél, részben a csoportelmélet kapcsán. Másrészt a következő fejezetben végig speciális gyűrűkkel: testekkel fogunk foglalkozni, és az azutáni fejezetben következő moduluselmélet is a gyűrűelmélet részének tekinthető. Végül könyvünk csak bevezetés az absztrakt algebrába, keretei csak *egy* elmélet széles alapokkal rendelkező, viszonylag mélyebbre hatoló bemutatását teszik lehetővé, és itt a csoportelméletre esett a választásunk. Feltételezzük, hogy az Olvasó lassan elég absztrakt algebrai tapasztalatot szerez ahhoz, hogy a következő lépcsőfokra már más, haladóbb szakkönyvek segítségével is fölléphessen. Ilyen magyar nyelvű tankönyv például Fried Ervin [**13**] műve.

Mindezek okán ebben a fejezetben csak azt mutatjuk be, ami a későbbiek megértéséhez szükséges, vagy a korábbi témák befejezésének tekinthető. Ezért szó lesz majd a számelmélet alaptételének általános bizonyításáról, illetve a számfogalom lezárásáról. A fenti alkalmazásokról csak egy rövid kitekintés formájában emlékezünk meg.

Ennek a fejezetnek az anyaga néhány helyen átfedi azt, ami Freud Róbert és Gyarmati Edit [**11**] könyvének utolsó, tizenegyedik fejezetében szerepel. Vannak eredmények, amelyek bizonyítása mindkét helyen olvasható, a [**11**] könyvben sokszor nagyon elemien és részletesen. Ez lehetővé tette számunkra, hogy ugyanezeket az állításokat hangsúlyozottan algebrai szemlélettel (és néhol a könyvünk korábbi részében megszokottnál kevésbé elemien) bizonyítsuk be. Az Olvasónak igen melegen ajánljuk, hogy vesse össze ezeket a bizonyításokat a két könyvben, mert így jobban megértheti a mögöttük húzódó algebrai és számelméleti gondolatokat. Ugyancsak ajánlatos a közös témakörökhöz tartozó feladatokat is megnézni (és megoldani) a [**11**] könyvben.

A csoportelmélethez hasonlóan ebben a fejezetben is fontos példák szerepelnek, amelyek megértéséhez hasznosak az elemi lineáris algebrai ismeretek. Ezek az 5.9. Szakasztól kezdve nélkülözhetetlenek, sőt itt használjuk a test fölötti algebra, és mátrixok minimálpolinomjának a fogalmát is.

5.1. Részgyűrű, ideál, direkt szorzat

A 2.2. Szakaszban már megismerkedtünk a gyűrű fogalmával. Megtanultuk az elemi számolási szabályokat (például, hogy bármely elemet nullával szorozva nullát kapunk). Számelméleti jellegű vizsgálatokban „szokásos", azaz nullosztómentes, kommutatív és egységelemes gyűrűket tekintettünk.

Szó volt részgyűrűkről is, és láttuk, hogy az R gyűrű egy részhalmaza akkor és csak akkor részgyűrű, ha nem üres, zárt az összeadásra, az ellentettképzésre és a szorzásra. Így részgyűrűk metszete is mindig részgyűrű. Ez azt jelenti, hogy gyűrűk esetén is beszélhetünk a generált részgyűrű fogalmáról.

5.1.1. Definíció. Legyen R gyűrű és $X \subseteq R$. Ekkor az X által *generált részgyűrű* R-ben a legszűkebb olyan részgyűrűje R-nek, amely X-et tartalmazza. Jele $\langle X \rangle$.

A generált részgyűrű mindig létezik, mint az X-et tartalmazó részgyűrűk metszete (lásd 4.4.26. Állítás), és persze most is tudjuk, hogy tetszőleges $S \leq R$ részgyűrű esetén

$$X \subseteq S \implies \langle X \rangle \subseteq S\,.$$

A lineáris algebrában és a csoportelméletben fontos volt, hogy a generált rész elemeit le tudtuk írni lineáris kombinációkkal, illetve a 4.4.27. Tételben megadott módon. Gyűrűk esetében csak egy speciális esetet tárgyalunk, mert ez megmutatja, hogy miért is nagyon természetes dolog a polinom fogalma.

5.1.2. Állítás. *Tegyük föl, hogy R kommutatív, egységelemes gyűrű és $r_1, \ldots, r_n \in R$. Ekkor*

$$\langle r_1, \ldots, r_n \rangle = \{p(r_1, \ldots, r_n) \,:\, p \in \mathbb{Z}[x_1, \ldots, x_n],\, p(0, \ldots, 0) = 0\}\,.$$

Bizonyítás. Jelölje S a jobb oldalon álló halmazt. A $p(0,\dots 0) = 0$ feltétel azt jelenti, hogy p-nek nincs konstans tagja. Ezért $p(r_1,\dots,r_n)$ megkapható az $r_1,\dots,r_n$ elemekből összeadás, kivonás és szorzás segítségével (voltaképpen ez a polinom definíciója), vagyis eleme $\langle r_1,\dots,r_n\rangle$-nek. Tehát $S \subseteq \langle r_1,\dots,r_n\rangle$.

A másik irányú tartalmazás bizonyításához vegyük észre, hogy S részgyűrű. Valóban, $0 \in S$, és ha p és q konstans tag nélküli polinomok, akkor $p \pm q$ és pq is ilyenek. A 2.6.9. Gyakorlathoz hasonlóan láthatjuk, hogy

$$p(r_1,\dots,r_n) \pm q(r_1,\dots,r_n) = (p \pm q)(r_1,\dots,r_n) \in S$$

és

$$p(r_1,\dots,r_n)q(r_1,\dots,r_n) = (pq)(r_1,\dots,r_n) \in S\,,$$

vagyis S tényleg részgyűrű. Az x_i polinom mutatja, hogy $r_i \in S$ minden i-re. Tehát S olyan részgyűrű, amely az $r_1,\dots,r_n$ elemeket tartalmazza, és ezért tartalmazza az a legszűkebb ilyen részgyűrűt is, vagyis $\langle r_1,\dots,r_n\rangle \subseteq S$. □

A 2.2. Szakaszban a gyűrű-homomorfizmus fogalmát is megismertük. Ha R és S gyűrűk, akkor $\varphi : R \to S$ gyűrű-homomorfizmus, ha tetszőleges $r_1, r_2 \in R$ esetén

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \quad \text{és} \quad \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)\,.$$

Izomorfizmusnak most is azokat a homomorfizmusokat nevezzük, amelyek bijektívek is.

Gyűrű-izomorfizmust kaptunk például, amikor a komplex számok precíz bevezetésekor (1.6. Szakasz) az $(a, 0)$ rendezett párhoz hozzárendeltük az a valós számot. Az $\mathbb{R}[x][y]$ és $\mathbb{R}[y][x]$ gyűrűk is izomorfak. Később kevésbé triviális példákat is fogunk látni.

A fenti definíció szerint $\varphi : R^+ \to S^+$ egy csoport-homomorfizmus R és S additív csoportjai között, ami a szorzás műveletét is tartja. Ebből következik, hogy mindazokat a fogalmakat és tételeket felhasználhatjuk, amelyek csoportok közötti homomorfizmusokról szólnak. Például a nullelem képe a nullelem, ellentett képe ellentett lesz.

5.1.3. Definíció. Ha $\varphi : R \to S$ egy gyűrű-homomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(r) \mid r \in R\} \subseteq S$$

a φ *képe* (vagyis a φ függvény értékkészlete).

A 4.5.3. és 4.5.4. Gyakorlatokhoz hasonlóan látjuk, hogy $\mathrm{Im}(\varphi)$ részgyűrű R-ben, és hogy egy homomorfizmus képéről nem mondhatunk többet annál, mint hogy részgyűrű, mert S minden részgyűrűje előáll alkalmas S-be vezető homomorfizmus képeként.

5.1.4. Definíció. Ha $\varphi : R \to S$ egy gyűrű-homomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{r \in R \,:\, \varphi(r) = 0_S\} \subseteq R$$

a φ *magja*. Itt 0_S az S gyűrű nulleleme.

Ha például $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ az a gyűrű-homomorfizmus, amely minden egész számhoz az n-nel való osztási maradékát rendeli (1.1.7. Feladat), akkor φ magja az n-nel osztható egészekből álló ideál $\mathbb{Z}$-ben. Ha viszont $\varphi : \mathbb{R}[x] \to \mathbb{C}$ az a homomorfizmus, amely az f polinomhoz az $f(i)$ értéket rendeli (az „i behelyettesítése"), akkor ennek magja azokból a polinomokból áll, amelyeknek az i gyöke (vagy másképp fogalmazva, azokból, amelyek $x^2 + 1$-gyel oszthatók, lásd a 4.5.22. Gyakorlat (5) pontját).

Tudjuk, hogy csoporthomomorfizmus magja normálosztó, de mivel R additív csoportja Abel-csoport, ez semmivel sem mond többet annál, mint hogy $\mathrm{Ker}(\varphi)$ részcsoport R^+-ban. Ahhoz, hogy a gyűrű-homomorfizmusok magjait jellemezhessük, persze a szorzást is figyelembe kell venni.

Jelölje I a $\mathrm{Ker}(\varphi)$ részcsoportot. Ha $a \in I$ és $r \in R$, akkor $\varphi(a) = 0$, ezért

$$\varphi(ar) = \varphi(a)\varphi(r) = 0\varphi(r) = 0\,.$$

Így $ar \in I$. Ugyanígy igazolhatjuk, hogy $ra \in I$. Ezzel beláttuk az alábbi tétel egyik irányát.

5.1.5. Tétel. *Az R gyűrű egy I részhalmaza akkor és csak akkor magja egy alkalmas, R-en értelmezett gyűrű-homomorfizmusnak, ha részcsoport R-ben az összeadásra nézve, és tetszőleges $a \in I$ és $r \in R$ esetén $ar, ra \in I$.*

A tétel másik irányát csoportokra a faktorcsoport bevezetésével igazoltuk. Ennek megfelelően most a faktorgyűrű fogalmát kell bevezetnünk. Ezt, tehát a tétel bizonyításának másik felét is, a következő szakaszban mutatjuk be, mert előbb az ideálok elemi tulajdonságaival ismerkedünk meg.

5.1.6. Definíció. Egy R gyűrű egy I részhalmazát *balideálnak* nevezzük, ha részcsoport, és tetszőleges $a \in I$, $r \in R$ esetén $ra \in I$. Hasonlóképpen I *jobbideál*, ha részcsoport, és tetszőleges $a \in I$, $r \in R$ esetén $ar \in I$. Az I (kétoldali) *ideál*, ha bal- és jobbideál is egyúttal. Azt, hogy I ideál R-ben, $I \lhd R$ jelöli.

5.1.7. Feladat. Adjunk példát olyan balideálra (alkalmas gyűrűben), amely nem jobbideál.

Az előző tétel szerint tehát a gyűrű-homomorfizmusok magjai pontosan az ideálok. Nyilván minden balideál és minden jobbideál részgyűrű is egyben. Az ideálokra (balideálokra, jobbideálokra) is használjuk a részcsoportoknál megszokott jelzőket, tehát $\{0\}$ és R az R gyűrű *triviális ideáljai*, és I *valódi ideál*, ha $I \neq R$.

5.1.8. Definíció. Tegyük föl, hogy X részhalmaza az R gyűrűnek. Az R legszűkebb, X-et tartalmazó ideálját az X által *generált ideálnak* nevezzük. Hasonlóképpen beszélhetünk az X által generált balideálról és jobbideálról is.

Ez a definíció azért értelmes, mert R ideáljainak a metszete is ideál R-ben, és így az X által generált ideál létezik, mint az X-et tartalmazó ideálok metszete. A korábbiak során már több ízben adtunk képletet a generált részstruktúra elemeire. Ezt ideálokra csak egy speciális esetben végezzük el (az általánosabb képletekre nézve lásd az 5.1.14. és az 5.1.15. Gyakorlatokat).

5.1.9. Állítás. *Legyen R egységelemes gyűrű, és $s_1, \ldots, s_n \in R$. Ekkor az $s_1, \ldots, s_n$ által generált balideál elemei az*

$$r_1 s_1 + \ldots + r_n s_n$$

alakú kifejezések, ahol $r_i \in R$.

Bizonyítás. Ez a képlet nagyon emlékeztet a 4.4.20. Állításban szereplőre, és a bizonyítás is teljesen hasonló. Meg kell mutatni, hogy a fenti elemek balideált alkotnak, mely az $s_1, \ldots, s_n$ elemeket tartalmazza, és megfordítva, hogy a fenti elemek benne vannak minden olyan balideálban, amely az $s_1, \ldots, s_n$ elemeket tartalmazza. A részletek kidolgozását az Olvasóra bízzuk. □

Ha az R gyűrű kommutatív, akkor a balideálok, a jobbideálok és az ideálok ugyanazok lesznek. Ezért ha R egységelemes is, akkor az előző állítás a generált ideálokat írja le. Vezessünk be jelölést a most kapott generált ideálokra!

5.1.10. Definíció. Legyen R kommutatív, egységelemes gyűrű, és $s_1, \ldots, s_n \in R$. Ekkor

$$(s_1, \ldots, s_n) = \{r_1 s_1 + \ldots + r_n s_n \,:\, r_i \in R\}$$

jelöli az $s_1, \ldots, s_n$ elemek által generált ideált. Speciálisan (s)-et, vagyis az s elem összes többszöröseinek a halmazát az s által generált *főideálnak* nevezzük. Egy ideál tehát akkor főideál, ha egy elemmel generálható.

5.1.11. Gyakorlat. Mutassuk meg, hogy a $\mathbb{Z}$ gyűrűben $(12, 18) = (6)$.

A $\mathbb{Z}$ gyűrűben az n többszöröseinek halmazára az (n) helyett korábban az $n\,\mathbb{Z}$ jelölést alkalmaztuk. Általában ha R gyűrű és $s \in R$, akkor legyen

$$Rs = \{rs \,:\, r \in R\} \quad \text{és} \quad sR = \{sr \,:\, r \in R\}\,.$$

Egységelemes R esetén tehát Rs az s által generált balideál, sR pedig az s által generált jobbideál. Ha még R ezenfelül kommutatív is, akkor $Rs = sR = (s)$.

Mindez felveti azt, hogy egy gyűrűben értelmezünk-e komplexus-szorzást (hiszen az Rs így is értelmezhető lenne). A válasz az, hogy igen, de úgy, hogy a komplexus-szorzat lehetőleg részcsoport is legyen. Ezért ha A és B részhalmazai egy R gyűrűnek, akkor az AB-be nemcsak az ab alakú szorzatokat szokás bevenni (ahol $a \in A$ és $b \in B$), hanem ezek véges összegeit is. Az Rs alakú szorzatoknál ez nem számít, mert a tagok összevonhatók, vagyis a fenti jelöléseket továbbra is használhatjuk.

5.1.12. Definíció. Legyen R gyűrű és A, B az R-nek részhalmazai. Ekkor az A és B *komplexus-összegét* az R additív csoportjában értjük, tehát

$$A + B = \{a + b \,:\, a \in A, b \in B\}\,,$$

az A és B *komplexus-szorzata* pedig

$$AB = \{a_1 b_1 + \ldots + a_n b_n \,:\, a_i \in A, b_i \in B, n \text{ nemnegatív egész}\}\,.$$

Ha A és B egyike zárt az ellentettképzésre (például egyoldali ideál, vagy részgyűrű), akkor tehát az AB komplexus-szorzat részcsoport.

5.1.13. Gyakorlat. Mutassuk meg, hogy ha R gyűrű, és I, J ideálok R-ben, akkor az IJ komplexusszorzat is ideál.

5.1.14. Gyakorlat. Legyen R tetszőleges gyűrű, és $s_1, \ldots, s_n \in R$. Mutassuk meg, hogy az $X = \{s_1, \ldots, s_n\}$ által generált balideál elemei az

$$m_1 s_1 + \ldots + m_n s_n + r_1 s_1 + \ldots + r_n s_n$$

alakú kifejezések, ahol $m_i \in \mathbb{Z}$ és $r_i \in R$. Hogyan változik ez a képlet, ha X végtelen halmaz?

5.1.15. Gyakorlat. Legyen R egységelemes gyűrű, és $X \subseteq R$. Bizonyítsuk be, hogy az X által generált (kétoldali) ideál elemei az rxs alakú elemekből képzett véges összegek, ahol $r, s \in R$ és $x \in X$ (ugyanazon x-hez az összegben több ilyen tag is szerepelhet). Hogyan változik ez a képlet, ha R-ről nem tesszük föl, hogy egységelemes?

A szakasz hátralévő részében gyűrűk direkt szorzatával ismerkedünk meg.

5.1.16. Definíció. Legyenek $R_1, \ldots, R_n$ tetszőleges gyűrűk, és tekintsük az additív csoportjaik R direkt szorzatát. Definiáljuk ezen a szorzást komponensenként:

$$(r_1, \ldots, r_n)(s_1, \ldots, s_n) = (r_1 s_1, \ldots, r_n s_n)\,.$$

A kapott R gyűrűt az $R_1, \ldots, R_n$ gyűrűk *direkt szorzatának* nevezzük, és $R_1 \times \ldots \times R_n$-nel jelöljük.

Nagyon könnyű ellenőrizni, hogy a direkt szorzat gyűrű lesz, ezt az Olvasóra hagyjuk. Természetesen végtelen sok gyűrű direkt szorzata is definiálható a fentihez hasonló módon. Ahogy csoportok esetén a direkt szorzatot normálosztókkal jellemezhettük, most az ideálokon a sor.

Az $R \times S$ direkt szorzat esetében igen fontosak azok a π_1 és π_2 homomorfizmusok, melyekre $\pi_1(r, s) = r$ illetve $\pi_2(r, s) = s$. Ezeket, ugyanúgy, mint a csoportoknál, *projekcióknak* hívjuk. A belső jellemzés ezek magjai segítségével történik, nem meglepő hát, ha csoportoknál normálosztókat, gyűrűknél ideálokat kapunk.

5.1.17. Állítás. *Legyen R_i^* az $R = R_1 \times \ldots \times R_n$ direkt szorzat azon elemeinek a halmaza, melyek i-edik komponense tetszőleges eleme R_i-nek, a többi komponensben pedig a megfelelő gyűrű nulleleme áll. Ekkor R_i^* az R_i-vel izomorf ideálja az R direkt szorzatnak, és az R_i^* ideálok teljesítik a következő tulajdonságokat:*

(1) *összegük az egész R gyűrű;*
(2) *bárhogy is veszünk $n-1$ darabot közülük, ezek összegének és a kimaradónak a metszete csak a nullelemből áll.*

Megfordítva, az ilyen tulajdonságú ideálok direkt szorzatra való felbontást adnak.

Bizonyítás. A 4.8.13. Gyakorlatban (illetve a 4.8. Szakasz korábbi részeiben) már beláttuk ezt az állítást csoportokra, speciálisan az R additív csoportjára is. Ezért most csak a szorzással kapcsolatos állításokat kell meggondolni.

Az R_i^* ideál, hiszen részcsoport, és elemei

$$(0, 0, \ldots, 0, r, 0 \ldots, 0)$$

alakúak. Ha egy ilyet egy másik elemmel megszorzunk, akkor az i-ediktől különböző komponensekben nyilván továbbra is nulla lesz. Az is világos, hogy az az $R_i^* \to R_i$ leképezés, amely a fenti elemhez r-et rendel, szorzattartó is, tehát gyűrű-izomorfizmus.

Megfordítva, tegyük föl, hogy az R gyűrűben adottak a fenti tulajdonságú R_i ideálok. Ekkor a csoportoknál tanultak miatt az R^+ csoport izomorf az R_i^+ csoportok direkt szorzatával, mégpedig úgy, hogy R minden eleme egyértelműen felírható

$$r = r_1 + \ldots + r_n$$

alakban, ahol $r_i \in R_i$ minden i-re, és a keresett izomorfizmusnál

$$r = r_1 + \ldots + r_n \leftrightarrow (r_1, \ldots, r_n)\,.$$

Azt kell ellenőrizni, hogy ez a megfeleltetés szorzattartó is.

Csoportokra ezt az biztosítja, hogy ha N és K normálosztók metszete csak az egységelem, akkor N minden eleme felcserélhető K minden elemével (lásd 4.7.27. Gyakorlat). Most az ezzel analóg állítást igazoljuk.

5.1.18. Lemma. *Legyenek I és J ideálok az R gyűrűben, melyek metszete csak a nullelemből áll. Ha $a \in I$ és $b \in J$, akkor $ab = 0$.*

Bizonyítás. Az ab eleme I-nek, hiszen $a \in I$ és $b \in R$. Ugyanígy ab eleme J-nek is, hiszen $b \in J$ és $a \in R$. Ezért $ab \in I \cap J = \{0\}$, tehát $ab = 0$. □

A tétel bizonyítására visszatérve tegyük föl, hogy

$$r = r_1 + \ldots + r_n \quad \text{és} \quad s = s_1 + \ldots + s_n\,.$$

A művelettartáshoz azt kell belátni, hogy

$$rs = r_1 s_1 + \ldots + r_n s_n\,.$$

Tudjuk, hogy $i \neq j$ esetén $R_i \cap R_j = \{0\}$ (sőt egy ennél erősebb feltételünk van). Ezért a lemma miatt $r_i s_j = 0$ ha $i \neq j$. Így a fenti két egyenletet összeszorozva pont az állítás adódik. □

Gyakorlatok, feladatok

5.1.19. Gyakorlat. Adjunk példát olyan $\varphi : R \to S$ nem azonosan nulla gyűrűhomomorfizmusra két egységelemes gyűrű között, amely az egységelemet nem az egységelembe viszi. Lehet-e φ szürjektív? Van-e olyan példa, ahol az S gyűrű nullosztómentes?

5.1.20. Gyakorlat. Mutassuk meg, hogy két test közötti gyűrű-izomorfizmus mindig „test-izomorfizmus" is, vagyis az (ellentett és) inverz képzését is tartja.

5.1.21. Gyakorlat. Mikor lesz két gyűrű direkt szorzata nullosztómentes?

5.1.22. Gyakorlat. Igazoljuk, hogy ha m és n relatív prím pozitív egészek, akkor $\mathbb{Z}_{nm}$ izomorf $\mathbb{Z}_n \times \mathbb{Z}_m$-mel (az additív csoportjaikra ezt beláttuk a 4.8.8. Következményben).

5.1.23. Gyakorlat. Mutassuk meg, hogy a $\mathbb{Z}$ és $\mathbb{Z}_n$ gyűrűkben minden részcsoport részgyűrű, sőt ideál.

5.1.24. Gyakorlat. Adjunk példát olyan részgyűrűre az $\mathbb{Z}[x]$ polinomgyűrűben, amely nem ideál, de tartalmaz minden n-re n-edfokú polinomot.

5.1.25. Gyakorlat. Jelölje R a $\mathbb{Z}[x]$ polinomgyűrű azon polinomjainak részgyűrűjét, amelyek konstans tagja nulla, és legyen S tetszőleges gyűrű, melyben rögzítünk egy s elemet. Mutassuk meg, hogy az a $\varphi : R \to S$ leképezés, amely a $p(x) = a_1x + \ldots + a_nx^n$ polinomhoz az $a_1r + \ldots + a_nr^n \in S$ elemet rendeli, gyűrűhomomorfizmus. Ennek neve az s *behelyettesítése*.

5.1.26. Gyakorlat. Igazoljuk, hogy ha $p \in \mathbb{R}[x]$ nem nulla polinom, akkor a p és az 1 által generált részgyűrű izomorf $\mathbb{R}[x]$-szel.

5.1.27. Gyakorlat. Legyen R tetszőleges gyűrű. Igazoljuk, hogy az $R^+ \times \mathbb{Z}^+$ csoport az $(r, n)(s, m) = (rs + mr + ns, nm)$ szorzásra nézve egységelemes gyűrű, melyben az $(r, 0)$ alakú elemek R-rel izomorf részgyűrűt alkotnak. Ezért *minden gyűrű beágyazható egységelemes gyűrűbe.*

5.1.28. Feladat. Igazoljuk, hogy ha van egységelem, akkor az összeadás kommutativitása következik a többi gyűrűaxiómából.

5.1.29. Feladat. Igazoljuk, hogy ha egy gyűrűben csak egyetlen bal oldali egységelem van, akkor ez kétoldali egységelem.

5.1.30. Feladat. Igazoljuk, hogy ha az $R \times S$ gyűrű akkor és csak akkor egységelemes, ha R és S is az, és ebben az esetben minden ideálja $I \times J$ alakú, ahol $I \lhd R$ és $J \lhd S$.

5.1.31. Feladat. Igazoljuk, hogy ha egy egységelemes gyűrűben $1 - ab$ invertálható, akkor $1 - ba$ is.

5.2. Faktorgyűrű

Ebben a szakaszban nemcsak a faktorgyűrű fogalmával ismerkedünk meg, hanem meglátjuk azt is, hogy egyes faktorgyűrűkben (például a polinomgyűrű faktoraiban) hogyan lehet jól számolni. Ez lehetővé teszi majd fontos testek konstrukcióját. Mindenek előtt bebizonyítjuk az 5.1.5. Tétel hiányzó másik felét.

Bizonyítás. Tegyük föl, hogy I ideál az R gyűrűben. Meg kell konstruálnunk egy S gyűrűt és egy $\varphi : R \to S$ homomorfizmust, amelyre $\mathrm{Ker}(\varphi) = I$. A munka nehezét már elvégeztük a 4.5.11. Tétel bizonyításában, ahol elkészíthetjük az $S = R^+/I$ faktorcsoportot, és hozzá a $\varphi : R \to S$ természetes homomorfizmust, melyről tudjuk, hogy magja I. Azt kell csak elérnünk, hogy S gyűrűvé váljon egy alkalmas szorzás bevezetésével úgy, hogy φ a szorzást is tartsa.

Az S elemei az I szerinti mellékosztályok, vagyis az $r + I$ alakú halmazok, ahol $r \in R$, és $\varphi(r) = r + I$. Tudjuk, hogy

$$r_1 + I = r_2 + I \iff r_1 - r_2 \in I\,.$$

Ha sikerül a tervünk, akkor az $r_1 + I$ és az $r_2 + I$ szorzatát csakis az

$$(r_1 + I)(r_2 + I) = r_1 r_2 + I$$

képlettel definiálhatjuk. Valóban, a bal oldalon $\varphi(r_1)\varphi(r_2)$, a jobb oldalon pedig $\varphi(r_1 r_2)$ áll, ha tehát azt akarjuk, hogy φ szorzattartó legyen, akkor ezeknek meg kell egyezniük. A kérdés az, hogy definiálhatjuk-e így az S-beli szorzást, és hogy gyűrűt kapunk-e.

Ahhoz, hogy ez a szorzás jóldefiniált, azt kell belátni (a faktorcsoportnál látott bizonyításhoz hasonlóan), hogy

$$\text{ha} \quad r_1 + I = r_1' + I \quad \text{és} \quad r_2 + I = r_2' + I\,, \quad \text{akkor} \quad r_1 r_2 + I = r_1' r_2' + I\,.$$

Az első feltétel azt jelenti, hogy $r_1 - r_1' \in I$, a második pedig, hogy $r_2 - r_2' \in I$. De akkor

$$r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I\,,$$

hiszen $r_2 - r_2' \in I$ és $r_1 \in R$ miatt $r_1(r_2 - r_2') \in I$, és hasonlóan $(r_1 - r_1')r_2' \in I$. A szorzás S-en tehát jóldefiniált. Azt, hogy S gyűrű, vagyis hogy az asszociativitás és a disztributivitás öröklődik R-ről S-re, könnyen látható, ahhoz hasonlóan, ahogy például csoportoknál a faktorcsoport asszociativitását beláttuk a 4.5.13. Gyakorlatban. Ezzel a tétel bizonyítását befejeztük. □

5.2.1. Definíció. Ha R gyűrű, és I ideál R-ben, akkor az előző tétel bizonyításában elkészített S gyűrűt az R gyűrű I szerinti *faktorgyűrűjének* nevezzük, és R/I-vel jelöljük.

A későbbi számolásokban hasznos lesz, ha rövidítést vezetünk be arra, hogy egy gyűrű két eleme ugyanazon mellékosztályban van az I ideál szerint. A számelméletben azt mondtuk, hogy $a \equiv b\ (n)$, ha $n \mid a - b$, vagyis ha $a - b$ eleme az (n) főideálnak.

5.2.2. Definíció. Ha R gyűrű és I ideál R-ben, akkor $r, s \in R$ esetén r *kongruens* s-sel modulo I, ha $r - s \in I$ (azaz ha $r + I = s + I$). Jelben $r \equiv s\ (I)$.

5.2.3. Gyakorlat. Igazoljuk, hogy a most definiált kongruenciáknak megvannak a számelméletből ismert tulajdonságai, vagyis

$$a \equiv b\ (I) \quad \text{és} \quad c \equiv d\ (I)$$

esetén

$$a + c \equiv b + d\ (I) \quad \text{és} \quad ac \equiv bd\ (I)$$

(azaz a kongruenciák összeadhatók és összeszorozhatók).

5.2.4. Gyakorlat. Mutassuk meg, hogy ha R kommutatív, illetve egységelemes, akkor minden faktorgyűrűje is ilyen. Mi lesz a faktorgyűrűben a nullelem és az egységelem?

5.2.5. Tétel [Homomorfizmus-tétel]. *Ha R és S gyűrűk, és $\varphi : R \to S$ homomorfizmus, akkor* $\operatorname{Im}(\varphi) \cong R/\operatorname{Ker}(\varphi)$.

Bizonyítás. A csoportoknál tanult homomorfizmus-tétel (4.5.15. Tétel) szerint $R/\operatorname{Ker}(\varphi)$ és $\operatorname{Im}(\varphi)$ izomorfak, mint csoportok, és ezt az izomorfizmust az a leképezés létesíti, amelynél $r + \operatorname{Ker}(\varphi)$ a $\varphi(r)$-nek felel meg. A faktorgyűrű szorzásának definíciójából világos, hogy ez a megfeleltetés a szorzást is tartja. □

Faktorgyűrűre talán a legfontosabb példa az, amikor az egész számok $\mathbb{Z}$ gyűrűjét faktorizáljuk az $(n) = n\,\mathbb{Z}$ főideál szerint (amelynek elemei az n-nel osztható egész számok). A 4.5.23. Gyakorlatban láttuk, hogy a kapott faktorcsoport izomorf $\mathbb{Z}_n^+$-szal. Valójában azonban ez gyűrű-izomorfizmus is, vagyis $\mathbb{Z}/(n) \cong \mathbb{Z}_n$. Ennek oka, hogy az a homomorfizmus, amely minden egész számhoz az n-nel való osztási maradékát rendeli, gyűrű-homomorfizmus is (lásd 1.1.7. Feladat), és a fenti homomorfizmus-tételt erre alkalmazhatjuk.

A $\mathbb{Z}/n\,\mathbb{Z}$ faktorgyűrű elemeit a számelméletben modulo n maradékosztályoknak nevezzük. Ezért a faktorgyűrűt általában is néha *maradékosztálygyűrűnek*, elemeit mellékosztály helyett maradékosztálynak hívják. Most már láthatjuk, hogy a „modulo n számolás" fogalmát miért a $\mathbb{Z}_n$ gyűrű segítségével, és miért nem maradékosztályokkal vezettük be: a maradékosztályok közötti művelet nehezebb fogalom, mint a számok közötti modulo n művelet, hiszen a jóldefiniáltságot is ellenőrizni kell.

A homomorfizmus-tételből egy másik fontos izomorfizmus is adódik. Tekintsük azt a $\varphi(f) = f(i)$ képlettel definiált leképezést, amely az $\mathbb{R}[x]$-ből $\mathbb{C}$-be képez (ez tehát az „i behelyettesítése" nevű leképezés). A 4.5.22. Gyakorlat (5) pontjában megmutattuk, hogy ez tartja az összeadást, és magja az $x^2 + 1$ polinom összes $\mathbb{R}[x]$-beli többszöröseiből áll, vagyis az $(x^2 + 1)$ főideál. A φ leképezés persze a szorzást is nyilván tartja, és ezért a homomorfizmus-tétel a következő állítást adja:

5.2.6. Állítás. $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

5.2.7. Gyakorlat. Az előző állításban megadott $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ izomorfizmusnál mi az $x + 1$, x^2, $x^3 + 3x + 7$, $bx + a$ polinomok maradékosztályainak a képe $\mathbb{C}$-ben?

5.2.8. Gyakorlat. Igazoljuk, hogy

$$\mathbb{Q}[x]/(x^3-2) \cong \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,:\, a, b, c \in \mathbb{Q}\}\,.$$

A homomorfizmus-tétel akkor alkalmazható, amikor a faktorgyűrű „már ismert", vagyis „van hová vezetni a homomorfizmust, amire alkalmazzuk". Az $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ bizonyítása tehát azért volt egyszerű, mert a komplex számokat már korábban megkonstruáltuk. Ezt az izomorfizmust azonban úgy is felfoghatjuk, hogy ha valaki még nem ismerné a komplex számokat, akkor ennek a faktorgyűrűnek a segítségével megtalálhatja őket. Ez a módszer tehát alkalmas lesz fontos testek konstruálására. Az alábbiakban az ehhez szükséges kiinduló lépéseket tesszük meg.

A faktorgyűrűben való számolás egy lehetséges útja a csoportokhoz hasonlóan az, ha alkalmas reprezentánsrendszert választunk (minden mellékosztályból egy elemet). A $\mathbb{Z}_n$ gyűrű is így származtatható, hiszen $\{0, 1, 2, \ldots, n-1\}$ egy reprezentánsrendszer az (n) főideál szerinti mellékosztályokban. A módszert érdemes megvizsgálni a polinomok példáján. Legyen T test, és $f \in T[x]$ egy nem nulla polinom, melynek foka d. Jelölje (f) az f által generált főideált, vagyis az f-fel osztható polinomok halmazát. A $T[x]/(f)$ faktorgyűrű elemei tehát a $g + (f)$ alakú mellékosztályok, és természetesen

$$g_1 + (f) = g_2 + (f) \iff g_1 - g_2 \in (f) \iff g_1 \equiv g_2 \ (f)$$

(ahol $g, g_1, g_2 \in T[x]$).

Ahogy egész számoknál az n-nel való osztási maradékok alkottak „jó" reprezentánsrendszert, most érdemes tekinteni az f-fel való lehetséges osztási maradékok halmazát. Ezek a legföljebb $d-1$ fokú polinomok (ahol d az f foka) és a nullapolinom, vagyis a

$$t(x) = r_0 + r_1 x + \ldots + r_{d-1}x^{d-1}$$

alakú polinomok, ahol $r_i \in T$. Ezek tényleg reprezentánsrendszert alkotnak, azaz a fenti kifejezésekből minden (f) szerinti mellékosztályban pontosan egy található. Valóban, ha $g \in T[x]$, akkor g-t f-fel maradékosan elosztva $g = fq + t$ adódik, ahol $t(x)$ már a fenti halmazban van, és nyilván $g - t \in (f)$, vagyis t benne van az f mellékosztályában. Ugyanakkor egyik mellékosztályban sem lehet két reprezentáns (lényegében a maradékos osztás egyértelműsége miatt): ha t_1 és t_2 is ugyanabban a mellékosztályban lenne, akkor $f \mid t_1 - t_2$, ami lehetetlen a fokszámok miatt, kivéve ha $t_1 - t_2$ a nullapolinom.

A fenti reprezentánselemeket nagyon könnyű összeadni, hiszen két ilyen elem összege

$$(r_0 + \ldots + r_{d-1}x^{d-1}) + (s_0 + \ldots + s_{d-1}x^{d-1}) = (r_0 + s_0) + \ldots + (r_{d-1} + s_{d-1})x^{d-1}$$

szintén egy reprezentánselem. A szorzás bonyolultabb, hiszen ha két reprezentánselemet összeszorzunk, akkor általában egy $d-1$-nél magasabb fokú polinomot kapunk, és így még f-fel maradékosan osztani kell, hogy a szorzat reprezentánsát megkapjuk.

Illusztrációként végezzük el a számolást a $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűben. Ekkor a reprezentánselemek az $a+bx$ alakú polinomok lesznek. Mivel $x^2+1 \equiv 0\ (x^2+1)$,

$$(a+bx)(c+dx) = ac + (ad+bc)x + bdx^2 \equiv$$
$$\equiv ac + (ad+bc)x - bd = (ac-bd) + (ad+bc)x\,.$$

Tehát $(a+bx)(c+dx)$ reprezentánsa $(ac-bd)+(ad+bc)x$, és így az $a+bx \leftrightarrow a+bi$ megfeleltetés kölcsönösen egyértelmű és művelettartó az $\mathbb{R}[x]/(x^2+1)$ és $\mathbb{C}$ között (hiszen a komplex számok összeadását és szorzását pontosan ugyanezzel a képlettel adtuk meg). Ezzel tehát újabb bizonyítást nyertünk az 5.2.6. Állításra, de immáron a komplex számok létezésének felhasználása nélkül!

A komplex számok újfajta bevezetése azonban még nem teljes, tisztáznunk kell több dolgot is, például hogy a most kapott $\mathbb{R}[x]/(x^2+1)$ faktorgyűrű miért test. Erre most egy „elemi" bizonyítást adunk. Fontos tudni azonban, hogy később olyan apparátust építünk ki, amelynek segítségével az $\mathbb{R}[x]$ összes ideálját át tudjuk majd tekinteni. A most következő állítás következik az 5.5.9. Tételből is.

5.2.9. Állítás. *Ha T test, és $f \in T[x]$ egy T fölött irreducibilis polinom, akkor $T[x]/(f)$ test.*

Bizonyítás. Azt kell megmutatni, hogy minden nem nulla $g+(f)$ mellékosztálynak van inverze. A $T[x]/(f)$ gyűrű nulleleme a $0+(f)=(f)$ mellékosztály, és így a „$g+(f)$ nem nulla" feltétel azt jelenti, hogy $g \notin (f)$, azaz hogy f nem osztója a g polinomnak. Mivel f irreducibilis, a g és f relatív prímek, a legnagyobb közös osztójuk az 1. A 3.2.6. Tétel miatt így léteznek olyan $p, q \in T[x]$ polinomok, hogy

$$1 = fp + gq\,.$$

Ezért $1+(f) = fp+gq+(f)$. De $fp \in (f)$, azaz $fp+(f)=(f)$. Így

$$1+(f) = gq+(f) = (g+(f))\,(q+(f))$$

a faktorgyűrűbeli szorzás definíciója miatt. Mivel $1+(f)$ a $T[x]/(f)$ egységeleme, ez azt jelenti, hogy $q+(f)$ inverze $g+(f)$-nek. □

A komplex számok $\mathbb{R}[x]/(x^2+1)$ alakban történő bevezetésével még mindig nem vagyunk készen. Ebben a faktorgyűrűben „meg kell találnunk" a valós számokat (annak analógiájára, ahogy a komplex számok párokkal történő bevezetésekor az $(r,0)$ párt azonosítottuk az r valós számmal), és definiálnunk kell az i számot is. Mindezt a 6.4. Szakaszban végezzük majd el.

5.2.10. Gyakorlat. Írjuk föl az $L = \mathbb{Z}_2[x]/(x^2 + x + 1)$ faktorgyűrű műveleti tábláit, és igazoljuk, hogy testet kaptunk. Keressünk benne $\mathbb{Z}_2$-vel izomorf $\{E, O\}$ résztestet (ahol E az egységelem, O a nullelem), és adjuk meg L-ben az $Ex^2 + Ex + E$ polinom gyökeit.

A csoportelméletben tanult izomorfizmus-tételek lényegében szó szerint átvihetők gyűrűkre is. A bizonyítás teljesen ugyanaz, csak azt kell észrevenni, hogy valamennyi szereplő leképezés most a szorzást is tartja. Ezért a tételeket csak kimondjuk, és a bizonyítás átgondolását az Olvasóra hagyjuk.

5.2.11. Tétel. *Tegyük föl, hogy $\varphi : R \to S$ szürjektív gyűrű-homomorfizmus, melynek magja I. Ekkor a következő állítások teljesülnek.*

(1) *Ha T tetszőleges részgyűrűje R-nek, akkor $\varphi(T)$ részgyűrűje S-nek, melynek teljes inverz képe R-ben a $T + I = I + T$ részgyűrű.*
(2) *Az S részgyűrűi kölcsönösen egyértelmű megfeleltetésben állnak az R gyűrű azon részgyűrűivel, amelyek I-t tartalmazzák. Egy $U \leq S$ részgyűrűhöz a $T = \varphi^{-1}(U)$ teljes inverz kép tartozik.*

Legyenek T és U ebben az értelemben egymásnak megfelelő részgyűrűk. Az U akkor és csak akkor ideál S-ben, ha T ideál R-ben. Ebben az esetben az R/T és az S/U faktorgyűrűk izomorfak.

5.2.12. Következmény [Első izomorfizmus-tétel]. *Tegyük föl, hogy I ideál az R gyűrűben, és S részgyűrű R-ben. Ekkor $S + I$ részgyűrű R-ben, $S \cap I$ ideál S-ben, és*

$$(S + I)/I \cong S/(S \cap I) .$$

5.2.13. Következmény [Második izomorfizmus-tétel]. *Tegyük föl, hogy I és J ideálok az R gyűrűben, és $I \subseteq J$. Ekkor*

$$(R/I)/(J/I) \cong R/J .$$

Az állításba beleértjük, hogy $I \lhd J$ és $(J/I) \lhd (R/I)$, vagyis hogy a felírt faktorgyűrűk értelmesek.

Gyakorlatok, feladatok

5.2.14. Gyakorlat. Készítsük el az alábbi faktorgyűrűk műveleti tábláit, majd osztályozzuk őket izomorfia szerint. (Ha n egész, akkor nR az R gyűrű $\{nr : r \in R\}$ részgyűrűjét jelöli.)

(1) $\mathbb{Z}_4/\{0\}$.
(2) $\mathbb{Z}_8/\{0, 4\}$.
(3) $\mathbb{Z}_{16}/\{0, 4, 8, 12\}$.
(4) $2\mathbb{Z}/(8)$.
(5) $2\mathbb{Z}_{16}/(8)$.
(6) $\mathbb{Z}/(4)$
(7) $4\mathbb{Z}/(16)$.
(8) $\mathbb{Z}[x]/(4, x)$.

5.2.15. Gyakorlat. A $\mathbb{Q}[x]/(x^2+x+1)$ gyűrűben mi az $x+(x^2+x+1)$ inverze?

5.2.16. Gyakorlat. Igazak-e az alábbi gyűrű-izomorfizmusok?

(1) $\mathbb{R}[x]/(x^2+2) \cong \mathbb{C}$.
(2) $\mathbb{R}[x]/(x^2-1) \cong \mathbb{C}$.
(3) $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R}\times\mathbb{R}$.
(4) $\mathbb{G}/(5) \cong \mathbb{Z}_5\times\mathbb{Z}_5$ (itt $\mathbb{G}$ a Gauss-egészek gyűrűje).
(5) $\mathbb{G}/(3) \cong \mathbb{Z}_3[x]/(x^2+1)$.

5.2.17. Gyakorlat. Van-e olyan gyűrű, amely nem egységelemes, de egy alkalmas faktorgyűrűje az?

5.3. Egyszerű gyűrűk

Egy csoport akkor egyszerű, ha csak triviális homomorfizmusai vannak. Ugyanez az elnevezés gyűrűk esetében is. A definíciót az ideálok nyelvén fogalmazzuk meg.

5.3.1. Definíció. Az R gyűrűt *egyszerű gyűrűnek* nevezzük, ha pontosan két ideálja van: a triviálisak (vagyis $\{0\}$ és maga R).

Egyszerű gyűrűre két alapvetően fontos példát ismerünk meg.

5.3.2. Állítás. *Minden ferdetest egyszerű gyűrű, sőt minden egyoldali ideálja is triviális.*

Bizonyítás. Legyen F ferdetest és J jobbideálja F-nek, amely nem csak a nullából áll. Ha $0 \neq a \in J$, akkor $1 = aa^{-1} \in J$, hiszen J jobbideál. Tehát tetszőleges $r \in R$ esetén $r = 1r \in J$. Ezért $J = R$. Hasonlóképpen a balideálok is triviálisak. □

5.3.3. Feladat. Igazoljuk, hogy ha T test, akkor a $T^{n\times n}$ teljes mátrixgyűrű egyszerű gyűrű.

Megjegyezzük, hogy a teljes mátrixgyűrű egyoldali ideáljait is leírhatjuk egy úgynevezett Galois-kapcsolat segítségével (lásd a 8.7.10. és a 8.7.12. Feladatokat). Egy testnél általánosabb gyűrű fölötti teljes mátrixgyűrű kétoldali ideáljait az 5.3.18. Feladat adja meg.

Az előző állításnak a megfordítása is lényegében igaz: egy balideálmentes egységelemes gyűrű mindig ferdetest. Ennek bizonyítása előtt egy könnyebb, de hasonló tételt igazolunk. Emlékeztetjük az Olvasót, hogy ha egy R gyűrűben az r elem nem bal oldali nullosztó, akkor szabad vele balról egyszerűsíteni, azaz $ra = rb$-ből $a = b$ következik (lásd 2.2.26. Gyakorlat).

5.3.4. Lemma. *Legyen R nullosztómentes gyűrű, és e olyan eleme R-nek, melyre $er = r$ teljesül alkalmas $r \neq 0$ esetén. Ekkor e egységeleme R-nek.*

A lemma állítását érdemes összevetni a 2.4.24. Feladat megoldásával.

Bizonyítás. Szorozzuk meg az $er = r$ egyenletet balról egy tetszőleges $t \in R$ elemmel. Ekkor $ter = tr$ adódik, és jobbról r-rel egyszerűsítve kapjuk, hogy $te = t$. Speciálisan $re = r$. Most szorozzuk meg ezt az egyenletet jobbról t-vel. Ekkor $ret = rt$, ahonnan r-rel egyszerűsítve $et = t$. Mivel $r \neq 0$, az e sem lehet nulla, azaz egységelem. □

Tudjuk, hogy minden ferdetest nullosztómentes (2.2.27. Tétel). A megfordítás nem igaz, hiszen például az egész számok gyűrűje nullosztómentes, de nem test. A $\mathbb{Z}_m$ gyűrűk esetében azonban a nullosztómentességből már következett, hogy testről van szó (akkor ez a helyzet, ha m prímszám). Ennek az állításnak a 2.2.30. Feladat megoldásában egy olyan bizonyítását adtuk, amely általánosítható.

5.3.5. Tétel. *Minden véges, legalább kételemű, nullosztómentes gyűrű ferdetest.*

Megjegyezzük, hogy Wedderburn tétele (6.7.11. Tétel) szerint minden véges ferdetest test (azaz kommutatív).

Bizonyítás. Tegyük föl, hogy R véges, nullosztómentes gyűrű. Soroljuk föl R elemeit: $R = \{r_1, \ldots, r_n\}$, és legyen $0 \neq r \in R$. Ha $i \neq j$, akkor $rr_i \neq rr_j$, hiszen r nem bal oldali nullosztó. Tehát az rr_i elemek páronként különbözőek, és így R végessége miatt kiadják R összes elemét. Ezt úgy is fogalmazhatjuk, hogy $r \neq 0$ esetén az $rx = s$ egyenlet tetszőleges $s \in R$ esetén x-re megoldható R-ben. Ugyanezt a gondolatmenetet jobbról végezve azt kapjuk, hogy az $xr = s$ egyenlet is mindig megoldható.

Mivel R legalább kételemű, van benne egy nem nulla r elem. Az $rx = r$ egyenlet megoldható, és így az előző lemma szerint R egységelemes gyűrű; az egységelemet a továbbiakban 1 jelöli. Az $rx = 1$ egyenlet megoldhatóságából kapjuk, hogy minden $r \neq 0$ elemnek van jobbinverze, és ugyanígy balinverze is. A 2.2.10. Feladat szerint ezek egyenlők, és így r invertálható. □

5.3.6. Definíció. Legyen R gyűrű, és X részhalmaza R-nek. Az X *bal oldali annullátorán* azoknak az $r \in R$ elemeknek a halmazát értjük, amelyekre $rX = \{0\}$ (vagyis $rx = 0$ minden $x \in X$-re). Ennek jele $\ell(X)$. Hasonlóképpen az X *jobb oldali annullátorán* azoknak az $r \in R$ elemeknek a halmazát értjük, amelyekre $Xr = \{0\}$, jele $r(X)$.

5.3.7. Lemma. *Egy R gyűrű minden X részhalmazának bal annullátora balideál, és ha X maga is balideál, akkor $\ell(X)$ kétoldali ideál.*

Bizonyítás. Az nyilvánvaló, hogy $\ell(X)$ zárt az összeadásra és a kivonásra. Ha $a \in \ell(X)$ és $r \in R$, akkor $x \in X$ esetén

$$(ra)x = r(ax) = r0 = 0\,.$$

Ezért $\ell(X)$ tényleg balideál. Ha X maga is balideál, akkor $rx \in X$, és ezért

$$(ar)x = a(rx) = 0\,,$$

vagyis $\ell(X)$ kétoldali ideál. □

5.3.8. Tétel. *Legyen R gyűrű, amelynek csak a két triviális balideálja van. Ekkor R vagy ferdetest, vagy olyan prímelemű gyűrű, amelyben bármely két elem szorzata nulla.*

Az olyan gyűrűket, amelyben bármely két elem szorzata nulla, *zérógyűrűknek* nevezzük. Ezt ne tévesszük össze a nullgyűrűvel (amelynek csak egyetlen eleme van, a nulla, és amely persze szintén zérógyűrű).

Bizonyítás. Tegyük föl először, hogy R nem nullosztómentes. Ekkor van olyan nullától különböző $r, s \in R$, hogy $rs = 0$. Persze $r \in \ell(s)$, tehát $\ell(s)$ nem csak a nullából áll. De balideál, tehát a feltevés miatt csak az egész R lehet. Ezért $Rs = 0$, vagyis $s \in r(R)$. Mivel R balideálja önmagának, a lemma szerint $r(R)$ kétoldali ideál, ami nem nulla, hiszen s eleme. Ezért $r(R)$ csak R lehet, de akkor R bármely két elemének a szorzata nulla, vagyis R zérógyűrű. Ilyenkor R^+ minden részcsoportja nyilván ideál, vagyis ennek a csoportnak csak a két triviális részcsoportja lehet. A 4.4.30. Következmény miatt R rendje prímszám. Ezzel tehát elintéztük azt az esetet, amikor R nem nullosztómentes.

Most azt az esetet vizsgáljuk, amikor R nullosztómentes. Legyen $0 \neq r \in R$. Ekkor Rr nem nulla (hiszen például r^2 nem nulla eleme a nullosztómentesség miatt). De ez nyilván balideál, tehát $Rr = R$. Ezért $er = r$ alkalmas $e \in R$ elemre. Az 5.3.4. Lemma miatt R-nek e egységeleme. Az $Rr = R$ összefüggés miatt van olyan s, hogy $sr = e$, vagyis minden nem nulla elemnek van balinverze (ami nyilván szintén nem nulla). A 4.1.12. Feladat miatt tehát az $R - \{0\}$ félcsoport valójában csoport, azaz R ferdetest. □

5.3.9. Következmény. *Egy kommutatív, egységelemes gyűrű, akkor és csak akkor egyszerű gyűrű, ha test.*

Az $\mathbb{R}[x]/(x^2 + 1)$ példája azt mutatja, hogy testeket faktorgyűrűként is származtathatunk. Le szeretnénk írni azokat az ideálokat, amelyek erre alkalmasak. Ezért a maximális részcsoport 4.10.6. Definíciójának mintájára bevezetjük a maximális ideál fogalmát.

5.3.10. Definíció. Egy R gyűrű egy I valódi (azaz R-től különböző) ideálját *maximális ideálnak* nevezzük, ha nincs R-nek I-t tartalmazó, valódi ideálja (az I-n kívül).

5.3.11. Állítás. *Ha R gyűrű, akkor az I ideálja akkor és csak akkor maximális, ha R/I egyszerű gyűrű.*

Bizonyítás. Az állítás következik az 5.2.11. Tételből, hiszen abban beláttuk, hogy az I-t tartalmazó ideálok kölcsönösen egyértelmű megfeleltetésben állnak az R/I faktorgyűrű összes ideáljaival. □

5.3.12. Következmény. *Ha R kommutatív, egységelemes gyűrű, akkor az I ideálja akkor és csak akkor maximális, ha R/I test.*

Bizonyítás. Valóban, az R/I is kommutatív, egységelemes gyűrű, így az 5.3.9. Következmény miatt pontosan akkor egyszerű gyűrű, ha test. □

Emiatt a következmény miatt fontos lenne tudni, hogy például az $\mathbb{R}[x]$ gyűrűnek mik a maximális ideáljai. A 5.5. Szakaszban meg fogjuk mutatni, hogy ezek pontosan azok, amelyek egy $\mathbb{R}$ fölött irreducibilis polinom összes többszöröseiből állnak. Ez magyarázza, hogy $\mathbb{R}[x]/(x^2 + 1)$ miért test.

A következő tétel azt mutatja, hogy a maximális ideálok minden egységelemes gyűrűben „elég sokan vannak”. A bizonyítás érdekessége, hogy egy nemtriviális halmazelméleti állítást használ. Az ehhez szükséges fogalmakat a következő szakaszban tárgyaljuk, és a tételt is ott bizonyítjuk be.

5.3.13. Tétel [Krull tétele]. *Ha R egységelemes gyűrű, akkor minden valódi ideálja része egy maximális ideálnak.*

Gyakorlatok, feladatok

5.3.14. Gyakorlat. Számítsuk ki a $\mathbb{Z}_{24}$ gyűrűben a 18 elem annullátorát. Általánosítsuk a kapott állítást!

5.3.15. Gyakorlat. Mely n-ekre igaz, hogy a $\mathbb{Z}_n$ gyűrűben a nullosztók a nullával együtt ideált alkotnak?

5.3.16. Gyakorlat. Legyen M az a kétszer kettes mátrix, amelynek mindegyik eleme 1. Számítsuk ki az $\mathbb{R}^{2\times 2}$ teljes mátrixgyűrűben az M-nek a jobb és a bal annullátorát.

5.3.17. Gyakorlat. Mutassuk meg, hogy ha r baloldali nullosztó, és sr nem nulla, akkor sr is baloldali nullosztó. Igaz-e, hogy ha r, s baloldali nullosztók, és $r+s\neq 0$, akkor $r+s$ is baloldali nullosztó?

5.3.18. Feladat. Legyen R egységelemes gyűrű. Mutassuk meg, hogy az $R^{n\times n}$ teljes mátrixgyűrű ideáljai pontosan az $I^{n\times n}$ részgyűrűk, ahol I ideálja R-nek.

5.3.19. Feladat. Legyen I ideál egy R gyűrűben, és J ideálja I-nek. Mutassuk meg, hogy a J által R-ben generált ideál köbe része J-nek. Vezessük le ebből, hogy egy gyűrű minden (a nem nulla ideálok között) minimális ideálja vagy egyszerű gyűrű, vagy zérógyűrű.

5.4. Láncfeltételek

Ebben a szakaszban halmazelméleti ízű fogalmakat vizsgálunk: a gyűrűk ideáljaira vonatkozó maximum- és minimumfeltételt. A maximum-feltétel a kommutatív, a minimumfeltétel a nemkommutatív gyűrűk elméletében játszik fontos szerepet, ezekről később érintőlegesen említést teszünk majd. A következő szakaszban, ahol a számelmélet alaptételével foglalkozunk, szintén előjön majd a maximum-feltétel. A tárgyalt fogalmak lehetővé teszik Krull tételének bizonyítását is. Ez a szakasz a többinél talán kicsit nehezebb, a könyv első olvasásakor átugorható.

A 4.4.23. Definícióban tanultunk halmazrendszer minimális és maximális elemeiről. Egy $\mathcal{H}$ halmazrendszer maximális eleme egy olyan $H\in\mathcal{H}$ halmaz, amelyet a $\mathcal{H}$ egyetlen más halmaza sem tartalmaz. Az előző szakaszban definiált „maximális ideál” fogalma ennek speciális esete: az R gyűrű egy maximális ideálján olyan ideált értünk, amely az R

valódi ideáljainak halmazában maximális (vagyis $\mathcal{H}$ speciálisan az R *összes* valódi ideáljaiból áll).

Fontos, hogy a „maximális ideál" és a „$\mathcal{H}$-ban maximális ideál" fogalmát ne keverjük össze abban az esetben sem, ha a $\mathcal{H}$ halmazrendszer véletlenül ideálokból áll. Ezt úgy kerülhetjük el, hogy odafigyelünk a fogalmazásra: ha a $\mathcal{H}$ meg van adva, akkor az *abban* maximális ideálokról, ha nincs megadva ilyen halmazrendszer, akkor a valódi ideálok között maximális ideálokról van szó.

5.4.1. Definíció. Azt mondjuk, hogy az R gyűrű ideáljaira érvényes a *maximum-feltétel*, ha R ideáljainak minden nem üres halmazában van maximális elem. Ugyanígy, az R gyűrű ideáljaira érvényes a *minimum-feltétel*, ha R ideáljainak minden nem üres halmazából kiválasztható minimális elem.

Például az egész számok gyűrűjének ideáljaira nem érvényes a minimum-feltétel, mert a

$$(2) \supsetneq (4) \supsetneq \ldots \supsetneq (2^m) \supsetneq \ldots .$$

ideálok között nincs minimális. Ugyanakkor ebben a gyűrűben érvényes a maximum-feltétel, ezt a következő szakaszban be is látjuk majd.

Másik példaként tekintsük a $\mathbb{Q}[x_1, x_2, \ldots]$ végtelen sok határozatlanú polinomgyűrűt (ennek elemei az összes olyan polinomok, amelyek határozatlanai az $x_1, x_2, \ldots$ közül kerülnek ki). Ebben a maximum-feltétel sem igaz az ideálokra, hiszen az

$$(x_1) \subsetneq (x_1, x_2) \subsetneq \ldots$$

ideálok halmazában nincs maximális, azaz mindegyik itt szereplő ideálnál van nagyobb *ugyanebben a halmazban*. Ennek igazolásához a következő gyakorlatot kell megoldani.

5.4.2. Gyakorlat. Igazoljuk, hogy a $\mathbb{Q}[x_1, x_2, \ldots]$ végtelen sok határozatlanú polinomgyűrűben tetszőleges $n \geq 1$ esetén

$$x_{n+1} \notin (x_1, \ldots, x_n) .$$

5.4.3. Tétel. *Tetszőleges R gyűrű esetében az alábbi négy feltétel ekvivalens.*

(1) *R ideáljaira érvényes a maximum-feltétel.*
(2) *Az R ideáljainak nem létezik végtelen, szigorúan növő lánca:*

$$I_1 \subsetneq I_2 \subsetneq \ldots .$$

(3) *Ha vesszük R ideáljainak egy végtelen növő láncát:*

$$I_1 \subseteq I_2 \subseteq \ldots ,$$

akkor van olyan n, hogy $I_n = I_{n+1} = I_{n+2} = \ldots$ (vagyis a lánc stabilizálódik).
(4) *R minden ideálja generálható véges sok elemmel.*

Bizonyítás. (1) $\Longrightarrow$ (4): legyen I ideálja R-nek, és jelölje $\mathcal{H}$ az R összes olyan végesen generált ideáljainak a halmazát, amelyek részei I-nek. Az (1) miatt a $\mathcal{H}$ halmazban van egy M maximális elem. Tegyük föl, hogy $M \neq I$, vagyis van olyan $a \in I$, amelyre $a \notin M$. Az M végesen generált, mondjuk az $r_1, \ldots, r_n$ elemek által. Ekkor az $r_1, \ldots, r_n, a$ elemek által generált J ideál is eleme $\mathcal{H}$-nak, hiszen végesen generált ideálja R-nek, és része I-nek (mert minden generátoreleme I-beli). A J ideál valódi módon tartalmazza M-et, hiszen $a \in J$ de $a \notin M$. Ez ellentmond M maximalitásának. Az ellentmondás azt mutatja, hogy $M = I$, vagyis I végesen generált.

A (4) $\Longrightarrow$ (3) igazolásához szükségünk van egy segédállításra, amit később is felhasználunk majd. Egy halmazrendszert láncnak nevezünk, ha bármely két eleme közül az egyik tartalmazza a másikat (lásd A.1.1. Definíció). Tipikus lánc például a (3) feltételben szereplő $I_1 \subseteq I_2 \subseteq \ldots$ ideálok sorozata.

5.4.4. Lemma. *Tegyük föl, hogy R gyűrű, és $\mathcal{L}$ egy ideálokból álló nem üres lánc. Ekkor az $\mathcal{L}$ elemeinek U uniója is ideál R-ben.*

Bizonyítás. Ha $a, b \in U$, akkor van olyan $L_1 \in \mathcal{L}$, hogy $a \in L_1$, és van olyan $L_2 \in \mathcal{L}$, hogy $b \in L_2$. Mivel $\mathcal{L}$ lánc, vagy $L_1 \subseteq L_2$, vagy $L_2 \subseteq L_1$. Az első esetben $a, b \in L_2$, és ekkor $a \pm b$ eleme L_2-nek (hiszen L_2 ideál R-ben), tehát U-nak is. Ha viszont $L_2 \subseteq L_1$, akkor ugyanez a gondolatmenet L_2 helyett L_1-re mondható el, és ekkor is $a \pm b \in U$ adódik. Tehát az U halmaz zárt az összeadásra és a kivonásra. Nyilván tartalmazza a nullát is, azaz részcsoport.

Tegyük most föl, hogy $a \in U$ és $r \in R$. Ekkor van olyan $L \in \mathcal{L}$, hogy $a \in L$. Mivel L ideál R-ben, ezért $ar, ra \in L \subseteq U$. Ezért U is ideál R-ben. □

A (4) $\Longrightarrow$ (3) bizonyítására visszatérve tegyük föl, hogy $I_1 \subseteq I_2 \subseteq \ldots$ az R ideáljainak egy növő lánca. Jelölje U e lánc elemeinek unióját. A lemma szerint U ideál R-ben, tehát (4) miatt végesen generált, generálják mondjuk az $r_1, \ldots, r_n$ elemek. Mivel $r_i \in U$, az r_i benne van az I_j ideálok valamelyikében: $r_i \in I_{j_i}$. Jelölje n a j_i számok közül a legnagyobbat, akkor $I_{j_i} \subseteq I_n$ minden i-re, és így I_n mindegyik r_i elemet tartalmazza. De az r_i elemek generálják az U ideált, és ezért I_n már az egész U-val egyenlő. Persze akkor $I_{n+1}, I_{n+2}, \ldots$ is ugyanez az ideál lesz, tehát a lánc I_n-től kezdve stabilizálódik.

(3) $\Longrightarrow$ (2): ez nyilvánvaló, hiszen a (2)-ben szereplő lánc soha nem stabilizálódik.

(2) $\Longrightarrow$ (1): tegyük föl, hogy van R ideáljainak egy nem üres $\mathcal{H}$ részhalmaza, amelynek nincs maximális eleme. Legyen I_1 tetszőleges eleme $\mathcal{H}$-nak. Mivel ez nem maximális, van $\mathcal{H}$-ban egy $I_2 \supsetneq I_1$ elem. Ez sem lehet maximális, ezért ezt a láncot tovább építhetjük, és így egy végtelen szigorúan növő láncot kapunk, ami (2)-nek ellentmond. Ezzel az 5.4.3. Tételt bebizonyítottuk. □

Az Olvasónak érdemes végiggondolnia, hogy a fenti bizonyítás (a lemmát is beleértve) szó szerint ugyanígy elmondható ideálok helyett balideálokra, jobbideálokra, részgyűrűkre, sőt egy csoport részcsoportjaira vagy normálosztóira is. Természetesen nem fogjuk a hasonló állításokat minden esetben külön kimondani, hanem a fenti tételt használjuk majd a többi rész-fogalom esetében is.

Ha egy gyűrűben érvényes a maximum-feltétel, akkor Krull tételének (5.3.13. Tétel) állítása nyilvánvaló. Ha nem, a bizonyítás nehézsége akkor sem algebrai, hanem halmazelméleti. Ezeket a nehézségeket azonban sikerült összegyűjteni egy állításba, ami Zorn-lemma néven ismeretes (lásd A.1.2. Tétel). Ez a lemma lehetővé teszi, hogy az algebrai gondolatmenetre koncentráljunk. A Zorn-lemmát később is használni fogjuk, például Birkhoff tételének bizonyításakor. Most lássuk *Krull tételének a bizonyítását.*

Bizonyítás. Azt kell megmutatni, hogy ha R egységelemes gyűrű, akkor minden valódi ideálja része egy maximális ideálnak. Tegyük föl, hogy I valódi ideál R-ben. Legyen $\mathcal{X}$ az R azon valódi ideáljainak a halmaza, melyek I-t tartalmazzák. Megmutatjuk, hogy a Zorn-lemma feltétele teljesül, vagyis bárhogyan választjuk ki $\mathcal{X}$ egy olyan $\mathcal{L}$ részrendszerét, amelyik lánc, az $\mathcal{L}$ elemeinek U uniója is eleme az $\mathcal{X}$ halmazrendszernek.

Az 5.4.4. Lemma szerint az U az R-nek ideálja, tehát csak azt kell ellenőrizni, hogy valódi ideál (azaz nem az egész R). Ha $U = R$ lenne, akkor speciálisan R egységeleme, 1 is benne lenne U-ban, és ezért valamelyik $L \in \mathcal{L}$ ideálban is. De ha $1 \in L$, akkor tetszőleges $r \in R$ esetén $r = 1r \in L$, hiszen L ideálja R-nek. Ezért $L = R$, ami ellentmond annak, hogy $\mathcal{L} \subseteq \mathcal{X}$ minden eleme valódi ideál. Ez az ellentmondás biztosítja, hogy U valódi ideál, vagyis $\mathcal{X}$ teljesíti a Zorn-lemma feltételét.

A Zorn-lemma miatt tehát $\mathcal{X}$-nek van egy maximális M eleme. Ez persze tartalmazza az I ideált, és maximális ideálja R-nek. Valóban, ha lenne R-nek egy M-et valódi módon tartalmazó N valódi ideálja, akkor $I \subseteq N$ miatt N is eleme lenne $\mathcal{X}$-nek, ami ellentmond M maximalitásának. □

Gyakorlatok, feladatok

5.4.5. Gyakorlat. Az $\mathbb{R}^{n\times n}$ teljes mátrixgyűrűben teljesül-e balideálokra a minimum-, illetve a maximum-feltétel?

5.4.6. Gyakorlat. Legyen I ideál az R gyűrűben. Mutassuk meg, hogy azon J ideálok között, melyekre $I \cap J = \{0\}$, van maximális.

5.4.7. Feladat. Mutassuk meg, hogy ha az $R \neq 0$ mullosztómentes, kommutatív gyűrű ideáljaira érvényes a minimumfeltétel, akkor R test.

5.4.8. Feladat. Igazoljuk, hogy minden végesen generált csoportnak van maximális részcsoportja, de a racionális számok additív csoportjának nincs.

5.5. A számelmélet alaptétele

Ebben a szakaszban azokat a szokásos (vagyis nullosztómentes, kommutatív, egységelemes) gyűrűket jellemezzük, amelyekben igaz a számelmélet alaptétele. Az itt szereplő fogalmakat és tételeket érdemes összevetni azzal, ami a [**11**] könyv 11.1 – 11.3 Szakaszaiban szerepel. A munka dandárját már elvégeztük a 3.2. Szakasz feladataiban. Láttuk, hogy

szerencsés esetben el lehet végezni a maradékos osztást, és ebből eljutunk az alaptételhez. Most elsőként ezt az esetet vizsgáljuk meg, immár teljes általánosságban.

Három olyan példánk is van gyűrűre, amelyben a maradékos osztást el lehet végezni: az egész számok körében, test fölötti polinomgyűrűben (lásd 3.2.1. Tétel), és a Gauss-egészek között (ez utóbbit nem bizonyítottuk, csak hivatkoztunk a [**11**] könyv 7.4. és 7.5. Szakaszára). Mindhárom esetben arról van szó, hogy bárhogyan is veszünk ki az R gyűrűből egy a és $b \neq 0$ elemet, létezik olyan $q, r \in R$, hogy $a = bq + r$, ahol az r valamilyen értelemben már „kisebb", mint b. Pontosabban,

- az egészek gyűrűjében az volt a feltétel, hogy $|r| < |b|$;
- test fölötti polinomgyűrűben az volt a feltétel, hogy r foka kisebb, mint b foka (vagy $r = 0$);
- a Gauss-egészek között pedig az a feltétel, hogy r „normája" kisebb, mint b „normája", ahol egy $u + vi$ Gauss-egész normáját $u^2 + v^2$-nek definiáljuk.

Hogyan lehetne mindezt általánosan megfogalmazni? Azt mindenesetre látjuk, hogy szükség van valamire, ami az r maradékot „méri", az abszolút érték, a fokszám és a norma közös általánosításaként. Ez egy φ függvény lesz, amely az R elemein van értelmezve, de hová képezzen, mik legyenek az értékei?

Ennek eldöntéséhez gondoljuk meg, hogy a maradékos osztást elsősorban az euklideszi algoritmusban használtuk. Az, hogy a maradék mindig „kisebb" az osztónál, azt biztosítja, hogy az eljárás véges sok lépésben véget ér. Ezért φ értékkészletének nem célszerű például valós, vagy negatív számokat megengedni, hiszen itt ki lehet választani számok monoton csökkenő végtelen sorozatát (és ha az algoritmusban a maradékok „normája" egy ilyen sorozatot alkot, akkor nincs garancia arra, hogy az eljárás véget ér). A nemnegatív egészek között azonban ilyen sorozat nem lehetséges. Ráadásul mindhárom fenti példa esetében nemnegatív egész számot rendeltünk a gyűrű elemeihez. Ez indokolja a következő definíciót.

5.5.1. Definíció. Az R szokásos gyűrűt *euklideszi gyűrűnek* nevezzük, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény (az úgynevezett *euklideszi norma*) a következő tulajdonsággal. Tetszőleges $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$ és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

A számelmélet alaptétele felé most nem elemi úton haladunk, mint a 3. Fejezetben, hanem az R gyűrű ideáljainak vizsgálatával. Érdemes átismételni a 3.2.6. Tétel bizonyítását, amely megmutatja, miért is hasznosak az ideálok ebben a témakörben.

5.5.2. Definíció. Az R szokásos gyűrűt *főideálgyűrűnek* nevezzük, ha minden ideálja főideál, vagyis egy elemmel generálható.

5.5.3. Tétel. *Minden euklideszi gyűrű főideálgyűrű.*

Bizonyítás. Legyen I ideálja az R euklideszi gyűrűnek. Ha I csak a nullából áll, akkor a 0 generálja. Ha nem, akkor készítsük el I minden nem nulla elemének az euklideszi normáját, és válasszunk ki egy olyan $0 \neq b \in I$ elemet, amelynek ez a φ-értéke a lehető legkisebb. Megmutatjuk, hogy $I = (b)$, vagyis hogy I a b elem többszöröseiből áll.

Az világos, hogy b minden többszöröse is benne van I-ben. Megfordítva, tegyük föl, hogy $a \in I$. Osszuk el a-t maradékosan b-vel:

$$a = bq + r\,,$$

ahol $r = 0$, vagy $\varphi(r) < \varphi(b)$. Mivel I ideál, $r = a - bq \in I$ (hiszen bq benne van I-ben, mint b többszöröse, és így $a - bq$ is, mert I zárt a kivonásra). Ezért $\varphi(r) < \varphi(b)$ nem lehetséges a $\varphi(b)$ minimális választása miatt. Így az marad, hogy $r = 0$, vagyis a tényleg többszöröse b-nek. De akkor $a \in (b)$, azaz $(b) = I$. □

A számelmélet alaptételét tehát elég főideálgyűrűre bizonyítani, akkor minden euklideszi gyűrűben is teljesülni fog. Érdemes átfogalmaznunk az oszthatóság és a kitüntetett közös osztó fogalmát főideálokra.

5.5.4. Lemma. *Legyen R szokásos gyűrű és $r, s \in R$. Ekkor $r \mid s$ akkor és csak akkor, ha $(r) \supseteq (s)$. Így az r és s akkor és csak akkor asszociáltak, ha $(r) = (s)$.*

Fontos odafigyelnünk arra, hogy az oszthatóságnak a fordított irányú tartalmazás felel meg, azaz ha egy elem oszthatóság szemszögéből „kisebb”, akkor az általa generált főideál „nagyobb”.

Bizonyítás. Tudjuk, hogy (s) az s elem összes R-beli többszöröseiből áll (5.1.9. Állítás). Ha $r \mid s$, akkor s minden többszöröse r-nek is többszöröse, vagyis $(s) \subseteq (r)$. Megfordítva, ha $(s) \subseteq (r)$, akkor $s \in (s) \subseteq (r)$, ezért s többszöröse r-nek. A lemma második állítása nyilvánvaló az elsőből, hiszen r és s akkor asszociáltak, ha egymás osztói. □

A következő lemma megmagyarázza, hogy miért nem baj, hogy az a és b által generált ideálra ugyanazt a jelölést alkalmaztuk, mint a és b legnagyobb közös osztójára.

5.5.5. Lemma. *Legyen R szokásos gyűrű és $a, b, d \in R$. Ekkor az a és b által generált (a, b) ideál akkor és csak akkor egyenlő a (d) főideállal, ha d olyan kitüntetett közös osztója a-nak és b-nek, amely felírható $ar + bs$ alakban alkalmas $r, s \in R$ elemekkel.*

Bizonyítás. A generált ideál 5.1.9. Állításbeli képlete szerint (a, b) elemei az $ar + bs$ alakú elemek, ahol $r, s \in R$. Ha tehát $(a, b) = (d)$, akkor d felírható a kívánt alakban. Mivel $(a) \subseteq (a, b) = (d)$, ezért az előző lemma szerint $d \mid a$, és hasonlóképpen $d \mid b$. Ha $c \in R$ is közös osztója a-nak és b-nek, akkor $a, b \in (c)$, vagyis a generált ideál definíciója miatt $(d) = (a, b) \subseteq (c)$. Ezért $c \mid d$, és ezzel beláttuk, hogy d kitüntetett közös osztója a-nak és b-nek.

Megfordítva, ha $d = ar + bs$, akkor persze $d \in (a, b)$, azaz $(d) \subseteq (a, b)$. Ha d emellett közös osztója is a-nak és b-nek, akkor $a, b \in (d)$, ahonnan $(a, b) \subseteq (d)$, tehát $(a, b) = (d)$. Ezzel az állítást beláttuk. □

5.5.6. Következmény. *Legyen R főideálgyűrű. Ekkor R bármely két elemének létezik kitüntetett közös osztója, és R minden irreducibilis eleme prím.*

Bizonyítás. Az előző lemma miatt $a, b \in R$ esetén a-nak és b-nek van olyan d kitüntetett közös osztója, ami felírható $ar + bs$ alakban. Ezért R-ben érvényes a kitüntetett közös osztó kiemelési tulajdonsága (lásd 3.1.26. Gyakorlat). Így pedig R minden irreducibilis eleme prím (3.1.27. Gyakorlat). □

A 3.1.32. Gyakorlatban megmutattuk, hogy a $\mathbb{Z}[x]$ gyűrűben a 2 és x elemek legnagyobb közös osztója (ami a konstans 1 polinom) nem írható fel $2p(x) + xq(x)$ alakban, ahol $p, q \in \mathbb{Z}[x]$. Ebből láthatjuk, hogy ebben a gyűrűben a $(2, x)$ ideál nem főideál (hiszen ha az lenne, akkor a generátorelem csakis a 2 és x kitüntetett közös osztója lehetne az előző lemma szerint, ami asszociáltság erejéig egyértelmű). Tehát $\mathbb{Z}[x]$ nem főideálgyűrű, de alaptételes. Ez a példa azt mutatja, hogy az alaptételes gyűrűk jellemzéséhez ki kell lépnünk a főideálgyűrűk köréből.

5.5.7. Tétel. *Az R szokásos gyűrű akkor és csak akkor alaptételes, ha az alábbi két feltétel teljesül.*

(1) *R-ben a főideálokra érvényes a maximum-feltétel (vö. 5.4.1. Definíció), vagyis főideálok minden nem üres halmazában van maximális elem.*
(2) *R minden irreducibilis eleme prím.*

Az (1) feltétel az 5.4.3. Tétel mintájára átfogalmazható a következőképpen: főideálok minden növő lánca előbb-utóbb stabilizálódik.

Bizonyítás. Tegyük föl, hogy R alaptételes. Ekkor a 3.1.27. Gyakorlat miatt R minden irreducibilis eleme prím, azaz (2) teljesül. Az (1) bizonyításához jelölje $\Omega(r)$ a nem nulla $r \in R$ elem prímosztóinak számát, mindegyiket annyiszor számolva, ahányszor r kanonikus alakjában szerepel. Képletben, ha r kanonikus alakja $r = ep_1^{\alpha_1} \dots p_k^{\alpha_k}$, akkor $\Omega(r) = \alpha_1 + \ldots + \alpha_k$. Nyilvánvaló, hogy ha r valódi osztója s-nek (vagyis nem asszociáltak), akkor $\Omega(r) < \Omega(s)$ (lásd a 3.1.20. Gyakorlat (2) pontját). Az 5.5.4. Lemma szerint tehát $(r) \supsetneq (s)$ esetén $\Omega(r) < \Omega(s)$. Ha adott R főideáljainak egy nem üres $\mathcal{H}$ halmaza, akkor kiválaszthatunk egy olyan $(s) \in \mathcal{H}$ főideált, amelyre nézve $\Omega(s)$ a lehető legkisebb. Ekkor (s) nyilván maximális lesz $\mathcal{H}$-ban.

A megfordítás bizonyításához tegyük föl, hogy (1) és (2) teljesül, meg kell mutatnunk, hogy R alaptételes. Az egyértelműséget már beláttuk a 3.1.28. Feladatban. A felbontás létezésének igazolásához a 3.4.10. Tétel bizonyítását alakítjuk át. Tegyük föl, hogy az R gyűrűben van olyan nullától és egységtől különböző elem, ami nem bontható felbonthatatlanok szorzatára. Minden ilyen r elemhez készítsük el az (r) főideált, és legyen $\mathcal{H}$ ezeknek a halmaza. Az (1) feltétel miatt létezik $\mathcal{H}$-ban egy maximális (m) elem.

Az m nem lehet irreducibilis, hiszen akkor létezne (egytényezős) felbontása irreducibilisek szorzatára. Ezért létezik egy $m = ab$ nemtriviális felbontás (azaz a és b egyike sem egység, és egyikük sem asszociáltja m-nek). Az 5.5.4. Lemma miatt tehát $(m) \subsetneq (a)$ és $(m) \subsetneq (b)$. Az (m) maximalitása miatt (a) és (b) már nem lehet $\mathcal{H}$-ban, és így létezik felbontásuk irreducibilisek szorzatára:

$$a = p_1 \dots p_k \quad \text{és} \quad b = q_1 \dots q_n\,.$$

De akkor $m = p_1 \dots p_k q_1 \dots q_n$ az m felbontása irreducibilisek szorzatára, ami ellentmond annak, hogy $(m) \in \mathcal{H}$. Ez az ellentmondás bizonyítja a tételt. □

5.5.8. Következmény. *Ha R főideálgyűrű (speciálisan ha euklideszi gyűrű), akkor alaptételes.*

Bizonyítás. Ha R főideálgyűrű, akkor minden ideálja végesen generált (hiszen egy elemmel generálható). Ezért az 5.4.3. Tétel miatt érvényes benne ideálokra a maximum-feltétel, és így az előző tétel (1) feltétele teljesül. Az 5.5.6. Következmény miatt (2) is teljesül. □

A számelméletben igen fontos az az eset is, amikor egy gyűrű nem alaptételes, de ehhez „közel áll". Ilyen például az $a + bi\sqrt{5}$ alakú számok R gyűrűje, ahol $a, b \in \mathbb{Q}$. Itt az alaptétel nem érvényes, hiszen

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

könnyen igazolhatóan két lényegesen különböző felbontás irreducibilisek szorzatára (lásd a 3.1.33. Feladatot, továbbá a [**11**] könyv 11.2.4. Feladatát).

A problémát az okozza, hogy ha $r, s \in R$, akkor az (r, s) ideál nem mindig főideál (és ezért a fenti bizonyítások nem működnek). A megoldás az, hogy az R elemei helyett a gyűrű ideáljait vizsgáljuk. Azt már az előbbiekben is láttuk, hogy ha az r elem helyett az (r) főideált nézzük, akkor az elemek oszthatósága ideálok között a (fordított irányú) tartalmazásnak felel meg. Az r és s kitüntetett közös osztóját helyettesíteni tudja az (r, s) ideál, akár főideál ez, akár nem. (Valójában az „ideál" szó is innen származik: az (r, s) egy „ideális szám", hasonlóan ahhoz, ahogy az i-t „imaginárius" számnak nevezték.) A számok szorzását az ideálok szorzása veszi át (lásd 5.1.13. Gyakorlat), a számelmélet alaptételét pedig az az állítás, hogy az R gyűrűben minden ideál egyértelműen felbontható „prímtulajdonságú" ideálok szorzatára (5.11.4. Definíció). Az ilyen tulajdonságú gyűrűket Dedekind-gyűrűknek nevezik, ezekről az Olvasó a [**11**] és a [**13**] könyvekből szerezhet több információt.

Az 5.2.9. Állítás korábban ígért általánosítása most már könnyen igazolható.

5.5.9. Tétel. *Ha R főideálgyűrű, akkor az R/I faktorgyűrű akkor és csak akkor test, ha I-t R egy irreducibilis eleme generálja.*

Bizonyítás. Megmutatjuk, hogy $I = (r)$ akkor és csak akkor maximális ideál R-ben, ha r irreducibilis eleme R-nek. Valóban, az (r) ideált tartalmazó ideálok az 5.5.4. Lemma szerint pontosan azok az (s) ideálok, amelyekre $s \mid r$. Az I maximalitása tehát azt jelenti, hogy r-nek asszociáltságtól eltekintve pontosan két osztója van csak: 1 és r, azaz hogy r irreducibilis. Az állítás tehát igaz az 5.3.12. Következmény miatt. □

Gyakorlatok, feladatok

5.5.10. Gyakorlat. Főideál-e $\mathbb{Z}[x]$-ben $(x + 1, x + 2)$ illetve $(2x + 2, x + 4)$?

5.5.11. Gyakorlat. Igazoljuk, hogy az R szokásos gyűrű $p \neq 0$ eleme akkor és csak akkor prím, ha $R/(p)$ nullosztómentes, nem egyelemű gyűrű. Adjunk példát olyan p prímre, amikor ez a faktor nem test.

5.5.12. Gyakorlat. Legyen R főideálgyűrű, és $r, s \in R$. Mutassuk meg, hogy $(r) \cap (s)$ az r és s legkisebb közös többszöröse által generált ideál.

5.5.13. Gyakorlat. Tegyük föl, hogy I, J és K ideálok a tetszőleges R gyűrűben. Mutassuk meg, hogy $I(J, K) = (IJ, IK)$, és $(I, J)(I \cap J) \subseteq IJ$. Itt az egymás mellé írás komplexusszorzást jelöl, (I, J) pedig az $I \cup J$ által generált ideál. Ha R főideálgyűrű, akkor milyen számelméleti állításokra fordulnak le ezek az összefüggések?

5.5.14. Gyakorlat. Van-e $\mathbb{Z}[x]$-ben olyan ideál, amely nem generálható 1000 elemmel?

5.5.15. Gyakorlat. Adjunk példát olyan szokásos gyűrűre, amelyben a főideálokra érvényes a maximum-feltétel, de tetszőleges ideálokra nem.

5.6. Hányadostest

A racionális számokat úgy kapjuk az egészekből, hogy törteket képzünk. Szeretnénk olyan törtekkel is számolni, ahol a számláló és a nevező polinom (vagy általában egy gyűrű eleme). Erre már szükségünk is lett volna a 3.4.11. Tétel bizonyításához, amikor a számelmélet alaptételét akartuk belátni $\mathbb{Z}[x]$ helyett tetszőleges, alaptételes gyűrű fölötti polinomgyűrűben. Ennek a tételnek a bizonyítása azáltal válik teljessé, ha a törtek bevezetését precízen elvégezzük (lásd a megjegyzéseket a tétel előtt).

A törtek azért hasznosak, mert osztani is korlátlanul lehet közöttük, tehát egy R gyűrűből egy T testet kapunk. A T minden eleme az R két elemének hányadosa, ez indokolja a következő elnevezést.

5.6.1. Definíció. A T test az R gyűrűnek a *hányadosteste*, ha R részgyűrűje T-nek, és T minden eleme előáll R két elemének hányadosaként.

A nullgyűrű ugyan bármely testnek részgyűrűje, de hányadosteste nincs, hiszen nullával nem oszthatunk, és így a hányadosok halmaza üres. Ezt, mint triviális esetet, a következő tételben kizárjuk.

5.6.2. Tétel. *Egy $R \neq 0$ gyűrűnek akkor és csak akkor létezik hányadosteste, ha kommutatív és nullosztómentes.*

Bizonyítás. Mivel egy test kommutatív és nullosztómentes, minden részgyűrűje is ilyen. A megfordítás bizonyításához legyen R kommutatív, nullosztómentes gyűrű. A T testet úgy konstruáljuk meg, hogy bevezetjük az R-beli törtek fogalmát.

Legyen tehát $a, b \in R$, ahol $b \neq 0$, és tekinteni szeretnénk az a/b törtek halmazát. Ezzel a jelöléssel azonban ugyanaz a gond, mint amit a komplex számok precíz bevezetésénél (az 1.6. Szakaszban) már láttunk: addig, amíg nincs meg a T test, addig nem beszélhetünk az osztás műveletéről, és így az a/b hányadosról sem! A komplex számok esetében ezt

úgy oldottuk meg, hogy az $a + bi$ számra gondoltunk, de a papírra az (a, b) rendezett párt írtuk. Ugyanezt tesszük most is, legyen

$$P = \{(a, b) \,:\, a, b \in R, b \neq 0\}\,.$$

Az (a, b) leírásakor az a/b törtre fogunk gondolni.

Van egy másik probléma is. A racionális számok esetében tudjuk, hogy a $2/4$ és a $4/8$ tört ugyanazt a számot adja. Ezért a P halmazban is azonosítani kellene azokat a törteket, amelyekről úgy gondoljuk, hogy az „értékük" egyforma. Mikor lesz a/b és c/d két ilyen tört? Ha már megvan a T test, akkor a kettő egyenlőségét keresztbe szorozva $ad = bc$ adódik. Legyen tehát

$$(a, b) \sim (c, d) \iff ad = bc\,.$$

Azokat a párokat, amelyekre ez teljesül, azonosítanunk kell.

Ezt a következőképpen valósítjuk meg. Belátjuk, hogy a fenti $\sim$ egy *ekvivalencia-reláció* (lásd 4.4.5. Definíció). Ez azt jelenti, hogy az S halmaznak egy partícióját létesíti (lásd 4.4.6. Tétel, ezt a technikát használtuk a mellékosztályok fogalmának bevezetésekor is). A T test elemei ennek a partíciónak az osztályai lesznek, ezeken kell majd a testműveleteket értelmeznünk.

Az, hogy $\sim$ ekvivalencia-reláció, nagyon könnyű állítás. Példaként a tranzitivitást látjuk be, a reflexivitás és a szimmetria ellenőrzését az Olvasóra hagyjuk. Tegyük föl tehát, hogy

$$(a, b) \sim (c, d) \quad \text{és} \quad (c, d) \sim (e, f)$$

(persze tudjuk, hogy $b, d, f \neq 0$). Ez azt jelenti, hogy $ad = bc$ és $cf = de$. Az első egyenlőséget szorozzuk meg f-fel:

$$adf = bcf = bde$$

a második egyenlőség miatt. Mivel $d \neq 0$, szabad d-vel egyszerűsíteni, és $af = be$ adódik, azaz $(a, b) \sim (e, f)$.

Érdemes észrevenni, hogy

$$(a, b) \sim (ac, bc) \tag{5.1}$$

tetszőleges nem nulla c esetén. Ez „keresztbe szorzással" azonnal adódik (az a feltevés, hogy $c \neq 0$, azért kell, hogy a jobb oldali „tört" „nevezője" se legyen nulla). Ezt az egyszerűsítési tulajdonságot később felhasználjuk majd.

Legyenek T elemei a most definiált ekvivalencia-osztályok. A műveletek bevezetéséhez a törtek szokásos összegét és szorzatát kell fölírnunk. Motivációnk az, hogy ha már készen lenne a T test, akkor közös nevezőre hozással

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{és nyilván} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}\,.$$

Ennek alapján legyen

$$(a, b) + (c, d) = (ad + bc, bd) \quad \text{és} \quad (a, b)(c, d) = (ac, bd)\,.$$

Ez két művelet, amit a P halmazon értelmeztünk. Mivel mi a T test műveleteit akarjuk definiálni, ugyanúgy kell eljárnunk, mint amikor a faktorcsoportban adtuk meg a szorzást, azaz reprezentánsokkal kell számolni. Vagyis ha u és v két eleme T-nek (azaz két ekvivalencia-osztály), akkor válasszunk ki egy-egy $(a, b) \in u$ és $(c, d) \in v$ reprezentánselemet, keressük meg, hogy $(a, b) + (c, d)$ melyik ekvivalencia-osztályban van, és ez az osztály legyen $u + v$. Hasonlóan definiáljuk u és v szorzatát is.

Elsősorban meg kell mutatnunk, hogy a kapott műveletek jóldefiniáltak. Ezt csak az összeadásra végezzük el, a szorzást az Olvasóra hagyjuk. A jóldefiniáltság azt jelenti (lásd a 4.5.12. Állítás bizonyításában a megjegyzéseket), hogy ha

$$(a, b) \sim (a', b') \quad \text{és} \quad (c, d) \sim (c', d') \quad \text{akkor} \quad (a, b) + (c, d) \sim (a', b') + (c', d') .$$

Ennek igazolása egyszerű számolás: $ab' = ba'$ és $cd' = dc'$, tehát

$$(ad + bc)b'd' = ab'dd' + cd'bb' = ba'dd' + dc'bb' = (a'd' + b'c')bd ,$$

vagyis $(ad + bc, bd) \sim (a'd' + b'c', b'd')$.

A következő lépés annak megmutatása, hogy T test. Ez is nagyon egyszerű, ezért csak mintabizonyításokat adunk. Az összeadás és a szorzás is könnyen láthatóan asszociatív és kommutatív, ellenőrizzük a disztributivitást.

$$[(a, b) + (c, d)](e, f) = (ad + bc, bd)(e, f) = (ade + bce, bdf)$$

$$(a, b)(e, f) + (c, d)(e, f) = (ae, bf) + (ce, df) = (adef + bcef, bdf^2) .$$

A kapott két pár nem egyenlő, de ekvivalensek a fenti (5.1) egyenlőség miatt. Ezért T-ben teljesül a disztributivitás is.

Könnyen ellenőrizhető, hogy $(0, b) + (e, f) \sim (e, f)$, és ezért $(0, b)$ osztálya T-nek nulleleme. (Itt $b \neq 0$; ilyen létezik, mert R nem a nullgyűrű.) Mivel a nullelem egyértelmű, a $(0, b)$ alakú párok mind ugyanabban az ekvivalencia-osztályban kell, hogy legyenek. Valójában ezek maguk egy osztályt alkotnak, hiszen $(0, b) \sim (c, d)$ akkor és csak akkor teljesül, ha $bc = 0d = 0$, azaz $b \neq 0$ miatt ha $c = 0$. Ez az osztály tehát T nulleleme. Az is azonnal látszik, hogy (a, b) osztályának $(-a, b)$ osztálya ellentettje lesz. Ezzel beláttuk, hogy T kommutatív gyűrű.

Most megkeressük T egységelemét. A racionális számok között az 1 számot úgy találhatjuk meg, hogy $2/2$, $3/3$, és így tovább. Tekintsük tehát a (b, b) pár osztályát, ahol $b \neq 0$. Ez az osztály egységeleme T-nek, hiszen tetszőleges $(e, f) \in P$ esetén

$$(b, b)(e, f) = (be, bf) \sim (e, f)$$

a fenti (5.1) egyenlőség miatt. Az egységelem osztálya az összes (c, c) párokból áll, ahol $c \neq 0$, hiszen $(b, b) \sim (c, d)$ akkor és csak akkor, ha $bd = bc$, azaz $b \neq 0$ miatt ha $c = d$.

Mivel T nulleleme pontosan a $(0, b)$ alakú párokból áll, ha (a, b) osztálya nem T nulleleme, akkor $a \neq 0$, és így $(b, a) \in P$. Persze (a, b) és (b, a) osztályai inverzek, hiszen szorzatuk az (ab, ab) elem osztálya, vagyis az egységelem. Ezért T test.

A bizonyítással még nem vagyunk készen, hiszen az állításban az szerepelt, hogy R részgyűrűje kell, hogy legyen T-nek. Ez most nem is igaz, hiszen T elemei R-beli párokból

készített halmazok. A probléma ugyanaz, mint a komplex számok precíz bevezetésekor: ha komplex számnak az (a, b) párokat tekintjük $a + bi$-re gondolva, akkor ezek között nincsenek ott a valós számok. A problémát úgy oldottuk meg, hogy az r valós számot azonosítottuk az $(r, 0)$ párral.

A 3 egész számot tört alakban felírhatjuk úgy is, hogy $6/2$, $9/3$, és így tovább. Ennek alapján ha $r \in R$, akkor r-et T-ben úgy találhatjuk meg, hogy az (rb, b) párokat tekintjük, ahol $b \neq 0$. Ezek is egyetlen osztályt alkotnak, hiszen $(rb, b) \sim (c, d)$ akkor és csak akkor, ha $rbd = bc$, azaz ha $c = rd$. Meg fogjuk mutatni, hogy ezek a párok az R-rel izomorf részgyűrűt alkotnak T-ben (és így ezt a részgyűrűt R-rel azonosítva készen is leszünk).

Azt kell tehát megmutatni, hogy az az α leképezés, amely $r \in R$-hez az (rb, b) alakú elemek osztályát rendeli, injektív és művelettartó (azaz beágyazás). Ha $r \neq s \in R$, akkor (rb, b) és (sb, b) nem lehetnek egy osztályban hiszen akkor $rbb = sbb$ teljesülne, ahonnan $r = s$. Az összegtartás igazolásához legyen $r, s \in R$. Ekkor $\alpha(r) + \alpha(s)$ az

$$(rb, b) + (sb, b) = (rbb + sbb, bb)$$

pár osztálya, $\alpha(r + s)$ pedig az

$$((r + s)b, b)$$

páré. Láthatjuk, hogy ez a két pár ekvivalens. A szorzattartás hasonló bizonyítását az Olvasóra hagyjuk.

Meg kell még mutatni, hogy T hányadosteste R-nek. Vegyük T tetszőleges u elemét, ez egy (a, b) pár osztálya. Azt fogjuk megmutatni, hogy ez az osztály az a és b elemeknek, pontosabban a velük T-ben azonosított $\alpha(a)$ és $\alpha(b)$ elemeknek a hányadosa, vagyis hogy $u\alpha(b) = \alpha(a)$. Mivel $\alpha(b)$ a (bd, d) elem osztálya (mindegy, hogy melyik d-re), és

$$(a, b)(bd, d) = (abd, bd)\,,$$

ami tényleg az $\alpha(a)$ osztályában van, ezért $u\alpha(b) = \alpha(a)$ tényleg teljesül, azaz T hányadosteste R-nek. □

A fenti bizonyításban állandóan használtuk, hogy R kommutatív. Ezért megkérdezhetjük, hogy ha R nem kommutatív (de nullosztómentes), akkor beágyazható-e mindig egy ferdetestbe. A válasz erre a kérdésre sajnos nemleges.

Ha R kommutatív, de nem nullosztómentes, akkor a fenti konstrukció módosításával megtehetjük, hogy csak bizonyos elemeknek készítünk inverzet. Ezek persze nem lehetnek nullosztók, hiszen egy nullosztó nem invertálható (lásd 2.2.28. Gyakorlat). A pontos állítást a következő gyakorlat tartalmazza. Az ebben leírt konstrukciót geometriai okokból szokás *lokalizáltnak* nevezni.

5.6.3. Gyakorlat. Legyen R kommutatív gyűrű, és F az R egy olyan részhalmaza, amely a szorzásra zárt, de sem a nullát, sem nullosztót nem tartalmaz. Mutassuk meg, hogy van olyan S kommutatív, egységelemes gyűrű, amelynek R részgyűrűje, S minden eleme előáll két R-beli elem hányadosaként, és F minden eleme S-ben már invertálható.

Speciálisan látjuk, hogy minden kommutatív gyűrű részgyűrűje egy egységelemes gyűrűnek. Ezt tetszőleges gyűrű esetén beláttuk már a 5.1.27. Gyakorlatban.

A hányadostest nemcsak létezik, hanem izomorfia erejéig egyértelműen meg is van határozva. Sőt, az R gyűrű két hányadosteste között mindig van olyan izomorfizmus is, ami R elemeit fixen hagyja.

5.6.4. Tétel. *Ha T és S hányadostestei az R kommutatív, nullosztómentes gyűrűnek, akkor létezik olyan $\varphi : T \to S$ izomorfizmus, amely R minden elemét önmagába viszi.*

Bizonyítás. Elegendő azt megmutatni, hogy az előző tételben konstruált T testre igaz az állítás. Ha ugyanis ezt már tudjuk, és S_1, S_2 két másik hányadosteste R-nek, akkor ezek mindketten T-vel izomorfak lesznek, és így e két izomorfizmus kompozíciója révén egymással is. Természetesen ez a kompozíció is fixen fogja hagyni R elemeit.

Legyen T az előző tételben konstruált test, és S tetszőleges test, amelynek R részgyűrűje. A $\varphi : T \to S$ leképezés megadásához vegyük T egy elemét, ez egy (a, b) pár ekvivalenciaosztálya. Itt $a, b \in R \subseteq S$, tehát $b \neq 0$ miatt az a/b osztás elvégezhető S-ben, jelölje $s \in S$ az eredményt. Definiáljuk a φ függvényt úgy, hogy az (a, b) pár osztályához s-et rendeljen.

Ez a φ függvény jóldefiniált. Valóban, ha $(a, b) \sim (c, d)$ akkor $ad = bc$, amit S-ben átrendezhetünk az $s = a/b = c/d$ alakba. Ezért a φ függvény akkor is s-et rendel az (a, b) osztályához, ha azt (c, d)-vel reprezentáljuk.

Annak megmutatásához, hogy φ összegtartó, csak azt kell észrevenni, hogy az S testben számolva

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}\,.$$

Hasonlóan igazolható a szorzattartás is.

Ha $r \in R$, akkor ezt azonosítottuk az (rb, b) alakú párok osztályával. Ehhez az osztályhoz φ az $rb/b = r$ elemet rendeli, vagyis φ fixen hagyja R elemeit.

A φ injektív, hiszen ha (a, b) osztályának képe nulla, akkor a/b értéke S-ben nulla, azaz $a = 0$. De akkor (a, b) osztálya a T nulleleme.

A φ injektivitásának bizonyításához hivatkozhattunk volna arra is, hogy egy testnek csak triviális ideáljai vannak (5.3.2. Állítás), és így φ magja is vagy nulla, vagy az egész T. A közvetlen számolás azonban egyszerűbb, és megvan az az előnye is, hogy könnyen általánosítható az 5.6.3. Gyakorlatban leírt szituációra.

Végül ha S hányadosteste R-nek, akkor φ szürjektív is, hiszen ekkor S minden eleme a/b alakú alkalmas $a, b \in R$ elemekre, és így az (a, b) ekvivalencia-osztályának a képe. □

Az előző tétel alapján beszélhetünk az R gyűrűnek „a" hányadostestéről (hiszen izomorfia erejéig csak egy ilyen van).

5.6.5. Következmény. *Ha R részgyűrűje egy S testnek, akkor S-nek van az R hányadostestével izomorf részgyűrűje, és ez az a/b alakú elemek halmaza, ahol $a, b \in R$.*

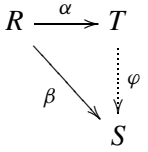
Bizonyítás. Könnyű számolással látszik, hogy az a/b alakú elemek, ahol $a, b \in R$, résztestet alkotnak S-ben. Ez persze hányadosteste R-nek. □

Az előző bizonyításban megspórolhatjuk a számolást, ha észrevesszük, hogy az 5.6.4. Tétel bizonyításának csak az utolsó bekezdésében használtuk ki, hogy S hányadosteste R-nek. Hiszen ekkor φ ugyanúgy megkonstruálható, csak általában nem lesz szürjektív. Viszont $\mathrm{Im}(\varphi)$ nyilván résztest, és pont az, amiről a következményben szó van.

Mindezek alapján látjuk, hogy az egész számok $\mathbb{Z}$ gyűrűjének hányadosteste $\mathbb{Q}$. Ha R szokásos gyűrű, akkor az $R[x_1, \ldots, x_n]$ polinomgyűrű hányadostestének az elemeit *racionális törtfüggvényeknek* nevezzük, és $R(x_1, \ldots, x_n)$-nel jelöljük.

Ha az Olvasót zavarja, hogy az 5.6.2. Tétel bizonyításában R-et azonosítottuk T egy részgyűrűjével, akkor maradhatunk annál, hogy egy $\alpha : R \to T$ injektív homomorfizmust definiáltunk, amelyre igaz, hogy T minden eleme $\alpha(a)/\alpha(b)$ alakú alkalmas $a, b \in R$ elemekre. Ezen a nyelven az előző tétel a következőképpen fogalmazható.

Ha $\beta : R \to S$ egy injektív homomorfizmus egy S testbe, akkor (egyértelműen) létezik egy $\varphi : T \to S$ injektív homomorfizmus, melyre $\varphi \circ \alpha = \beta$ (ez az egyenlőség fejezi ki azt, amit korábban úgy fogalmaztunk, hogy φ az R elemeit fixen hagyja). Mindezt le is rajzolhatjuk:



Ez a fogalmazás első olvasásra nagyon nyakatekertnek tűnik. Van azonban előnye is: hasonló diagrammokkal nagyon egyszerűen számolhatunk abban az esetben, ha sok homomorfizmust kell egyszerre vizsgálnunk. Az ilyesfajta ábrákat *kommutatív diagrammoknak* nevezik, lásd 475. oldal.

Gyakorlatok, feladatok

5.6.6. Gyakorlat. Melyik „ismert" testtel izomorf a páros számok gyűrűjének, a $\mathbb{Z}[x]$ polinomgyűrűnek, illetve a Gauss-egészek gyűrűjének a hányadosteste?

5.6.7. Gyakorlat. Mutassuk meg, hogy ha az R kommutatív, nullosztómentes gyűrű és I nem nulla ideál R-ben, akkor R és I hányadosteste izomorf.

5.6.8. Gyakorlat. Általánosítsuk a Schönemann-Eisenstein kritériumot (3.5.2. Tétel) tetszőleges R alaptételes gyűrűre. (Lásd 3.5.15. Gyakorlat.)

5.7. Karakterisztika és prímtest

Ebben a szakaszban két témakört tárgyalunk. Először megvizsgáljuk, hogy egy nullosztómentes gyűrűben milyen lehet az elemek rendje az összeadásra. Ez vezet el a karakterisztika fogalmához. Ebből kiindulva leírjuk azoknak a testeknek a szerkezetét, amelyeknek már nincs valódi részteste.

Amikor polinomok többszörös gyökeit vizsgáltuk deriválás segítségével a 3.6. Szakaszban, már találkoztunk azzal a jelenséggel, hogy egy nullosztómentes gyűrű nem nulla elemének nem nulla egész számszorosa lehet nulla. Például a $\mathbb{Z}_2[x]$ polinomgyűrűben minden elem kétszerese nulla. Ilyesmi a $\mathbb{C}[x]$-ben nem fordulhat elő. Most ezt a jelenséget fogjuk megvizsgálni. Ehhez érdemes a 2.2.36. Gyakorlat segítségével felfrissíteni a gyűrűelemek egész számszorosaira vonatkozó azonosságokat.

5.7.1. Tétel. *Tegyük föl, hogy R nullosztómentes gyűrű. Ekkor vagy*

(1) *van olyan p prímszám, hogy R minden elemének p-szerese nulla, vagy*
(2) *tetszőleges $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$ esetén $nr \neq 0$.*

Bizonyítás. Tegyük föl, hogy (2) nem igaz, vagyis van olyan $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, hogy $nr = 0$. Az R az összeadásra nézve csoport, amelyben egy r elem rendjét a szokásos módon $o(r)$-rel jelöljük. Az elemrendről tanultak szerint az $nr = 0$ miatt $o(r)$ (véges, és) osztója n-nek. Legyen $m = o(r)$. Persze $mr = 0$.

Tetszőleges $s \in R$ esetén

$$0 = (mr)s = r(ms)\,.$$

Mivel R nullosztómentes és $r \neq 0$, innen $ms = 0$ adódik. Tehát $o(s)$ véges, és osztója $m = o(r)$-nek. Ha s sem nulla, akkor ugyanez a gondolatmenet az r és s felcserélésével azt adja, hogy $o(r) \mid o(s)$, és így e két elemrend egyenlő.

Azt láttuk be, hogy R-ben mindegyik nem nulla elem rendje ugyanaz az m szám. Az (1) igazolásához már csak azt kell megmutatni, hogy m prímszám. Tegyük föl, hogy $m = ab$, ahol a, b pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br)\,.$$

Mivel R nullosztómentes, $ar = 0$ vagy $br = 0$. Az első esetben $m = o(r) \mid a$, vagyis $a \mid m$ miatt $a = m$. A második esetben ugyanígy azt kapjuk, hogy $b = m$. Ezért m tényleg prímszám. □

5.7.2. Definíció. Az előző tételbeli (1) esetben azt mondjuk, hogy az R nullosztómentes gyűrű *karakterisztikája* a p prímszám. A (2) esetben R karakterisztikája nulla.

Miért nullának, miért nem végtelennek mondjuk a (2) esetben a karakterisztikát? Hiszen ilyenkor a nem nulla elemek rendje végtelen!

A magyarázathoz térjünk vissza a 4.3.2. Gyakorlat megoldásához, de fogalmazzunk most már az ideálok nyelvén. Ha g eleme egy G csoportnak, akkor a g elem „jó kitevői” egy I ideált alkotnak a $\mathbb{Z}$ gyűrűben. Mivel $\mathbb{Z}$ euklideszi gyűrű, ez az ideál főideál. Ha nem csak a nullából áll, akkor g rendje véges, és ez a rend az I ideálnak a pozitív generátoreleme,

vagyis $I = (o(g))$. Ha viszont $I = \{0\}$, akkor az I ideált a nulla generálja. Ezért kézenfekvő lenne azt mondani, hogy ebben az esetben a g elem rendje nulla, hiszen akkor minden g-re teljesülne, hogy $I = (o(g))$. A csoportelmélet terminológiáját emiatt nem változtatjuk meg, de a következő fejezetben, amikor modulusok elemeinek rendjét definiáljuk, már ezt az újfajta elnevezést fogjuk használni.

A most bevezetett fogalom segítségével a 3.6.4. Tétel a következőképpen fogalmazható.

5.7.3. Tétel. *Legyen R szokásos gyűrű, $b \in R$, és tegyük föl, hogy b az $f \in R[x]$ polinomnak pontosan k-szoros gyöke ($k \geq 1$ egész). Ekkor b az f deriváltjának legalább $k-1$-szeres gyöke. Ha az R gyűrű karakterisztikája nem osztója k-nak, akkor b az f deriváltjának pontosan $k-1$-szeres gyöke.* □

A $p \neq 0$ karakterisztikájú kommutatív gyűrűknek van egy alapvetően fontos tulajdonsága, amiről egy feladatban már beszéltünk: *tagonként lehet p-edik hatványra emelni.*

5.7.4. Tétel. *Legyen R egy p karakterisztikájú kommutatív gyűrű, ahol p prímszám. Ekkor tetszőleges $r, s \in R$ esetén*

$$(r+s)^p = r^p + s^p\,.$$

Ezért a $\varphi(r) = r^p$ leképezés az R gyűrűnek önmagába vezető homomorfizmusa. Ugyanez az állítás érvényes p helyett p minden hatványára.

Bizonyítás. Az $(r+s)^p = r^p + s^p$ összefüggést már beláttuk a 3.3.18. Feladatban. Mivel $(rs)^n = r^n s^n$ minden kommutatív gyűrűben nyilvánvalóan igaz (2.2.18. Gyakorlat), a φ tényleg homomorfizmus. Mivel homomorfizmusok kompozíciója is homomorfizmus, a φ leképezést önmagával k-szor komponálva is homomorfizmust kapunk. Ez a leképezés minden r elemhez r^{p^k}-t rendel, és így az utolsó állítást is beláttuk. □

5.7.5. Definíció. Egy $p \neq 0$ karakterisztikájú kommutatív gyűrűben az $x \mapsto x^p$ leképezést a gyűrű *Frobenius-endomorfizmusának* nevezzük.

(Általában az endomorfizmusnak egy struktúra önmagába menő homomorfizmusát hívjuk, lásd 4.7.14. Definíció.)

5.7.6. Gyakorlat. Igazoljuk, hogy egy nullosztómentes, $p \neq 0$ karakterisztikájú kommutatív gyűrűben a Frobenius-endomorfizmus injektív leképezés, és ezért minden elemnek minden k-ra legföljebb egy p^k-adik gyöke lehet.

Most térjünk rá a „minimális” testek vizsgálatára.

5.7.7. Tétel. *Legyen T test. Ekkor T-nek létezik a legszűkebb P részteste (ami T minden résztestének része), és P tartalmazza T egységelemét. Ha T karakterisztikája nulla, akkor P izomorf a racionális számok testével. Ha T karakterisztikája a p prímszám, akkor P izomorf $\mathbb{Z}_p$-vel.*

Bizonyítás. Csoportoknál, gyűrűknél megszoktuk, hogy a „legszűkebb” részstruktúra mindig egyelemű, csoportoknál a neutrális elemből, gyűrűknél a nullelemből áll. Testeknél azonban vigyázni kell, mert az egyelemű gyűrűt (vagyis a nullgyűrűt) nem tekintettük testnek. Persze résztestek metszete résztest, és ezért a legszűkebb P résztest létezik, mint a T összes résztestének a metszete.

Nullosztómentes gyűrűben egy egységelemes részgyűrű egységeleme ugyanaz, mint az egész gyűrű egységeleme (a 2.4.24. Gyakorlat, vagy akár az 5.3.4. Lemma miatt). Ezért a T test e egységeleme benne van T minden résztestében, és így P-ben is.

A bizonyítás a következőképpen fog haladni. Ha T karakterisztikája egy p prímszám, akkor megmutatjuk, hogy P az $e, 2e, \dots, (p-1)e$, $pe = 0$ elemekből áll, és $ke \leftrightarrow k$ izomorfizmus $\mathbb{Z}_p$ és P között. Ha viszont T karakterisztikája nulla, akkor az fog kiderülni, hogy P elemei az $(me)/(ne)$ törtek, ahol m, n egész számok, és ezt a hányadost az m/n racionális számnak megfeleltetve izomorfizmust kapunk.

5.7.8. Gyakorlat. Igazoljuk, hogy a nulla karakterisztikájú esetben $(me)/(ne) = (ke)/(\ell e)$ akkor és csak akkor, ha $m\ell = nk$, és így az $m/n \to (me)/(ne)$ leképezés $\mathbb{Q}$-ból T-be jóldefiniált. Ellenőrizzük, hogy művelettartó, és izomorfizmus $\mathbb{Q}$ és P között.

Az előző bekezdés többi állítása is hasonlóan, egyszerűen kiszámolható. Tanulságos azonban ehelyett felhasználni a korábban tanultakat, most egy ilyen bizonyítás következik. Tekintsük azt a $\mathbb{Z}$-ből T-be menő φ leképezést, amelyre $\varphi(n) = ne$. Ez a leképezés gyűrűhomomorfizmus, hiszen

$$\varphi(m+n) = (m+n)e = me + ne = \varphi(m) + \varphi(n)\,,$$

és $e^2 = e$ miatt

$$\varphi(mn) = (mn)e = (mn)e^2 = (me)(ne) = \varphi(m)\varphi(n)\,.$$

Emiatt az

$$R = \{ne \,:\, n \in \mathbb{Z}\} = \mathrm{Im}(\varphi)$$

halmaz részgyűrű T-ben. Az is világos, hogy $R \subseteq P$, hiszen R elemei az e-ből összeadással és kivonással kaphatók.

Vizsgáljuk először azt az esetet, amikor T karakterisztikája nulla. Ekkor az e elem rendje az összeadásra végtelen, vagyis $m \neq n \in \mathbb{Z}$ esetén $me \neq ne$. Így φ izomorfizmus $\mathbb{Z}$ és R között. Mivel P osztásra is zárt, benne vannak az $(me)/(ne)$ hányadosok is minden olyan esetben, amikor $m, n \in \mathbb{Z}$ és $m \neq 0$. Az 5.6.5. Következmény miatt ezek résztestet alkotnak, amely hányadosteste R-nek. Mivel R izomorf $\mathbb{Z}$-vel, és $\mathbb{Z}$ hányadosteste $\mathbb{Q}$, az R hányadosteste is $\mathbb{Q}$-val izomorf a hányadostest egyértelműsége miatt.

Most tegyük föl, hogy T karakterisztikája a p prímszám. Ekkor

$$\mathrm{Im}(\varphi) = R = \{e, 2e, 3e, \dots, (p-1)e, 0\}\,,$$

hiszen e rendje az összeadásra p. Megmutatjuk, hogy $R = P$, és hogy ez a résztest $\mathbb{Z}_p$-vel izomorf. A homomorfizmus-tétel szerint $\mathrm{Im}(\varphi) \cong \mathbb{Z} \,/\, \mathrm{Ker}(\varphi)$. A $\mathrm{Ker}(\varphi)$ elemei azok az n

egészek, melyekre $ne = 0$. Mivel e rendje p, az elemrend tulajdonságai miatt ezek az n számok pont p többszörösei, tehát

$$R = \mathrm{Im}(\varphi) \cong \mathbb{Z}/(p) \cong \mathbb{Z}_p \ .$$

Tehát R test, részteste T-nek. Mivel P a legszűkebb résztest, $P \subseteq R$. Azt, hogy $R \subseteq P$ már korábban beláttuk. Ezért $P = R \cong \mathbb{Z}_p$. □

A fenti bizonyításból az is kiderült, hogy P a T egységeleme által generált résztest. Testek között generálásról a következő fejezetben lesz szó.

5.7.9. Definíció. Egy testet *prímtestnek* nevezünk, ha nincs valódi részteste.

Azt láttuk tehát be, hogy a prímtestek izomorfia erejéig a $\mathbb{Z}_p$ testek, ahol p prímszám, valamint a $\mathbb{Q}$. Minden testnek a legszűkebb részteste prímtest. Az eddig elmondottak ferdetestekre is ugyanúgy érvényesek.

Gyakorlatok, feladatok

5.7.10. Gyakorlat. Legyen $\varphi : T \to S$ nem azonosan nulla homomorfizmus, ahol S és T testek. Mutassuk meg, hogy φ injektív, és a T és az S karakterisztikája egyenlő.

5.7.11. Gyakorlat. Legyen T test és $\varphi : T \to T$ nem azonosan nulla homomorfizmus. Mutassuk meg, hogy φ fixen hagyja T prímtestének az elemeit.

5.7.12. Gyakorlat. Mutassuk meg, hogy ha egy K test karakterisztikája nem kettő, akkor felírható benne a másodfokú egyenlet megoldóképlete, és ezért ha K minden eleméből vonható négyzetgyök, akkor nincs K fölött másodfokú irreducibilis polinom. Igaz-e ez az utóbbi állítás kettő karakterisztikájú testben is?

5.8. Rendezett gyűrűk és testek

Ebben a szakaszban vázlatosan áttekintjük, melyek azok a részben algebrai, részben halmazelméleti, részben az analízisből származó konstrukciók, amelyek segítségével a számok fogalmát felépíthetjük egészen a komplex számokig. Menet közben arra a kérdésre fogunk koncentrálni, hogy mely gyűrűkben lehet egyenlőtlenségeket használni, és ennek mik a pontos szabályai.

Kiindulópontunk a természetes számok halmaza. Ezek értelmezése már nem az algebrához, hanem a matematika alapjaihoz (tehát a halmazelmélethez és a logikához) tartozó feladat. Kétféle megközelítés szokásos. Az egyik, úgynevezett Peano-féle axiómarendszer csak a természetes számokat axiomatizálja. Alapvető fogalma a „rákövetkező”, vagyis az adottnál eggyel nagyobb természetes szám fogalma. Fontos még megemlíteni azt az axiómát, amely a teljes indukcióval való bizonyítást teszi lehetővé. A Peano-axiómák segítségével föl lehet építeni a természetes számok közötti műveleteket is, és be lehet bizonyítani a szokásos tulajdonságaikat, például az összeadás asszociativitását.

Ennél sokkal gyakrabban alkalmazott, és messzebbre mutató az a bevezetési mód, amely a természetes számok fogalmát a halmazelmélet szokásos, *Zermelo-Fraenkel-féle* axiómarendszerén belül tárgyalja. A természetes számokat az úgynevezett rendszámok speciális eseteként lehet megfogni. A teljes indukció axiómáját itt az a tétel helyettesíti, hogy természetes számok minden nem üres halmazának van legkisebb eleme.

Akármelyik felépítést választjuk is, a természetes számok halmazáról (a nullát is beleértve) kiderül, hogy az összeadásra és a szorzásra nézve is neutrális elemes félcsoport, továbbá érvényes a disztributivitás. Van azonban a természetes számoknak még egy tulajdonsága, amelyről eddig algebrai szemmel nem volt szó, ez pedig az, hogy közöttük egyenlőtlenségeket írhatunk föl, amelyek a műveletekkel kapcsolatban „jól" viselkednek.

5.8.1. Definíció. Legyen P nem üres halmaz. Azt mondjuk, hogy a kétváltozós $\leq$ reláció *részben rendezés* (vagy *parciális rendezés*) a P halmazon, ha

(1) reflexív (vagyis $a \leq a$ minden $a \in P$-re);
(2) tranzitív (vagyis $a \leq b$ és $b \leq c$-ből $a \leq c$ következik);
(3) *antiszimmetrikus*, vagyis $a \leq b$ és $b \leq a$ esetén $a = b$.

A $\leq$ részben rendezést *elrendezésnek* nevezzük, ha

(4) *trichotóm*, vagyis tetszőleges $a, b \in P$ esetén $a \leq b$ vagy $b \leq a$.

Ha $\leq$ részben rendezés, akkor használjuk a szokásos többi jelölést is: $a \geq b$ azt jelenti, hogy $b \leq a$, és $a < b$ azt, hogy $a \leq b$ de $a \neq b$. Egy részben rendezéssel ellátott P halmazt *részben rendezett* halmaznak nevezünk. Ha a rendezés trichotom, akkor a részben rendezett halmaz neve *lánc*.

Szokás az elrendezést néha teljes rendezésnek is nevezni. Mi ezt az elnevezést nem használjuk, mert összekeverhető egy másik ugyanilyen nevű fogalommal, amelyről ebben a szakaszban később lesz szó.

Ha P egy X halmaz összes részhalmazaiból áll, és $\leq$ a „részhalmaz"-reláció (vagyis a $\subseteq$), akkor részben rendezett halmazt kapunk, amelynek a rendezése azonban nem trichotóm (ha X elemszáma legalább kettő), hiszen meg lehet adni két részhalmazt úgy, hogy egyik se tartalmazza a másikat. Ha viszont a valós számok halmazát nézzük a szokásos $\leq$ relációra nézve, akkor elrendezett halmazt kapunk.

5.8.2. Definíció. Ha $P \subseteq Q$, és Q részben rendezett halmaz a $\leq$ rendezésre, akkor a $\leq$ rendezés *megszorítása* P-re az a $\leq'$ rendezés, amelyre $a, b \in P$ esetén $a \leq' b$ akkor és csak akkor, ha $a \leq b$. Ilyenkor a $\leq$ rendezést a $\leq'$ rendezés (P-re való egyik) *kiterjesztésének* nevezzük.

A rendezés kiterjesztésének a fogalma azért fontos, mert amikor a természetes számokból kiindulva a valós számokat szeretnénk felépíteni, akkor nemcsak a műveleteket, hanem a rendezést is ki szeretnénk terjeszteni rájuk.

Akár a Peano-axiómákat, akár a halmazelmélet axiómarendszerét választjuk kiindulópontnak, a természetes számok halmazán definiálhatjuk a szokásos $\leq$ relációt, amely elrendezés, és érvényes, hogy

$$a \leq b \quad \text{esetén} \quad a + c \leq b + c \quad \text{és} \quad ac \leq bc\,.$$

A következő lépés az, hogy a természetes számokból elkészítjük az egész számokat. Ez az eljárás nagyon hasonlít ahhoz, amikor a hányadostestet konstruáltuk, és ezért részletesen nem beszélünk róla. Természetesen a pozitív egészek rendezését is ki akarjuk terjeszteni az egész számok rendezésévé.

Az eljárás során tekinteni kell az (a, b) párok halmazát, ahol a és b természetes számok, de most az (a, b) párt nem a/b-nek, hanem $a - b$-nek képzeljük. Ennek megfelelően definiáljuk a $\sim$ relációt is közöttük: $(a, b) \sim (c, d)$ akkor és csak akkor, ha $a + d = b + c$. Az egész számok a $\sim$ reláció osztályai lesznek. A természetes számokat ennek egy részhalmazával azonosítjuk a hányadostestnél látott módon.

Így megkapjuk az egész számok halmazát, amelyről kiderül, hogy gyűrű, sőt rendezett gyűrű az alábbi értelemben.

5.8.3. Definíció. Egy R szokásos gyűrűt *részben rendezett gyűrűnek* nevezünk, ha értelmezett rajta egy $\leq$ részben rendezés úgy, hogy tetszőleges $a, b, c \in R$-re

(1) $a \leq b$ esetén $a + c \leq b + c$;
(2) $a \leq b$ és $c \geq 0$ esetén $ac \leq bc$.

Az R *rendezett gyűrű*, ha a $\leq$ elrendezés.

Vigyázzunk tehát, egy egyenlőtlenséget csak nemnegatív számmal szabad megszorozni (mint ezt középiskolából tudjuk is). Az egész számok gyűrűje tehát rendezett gyűrű.

5.8.4. Gyakorlat. Mutassuk meg, hogy ha R részben rendezett gyűrű, $a \leq b \in R$ és $c < 0$, akkor $ac \geq bc$.

A következő lépcső az, hogy a racionális számokat megkonstruáljuk az egész számokból. Ezt a módszert részletesen leírtuk a hányadostestről szóló 5.6. Szakaszban, a rendezésről azonban nem ejtettünk szót. Most ezt a hiányt pótoljuk.

5.8.5. Definíció. Az R részben rendezett gyűrű *pozitivitástartományán* azon r elemeinek halmazát értjük, melyekre $r > 0$. Ezeket az elemeket *pozitívnak* nevezzük.

Vegyük észre, hogy a P pozitivitástartomány egyértelműen meghatározza a rendezést, hiszen $a < b$ akkor és csak akkor igaz, ha $b - a \in P$.

5.8.6. Gyakorlat. Legyen R szokásos gyűrű. Mutassuk meg, hogy egy $P \subseteq R$ halmaz akkor és csak akkor pozitivitástartomány az R egy alkalmas részben rendezésére nézve, ha zárt az összeadásra, a szorzásra, és nem tartalmazza R nullelemét. Igazoljuk, hogy a P-hez tartozó részben rendezés pontosan akkor elrendezés, ha minden $r \neq 0$ esetén r vagy $-r$ eleme P-nek.

5.8.7. Gyakorlat. Legyen R részben rendezett szokásos gyűrű, és T a hányadosteste. Mutassuk meg, hogy T-nek egyetlen olyan rendezése van, amely R rendezésének kiterjesztése, és ennek a pozitivitástartománya

$$P = \{a/b \in T \,:\, a, b > 0\}\,.$$

Mutassuk meg azt is, hogy ha R rendezése elrendezés, akkor T rendezése is az.

A valós számok konstrukciója a racionális számokból az analízis eszközeivel történik. Úgy képzelhetjük, hogy „be kell tömködni a lukakat a számegyenesen". A „lukak" megadásának több módja ismeretes. Szokásos például hozzájuk tartó Cauchy-sorozatokkal megadni őket. Ekkor a valós számokat Cauchy-sorozatoknak definiálhatjuk, két ilyen sorozatot ekvivalensnek mondva, ha „ugyanoda konvergálnak", azaz ha a különbségük nullához tart. Az így kapott ekvivalencia-osztályokon bevezethetjük a műveleteket (ez valójában egy faktorgyűrű), és a rendezést. Szokás ezt az eljárást úgy fogalmazni, hogy a racionális számokat „teljessé tesszük".

Ezt az eljárást általánosabban is elvégezhetjük. Ahhoz, hogy Cauchy-sorozatokról beszélhessünk, szükség van egy *távolságfogalomra* a gyűrű elemei között (a racionális számok esetében ez a két szám különbségének az abszolút értéke). Ez a távolságfogalom az általános esetben származhat a topológiából, de az algebrából is az úgynevezett *értékeléselmélet* keretében.

A lukak betömésének másik lehetséges módja a racionális számok rendezésén alapszik. Ha például a $\sqrt{2}$ számot akarjuk megtalálni, akkor a racionális számokat két részre vághatjuk: azokra, amelyek négyzete kisebb kettőnél, és a többiekre. Az első halmaz mindegyik eleme kisebb a második halmaz mindegyik eleménél, és a két halmaz uniója kiadja az összes racionális számot. Az ilyen felbontást *Dedekind-szeletnek* nevezzük. Ha ezek segítségével bővítünk, akkor azt szokás mondani, hogy „a rendezést teljessé tettük". Az ennek megfelelő általános fogalom a teljes háló, amit a hálóelmélet során tárgyalunk.

A komplex számok halmazát szintén részletesen megkonstruáltuk már a valós számokból kiindulva (lásd 1.6. Szakasz). A rendezést azonban nem lehet a komplex számokra kiterjeszteni.

5.8.8. Állítás. *Ha egy gyűrű elrendezhető, akkor minden nem nulla elem négyzete pozitív bármelyik rendezésnél, és nem nulla elemek négyzetösszege nem lehet nulla.*

Bizonyítás. Legyen $\leq$ elrendezés az R szokásos gyűrűn, és $r \neq 0$ eleme R-nek. Ha $r > 0$, akkor nyilván $r^2 \geq 0$, de nem lehet nulla, hiszen R nullosztómentes. Ha r nem pozitív, akkor a trichotómia miatt $r < 0$, vagyis $-r > 0$, és ekkor is $r^2 = (-r)(-r) > 0$. Tehát a nem nulla elemek négyzetei benne vannak R pozitivitástartományában, és így az 5.8.6. Gyakorlat miatt összegük is pozitív. □

Speciálisan a komplex számok teste nem elrendezhető, hiszen itt $i^2 + 1^2 = 0$.

5.8.9. Feladat. Igazoljuk az előző állítás megfordítását, vagyis azt, hogy ha egy R szokásos gyűrűben igaz, hogy nem nulla elemek négyzetösszege nem lehet nulla, akkor R elrendezhető.

Végül megemlítjük Frobenius tételét (5.10.4. Tétel, be is látjuk majd), amely egyfajta bizonyíték arra, hogy a számok fogalmát nem érdemes a komplex számokon túlmenően kiterjeszteni.

Egy érdekes kezdeményezés az úgynevezett *nem sztenderd analízis*, amely a matematikai logika eszközeivel bevezeti a végtelen kis számok fogalmát. Ezek segítségével az analízis elemi fogalmai szemléletesen (de mégis teljesen precízen) tárgyalhatók. Például egy függvény akkor folytonos, ha az argumentumát végtelen kis értékkel megmozdítva az értéke is végtelen kicsit változik. Ez a fogalmazás sokkal közelebb áll a fizikához és a mindennapi szemléletünkhöz, mint az „epszilon-deltás" definíció. A nem sztenderd analízis is a számfogalom kiterjesztésének tekinthető. Hasonló, nem sztenderd számfogalom segítségével vizsgálhatók a fizika idővel kapcsolatos paradoxonjai, és számítógépes programok helyessége is.

Gyakorlatok, feladatok

5.8.10. Gyakorlat. Bizonyítsuk be, hogy a $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ gyűrűknek csak egy rendezése van, a szokásos.

5.8.11. Gyakorlat. Hány rendezése van a $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}\}$ gyűrűnek?

5.9. Minimálpolinom algebrákban

Az euklideszi gyűrűkről tanultak lehetővé teszik, hogy a lineáris algebrában tanult minimálpolinom fogalmát általánosítsuk. A kapott eredményeket föl fogjuk használni testek vizsgálatára a következő fejezetben, és Frobenius tételének bizonyításában is.

Lineáris algebrában mátrixok és lineáris transzformációk minimálpolinomjáról beszéltünk. Ha például F a 90 fokos forgatás a síkon, akkor $F^2 + I = 0$, ahol I a sík identikus leképezése. Ezt úgy is felfoghatjuk, hogy F „gyöke" az x^2+1 polinomnak. Igen hasznosnak bizonyult meghatározni, hogy egy transzformáció mely polinomoknak a gyöke, mert ez segített a transzformáció megértésében (sajátértékek, invariáns alterek, diagonalizálhatóság). Az derült ki, hogy minden A transzformációnak van egy m_A-val jelölt *minimálpolinomja*, amelyre igaz, hogy

$$f(A) = 0 \iff m_A \mid f$$

tetszőleges f polinom esetén. Más szóval A pontosan az m minimálpolinom többszöröseinek lesz gyöke.

Hasonló jelenséggel már ebben a könyvben is találkoztunk. Melyek azok a *valós együtthatós* f polinomok, melyeknek az i komplex szám gyöke? A 4.5.22. Gyakorlat megoldásában már látott gondolatmenet szerint ha $f(i) = 0$, akkor az i konjugáltja, vagyis a $-i$ is gyöke f-nek, és ezért a polinomból kiemelhető $(x + i)(x - i) = x^2 + 1$. Vagyis az olyan $f \in \mathbb{R}[x]$ polinomok, amelyeknek az i gyöke, pontosan az $x^2 + 1$ többszörösei. Ezért az $x^2 + 1$ polinomot az i minimálpolinomjának is tekinthetjük a valós számok fölött.

A számelméletben sokszor nem valós, hanem racionális együtthatós polinomokat keresünk, melyeknek egy adott komplex szám gyöke. Hogyan lehet ezeket áttekinteni? Például

a $\sqrt[3]{2}$ gyöke az $x^3 - 2$ racionális együtthatós polinomnak. Igaz-e, hogy egy racionális együtthatós f polinomnak csak akkor lehet gyöke, ha f osztható $x^3 - 2$-vel? Az Olvasó, ha megoldotta a 3.5.16. Feladatot, könnyen láthatja, hogy a válasz igenlő. Az $x^3 - 2$ ugyanis irreducibilis a Schönemann–Eisenstein-kritérium miatt, és így f-vel vett kitüntetett közös osztója vagy 1, vagy $x^3 - 2$ lesz. De ha $f(\sqrt[3]{2}) = 0$, akkor az első esetet kizárhatjuk, mert ekkor $x - \sqrt[3]{2}$ közös osztója $\mathbb{C}[x]$-ben ennek a két polinomnak, vagyis $\mathbb{C}$ fölött nem konstans a kitüntetett közös osztó. De a kitüntetett közös osztó ugyanaz $\mathbb{Q}$ és $\mathbb{C}$ fölött (3.2.5. Gyakorlat), és így $\mathbb{Q}$ fölött sem lehet konstans. Összefoglalva: egy racionális együtthatós polinomnak akkor és csak akkor gyöke a $\sqrt[3]{2}$ szám, ha osztható $x^3 - 2$-vel.

5.9.1. Definíció. Az $m \in \mathbb{Q}[x]$ polinomot akkor nevezzük a z komplex szám minimálpolinomjának $\mathbb{Q}$ fölött, ha minden racionális együtthatós f polinomra igaz, hogy z akkor és csak akkor gyöke f-nek, ha $m \mid f$.

Ez a definíció-kísérlet több problémát fölvet. Honnan tudhatjuk, hogy ilyen m polinom létezik-e minden z számhoz? Legyen például $z = \sqrt{2} + \sqrt{3}$. Ekkor $z - \sqrt{2} = \sqrt{3}$, ahonnan négyzetre emeléssel $z^2 - 2\sqrt{2}z + 2 = 3$. Átrendezve $z^2 - 1 = 2\sqrt{2}z$, és ismét négyzetre emelve a másik négyzetgyök is eltűnik, végül $z^4 - 10z^2 + 1 = 0$ adódik. Tehát z gyöke az $m(x) = x^4 - 10x^2 + 1$ polinomnak. Szerencsénk van: ez a polinom is irreducibilis $\mathbb{Q}$ fölött a 3.3.20. Feladat miatt, és így a fenti $\sqrt[3]{2}$-re alkalmazott gondolatmenet most is működik. Ebből arra gondolhatnánk, hogy a minimálpolinom és az irreducibilitás összefügg. Vigyáznunk kell azonban, hiszen tudjuk lineáris algebrából, hogy nem minden lineáris transzformációnak irreducibilis a minimálpolinomja.

Ha viszont $z = \sqrt[3]{7 + 5\sqrt{2}} + \sqrt[3]{7 - 5\sqrt{2}}$, akkor az előző bekezdés technikája csődöt mond: a nyilvánvalónak látszó átrendezés utáni kétszeri köbre emelés nem ejti ki a köbgyököket (és ekkor már kilencedfokú polinomnál tartunk, ha még a négyzetgyököket is meg akarjuk szüntetni, arra gondolhatnánk, hogy 36-nál alacsonyabb fokú polinomnak ez a szám nem lesz gyöke).

5.9.2. Gyakorlat. Bizonyítsuk be, hogy a $z = \sqrt[3]{7 + 5\sqrt{2}} + \sqrt[3]{7 - 5\sqrt{2}}$ szám minimálpolinomja $\mathbb{Q}$ fölött $x^3 + 3x - 14$.

Azt, hogy egy ilyesfajta, gyökvonásokat és alapműveleteket tartalmazó kifejezés mindig gyöke egy nem nulla, racionális együtthatós polinomnak, a 6.2. Szakaszban látjuk majd be, nem számolással, hanem elegáns, testelméleti módszerekkel.

Az 5.9.1. Definícióval a fentieken kívül az is gond, hogy nem eléggé általános: sem a lineáris transzformációk minimálpolinomja, sem pedig az i szám valós fölötti minimálpolinomja nem fér bele. Ebben a szakaszban ezt orvosoljuk, fényt derítünk a minimálpolinom létezésének kérdésére, és az irreducibilitás kérdését is megvizsgáljuk.

Milyen algebrai struktúra lesz a komplex számoknak és a lineáris transzformációk halmazának a közös általánosítása? Ennek a struktúrának az elemeit polinomokba akarjuk helyettesíteni. Ehhez az elemeket össze kell tudni adni, és össze kell tudni szorozni, tehát egy gyűrűre

van szükség. De mik lesznek a keresett minimálpolinom együtthatói? Mátrixok esetében ezek az alaptestben voltak, a fenti példákban valós és racionális számok. Vagyis a keresett struktúra nemcsak gyűrű kell, hogy legyen, hanem még „skalárokkal" is kell tudni szorozni benne. Ilyen struktúráról már tanultuk lineáris algebrában, és algebrának neveztük.

5.9.3. Definíció. Legyen T test. Azt mondjuk, hogy A *algebra* a T fölött, ha A-ban értelmezve van az összeadás, a szorzás, és a T elemeivel, mint skalárokkal való szorzás úgy, hogy

(1) A az összeadásra és a szorzásra gyűrű;
(2) A az összeadásra és a skalárral való szorzásra vektortér T fölött;
(3) tetszőleges $a, b \in A$ és $\lambda \in T$ esetén $\lambda(ab) = (\lambda a)b = a(\lambda b)$.

Az A algebráról akkor mondjuk, hogy egységelemes, kommutatív, vagy nullosztómentes, ha mint gyűrű ilyen. Hasonlóképpen beszélni fogunk az A algebra T fölötti dimenziójáról is (ez alatt a megfelelő vektortér dimenzióját értjük). Az algebrák közötti homomorfizmus egy olyan leképezés, amelyik mindegyik műveletet tartja, azaz lineáris leképezés és gyűrű-homomorfizmus is egyben. Hasonlóan fogunk beszélni részalgebráról is, amely részgyűrű és altér is egyúttal.

Algebrára a legfontosabb példák a következők.

(1) A T test fölötti $n \times n$-es mátrixok halmaza a mátrixok szokásos műveleteire nézve (jele $T^{n\times n}$). Lineáris algebrából tudjuk, hogy egy T fölötti n-dimenziós vektortér lineáris transzformációi egy ezzel izomorf algebrát alkotnak.
(2) A $T[x_1, \ldots, x_n]$ polinomgyűrű a T test fölött.
(3) Tetszőleges K test, amelynek T részteste, a T fölött. Például $\mathbb{C}$ algebra $\mathbb{R}$ vagy $\mathbb{Q}$ fölött.

A (2) és a (3) példában még nem mondtuk meg, mik is a műveletek, a következő gyakorlat ezt pótolja.

5.9.4. Gyakorlat. Tegyük föl, hogy R egységelemes gyűrű, melyben a szorzás műveletét $*$ jelöli. Legyen T részteste R-nek, amely R egységelemét tartalmazza. Definiáljuk a T elemeivel, mint skalárokkal való szorzást R-en úgy, hogy a $\lambda \in T$ és az $r \in R$ elemek szorzata $\lambda * r$ legyen. Igazoljuk a következő állításokat.

(1) Az R gyűrű összeadására, és a most definiált skalárral való szorzásra nézve R vektortér T fölött.
(2) Az R akkor és csak akkor algebra T fölött a megadott műveletekre, ha tetszőleges $\lambda \in T$ és $r \in R$ esetén $\lambda * r = r * \lambda$.

A $\lambda * r = r * \lambda$ feltételt szokás úgy is fogalmazni, hogy T benne van az R gyűrű centrumában. Általában (a csoportokhoz hasonlóan) egy gyűrű (vagy algebra) *centrumán* azoknak az elemeknek a halmazát értjük, amelyek R minden elemével felcserélhetők.

5.9.5. Gyakorlat. Igazoljuk, hogy ha A algebra a T test fölött, és e egységeleme A-nak, akkor a λe alakú elemek, ahol λ befutja T-t, a T-vel izomorf résztestet alkotnak, amely része az algebra centrumának. Igazoljuk, hogy ez a résztest altér is, vagyis részalgebra.

Ha A algebra a T test fölött, és $f \in T[x]$, akkor be szeretnénk helyettesíteni az $a \in A$ elemeket f-be. Például ha $f(x) = x^2 + 1$, akkor mi legyen $f(a)$? Ha x helyébe a-t írunk, akkor $a^2 + 1$ adódik, ami értelmetlen, hiszen az a^2 az A algebrának, az 1 pedig a T testnek az eleme, és így nincs hol összeadni őket. A fenti, forgatásos példában nem is az $F^2 + 1$-et, hanem az $F^2 + I$-t tekintettük. Itt I a lineáris leképezések algebrájának az egységeleme. Vagyis a polinom konstans tagját az algebra egységelemével lesz célszerű megszorozni.

5.9.6. Definíció. Legyen A egy egységelemes algebra a T test fölött, melynek egységelemét e jelöli. Ha

$$f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n \in T[x]\,,$$

és $a \in A$, akkor legyen

$$f(a) = \lambda_0 e + \lambda_1 a + \ldots + \lambda_n a^n \in A\,.$$

Az *a gyöke* f-nek, ha $f(a) = 0$. Az a elem nulladik hatványát is e-nek értelmezzük.

5.9.7. Gyakorlat. Legyen A egységelemes algebra T fölött, $f, g \in T[x]$ és $a \in A$. Mutassuk meg, hogy

$$(f + g)(a) = f(a) + g(a) \quad \text{és} \quad (fg)(a) = f(a)g(a)\,,$$

vagyis az a elem behelyettesítése homomorfizmus $T[x]$-ből A-ba.

Ha A egységelemes algebra, akkor minden $a \in A$ gyöke egy $T[x]$-beli polinomnak: a nullapolinomnak. Az érdekes eset az lesz, amikor az a nemcsak a nullapolinomnak gyöke. Érdemes erre elnevezést is bevezetni, ami a számelméletből származik.

5.9.8. Definíció. Legyen A egységelemes algebra. Az $a \in A$ elemet *algebrai elemnek* nevezzük, ha van olyan nem nulla $T[x]$-beli polinom, amelynek az a elem gyöke. Ha nincs ilyen polinom, akkor az a elem *transzcendens*.

A számelméletben algebrai és transzcendens *számokról* beszélnek, amik a komplex számok $\mathbb{Q}$ fölötti algebrájának algebrai illetve transzcendens elemei. Ezeket tüzetesen megvizsgáljuk majd a következő, Galois-elméletről szóló fejezetben. Például π vagy $2^{\sqrt{3}}$ transzcendens számok, azaz nem gyökei nem nulla racionális együtthatós polinomnak (ezek igen nehéz számelméleti tételek).

A mátrixok között minden elem algebrai. Ennek oka az, hogy az $n \times n$-es mátrixok algebrája n^2, azaz véges dimenziós.

5.9.9. Állítás. *Egy egységelemes, véges dimenziós algebra minden eleme algebrai.*

Bizonyítás. Jelölje e az A algebra egységelemét, dimenzióját pedig n. Ha $a \in A$, akkor az $n + 1$ darab

$$e, a, a^2, \ldots, a^n$$

elem biztosan lineárisan összefügg, vagyis vannak olyan $\lambda_i \in T$ elemek, hogy

$$\lambda_0 e + \lambda_1 a + \ldots + \lambda_n a^n = 0\,,$$

de nem minden együttható nulla. Ezért az a elem gyöke a

$$\lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$$

(legföljebb n-edfokú) nem nulla polinomnak. □

5.9.10. Tétel. *Legyen A egységelemes algebra a T fölött, és $a \in A$ egy algebrai elem. Ekkor egyértelműen létezik egy $T[x]$-beli m_a normált polinom a következő tulajdonsággal: tetszőleges $f \in T[x]$ esetén*

$$f(a) = 0 \iff m_a \mid f\,.$$

Az m_a egyértelműen meghatározható úgy is, mint a legkisebb fokú olyan normált, $T[x]$-beli polinom, amelynek az a elem gyöke.

Bizonyítás. Legyen I azoknak az $f \in T[x]$ elemeknek a halmaza, amelyekre $f(a) = 0$. Azonnal látszik, hogy I ideál $T[x]$-ben, hiszen ha $f, g \in I$, akkor

$$(f+g)(a) = f(a) + g(a) = 0 + 0 = 0\,,$$

és ha $f \in I$, $g \in T[x]$, akkor

$$(fg)(a) = f(a)g(a) = 0g(a) = 0$$

(az 5.9.7. Gyakorlat miatt; hivatkozhattunk volna arra is, hogy az I valójában az ebben a gyakorlatban definiált „a behelyettesítése" homomorfizmus magja). Mivel $T[x]$ euklideszi gyűrű, az 5.5.3. Tétel miatt I főideál, vagyis egy alkalmas m polinom többszöröseiből áll, és az m asszociáltság erejéig egyértelműen meghatározott. Mivel az a elem algebrai, az I ideál nemcsak a nullapolinomból áll, vagyis $m \neq 0$. Ezért m asszociáltjai között egyetlen normált polinom van, ezt jelöljük m_a-val. Nyilván ez az egyetlen polinom, ami kielégíti az (1) állításban szereplő feltételt.

A (2) bizonyításához legyen f olyan normált $T[x]$-beli polinom, amelynek a gyöke. Ekkor persze $f \in I$, és így $m_a \mid f$. Ezért f foka legalább akkora, mint m_a foka. Ha tehát f a lehető legkisebb fokú ilyen polinom, akkor f és m_a foka megegyezik, azaz asszociáltak. Mivel normáltak is, megegyeznek. □

5.9.11. Definíció. Az előző tételben szereplő m_a polinomot az a elem *minimálpolinomjának* nevezzük (és m_a-val jelöljük).

Ha az a elem transzcendens, akkor az I ideál csak a nullapolinomból áll. Ezért szokás azt mondani, hogy transzcendens elem minimálpolinomja a nullapolinom, de azt is, hogy egy transzcendens elemnek nincs minimálpolinomja.

A minimálpolinom nem feltétlenül irreducibilis. Például ha T tengelyes tükrözés a síkon, akkor minimálpolinomja $x^2 - 1$. Van azonban egy nagyon fontos eset, amikor a minimálpolinom irreducibilis lesz.

5.9.12. Tétel. *Legyen A egységelemes algebra T fölött. Ha az $a \in A$ elem gyöke egy normált, irreducibilis $g \in T[x]$ polinomnak, akkor $g = m_a$. Megfordítva, ha A **nullosztómentes**, akkor minden $a \in A$ algebrai elem minimálpolinomja irreducibilis T fölött.*

Bizonyítás. Tegyük föl, hogy $g(a) = 0$, ahol $g \in T[x]$ normált, és irreducibilis T fölött. Ekkor $m_a \mid g$, és g irreducibilitása miatt m_a vagy nem nulla konstans, vagy g-nek asszociáltja. Az első eset nem lehetséges, mert nem nulla konstans polinomnak nincs gyöke A-ban. A második esetben $m_a = g$, hiszen asszociált normált polinomok egyenlőek.

Megfordítva, ha A nullosztómentes, m_a az $a \in A$ elem minimálpolinomja, és $m_a = fg$, ahol $f, g \in T[x]$, akkor

$$0 = m_a(a) = f(a)g(a)$$

miatt vagy $f(a)$, vagy $g(a)$ nulla. Az első esetben $m_a \mid f$ az 5.9.10. Tétel miatt, tehát m_a és f asszociáltak. A második esetben ugyanígy látjuk, hogy m_a és g asszociáltak, és így az $m_a = fg$ felbontás triviális, azaz m_a irreducibilis. □

Ezt a tételt állandóan használjuk majd a Galois-elmélet tárgyalása során. Mivel a komplex számok teste nullosztómentes, a most bizonyított tétel megmagyarázza, hogy miért kaptunk irreducibilis polinomokat, amikor a szakasz elején meghatároztuk i, $\sqrt[3]{2}$ és $\sqrt{2} + \sqrt{3}$ minimálpolinomját.

Gyakorlatok, feladatok

5.9.13. Gyakorlat. Tegyük föl, hogy egy racionális együtthatós polinomnak az $1 + \sqrt{2}$ szám gyöke. Mutassuk meg, hogy akkor az $1 - \sqrt{2}$ is gyöke.

5.9.14. Gyakorlat. Tegyük föl, hogy egy racionális együtthatós polinomnak az $1 + \sqrt[3]{2}$ szám gyöke. Mutassuk meg, hogy akkor a polinom legalább harmadfokú. Meg tudunk adni két másik (komplex) gyököt?

5.9.15. Feladat. Tekintsük a komplex számok $A = \mathbb{C}$ algebráját a racionális számok $\mathbb{Q}$ teste fölött. Határozzuk meg ebben az alábbi elemek minimálpolinomját.

(1) $1 + i$.
(2) $\sqrt{2} + i$.
(3) $\sqrt[3]{2 + \sqrt{2}}$.
(4) $\cos 20^\circ + i \sin 20^\circ$.
(5) Tetszőleges primitív n-edik egységgyök.
(6) $\cos 20^\circ$.

5.9.16. Gyakorlat. Legyen A algebra a T test fölött, és $a \in A$. Mutassuk meg, hogy az a által generált részalgebra A-ban

$$\{f(a) \,:\, f \in T[x],\, f(0) = 0\}\,.$$

Ha A kommutatív, akkor mik lesznek az $a_1, \ldots, a_n$ által generált részalgebra elemei?

5.10. A számfogalom lezárása

A számfogalom felépítése kapcsán fölmerült a kérdés, hogy „meddig kell elmennünk”, mi az, amit még számnak érdemes tekinteni. Ahogy régebben a valós számokat gondoltuk „számnak”, és mégis rájöttünk, hogy a komplex számokat is érdemes számnak tekinteni, nem lehetséges-e, hogy a valós számokat máshogy is kibővíthetjük? Ebben a szakaszban bebizonyítjuk Frobenius tételét, amely azt mutatja, hogy természetes feltételek mellett a komplex számoknál nem érdemes tovább lépni, illetve ha a kommutativitástól eltekintünk, akkor még egy ferdetest az, ami esetleg szóba jön. Elsőként ezt a ferdetestet ismertetjük.

A 4.6.14. Gyakorlat előtt definiáltuk a nyolcelemű kvaterniócsoport fogalmát. Ennek elemeiből most egy algebrát fogunk készíteni, mely a

$$p + qi + rj + sk$$

alakú formális kifejezésekből áll, ahol p, q, r, s valós számok, i, j, k pedig a Q kvaterniócsoport elemei. A műveleteket a komplex számok nem precíz bevezetéséhez hasonlóan definiáljuk, vagyis két ilyen elem összegét összevonással:

$$(p+qi+rj+sk)+(p'+q'i+r'j+s'k) = (p+p')+(q+q')i+(r+r')j+(s+s')k\,,$$

két ilyen elem szorzatát pedig úgy, hogy a disztributivitás alapján kibontjuk a zárójeleket (ekkor $4\cdot 4 = 16$ tag keletkezik), a valós együtthatókat minden tagon belül kigyűjtjük balra (vagyis feltesszük, hogy a valós együtthatók Q elemeivel felcserélhetők), a szorzásokat a kvaterniócsoportban elvégezzük, majd az egyforma tagokat összevonjuk. A kvaterniócsoportban szereplő $-i$ elemet azonosítjuk az i elem -1-szeresével, és hasonlóan járunk el a $-j$ és a $-k$ esetében is. Így például

$$(j+k)^2 = jj + jk + kj + kk = (-1) + i + (-i) + (-1) = -2\,.$$

A kapott elemeket *kvaternióknak* nevezzük, halmazukat $\mathbb{K}$ jelöli.

5.10.1. Gyakorlat. A fenti definíció alapján írjuk föl két általános elem szorzatát a kvaterniók között. Mutassuk meg, hogy a

$$\varphi(p+qi+rj+sk) = \begin{bmatrix} p+qi & r+si \\ -r+si & p-qi \end{bmatrix}$$

leképezés injektív gyűrű-homomorfizmus a $\mathbb{K}$-ból a $\mathbb{C}^{2\times 2}$ gyűrűbe, és így a kvaterniók maguk is gyűrűt alkotnak a megadott műveletekre.

Az 5.9.4. Gyakorlat miatt $\mathbb{K}$ algebra lesz $\mathbb{R}$ fölött, hiszen a szorzás definíciójánál láttuk, hogy a valós számok felcserélhetők a kvaterniókkal. Most megmutatjuk, hogy $\mathbb{K}$ ferdetest. Ezzel az első példát látjuk (nemkommutatív) ferdetestre.

5.10.2. Definíció. A $z = p + qi + rj + sk$ kvaternió *konjugáltján* a

$$\overline{z} = p - qi - rj - sk$$

kvaterniót értjük. A z *normája*

$$N(z) = z\overline{z} = p^2 + q^2 + r^2 + s^2 .$$

5.10.3. Gyakorlat. Igazoljuk az előző definícióban szereplő $z\overline{z} = p^2 + q^2 + r^2 + s^2$ összefüggést, továbbá azt, hogy $z, w \in \mathbb{K}$ esetén

$$\overline{zw} = \overline{w}\,\overline{z} ,$$

és ebből hogy $N(zw) = N(z)N(w)$. A komplex számok analógiájára adjunk képletet egy kvaternió inverzére, és mutassuk meg, hogy $\mathbb{K}$ ferdetest.

5.10.4. Tétel [Frobenius-tétel]. *Ha A egy $\mathbb{R}$ fölötti véges dimenziós, nullosztómentes nem nulla algebra, akkor A izomorf a valós számok, a komplex számok, vagy a kvaterniók algebrájával.*

Bizonyítás. Elsőként azt látjuk be, hogy az algebra ferdetest. Legyen $0 \neq a \in A$, és tekintsük az $x \mapsto xa$ leképezést. A műveletek tulajdonságai miatt ez összeg- és skalárszorostartó, vagyis lineáris leképezés. Mivel A nullosztómentes, ez a leképezés injektív. Lineáris algebrából tudjuk (a dimenziótétel miatt), hogy egy véges dimenziós vektortéren minden injektív lineáris transzformáció szürjektív is. Ez azt jelenti, hogy $Ra = R$. Ezzel beláttuk, hogy A-nak nincs nemtriviális balideálja (hiszen minden nem nulla eleme az egész A-t generálja, mint balideált). Az 5.3.8. Tétel miatt A ferdetest, speciálisan egységelemes.

Érdemes a fenti gondolatmenetet összevetni a 5.3.5. Tétel bizonyításával. Látszik, hogy a végességet sokszor helyettesíthetjük azzal, ha a vizsgált dolog véges dimenziós.

Az A algebra egységelemét e-vel fogjuk jelölni. Az 5.9.5. Gyakorlat szerint az re alakú elemek, ahol $r \in \mathbb{R}$, a valós számok testével izomorf résztestet, sőt részalgebrát alkotnak A-ban. Ezt a résztestet R jelöli. Ha A dimenziója 1, akkor $R = A$, és így A izomorf a valós számok önmaga fölötti algebrájával. Ebben az esetben tehát készen vagyunk a bizonyítással.

5.10.5. Állítás. *Legyen $a \in A$, melyre $a \notin R$. Ekkor létezik olyan $a' \in A$ elem, hogy $(a')^2 = -e$, az $\{e, a\}$ és az $\{e, a'\}$ halmazok ugyanazt az alteret generálják, és ez a komplex számok $\mathbb{R}$ fölötti algebrájával izomorf részalgebra A-ban.*

Bizonyítás. Mivel A véges dimenziós, minden eleme algebrai (5.9.9. Tétel). De A nullosztómentes is, tehát minden elemének a minimálpolinomja irreducibilis $\mathbb{R}$ fölött (5.9.12. Tétel). A valós test fölött az irreducibilis polinomok első, vagy másodfokúak (3.3.7. Tétel).

Ha az a elem minimálpolinomja elsőfokú, azaz $x - r$ alakú, ahol $r \in \mathbb{R}$, akkor $a - re = 0$, vagyis $a = re$. Az ilyen a elemek tehát pontosan az R résztest elemei. Mivel föltettük, hogy $a \notin R$, ez az eset nem lehetséges.

Ha az a elem minimálpolinomja másodfokú, mondjuk $x^2 + 2px + q$, akkor teljes négyzetté való kiegészítéssel

$$0 = a^2 + 2pa + qe = (a + pe)^2 + (q - 4p^2)e .$$

Itt $q - 4p^2 > 0$, különben az $x^2 + 2px + q$ polinomnak volna valós gyöke, és így nem lenne irreducibilis. Jelölje s a $q - 4p^2$ számnak az egyik (valós) négyzetgyökét. Ekkor s^2-tel osztva $(a')^2 = -e$ adódik, ahol $a' = (1/s)a + (p/s)e$. De így az $ue + va'$ alakú elemek, ahol $u, v \in \mathbb{R}$, a komplex számokkal izomorf résztestet (sőt részalgebrát) alkotnak A-ban, hiszen a $\varphi : u + vi \to ue + va'$ kölcsönösen egyértelmű, művelettartó leképezés.

A szorzás művelettartása a közvetlen számoláson túl abból látszik, hogy az egyetlen szabály, amit felhasználunk a szorzatok kiszámítására egyforma a két algebrában: a komplex számoknál $i^2 = -1$, az A algebrában pedig $(a')^2 = -e$. A 6.4.8. Tételben általánosítjuk majd ezt az észrevételt.

Természetesen az $\{e, a\}$ és az $\{e, a'\}$ ugyanazt az alteret generálják A-ban, hiszen a' az e és a elemek lineáris kombinációja, és fordítva, $a = sa' - pe$ az e és az a' lineáris kombinációja. □

Ezzel beláttuk a Frobenius-tételt abban az esetben, ha A dimenziója legföljebb kettő. Megjegyezzük, hogy ha $e, a_1, \ldots, a_k$ lineárisan független rendszer, akkor az előző állítást mindegyik a_i-re alkalmazva egy olyan $e, a_1', \ldots, a_k'$ rendszert kapunk, hogy minden i-re $(a_i')^2 = -e$, az új rendszer szintén lineárisan független, és az általa generált altér ugyanaz, mint az $e, a_1, \ldots, a_k$ által generált altér. Ennek igazolása egyszerű számolás lineáris kombinációkkal, amit az Olvasóra hagyunk.

5.10.6. Állítás. *Legyen $a \in A$, melyre $a \notin R$. Ha az $x \in A$ elemre $xa = ax$, akkor x benne van az e és a által generált altérben.*

Bizonyítás. Ha $x \in R$, akkor készen vagyunk, tegyük föl, hogy nem ez a helyzet. Mivel a és x fölcserélhető, nyilván a $pe + qa$ és az $re + sx$ elemek is fölcserélhetők tetszőleges $p, q, r, s \in \mathbb{R}$ esetén. Speciálisan az előző állításból kapott a' és x' elemek is felcserélhetők. Így viszont

$$(x' + a')(x' - a') = (x')^2 - (a')^2 = -e + e = 0\,.$$

Ezért A nullosztómentessége miatt $x' = a'$ vagy $x' = -a'$. Mindkét esetben ugyanaz az $\{e, a'\}$ és az $\{e, x'\}$ halmazok által generált altér. Az előző állítás szerint tehát az $\{e, a\}$ és az $\{e, x\}$ generálta altér is ugyanaz, vagyis x benne van az e és a által generált altérben. □

5.10.7. Állítás. *Ha az $e, a, b \in A$ elemek lineárisan függetlenek, és $a^2 = b^2 = -e$, akkor $ab + ba \in R$.*

Bizonyítás. Az $x = ab + ba$ elem felcserélhető a-val, hiszen $a^2b = -eb = -b = ba^2$ miatt

$$a(ab + ba) = -b + aba = (ab + ba)a\,.$$

Ezért az előző állítás miatt x benne van az $\{e, a\}$ által generált altérben. Az a és b cseréjével kapjuk, hogy x benne van az $\{e, b\}$ által generált altérben is. Mivel e, a, b lineárisan függetlenek, e két altér metszete az e által generált altér, vagyis R. □

Az imént „bázistranszformációt” hajtottunk végre, hogy megkapjuk az $\{e, a\}$ által generált altérben az i-nek megfelelő elemet. Most is ugyanezt tesszük, hogy a kvaterniókkal való izomorfizmust bizonyíthassuk.

5.10.8. Állítás. *Tegyük föl, hogy az $e, a, b \in A$ lineárisan független elemekre teljesül, hogy $a^2 = b^2 = -e$. Ekkor az $\{e, ab\}$ által generált altérnek van olyan c eleme, amelyre $c^2 = -e$. Minden ilyen c elemre $ac = -ca$, az $\{e, a, b, ab\}$ és az $\{e, a, c, ac\}$ ugyanazt a K alteret generálják, és K a kvaterniók algebrájával izomorf részalgebra A-ban.*

Bizonyítás. Tudjuk, hogy az e és a által generált altér részteste A-nak (ami $\mathbb{C}$-vel izomorf). Az ab ebben tehát nem lehet benne, mert ha így lenne, akkor a-val balról osztva kapnánk, hogy b is benne van ebben az altérben, ami ellentmond annak, hogy e, a, b függetlenek. Hasonlóan kapjuk, hogy ab nincs benne az e és b által generált altérben sem.

Speciálisan e és ab is függetlenek, vagyis az 5.10.5. Állítás miatt van olyan c elem az e és ab által generált altérben, melyre $c^2 = -e$. Minden ilyen c-re igaz, hogy felcserélhető ab-vel, továbbá, hogy e, a, c és e, b, c is független rendszer. Ezért az előző állítás miatt $ac + ca = ue$ és $bc + cb = ve$ alkalmas $u, v \in \mathbb{R}$ számokra. De akkor

$$ub = (ac + ca)b = acb + c(ab) = acb + (ab)c = a(cb + bc) = av\,.$$

Mivel a és b függetlenek, innen $u = v = 0$, vagyis $ac + ca = 0$.

Megmutatjuk, hogy a

$$\varphi : p + qi + rj + sk \to pe + qa + rc + sac$$

megfeleltetés injektív homomorfizmus a kvaterniók $\mathbb{K}$ algebrájából A-ba. Az összegtartás nyilvánvaló. Ahogy a komplex számok esetében elég volt ellenőrizni, hogy az i komplex szám a' képére $(a')^2 = -e$ teljesül, úgy most is elegendő a szorzattartást az $\{i, j, k\}$ halmazon ellenőrizni, hiszen ha itt ismerjük a szorzatokat, abból már bármely két elem szorzata felírható. Tudjuk, hogy $a^2 = c^2 = -e$, és $ac = -ca$. Ezek felhasználásával az $\{a, c, ac\}$ halmaz bármely két elemének a szorzata már triviálisan kiszámítható, és könnyű ellenőrizni, hogy a szorzattartás tényleg teljesül.

A φ leképezés képhalmaza az e, a, c, ac által generált K altér. Mivel $\mathbb{K}$ ferdetest, nincs nemtriviális ideálja, és így a φ (nyilvánvalóan nem azonosan nulla) gyűrű-homomorfizmus magja csak a $\{0\}$ lehet. Ezért φ injektív. Ez azt jelenti, hogy a K altér egy $\mathbb{K}$-val izomorf részalgebra.

Tudjuk, hogy e és c ugyanazt az alteret generálja, mint e és ab (hiszen $c^2 = -e$ miatt $c \notin R$). Ezért ab eleme K-nak. Mivel K részalgebra, benne van $-a(ab) = b$ is. Legyen $V \subseteq K$ az $\{e, a, b, ab\}$ által generált altér. Ebben benne van c, de ac is mert $c = ue + vab$ alkalmas $u, v \in \mathbb{R}$ számokra, és így $ac = ua + va^2b = ua - vb$. Ezért $V = K$. □

Most már rátérhetünk a tétel bizonyítására. Tegyük föl, hogy A legalább három dimenziós. Válasszunk az e mellé két független elemet. Az 5.10.5. Állítást követő megjegyzés szerint ezeket módosíthatjuk olyan a és b független elemekké, amelyek négyzete $-e$. Az

előző állítás szerint kapunk egy c elemet, és egy $\mathbb{K}$-val izomorf K részalgebrát. Meg kell mutatni, hogy A-nak nincs több eleme.

Tegyük föl, hogy van egy elem K-n kívül is. Az 5.10.5. Állítás szerint ezt módosíthatjuk egy $d \notin K$ elemmé, amelyre $d^2 = -e$. Az előző állítás miatt e-hez, a-hoz és d-hez van olyan $f \in A$, melyre $\{e, a, f, af\}$ szintén a $\mathbb{K}$-val izomorf L részalgebrát generál. Szintén az előző állítás szerint $d \in L$, és így L nem része K-nak. Emiatt f sincs K-ban, hiszen akkor $L \subseteq K$ lenne, mert az e, a, f elemek már generálják az L részalgebrát.

Tudjuk, hogy $fa = -af$ és $ca = -ac$. Ezért $cfa = -caf = acf$. Ez azt jelenti, hogy cf felcserélhető a-val, vagyis az 5.10.6. Állítás miatt cf benne van az e és a által generált altérben, tehát K-ban is. De $c \in K$, és mivel K részalgebra, $-c(cf) = f \in K$. Ez az ellentmondás bizonyítja Frobenius tételét. □

Frobenius tételét általánosítani lehet úgynevezett *valósan zárt testek* fölötti algebrákra. Ezek a testek olyanok, mint a valós számok, vagyis karakterisztikájuk nulla, rendezhetők, és minden páratlan fokú polinomnak van bennük gyöke. Erről az Olvasó a [**13**] könyv 10.7. Szakaszában találhat részletes információt.

Gyakorlatok, feladatok

5.10.9. Gyakorlat. Mutassuk meg, hogy a Frobenius-tételben szereplő mindhárom feltétel szükséges, vagyis adjunk példát olyan algebrára, amely nem a tételben felsoroltak valamelyike, de

(1) $\mathbb{R}$ fölötti, nullosztómentes (csak nem véges dimenziós);
(2) $\mathbb{R}$ fölötti, véges dimenziós (csak nem nullosztómentes);
(3) nullosztómentes és véges dimenziós (csak nem $\mathbb{R}$ fölötti).

A (3)-ban keressünk olyan példát, amelynek a dimenziója nem 1, 2 vagy 4.

5.10.10. Gyakorlat. Határozzuk meg az $i + j$ és $i + j + k$ kvaterniók négyzetét, inverzét és minimálpolinomját.

5.10.11. Feladat. Adjuk meg az $x^2 - 1$ és az $x^2 + 1$ polinomok összes gyökeit a kvaterniótestben.

5.10.12. Feladat. Bizonyítsuk be, hogy a kvaterniócsoport automorfizmus-csoportja az S_4 szimmetrikus csoporttal izomorf.

5.11. Kommutatív gyűrűk

Ebben a szakaszban kommutatív gyűrűkről mesélünk, az állításokat nem bizonyítjuk. Csak odáig jutunk, hogy megismerkedünk néhány alapvető fogalommal és bevezető tétellel. Kicsit bővebb ismertető olvasható Fried Ervin [**13**] könyvében, ahol az alábbi tételek bizonyítása is szerepel.

A kommutatív gyűrűk legfőbb alkalmazása az, hogy olyan görbéket és felületeket vizsgálhatunk a segítségükkel, amelyeket egy polinom gyökeiként adunk meg. Például az egységgömb felülete az

$$x^2 + y^2 + z^2 - 1$$

polinom összes $\mathbb{R}^3$-beli gyökeiből áll. Az ezzel foglalkozó elmélet az *algebrai geometria*.

Legyen T test (tipikusan a valós, vagy a komplex számtest), és $p \in T[x_1, \ldots, x_n]$ egy polinom. Az $X = (t_1, \ldots, t_n) \in T^n$ pont akkor gyöke p-nek, ha

$$p(t_1, \ldots, t_n) = 0\,.$$

A p összes gyökeinek a halmazát algebrai görbének vagy felületnek, általában algebrai halmaznak nevezzük. Ugyancsak algebrai halmaznak nevezzük több (akár végtelen sok) polinom közös gyökeinek a halmazát is.

Itt egy Galois-kapcsolatról van szó (lásd 8.7. Szakasz): egy $p \in T[x_1, \ldots, x_n]$ polinomot akkor „kötünk össze" egy $X \in T^n$ ponttal, ha X gyöke p-nek, vagyis $p(X) = 0$. A T^n-beli zárt halmazok az algebrai halmazok. A $T[x_1, \ldots, x_n]$ zárt halmazai bizonyos ideálok lesznek.

Legyen V egy algebrai halmaz, és jelölje I azoknak a polinomoknak a halmazát, amelyek V-n eltűnnek (vagyis amelyeknek V minden eleme gyöke). Ezek nyilván ideált alkotnak $T[x_1, \ldots, x_n]$-ben. Van ennek az ideálnak azonban még egy fontos tulajdonsága, nevezetesen az, hogy ha egy p polinomra $p^n \in I$, akkor $p \in I$. Valóban, ha $p^n(X) = 0$, akkor mivel T nullosztómentes, innen $p(X) = 0$ következik. Algebrailag zárt test fölött ezzel le is írtuk az ilyen ideálokat.

5.11.1. Tétel [Hilbert nullahelytétele, „Nullstellensatz"]. *Legyen T algebrailag zárt test, és V a $p_1, \ldots, p_k \in T[x_1, \ldots, x_n]$ polinomok közös T^n-beli gyökeinek a halmaza. Ekkor a V halmazon pontosan azok a p polinomok tűnnek el, amelyek egy alkalmas hatványa benne van a $p_1, \ldots, p_k$ által generált ideálban, vagyis amelyekre létezik olyan n pozitív egész és $f_1, \ldots, f_k \in T[x_1, \ldots, x_n]$, hogy*

$$p^n = p_1 f_1 + \ldots + p_k f_k\,.$$

A tétel végtelen sok p_i polinomra is érvényes, de nevezetes tény, hogy minden algebrai halmaz megadható véges sok polinommal is, mert $T[x_1, \ldots, x_n]$ minden ideálja végesen generált. Az 5.4.3. Tétel szerint ez azzal ekvivalens, hogy az ideálokra érvényes a maximum-feltétel.

5.11.2. Definíció. Az R kommutatív gyűrűt *Noether-gyűrűnek* nevezzük, ha ideáljaira érvényes a maximum-feltétel.

Természetesen minden főideálgyűrű (és ezért minden euklideszi gyűrű, például $\mathbb{Z}$ is) Noether-gyűrű. A $\mathbb{Z}[x, y]$-ról láttuk, hogy nem főideálgyűrű. Az azonban igaz, hogy Noether-gyűrű, vagyis minden ideálja végesen generált.

5.11.3. Tétel [Hilbert bázis-tétele]. *Ha R egységelemes (kommutatív) Noether-gyűrű, akkor az $R[x]$ polinomgyűrű is az. Speciálisan ha T test, vagy euklideszi gyűrű, akkor a $T[x_1, \ldots, x_n]$ gyűrű minden ideálja végesen generált.*

Tekintsük az

$$(x^2 + y^2 - 1)(x - y - 1) = 0$$

egyenletű görbét a síkon. Láthatjuk, hogy ez egy kör és egy egyenes uniója lesz. Ehhez hasonlóan minden algebrai halmazt felbonthatunk véges sok olyan részre, amelyek tovább már nem bonthatók. Az ezekhez tartozó ideálok az úgynevezett prímideálok lesznek.

5.11.4. Definíció. Az R kommutatív gyűrű egy P ideálját *prímideálnak* nevezzük, ha tetszőleges $p, q \in R$ elemekre $pq \in P$-ből $p \in P$ vagy $q \in P$ következik.

A $\mathbb{Z}$ gyűrű (vagy általában egy főideálgyűrű) egy (u) ideálja akkor és csak akkor prímideál, ha az u elem prím. A prímideálok nemcsak az algebrai geometriában, hanem az algebrai számelméletben is fontos szerepet játszanak, hiszen (a Dedekind-gyűrűk kapcsán) már meséltünk arról, hogy ha egy R gyűrűben nem érvényes a számelmélet alaptétele, akkor ezt helyettesítheti, ha a gyűrű ideáljait föl tudjuk bontani egyértelműen prímideálok szorzatára.

Ha egy R Noether-gyűrű összes ideálját meg akarjuk érteni, akkor az prímideálok segítségével nem megy, mert sajnos nem igaz, hogy mindegyik ideál előáll prímideálok szorzataként. Minden ideált elő lehet azonban állítani olyan ideálok metszeteként, amelyek a prímhatványokhoz hasonló tulajdonságúak. A metszet-előállítás azért is hasznos, mert az algebrai halmazok uniójához ideálok metszete tartozik. A prímhatvány helyes általánosításának módját egy könnyű észrevétel világítja meg. Az $n \in \mathbb{Z}$ szám akkor és csak akkor prímhatvány, ha igaz rá a következő: tetszőleges $a, b \in \mathbb{Z}$ esetén, ha $n \mid ab$, de n nem osztója az a-nak, akkor n osztója b egy alkalmas hatványának.

5.11.5. Definíció. Az R kommutatív gyűrű egy Q ideálját *primér ideálnak* nevezzük, ha tetszőleges $p, q \in R$ elemekre, igaz a következő: ha $pq \in Q$, de $p \notin Q$, akkor van olyan n pozitív egész, hogy $q^n \in Q$.

Az egész számok gyűrűjében az $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ szám által generált főideál a $(p_j^{\alpha_j})$ főideálok metszete, és ezek metszetre tovább már nem bonthatók. Így az alábbi tétel a számelmélet alaptételét általánosítja.

5.11.6. Tétel [Noether–Lasker-tétel]. *Legyen R egységelemes Noether-gyűrű. Ekkor minden ideálja felbontható primér ideálok metszetére.*

Emanuel Lasker, a tétel egyik társszerzője filozófus is volt, és talán arról a legnevezetesebb, hogy a leghosszabb ideig, 27 éven keresztül volt a sakkozás világbajnoka. A másik szerző, Emmy Noether algebrai eredményei komolyan segítették Einsteint az általános relativitáselmélet matematikai hátterének megalkotásában.

Az algebrai geometria manapság a matematikának az egyik legdivatosabb területe, rendkívül nehéz problémákkal, és olyan mély eredményekkel, amelyeknek nemcsak a geometriában, hanem a számelméletben is alapvető alkalmazásai vannak.

Gyakorlatok, feladatok

5.12. Nemkommutatív gyűrűk

A nemkommutatív gyűrűkről bizonyított tételek természetesen kommutatív gyűrűkben is érvényesek (és hasznosak is, bár a kommutativitás miatt sokszor lényegesen egyszerűbb belátni őket, mint általában). A nemkommutatív jelző azt hangsúlyozza, hogy a tételek még a sokkal nehezebben kezelhető nem kommutatív esetben is igazak. Ebben a szakaszban is csak mesélünk, nem bizonyítjuk a tételeket, és most is a [**13**] könyvet ajánljuk a részletesebb elmélyedéshez.

Ha R gyűrű, akkor sokszor lehetséges egy olyan I ideált találni, hogy I maga viszonylag „csúnya", de az R/I faktorgyűrű már „szép". Például ha $R = \mathbb{Z}_4$, akkor legyen $I = \{0, 2\}$. Ekkor I zérógyűrű, bármely két elemének szorzata nulla. Ugyanakkor R/I a kételemű test lesz. Az I ideál elemei pontosan azok az $a \in \mathbb{Z}_4$ elemek, amelyekre $1 - a$ invertálható. Az egyszerűség kedvéért egységelemes R gyűrűben mutatjuk meg, hogy ezt az ideált hogyan lehet általában megtalálni.

5.12.1. Definíció. Legyen R egységelemes gyűrű. Azoknak az $a \in R$ elemeknek a halmazát, amelyekre minden $r \in R$ esetén $1 - ra$ invertálható, az R *Jacobson-radikáljának* nevezzük, és $J(R)$-rel jelöljük.

Meg lehet mutatni, hogy a Jacobson-radikál kétoldali ideál. A gyűrű akkor viselkedik igazán szépen, ha balideáljaira érvényes a *minimum-feltétel*.

5.12.2. Definíció. Egy gyűrűt *Artin-gyűrűnek* nevezünk, ha balideálok minden nem üres halmazának van minimális eleme.

Ez a maximum-feltétel analogonja. Az 5.4.3. Tételhez hasonlóan a minimum-feltétel is jellemezhető a fogyó láncok megszakadásával (de a végesen generáltsággal nem). A helyzet annyiban sem szimmetrikus, hogy a minimum-feltétel erősebb a maximum-feltételnél.

5.12.3. Tétel. *Ha R egységelemes Artin-gyűrű, akkor bal Noether-féle abban az értelemben, hogy balideáljaira érvényes a maximum-feltétel.*

Az Artin-gyűrűk struktúrája az alábbi tétel miatt nagymértékben meghatározott.

5.12.4. Tétel [Wedderburn–Artin-tétel]. *Legyen R Artin-gyűrű. Ekkor*

(1) *az R Jacobson-radikálja* nilpotens ideál, *vagyis $J(R)^n = \{0\}$ alkalmas egészre.*
(2) *Az $R/J(R)$ faktorgyűrű véges sok, ferdetest fölötti teljes mátrixgyűrű direkt szorzatával izomorf.*

Ha elhagyjuk azt a feltételt, hogy a gyűrű Artin-féle legyen, akkor a Jacobson-radikálról sokkal kevesebbet állíthatunk, akár még nullosztómentes is lehet. A szerinte vett faktor azonban most is a mátrixgyűrűkhöz fog kapcsolódni, csak végtelen mátrixok is megjelenhetnek, és általában csak egy végtelen direkt szorzat egy speciális részgyűrűjéről lesz szó. De már ennyi is elegendő nemtriviális tételek bizonyításához, mint például a következő.

5.12.5. Tétel. *Ha az R gyűrű minden r eleméhez van olyan n egész, hogy $r^n = r$, akkor R kommutatív.*

Az Artin-féle tulajdonságot úgy lehet egyszerűen biztosítani, hogy egy véges dimenziós, egységelemes algebrát tekintünk. Ekkor ugyanis minden balideál altér lesz, és így a minimum-feltétel teljesül. Igen fontos példa erre az úgynevezett *csoportalgebra*.

Legyen $G = \{g_1, \ldots, g_n\}$ véges csoport, T egy test, és tekintsük a

$$\lambda_1 g_1 + \ldots + \lambda_n g_n$$

alakú formális lineáris kombinációkat, ahol $\lambda_i \in T$. Ezek nyilván vektorteret alkotnak az összeadásra, de össze is szorozhatjuk őket (a kvaterniókhoz hasonló módon): a disztributivitás alapján kifejtjük a szorzatot, a G csoportban elvégezzük a műveletet, és végül G elemei szerint rendezünk. Így egy $T[G]$ algebrát kapunk T fölött.

Erre az algebrára alkalmazhatjuk a Wedderburn–Artin-tételt. Ha T karakterisztikája nem osztja G rendjét (T leggyakrabban a komplex számtest), akkor a Jacobson-radikál nulla lesz, és így a csoportalgebra teljes mátrixgyűrűk direkt szorzata. Ez lehetővé teszi, hogy a csoportelemek helyett mátrixokkal számoljunk. Az így kapott *reprezentációelméletről* már meséltünk a csoportelméletben Burnside és Frobenius tételei kapcsán (4.12.10. és 4.11.25. Tételek).

Gyakorlatok, feladatok

5.12.6. Gyakorlat. Legyen D ferdetest. Mutassuk meg, hogy a $D^{n\times n}$ teljes mátrixgyűrű centruma a dE skalármátrixokból áll, ahol $d \in Z(D)$ és E az egységmátrix.

5.13. Összefoglaló

6. GALOIS-ELMÉLET

Az egyenletek elméletében a gyökjelekkel való megoldhatóság feltételét kutattam; ez lehetővé tette, hogy [...] leírjam egy egyenlet lehetséges szimmetriáit akkor is, ha az gyökjelekkel nem oldható meg.

***Evariste Galois** 21 évesen írott levele (a halálos párbaja előtti éjszakán)*

Ebben a fejezetben a testeket vesszük górcső alá. Az algebra általános filozófiája, hogy a megvizsgálandó dolgok helyett egy őket jól leíró algebrai struktúrát tekintünk. Például ha adott egy polinom, akkor a gyökeinek viselkedését úgy próbáljuk megérteni, hogy az ezeket tartalmazó legszűkebb testet nézzük. Galois zseniális ötlete, hogy ennek a testnek a megértéséhez egy másik struktúrát, nevezetesen a szimmetriáinak a csoportját érdemes vizsgálni. Ilyen értelemben a Galois-elmélet az absztrakt algebra kezdetének tekinthető. Alkalmazásként nemcsak az egyenletek gyökjelekkel való megoldhatóságáról, hanem a geometriai szerkeszthetőség elméletéről is szó lesz. Módszereink alkalmasak testek konstruálására is, és így át tudjuk majd tekinteni a véges testek szerkezetét. Ezeknek a kombinatorikában és a kódelméletben is komoly jelentősége van.

Az előző fejezethez hasonlóan a mostani fejezet első három szakaszára is érvényes, hogy a benne foglaltakat érdemes összevetni a [**11**] könyv $9.1-9.3$ és $10.1-10.2$ Szakaszaival, a feladatanyagot is beleértve. Az elemi lineáris algebrai ismeretek most már megkerülhetetlen szerepet játszanak.

6.1. Testbővítések

Ha adott egy T test fölötti polinom, akkor elképzelhető, hogy ennek nincs gyöke T-ben, de egy bővebb testben már van. Ilyenek például az x^2-2 és az $x^3-2 \in \mathbb{Q}[x]$ polinomok, amelyeknek gyökeit a valós, vagy a komplex számok között találjuk meg.

6.1.1. Kérdés. Melyik az a legszűkebb részteste a komplex számok testének, amely a racionális számokat és a $\sqrt{2}$, illetve a $\sqrt[3]{2}$ számot tartalmazza?

Ha egy résztest tartalmazza $\mathbb{Q}$-t és $\sqrt{2}$-t, akkor biztosan tartalmazza az $a+b\sqrt{2}$ számokat is, ahol $a, b \in \mathbb{Q}$. A 2.2.34. Gyakorlatban megmutattuk, hogy ezek a számok már testet alkotnak. Ezt a testet $\mathbb{Q}(\sqrt{2})$-vel jelöljük majd.

Hasonlóképpen, ha egy test tartalmazza $\mathbb{Q}$-t és $\sqrt[3]{2}$-t, akkor biztosan benne vannak az $a + b\sqrt[3]{2}$ alakú számok, ahol $a, b \in \mathbb{Q}$. De így még nem kapunk testet, mert ebben nem lesz benne a $\sqrt[3]{4} = \sqrt[3]{2} \cdot \sqrt[3]{2}$ (lásd 3.5.16. Feladat). Ezért biztosan szükség van az

$$a + b\sqrt[3]{2} + c\sqrt[3]{4}$$

alakú kifejezésekre, ahol $a, b, c \in \mathbb{Q}$. Jelölje ezek halmazát T.

A T halmaz nyilvánvalóan zárt az összeadásra. De zárt a szorzásra is, mert ha két elemét összeszorozzuk, akkor ez a disztributivitás szerint kifejthető. Tudjuk, hogy

$$\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}\,, \quad \sqrt[3]{2} \cdot \sqrt[3]{4} = 2\,, \quad \sqrt[3]{4} \cdot \sqrt[3]{4} = 2\sqrt[3]{2}\,.$$

Ezért a kapott összeget rendezhetjük 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ szerint, és így ismét T egy elemét kapjuk. Az egész eljárás ahhoz hasonlít, ahogy a kvaterniók algebrájában a szorzást definiáltuk.

6.1.2. Gyakorlat. Adjunk képletet T két általános elemének a szorzatára a fentiek alapján.

A kapott eredményt fogalmazzuk át polinomok segítségével. Ha $f(x) = a + bx + cx^2$, akkor

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} = f(\sqrt[3]{2})\,.$$

Tehát T elemeit úgy is felfoghatjuk, mint az $f(\sqrt[3]{2})$ alakú számokat, ahol $f \in \mathbb{Q}[x]$. Nyilván minden ilyen alakú szám benne van T-ben, és most azt láttuk be, hogy elegendő a legföljebb másodfokú polinomokat tekinteni (a nullapolinommal együtt), ezek már kiadják T összes elemét.

Azt szeretnénk megmutatni, hogy T nemcsak gyűrű, hanem test is. Ehhez először érdemes egy konkrét elem reciprokát kiszámítani. Legyen $z = 1 + \sqrt[3]{2} + \sqrt[3]{4}$, és keressük a reciprokát

$$t = a + b\sqrt[3]{2} + c\sqrt[3]{4}$$

alakban, ahol a, b, c ismeretlen racionális számok. A zt szorzatot az előző gyakorlat szerint kiszámítva

$$zt = (a + 2b + 2c) + (a + b + 2c)\sqrt[3]{2} + (a + b + c)\sqrt[3]{4}$$

adódik, azt szeretnénk, hogy ez 1 legyen. Ha szerencsénk van, ezt elérhetjük úgy is, hogy az 1 együtthatóját 1-nek, a $\sqrt[3]{2}$ és a $\sqrt[3]{4}$ együtthatóját nullának választjuk. Így egy lineáris egyenletrendszert kapunk az a, b, c számokra:

$$\begin{aligned} a + 2b + 2c &= 1 \\ a + \ \ b + 2c &= 0 \\ a + \ \ b + \ \ c &= 0\,. \end{aligned}$$

Szerencsére ez megoldható, $a = -1$, $b = 1$, $c = 0$ az eredmény. Ezért t inverze $-1 + \sqrt[3]{2}$. Ezt a mértani sor összegképlete alapján könnyen ellenőrizhetjük is.

6.1.3. Gyakorlat. Írjuk fel a $2+\sqrt[3]{2}+\sqrt[3]{4}$ szám reciprokát $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ alakban (ahol a, b, c racionális számok).

Ezt a módszert minden konkrét T-beli elem inverzének kiszámítására megpróbálhatjuk alkalmazni. Nem tudjuk azonban, hogy a kapott lineáris egyenletrendszernek van-e mindig megoldása. A válasz az, hogy van, és ezt ki is hozhatnánk némi számolással. Noha a most tanult módszer nagyon hasznos, ha konkrét elem reciprokát kell kiszámolni, azt, hogy ez a módszer mindig működik, sokkal rövidebben és általánosabban fogjuk bizonyítani a gyűrűkről tanultak segítségével.

6.1.4. Definíció. Ha K részteste az L testnek, akkor ezt úgy is fogalmazzuk majd, hogy L (test)bővítése K-nak, vagy hogy $K \leq L$ egy *testbővítés*.

Néha szokás $K \leq L$ helyett az L/K bővítésről beszélni. Az eddig elhangzottak a generálás fogalmát idézik föl: az adott elemeket tartalmazó legszűkebb résztestet keressük.

6.1.5. Definíció. Legyen $K \leq L$ testbővítés, és $\alpha, \beta, \ldots$ az L test néhány eleme. Ekkor

$$K(\alpha, \beta, \ldots)$$

jelöli az L test legszűkebb olyan résztestét, amely K-t és az $\alpha, \beta, \ldots$ elemeket is tartalmazza (ez tehát a K és az $\alpha, \beta, \ldots$ elemek által generált résztest). Speciálisan a $K \leq K(\alpha)$ alakú testbővítéseket (amelyek tehát K fölött egy elemmel generálhatóak) *egyszerű* bővítésnek nevezzük.

A generálásról általában tanultak szellemében tudjuk, hogy $K(\alpha, \beta, \ldots)$ mindig létezik: ez az L összes olyan résztesteinek metszete, amelyek K-t és az $\alpha, \beta, \ldots$ elemeket mind tartalmazzák. Láttuk korábban, hogy igen hasznos a generált részstruktúra elemeire konkrét leírást is adni (például lineáris algebrában lineáris kombinációkkal, csoportelméletben a 4.4.27. Tételben leírt módon). A fentiekben már csaknem megoldottuk a problémát a $\mathbb{Q}(\sqrt[3]{2})$ esetében, most ezt a leírást szeretnénk általánosítani.

6.1.6. Gyakorlat. Tegyük föl, hogy $K \leq L$ testbővítés, és $\alpha_1, \ldots, \alpha_n \in L$. Igazoljuk, hogy $\alpha \in K(\alpha_1, \ldots, \alpha_n)$ akkor és csak akkor, ha α előállítható $\alpha_1, \ldots, \alpha_n$-ből és K elemeiből a négy alapművelet véges sokszori alkalmazásával.

6.1.7. Gyakorlat. Igazoljuk, hogy $\mathbb{Q}(\sqrt{6}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{2}+1)$ és $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

6.1.8. Tétel. *Ha $K \leq L$ testbővítés és $\alpha \in L$, akkor*

$$K(\alpha) = \{f(\alpha)/g(\alpha) \,:\, f, g \in K[x],\, g(\alpha) \neq 0\}\,.$$

Bizonyítás. Jelölje T a jobb oldalon álló halmazt. Ez biztosan test, hiszen az elemeivel mint törtekkel számolhatunk:

$$\frac{f_1(\alpha)}{g_1(\alpha)} \pm \frac{f_2(\alpha)}{g_2(\alpha)} = \frac{f_1(\alpha)g_2(\alpha) \pm f_2(\alpha)g_1(\alpha)}{g_1(\alpha)g_2(\alpha)}\,,$$

és itt $f_1g_2 \pm f_2g_1$ valamint g_1g_2 is K fölötti polinomok, ahol $g_1g_2(\alpha) \neq 0$ mert L nullosztómentes. Hasonlóan láthatjuk, hogy T zárt a szorzásra is. Ha $f(\alpha)/g(\alpha) \neq 0$, akkor $f(\alpha)$ sem nulla, és így $g(\alpha)/f(\alpha) \in T$. Tehát T zárt a reciprok képzésére is, és így tényleg test.

A T tartalmazza az α elemet: ezt úgy kaphatjuk meg, hogy f-et x-nek, g-t konstans 1-nek választjuk. Hasonlóképpen T tartalmazza K elemeit is, ekkor f-et konstansnak kell választani. Ezért T egy olyan test, ami K-t és α-t tartalmazza, $K(\alpha)$ pedig a legszűkebb ilyen test. Ez azt jelenti, hogy $K(\alpha) \subseteq T$.

Megfordítva, ha $f \in K[x]$, akkor $f(\alpha)$ megkapható K elemeiből és α-ból összeadással és szorzással. Mivel $K(\alpha)$ test, $f(\alpha) \in K(\alpha)$. Ugyanígy $g(\alpha) \in K(\alpha)$, és mivel $K(\alpha)$ zárt az osztásra is, $f(\alpha)/g(\alpha) \in K(\alpha)$. Így $T \subseteq K(\alpha)$. □

A most bizonyított képlet pont azt a problémát nem oldja meg, amit a $K = \mathbb{Q}$ és $\alpha = \sqrt[3]{2}$ esetében felvetettünk, hiszen azt szeretnénk bizonyítani, hogy (ebben a konkrét esetben) osztásra nincsen szükség. Ebben a minimálpolinom fogalma lesz a segítségünkre. Az Olvasónak azt javasoljuk, nézze át az 5.9. Szakaszban tanultakat, a konkrét példákat is beleértve, röviden most mi is ezt tesszük. Ha $K \leq L$ testbővítés, akkor L algebra lesz K fölött (5.9.4. Gyakorlat). Az 5.9.8. Definíció ebben a speciális esetben a következőt jelenti.

6.1.9. Definíció. Ha $K \leq L$ testbővítés és $\alpha \in L$, akkor α *algebrai* K fölött, ha gyöke egy nem nulla, K-beli együtthatós polinomnak. Ellenkező esetben α *transzcendens* K fölött. A $K \leq L$ bővítés *algebrai*, ha L minden eleme algebrai K fölött.

6.1.10. Definíció. Az $\alpha \in \mathbb{C}$ *algebrai szám* illetve *transzcendens szám*, ha $\mathbb{Q}$ fölött algebrai illetve transzcendens. Az algebrai számok halmazát $\mathbb{A}$ jelöli.

Az 5.9.10. Tétel és az 5.9.12. Tétel egy testbővítés esetében a következőket mondja.

6.1.11. Tétel. *Legyen $K \leq L$ testbővítés, és $\alpha \in L$ egy K fölött algebrai elem.*

(1) *Egyértelműen létezik egy normált, $K[x]$-beli s polinom a következő tulajdonsággal: tetszőleges $f \in K[x]$ esetén*

$$f(\alpha) = 0 \iff s \mid f\,.$$

(2) *Az s a legalacsonyabb fokú olyan nem nulla, $K[x]$-beli polinom, amelynek α gyöke.*
(3) *Az s polinom irreducibilis K fölött.*
(4) *Ha egy normált, irreducibilis $g \in K[x]$ polinomnak α gyöke, akkor $g = s$.*

Az s polinomot az α elem K fölötti minimálpolinomjának nevezzük. Például a $\sqrt[3]{2}$ minimálpolinomja $\mathbb{Q}$ fölött $x^3 - 2$, hiszen ez egy $\mathbb{Q}$ fölött (a Schönemann-Eisenstein kritérium miatt) irreducibilis, normált polinom, amelynek $\sqrt[3]{2}$ gyöke.

Hogyan lehetne az $f(\alpha)/g(\alpha)$ kifejezéseket egyszerűsíteni akkor, ha tudjuk, hogy α minimálpolinomja az n-edfokú s polinom? Először az $f(\alpha)$ kifejezést szeretnénk átalakítani úgy, hogy α egy legföljebb $n-1$-edfokú polinomját kapjuk.

6.1.12. Gyakorlat. Legyen α az x^3+3x+1 polinom (egyetlen) valós gyöke. Határozzuk meg az α minimálpolinomját $\mathbb{Q}$ fölött, majd írjuk föl az $\alpha^5+2\alpha^3$ és az $\alpha/(\alpha-3)$ számokat $a+b\alpha+c\alpha^2$ alakban, ahol $a, b, c \in \mathbb{Q}$.

Az előző gyakorlat megoldásából már látjuk általában is, hogy hogyan lehet az f fokát redukálni az $f(\alpha)$ kifejezésben. Ha

$$s(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1} + x^n \,,$$

akkor $k \geq n$ esetén az $s(\alpha)=0$ egyenlőséget α^{k-n}-nel szorozva és átrendezve

$$\alpha^k = -b_{n-1}\alpha^{k-1} - \ldots - b_0\alpha^{k-n} \,.$$

Ezt behelyettesíthetjük az

$$f(\alpha) = a_0 + a_1\alpha + \ldots + a_k\alpha^k$$

kifejezésbe, és így α-nak egy legföljebb $k-1$-edfokú polinomja marad. Ezt az eljárást addig ismételgethetjük, amíg minden legalább n-edfokú tag eltűnik.

Az Olvasó bizonyára rájött, hogy igazából egy maradékos osztást végeztünk el. Hiszen ha f-et maradékosan elosztjuk s-sel: $f = sq + r$, ahol $r = 0$ vagy r foka kisebb, mint n, akkor persze

$$f(\alpha) = s(\alpha)q(\alpha) + r(\alpha) = r(\alpha) \,,$$

hiszen $s(\alpha)=0$. Így az $f(\alpha)$ elemet felírtuk az α legföljebb $n-1$-edfokú polinomjaként.

A következő feladat az, hogy $g(\alpha) \neq 0$ esetén keressünk olyan $q \in K[x]$ polinomot, hogy

$$\frac{1}{g(\alpha)} = q(\alpha) \,.$$

Keresztbe szorozva $g(\alpha)q(\alpha) - 1 = 0$. Más szóval azt szeretnénk, hogy α gyöke legyen a $gq-1$ polinomnak. Azok a polinomok, amelyeknek α gyöke, a minimálpolinom többszörösei. Ezért q mellett egy olyan p polinomot is keresünk, melyre $ps = gq - 1$, azaz

$$gq - sp = 1 \,.$$

Ilyen polinomok a 3.2.6. Tétel miatt akkor léteznek, ha g és s legnagyobb közös osztója 1.

A g és s legnagyobb közös osztója osztója s-nek, és mivel s irreducibilis, vagy s, vagy 1. Ha s lenne, akkor s osztaná g-t, ami lehetetlen, hiszen $g(\alpha) \neq 0$. Ezért s és g relatív prímek, vagyis a keresett q polinom tényleg létezik.

Az Olvasó azt is biztos észrevette, hogy a fentiekben az 5.2.9. Tétel bizonyítását másoltuk le. Természetesen bizonyíthattuk volna állításunkat e tétel felhasználásával is, vagyis a $K(\alpha)$ szerkezetét a $K[x]/(s)$ faktorgyűrű vizsgálatával is leírhattuk volna. Ezt meg is fogjuk tenni a 6.4. Szakaszban. Talán jobb azonban, ha az Olvasó először az elemi, nem absztrakt gondolatmenetekkel ismerkedik meg.

Az eddigieket összefoglalva tehát az $f(\alpha)/g(\alpha)$ kifejezésből eltüntethetjük a nevezőt, majd a kapott polinomot redukálhatjuk legföljebb $n-1$-edfokúvá. Ez bizonyítja az alábbi tétel állításainak első felét.

6.1.13. Tétel. *Legyen $K \leq L$ testbővítés, és $\alpha \in L$ egy K fölött algebrai elem, melynek K fölötti minimálpolinomja n-edfokú. Ekkor $K(\alpha)$ elemei felírhatók*

$$\beta = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$$

alakban, ahol $a_0, \ldots, a_{n-1} \in K$. Az $a_0, \ldots, a_{n-1}$ elemeket a β egyértelműen meghatározza.

Bizonyítás. Csak az egyértelműség bizonyítása van hátra. Tegyük föl, hogy $K(\alpha)$ egy β elemét kétféleképpen is felírtuk a fenti alakban:

$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}\,.$$

Ekkor

$$(a_0 - b_0) + (a_1 - b_1)\alpha + \ldots + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0\,.$$

Ezért α gyöke az

$$f(x) = (a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_{n-1} - b_{n-1})x^{n-1}$$

polinomnak. Mivel a minimálpolinom a legalacsonyabb fokú olyan polinom, amelynek α gyöke, és ha $f \neq 0$, akkor foka kisebb a minimálpolinom fokánál (ami n), ezért f csak a nullapolinom lehet. Ekkor viszont $a_i = b_i$ minden i-re, vagyis az együtthatókat β tényleg egyértelműen meghatározza. □

Mindezt lineáris algebrai nyelven is elmondhatjuk. Tudjuk, hogy a $K(\alpha)$ test vektortérnek tekinthető K fölött (sőt, az imént a minimálpolinom bevezetésekor már azt is megbeszéltük, hogy valójában algebra K fölött). A fenti állítás azt mutatja, hogy az $1, \alpha, \ldots, \alpha^{n-1}$ bázis ebben a vektortérben, hiszen $K(\alpha)$ minden eleme egyértelműen írható föl ezeknek az elemeknek K-beli együtthatós lineáris kombinációjaként. Vagyis a $K(\alpha)$ dimenziója K fölött n lesz, annyi, mint α minimálpolinomjának a foka. Ezért érdemes bevezetni az alábbi elnevezéseket.

6.1.14. Definíció. A $K \leq L$ testbővítés *véges bővítés*, ha L-nek, mint K fölötti vektortérnek (algebrának) a dimenziója véges. Ezt a dimenziót a bővítés *fokának* nevezzük, jele $|L : K|$. Ugyanezt értjük az L test K fölötti fokán is.

6.1.15. Definíció. Legyen $K \leq L$ testbővítés. Ha $\alpha \in L$ egy K fölött algebrai elem, akkor α *foka K fölött* az α elem K fölötti minimálpolinomjának a foka, jele $\mathrm{gr}_K(\alpha)$.

Az 5.9.15. Feladat alapján tehát láthatjuk, hogy például $1 + i$ másodfokú, $\sqrt[3]{2 + \sqrt{2}}$ pedig hatodfokú szám $\mathbb{Q}$ fölött. A $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, a $\mathbb{Q}(\sqrt[3]{2})$ fölött azonban csak 1, hiszen itt $x - \sqrt[3]{2}$ a minimálpolinomja.

6.1.16. Gyakorlat. Mutassuk meg, hogy $K \leq L$ akkor és csak akkor elsőfokú bővítés, ha $K = L$, és egy elem akkor és csak akkor elsőfokú K fölött, ha K-nak eleme.

6.1.17. Következmény. *Ha $K \leq L$ testbővítés, és $\alpha \in L$, akkor a $K(\alpha)$ foka K fölött $\mathrm{gr}_K(\alpha)$, ha α algebrai K fölött, és végtelen egyébként.*

Bizonyítás. Az állítást algebrai α esetén már beláttuk. Ha α transzcendens K fölött, akkor $1, \alpha, \alpha^2, \ldots$ lineárisan független elemek lesznek, hiszen ha lenne közöttük egy nemtriviális lineáris összefüggés:

$$a_0 + a_1\alpha + \ldots + a_k\alpha^k = 0\,,$$

akkor ezzel egy olyan nem nulla $K[x]$-beli polinomot kapnánk, amelynek α gyöke. □

A mostani bizonyításban szereplő állítás erősebb formában is igaz: ha α transzcendens, akkor a $K(\alpha)$ elemeinek $f(\alpha)/g(\alpha)$ alakú felírása egyértelmű. Mit is értünk pontosan ez alatt? Ha $f(x) = x^2$ és $g(x) = x$, akkor persze $f(\alpha)/g(\alpha) = \alpha^2/\alpha = \alpha$, tehát ezen a felíráson lehet egyszerűsíteni. Azonban ebben az esetben az $f(x)/g(x)$ polinom is x-szé egyszerűsödik. Az egyértelműség tehát azt jelenti, hogy $f(\alpha)/g(\alpha)$ nem egyszerűsíthető „jobban", mint $f(x)/g(x)$. Ez még mindig nem pontos fogalmazás, de azzá tehetjük, ha észrevesszük, hogy az $f(x)/g(x)$ kifejezések a $K[x]$ hányadostestének elemei.

6.1.18. Gyakorlat. Mutassuk meg, hogy ha $K \leq L$ testbővítés, és az $\alpha \in L$ elem transzcendens K fölött, akkor a $K(\alpha)$ test izomorf $K[x]$ hányadostestével, és az izomorfizmust az $f(x)/g(x) \leftrightarrow f(\alpha)/g(\alpha)$ megfeleltetés adja.

Végül megjegyezzük, hogy ha több algebrai elemmel egymás után bővítünk, akkor sincs szükség osztásra.

6.1.19. Gyakorlat. Tegyük föl, hogy $K \leq L$ testbővítés, és $\alpha_1, \ldots, \alpha_n \in L$ a K fölött algebrai elemek. Igazoljuk, hogy

$$K(\alpha_1, \ldots, \alpha_n) = \{p(\alpha_1, \ldots, \alpha_n) \,:\, p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]\}\,.$$

Gyakorlatok, feladatok

6.1.20. Gyakorlat. Lineárisan független-e

(1) $\{1, i, \sqrt{2} + 3i\}$ a $\mathbb{Q}$ fölött;
(2) $\{1, i, \sqrt{2} + 3i\}$ az $\mathbb{R}$ fölött;
(3) $\{1, \pi, 1/\pi\}$ a $\mathbb{Q}$ fölött? (Használjuk föl, hogy π transzcendens szám.)

6.1.21. Gyakorlat. Mutassuk meg, hogy ha $K \leq L$ testbővítés és $\alpha, \beta \in L$, akkor

(1) $\big(K(\alpha)\big)(\beta) = K(\alpha, \beta) = K(\beta)(\alpha)$.
(2) $K(\alpha, \beta) = K(\alpha, \alpha + \beta)$.
(3) Ha $\alpha \neq 0$, akkor $K(\alpha, \beta) = K(\alpha, \alpha\beta)$.

6.1.22. Feladat. Adjunk meg egy olyan c számot, melyre $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(c)$.

6.1.23. Gyakorlat. Legyen K részteste $\mathbb{C}$-nek és b, c racionális számok. Tegyük föl, hogy $\sqrt{b} \in K(\sqrt{c})$. Bizonyítsuk be, hogy ekkor $\sqrt{b} \in K$, vagy $\sqrt{b/c} \in K$.

6.1.24. Feladat. Legyen b négyzetmentes racionális szám (azaz két négyzetmentes egész hányadosa), és $p_1, \ldots, p_n$ prímek. Tegyük föl, hogy $\sqrt{b} \in \mathbb{Q}(\sqrt{p}_1, \ldots, \sqrt{p}_n)$. Bizonyítsuk be, hogy b (számlálójának és nevezőjének) kanonikus alakjában csak $p_1, \ldots, p_n$ szerepelhet. Ennek alapján mutassuk meg, hogy a prímszámok négyzetgyökei lineárisan függetlenek $\mathbb{Q}$ fölött.

6.2. A szorzástétel és következményei

Ennek a szakasznak a fő eredménye az, hogy ha egymás után végzünk testbővítéseket, akkor azok fokai összeszorzódnak. Ebből következik, hogy egy bővítés minden elemének a foka osztója a bővítés fokának. Becslést adunk összeg és szorzat fokára, és megmutatjuk, hogy az algebrai számok testet alkotnak, mely algebrailag zárt.

6.2.1. Gyakorlat. Mutassuk meg, hogy ha V vektortér $\mathbb{C}$ fölött, melynek $b_1, \ldots b_n$ bázisa, akkor V vektortér $\mathbb{R}$ fölött is ugyanazokra a műveletekre, és $b_1, \ldots, b_n, ib_1, \ldots, ib_n$ bázis lesz $\mathbb{R}$ fölött. Vagyis az $\mathbb{R}$ fölötti dimenzió a $\mathbb{C}$ fölötti dimenziónak a kétszerese.

A dimenzió azért nő a kétszeresére, mert $\mathbb{C}$ másodfokú bővítése $\mathbb{R}$-nek. Ebben a bővítésben $1, i$ bázis. Az előző gyakorlatban szereplő $\mathbb{R}$ fölötti bázist úgy kaptuk, hogy a $\mathbb{C}$ fölötti bázis elemeit 1-gyel és i-vel megszoroztuk. Most ezt az észrevételt általánosítjuk.

6.2.2. Tétel. *Legyen $K \leq L$ egy testbővítés, és V vektortér L fölött, melynek dimenziója n. Ekkor V vektortér K fölött is ugyanazokra a műveletekre, és dimenziója $|L : K| \cdot n$. A V dimenziója akkor és csak akkor véges K fölött, ha véges L fölött, és $K \leq L$ véges bővítés.*

Bizonyítás. Legyen $b_1, \ldots b_n$ bázis V-ben L fölött, és $c_1, \ldots, c_m$ bázis L-ben K fölött. Ekkor $|L : K| = m$, tekintsük az mn darab

$$c_1b_1, \ldots, c_1b_n, c_2b_1, \ldots, c_2b_n, \ldots, c_mb_1, \ldots, c_mb_n$$

vektort. Megmutatjuk, hogy ezek bázist alkotnak V-ben K fölött. Ebből persze következik, hogy V dimenziója K fölött mn.

Ez közvetlen számolással adódik. Legyen $v \in V$, ekkor ez felírható

$$v = \ell_1b_1 + \ldots + \ell_nb_n$$

alakban alkalmas $\ell_1, \ldots, \ell_n \in L$ elemekkel. Mindegyik ℓ_i felírható $k_{i1}c_1 + \ldots + k_{im}c_m$ alakban alkalmas $k_{ij} \in K$-ra, hiszen $c_1, \ldots, c_m$ generátorrendszer L-ben K fölött. Ezeket behelyettesítve és a zárójeleket felbontva

$$v = \sum k_{ij}(c_jb_i)$$

adódik, ahol az összegezésnél $1 \leq i \leq n$ és $1 \leq j \leq m$. Ezért a $c_j b_i$ vektorok generátorrendszert alkotnak V-ben K fölött.

A függetlenségük bizonyításához meg kell mutatni, hogy ha

$$\sum k_{ij}(c_j b_i) = 0$$

valamilyen $k_{ij} \in K$ elemekre, akkor ezek mindegyike nulla. Ezt az összeget a fenti számoláshoz hasonlóan rendezzük a b_i szerint. Ekkor

$$\ell_1 b_1 + \ldots + \ell_n b_n = 0$$

adódik, ahol $\ell_i = k_{i1}c_1 + \ldots + k_{im}c_m \in L$. Mivel $b_1, \ldots, b_n$ független L fölött, mindegyik $\ell_i = 0$. De $c_1, \ldots, c_m$ független K fölött, ezért

$$k_{i1}c_1 + \ldots + k_{im}c_m = \ell_i = 0$$

miatt $k_{i1} = \ldots = k_{im} = 0$. Ez minden i-re igaz, vagyis mindegyik k_{ij} nulla. Tehát a $c_j b_i$ tényleg függetlenek is. Ezzel a tétel első állítását beláttuk.

Ha V véges dimenziós L fölött, és $K \leq L$ véges bővítés, akkor a fenti bizonyítás egy véges bázist konstruál V-ben K fölött. Megfordítva, tegyük föl, hogy V véges dimenziós K fölött. Mivel minden K fölötti generátorrendszer L fölött is generátorrendszer, a dimenzió L fölött is véges. Ha L-ben lenne egy $c_1, c_2, \ldots$ végtelen független rendszer K fölött, akkor tetszőleges $0 \neq v$ esetén $c_1 v, c_2 v, \ldots$ is végtelen független rendszer V-ben K fölött, ami lehetetlen. Ezért $K \leq L$ is véges. □

Ha egy vektortér dimenzióját számosságként értelmezzük, akkor a fenti tételek végtelen dimenziós vektorterekre is érvényesek, ugyanezzel a bizonyítással. Ekkor a tételben számosságok szorzata szerepel, és a bizonyítás utolsó bekezdése fölöslegessé válik. Ugyanez a megjegyzés az alábbi következményre is vonatkozik.

6.2.3. Következmény [A testbővítések fokának szorzástétele]. *Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ akkor és csak akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek, és $|M : K| = |M : L| \cdot |L : K|$.*

Bizonyítás. Az előző tételt kell alkalmazni $V = M$ esetén. □

6.2.4. Állítás. *Ha $K \leq L$ véges bővítés, és $\alpha \in L$, akkor α algebrai K fölött, és*

$$\mathrm{gr}_K(\alpha) \,\Big|\, |L : K|\,,$$

azaz elem foka osztója a bővítés fokának. Tehát minden véges bővítés algebrai.

Bizonyítás. Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$. Véges dimenziós vektortér altere is véges dimenziós, ezért $|K(\alpha) : K|$ véges. Így a 6.1.17. Következmény miatt α algebrai K fölött, és $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$. A

$$K \leq K(\alpha) \leq L$$

testláncra alkalmazzuk a szorzástételt. Azt kapjuk, hogy $|L : K| = |L : K(\alpha)| \cdot \mathrm{gr}_K(\alpha)$. Ezért $\mathrm{gr}_K(\alpha)$ tényleg osztója $|L : K|$-nak. □

Például a $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ bővítés minden eleme első, vagy harmadfokú. Az elsőfokú elemek azok, amelyek minimálpolinomja $x - q$ valamilyen $q \in \mathbb{Q}$-ra. Ha ennek α gyöke, akkor $\alpha = q$. Tehát az elsőfokú számok az alaptest, azaz $\mathbb{Q}$ elemei. Ezért minden nem racionális szám ebben a bővítésben harmadfokú. Ez erős állítás, hiszen ha mondjuk „kézzel" kellene kiszámolni $3 + 7\sqrt[3]{2} - 5\sqrt[3]{4}$ fokát, akkor már azzal is komoly bajban lennénk, hogy egy olyan racionális együtthatós polinomot felírjunk, amelynek ez a szám gyöke. Ha találnánk is mondjuk egy kilencedfokú ilyen polinomot, hogyan bontanánk föl irreducibilisek szorzatára, hogy a minimálpolinomot megtaláljuk?

Hasonló probléma a következő. Tekintsünk egy jó bonyolult gyökös kifejezést, mint például

$$\sqrt[7]{3 - \sqrt[5]{23}} - \sqrt[4]{5 + i\sqrt{7 + \sqrt[6]{3}}}\,.$$

Algebrai szám ez egyáltalán? Ha igen, tudunk valamit mondani a fokáról?

A gyökvonással önmagában nincs probléma. Hiszen ha α algebrai, mondjuk gyöke az $f \in K[x]$ nem nulla polinomnak, akkor $f(x^k)$ is egy K fölötti nem nulla polinom, amelynek gyöke $\sqrt[k]{\alpha}$ mindegyik értéke. Az $f(x^k)$ foka f fokának k-szorosa, ezért igaz a következő.

6.2.5. Állítás. *Legyen $K \leq L$ testbővítés, és $\alpha \in L$ egy algebrai elem. Ekkor $\sqrt[k]{\alpha}$ is algebrai K fölött, és foka legföljebb $k \cdot \mathrm{gr}_K(\alpha)$.*

De igaz-e, hogy algebrai számok összege és szorzata is algebrai? Megdöbbentő, az absztrakt algebrai módszerek erejét mutatja, hogy az eddig felépített apparátussal triviálisan igenlő válasz adható erre a kérdésre. Ehhez először vizsgáljuk meg, hogy hogyan változik egy elem foka, ha az alaptestet növeljük.

6.2.6. Gyakorlat. Határozzuk meg $\sqrt[4]{2}$ fokát $\mathbb{Q}$ és $\mathbb{Q}(\sqrt{2})$ fölött.

6.2.7. Lemma. *Ha $K \leq L \leq M$ testbővítések és $\alpha \in M$ algebrai K fölött, akkor α algebrai L fölött is, és*

$$\mathrm{gr}_L(\alpha) \leq \mathrm{gr}_K(\alpha)\,,$$

azaz nagyobb test fölött egy elem foka csak csökkenhet.

Bizonyítás. Legyen s az α minimálpolinomja K fölött. Az s-nek α gyöke, és s persze $L[x]$-beli polinom is, tehát α algebrai L fölött. Ha t jelöli az α minimálpolinomját L fölött, akkor $t \mid s$ a 6.1.11. Tétel miatt. Ezért

$$\mathrm{gr}_L(\alpha) = \mathrm{gr}(t) \leq \mathrm{gr}(s) = \mathrm{gr}_K(\alpha)\,.$$

□

6.2.8. Feladat. Adjunk példát arra, hogy az előző lemmában általában nem igaz, hogy $\mathrm{gr}_L(\alpha)$ osztója $\mathrm{gr}_K(\alpha)$-nak.

6.2.9. Következmény. *Legyen $K \leq L$ testbővítés, és $\alpha, \beta \in L$ algebrai elemek K fölött. Ekkor $\alpha \pm \beta$, továbbá $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai elemek K fölött, és fokuk legföljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.*

Bizonyítás. Tekintsük a

$$K \leq K(\alpha) \leq K(\alpha)(\beta)$$

egymás utáni bővítéseket. Az első bővítés a 6.1.17. Következmény szerint véges, és foka $\mathrm{gr}_K(\alpha)$. A második bővítés foka az előző lemma miatt legföljebb $\mathrm{gr}_K(\beta)$. Így a szorzástétel szerint

$$|K(\alpha)(\beta) : K| = |K(\alpha)(\beta) : K(\alpha)| \cdot |K(\alpha) : K| \leq \mathrm{gr}_K(\beta)\mathrm{gr}_K(\alpha)\,.$$

Speciálisan $K \leq K(\alpha)(\beta)$ véges bővítés. Ezért a 6.2.4. Állítás miatt minden eleme algebrai K fölött, és foka legföljebb a bővítés foka, azaz legföljebb $\mathrm{gr}_K(\beta)\mathrm{gr}_K(\alpha)$. De mivel $\alpha, \beta \in K(\alpha)(\beta)$, ezért a tételben felsorolt elemek mind benne vannak $K(\alpha)(\beta)$-ban. □

6.2.10. Következmény. *Ha $K \leq L$ testbővítés, akkor a K fölött algebrai elemek résztestet alkotnak L-ben. Speciálisan az algebrai számok $\mathbb{A}$ halmaza részteste $\mathbb{C}$-nek.*

Az előző bizonyítás ötletét persze kettőnél több elemre is alkalmazhatjuk.

6.2.11. Következmény. *Véges sok algebrai elemmel való bővítés mindig véges (és ezért algebrai).*

A fenti bizonyítás kapcsán megvizsgáljuk, hogy ha relatív prím fokú elemekkel bővítünk, akkor ez miért segít a bővítés fokának meghatározásában.

6.2.12. Állítás. *Tegyük föl, hogy $K \leq L$ testbővítés, és $\alpha, \beta \in L$, melyek K fölötti fokai relatív prímek. Legyen $m = \mathrm{gr}_K(\alpha)$ és $n = \mathrm{gr}_K(\beta)$. Ekkor a következők teljesülnek.*

(1) $|K(\alpha, \beta) : K| = mn$.
(2) *A β foka $K(\alpha)$ fölött is n.*
(3) *A β elem K fölötti minimálpolinomja irreducibilis $K(\alpha)$ fölött is.*

Bizonyítás. A 6.1.21. Gyakorlat szerint $K(\alpha, \beta) = K(\alpha)(\beta)$, jelölje k ennek a testnek a K fölötti fokát. A 6.2.9. Következmény bizonyításából tudjuk, hogy $k \leq mn$. Másfelől α és β is eleme $K(\alpha, \beta)$-nak, és így fokuk (a 6.2.4. Állítás miatt) osztója a bővítés fokának, vagyis $m \mid k$ és $n \mid k$. Mivel m és n relatív prímek, $mn \mid k$, vagyis $k = mn$. Ezzel (1)-et beláttuk.

Ismét a szorzástételt alkalmazva a $K \leq K(\alpha) \leq K(\alpha, \beta)$ testláncra

$$|K(\alpha, \beta) : K(\alpha)| = \frac{|K(\alpha, \beta) : K|}{|K(\alpha) : K|} = \frac{mn}{n} = m\,.$$

Ezért (2) is igaz. Ha s jelöli β minimálpolinomját K fölött, t pedig $K(\alpha)$ fölött, akkor $s(\beta) = 0$ miatt $t \mid s$. A két polinom foka azonban (2) miatt egyenlő, és így (mivel normáltak is) $s = t$. Mivel t egy $K(\alpha)$ fölötti minimálpolinom, irreducibilis $K(\alpha)$ fölött. Ezért $s = t$ is az. □

A komplex számok bevezetésekor arra törekedtünk, hogy egyetlenegy polinomnak, az $x^2 + 1$-nek gyököt találjunk. Ez nagyon jól sikerült, hiszen a komplex számok között nemcsak az $x^2 + 1$-nek, hanem minden komplex együtthatós nem konstans polinomnak van gyöke. Ezt úgy fejeztük ki, hogy a komplex számok teste algebrailag zárt.

Az algebrai számok $\mathbb{A}$ teste hasonlóképpen keletkezik, csak most az összes racionális együtthatós polinom összes komplex gyökét vettük be. Most is igaz, hogy ez a konstrukció jól sikerült, ugyanis $\mathbb{A}$-ban minden nem konstans $\mathbb{A}$-beli együtthatós polinomnak is van gyöke, vagyis az algebrai számok $\mathbb{A}$ teste algebrailag zárt. Ennek bizonyítása megtalálható a Freud-Gyarmati könyvben ([**11**], 9.3.6. Tétel). Mi egy másik (egyszerű) bizonyítást adunk a tételre. Érdemes ezt összevetni a 6.4.17. Feladat állításával, ami ennek a tételnek egy általánosítása.

6.2.13. Tétel. *Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.*

Bizonyítás. Be kell látni, hogy minden nem konstans $f \in \mathbb{A}[x]$ polinomnak van gyöke $\mathbb{A}$-ban. Legyen

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n ,$$

és α az f polinomnak egy komplex gyöke (ezen a ponton kihasználjuk, hogy $\mathbb{C}$ algebrailag zárt). Tekintsük a

$$\mathbb{Q} \leq \mathbb{Q}(a_0) \leq \mathbb{Q}(a_0, a_1) \leq \ldots \leq \mathbb{Q}(a_0, a_1, \ldots, a_n) \leq \mathbb{Q}(a_0, a_1, \ldots, a_n, \alpha)$$

testláncot. Mindegyik a_i algebrai $\mathbb{Q}$ fölött, hiszen a $a_i \in \mathbb{A}$. Ezért a fenti láncban a bővítések végesek a $\mathbb{Q}(a_0, a_1, \ldots, a_n)$-ig bezárólag.

Azonban α algebrai $\mathbb{Q}(a_0, a_1, \ldots, a_n)$ fölött, hiszen az $f \neq 0$ polinomnak gyöke, és f együtthatói benne vannak ebben a testben. Ezért α-val bővítve szintén véges bővítést kapunk. A szorzástétel szerint így $\mathbb{Q} \leq \mathbb{Q}(a_0, a_1, \ldots, a_n, \alpha)$ is véges bővítés. Ez pedig azt jelenti, hogy α algebrai $\mathbb{Q}$ fölött, vagyis $\alpha \in \mathbb{A}$. Tehát az f polinomnak tényleg van gyöke az $\mathbb{A}$ testben. □

Megjegyezzük, hogy sem a véges testek, sem a $\mathbb{Q}$ véges bővítései nem algebrailag zártak (2.5.17. Feladat, 6.2.20. Gyakorlat). Ugyanakkor minden testnek van algebrailag zárt bővítése (6.4.6. Tétel).

Gyakorlatok, feladatok

6.2.14. Gyakorlat. Fölírható-e $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ alakban a $\sqrt[6]{2}$ illetve a $\sqrt{2}$, ahol a, b, c racionális számok?

6.2.15. Gyakorlat. Számítsuk ki az alábbi fokszámokat.

(1) $|\,\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}\,|$.
(2) $|\,\mathbb{Q}(\sqrt{2}\sqrt[3]{3}) : \mathbb{Q}\,|$.
(3) $\sqrt[4]{2}$ foka $\mathbb{Q}(\sqrt{8})$ fölött.
(4) $\sqrt[4]{2}$ foka $\mathbb{Q}(\sqrt[3]{7})$ fölött.

(5) $\sqrt{2}+\sqrt[4]{2}$ foka $\mathbb{Q}(\sqrt{2})$ fölött.
(6) $\sqrt{2}+\sqrt[4]{2}$ foka $\mathbb{Q}$ fölött.

6.2.16. Gyakorlat. Bizonyítsuk be, hogy ha a és b valós, akkor $a+bi$ pontosan akkor algebrai ($\mathbb{Q}$ fölött), ha a is és b is az.

6.2.17. Gyakorlat. Az alábbi számok közül melyek algebraiak, és melyek transzcendensek: $\pi+3$, $5\pi+6$, $\pi+\sqrt{2}$, $\pi^2+2\pi+2$, $\sqrt{\pi}$. A megoldásban használjuk föl, hogy π transzcendens szám.

6.2.18. Gyakorlat. Egy algebrai szám és egy transzcendens szám összege mikor algebrai? És a szorzatuk? Egy transzcendens szám négyzete lehet-e algebrai? És a négyzetgyöke?

6.2.19. Gyakorlat. Igazoljuk, hogy egy test pontosan akkor algebrailag zárt, ha minden algebrai bővítése elsőfokú.

6.2.20. Gyakorlat. Igazoljuk, hogy $\mathbb{Q}$ egyetlen véges bővítése sem lehet algebrailag zárt.

6.2.21. Gyakorlat. Igazoljuk, hogy algebrai bővítések egymás utánja is algebrai.

6.2.22. Gyakorlat. Adjunk példát olyan algebrai bővítésre, amely nem véges.

6.3. Normális bővítések

Eddig egyszerű bővítéseket vizsgáltunk, mint például a $\mathbb{Q}\leq\mathbb{Q}(\sqrt[3]{2})$. Ha azonban az x^3-2 polinomot igazán meg akarjuk érteni, akkor érdemes a többi gyökével is bővíteni. A másik két gyök az $\varepsilon\sqrt[3]{2}$ és az $\varepsilon^2\sqrt[3]{2}$, ahol $\varepsilon=\cos 120^\circ+i\sin 120^\circ$ primitív harmadik egységgyök.

6.3.1. Gyakorlat. Igazoljuk, hogy $\mathbb{Q}(\sqrt[3]{2},\varepsilon\sqrt[3]{2},\varepsilon^2\sqrt[3]{2})=\mathbb{Q}(\sqrt[3]{2},\varepsilon)$. Mutassuk meg, hogy a kapott test $\mathbb{Q}$-nak hatodfokú bővítése.

Hasonlóan, ha adott egy f polinom a K test fölött, akkor szeretnénk az „összes" gyökével bővíteni. Az „összes" gyökkel azonban probléma van. Például mi lesz az x^2+1 polinom összes gyöke? Aki csak a valós számokat ismeri, annak az üres halmaz. Aki a komplex számokat is, annak az i és a $-i$. De gyöke ennek a polinomnak például a síkon a 90 fokos forgatás, meg egy csomó kvaternió is.

Amikor testbővítésekkel foglalkozunk, akkor az $f\in K[x]$ polinomnak csak egy $K\leq L$ bővítésben szereplő gyökeit keressük. De honnan tudhatjuk, hogy mindet megtaláltuk-e már? Onnan, hogy ha igen, akkor f gyöktényezőkre bomlik L fölött:

$$f(x)=c(x-\alpha_1)\dots(x-\alpha_n)$$

(ahol $c\in K$ az f főegyütthatója). Mivel minden test nullosztómentes, a 2.4.7. Tétel szerint az ilyen f polinomoknak már L egyetlen bővítésében sem lehet más gyöke, mint $\alpha_1,\dots,\alpha_n$. Amikor tehát a testek elméletében f „összes" gyökéről beszélünk, akkor mindig arra gondolunk, hogy a felsorolt gyökök már elegendőek az f gyöktényezőkre bontásához. Persze ha L a $\mathbb{C}$ részteste, akkor egyszerűen beszélhetünk az f összes komplex gyökéről.

6.3.2. Definíció. Legyen $K \leq L$ test, és tegyük föl, hogy L tartalmazza egy nem nulla $f \in K[x]$ polinom összes gyökét (vagyis $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$ alkalmas $\alpha_i \in L$ elemekre, ahol $c \in K$). Ekkor $K(\alpha_1, \dots, \alpha_n)$ az f polinom *felbontási teste* K fölött.

6.3.3. Gyakorlat. Mutassuk meg, hogy egy K fölötti n-edfokú polinom felbontási testének a foka K fölött legföljebb $n!$ (n faktoriális) lehet.

Az f polinom felbontási testének van egy meglepő, de fontos tulajdonsága. Attól, hogy az f összes gyökét bevettük, természetesen maradhatnak még olyan polinomok, amelyeknek nincsen gyöke az új bővítésben sem. Például az $x^4 - 2$ polinom $\mathbb{Q}$ fölötti L felbontási testének foka $\mathbb{Q}$ fölött legföljebb $4! = 24$ (látni fogjuk a 6.3.12. Gyakorlatban, hogy valójában nyolc). Így az $x^5 - 2$ polinomnak egyetlen gyöke sem lehet benne (a 6.2.4. Állítás miatt), hiszen ennek mindegyik gyöke ötödfokú. Ugyanígy az $(x^2+1)(x^2-7)$ polinomról könnyű kiszámolni, hogy pontosan két gyöke van L-ben, a $\pm i$. Elvileg előfordulhatna, hogy mondjuk egy negyedfokú irreducibilis polinomnak is két gyökét tartalmazza ez a bővítés, a másik kettőt nem. De az ilyesmi lehetetlen, ezt mondja ki a következő tétel.

6.3.4. Tétel. *Legyen L felbontási teste az $f \neq 0$ polinomnak K fölött. Ha $g \in K[x]$ irreducibilis polinom, akkor g-nek vagy az összes gyöke benne van L-ben (vagyis g gyöktényezős alakra bomlik L fölött), vagy egyetlen gyöke sincs L-ben.*

Bizonyítás. Legyen $L = K(\alpha_1, \dots, \alpha_n)$, ahol ezek az f összes gyökei, azaz

$$f(x) = a_0 + \dots + a_n x^n = a_n(x-\alpha_1)\dots(x-\alpha_n).$$

Az L minden eleme $p(\alpha_1, \dots, \alpha_n)$ alakban írható, ahol $p(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$, hiszen mindegyik α_i algebrai K fölött (6.1.19. Gyakorlat).

Tegyük föl, hogy a g polinomnak van egy β gyöke L-ben, ekkor tehát $\beta = p(\alpha_1, \dots, \alpha_n)$ alkalmas p-re. Belátjuk, hogy g összes gyökét megkaphatjuk úgy, hogy a $p(\alpha_1, \dots, \alpha_n)$ kifejezésben az $\alpha_1, \dots, \alpha_n$ elemeket cserélgetjük. Természetesen az így kapott elemek szintén L-ben vannak.

> Az előző bekezdésben szereplő észrevétel a Galois-elmélet egyik fő kiinduló ötlete. Később látni fogjuk, hogy azok a leképezések, amelyek az α_i elemek cserélgetéséből adódnak, az egész $K \leq L$ bővítés szerkezetét megfogják.

Az α_i elemek cserélgetésével kapott elemek $b_\sigma = p(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$ alakúak, ahol σ az $\{1, 2, \dots, n\}$ halmaz egy permutációja, vagyis S_n-nek eleme. Szorozzuk össze az ezekhez tartozó gyöktényezőket:

$$h(x) = \prod_{\sigma \in S_n} (x - b_\sigma)\,.$$

Megmutatjuk, hogy $h(x) \in K[x]$.

A h polinomra alkalmazzuk a gyökök és együtthatók közötti összefüggéseket (2.5.8. Tétel). Például a felülről második tag (vagyis az $x^{n!-1}$ együtthatója) a

$$\sum_{\sigma \in S_n} b_\sigma$$

összeg ellentettje lesz. De

$$s(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

szimmetrikus polinomja $x_1, \ldots, x_n$-nek (lásd 2.7.1. Definíció), hiszen ha az x_i határozatlanokat cserélgetjük, akkor csak a fenti összeg tagjainak sorrendje változik, az összeg maga ugyanaz marad. A szimmetrikus polinomok alaptétele (2.7.3. Tétel) miatt tehát s felírható az elemi szimmetrikus polinomok polinomjaként:

$$s = F(\sigma_1, \ldots, \sigma_n)\,,$$

ahol $F \in K[y_1, \ldots, y_n]$. A gyökök és együtthatók összefüggését az f polinomra alkalmazva

$$\sigma_k(\alpha_1, \ldots, \alpha_n) = (-1)^k a_{n-k}/a_n \in K\,.$$

Ezt az előző egyenletbe visszahelyettesítve $s(\alpha_1, \ldots, \alpha_n) \in K$ adódik (mert F együtthatói K-beliek). De $s(\alpha_1, \ldots, \alpha_n) = \sum b_\sigma$, és így a h polinom felülről második együtthatója K-beli. A többi együtthatóra ugyanez a bizonyítás, hiszen azok is a b_σ elemek elemi szimmetrikus polinomjai, és így az $\alpha_1, \ldots, \alpha_n$ elemeknek is szimmetrikus polinomjai. Ezért a h polinom együtthatói tényleg K-ból valók.

A $\beta = p(\alpha_1, \ldots, \alpha_n)$ minimálpolinomja K fölött g (konstansszorosa), hiszen g irreducibilis, és gyöke β. De β gyöke h-nak is, és mivel ez $K[x]$-beli polinom, $g \mid h$. A h a definíciója szerint gyöktényezőkre bomlik L fölött, és ezért g is. □

6.3.5. Definíció. A $K \leq L$ bővítést *normális bővítésnek* nevezzük, ha algebrai, és tetszőleges $g \in K[x]$ irreducibilis polinomra teljesül, hogy g-nek vagy az összes gyöke benne van L-ben (vagyis g gyöktényezős alakra bomlik L fölött), vagy egyetlen gyöke sincs L-ben.

6.3.6. Következmény. *Minden polinom felbontási teste normális bővítés.*

Bizonyítás. Ha $f \in K[x]$ felbontási teste L, akkor L a K-nak véges bővítése, hiszen f gyökei, azaz véges sok algebrai elem generálja. Ezért ez a bővítés algebrai, és az állítás következik az előző tételből. □

Így például az imént tekintett $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ bővítés normális. Normális bővítéseket tipikusan felbontási testként kapunk (hiszen a definícióban szereplő tulajdonságot nagyon fáradságos lenne ellenőrizni minden g polinomra). A következő gyakorlat mutatja, hogy minden véges (sőt minden végesen generált) normális bővítés felbontási test.

6.3.7. Gyakorlat. Tegyük föl, hogy $K \leq L$ normális bővítés, és $L = K(\alpha_1, \ldots, \alpha_m)$. Legyen $f \in K[x]$ az α_i elemek K fölötti minimálpolinomjainak szorzata. Igazoljuk, hogy L az f polinom K fölötti felbontási teste.

Ugyanakkor $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nem normális, mert az $x^3 - 2$ irreducibilis polinomnak csak egy gyökét tartalmazza. Ezért ez semmilyen más polinomnak sem lesz $\mathbb{Q}$ fölött a felbontási teste.

Úgy tűnik, hogy ha egy vizsgálni kívánt polinomnak csak egy gyökével bővítünk, akkor a kapott egyszerű bővítés elemeit teljesen ismerjük (a 6.1.13. Tétel miatt), de ez általában nem normális bővítés. Ha az f többi gyökét is bevesszük, akkor viszont esetleg nem egyszerű a bővítés, nehezebb áttekinteni az elemeit. Jó lenne a két előnyt egyesíteni. Ez lehetséges: meg fogjuk mutatni, hogy $\mathbb{C}$ résztestei esetében minden véges bővítés egyszerű. Ez általánosabban is igaz, de a bizonyítás lényegét ezen a speciális eseten érthetjük meg a legjobban. Az általánosításhoz szükséges technikai segédfogalmakat (tökéletes test, szeparábilis bővítés) csak nagyon vázlatosan tárgyaljuk, részben feladatok formájában.

A 3.6.13. Feladatban beláttuk, hogy egy $\mathbb{Q}$ fölött irreducibilis f polinomnak nem lehet többszörös gyöke $\mathbb{C}$-ben. A megoldás azon múlott, hogy f deriváltja f-nél alacsonyabb fokú, de nem azonosan nulla, és így (f, f'), ami f-nek osztója, csak konstans polinom lehet. Ez a gondolatmenet nyilván $\mathbb{C}$ minden részteste fölötti polinomokra érvényes, és az alábbi bizonyítás egyik kulcsmozzanata.

6.3.8. Tétel. *Legyenek $K \leq L \leq \mathbb{C}$ testek. Ha a $K \leq L$ bővítés véges, akkor egyszerű.*

Bizonyítás. Elegendő megmutatni, hogy ha $\alpha, \beta \in L$, akkor $K(\alpha, \beta)$ generálható K fölött egy alkalmas γ elemmel. Ezt többször egymás után alkalmazva ugyanis azt kapjuk, hogy ha L véges sok elemét vesszük hozzá K-hoz, a kapott bővítés szintén generálható egy elemmel. Márpedig minden véges bővítés (így maga L is) generálható véges sok elemmel K fölött (például egy bázissal). Ezért ekkor készen leszünk.

Azt igazoljuk, hogy $K(\alpha, \beta) = K(\alpha + k\beta)$ véges sok kivétellel minden $k \in K$ elemre. Ebből természetesen következik az állítás, hiszen a K testnek végtelen sok eleme van (biztosan tartalmazza például az 1 többszöröseit), és így választható megfelelő k érték. Legyen $\gamma = \alpha + k\beta$ és $M = K(\gamma)$. Nyilván $M \subseteq K(\alpha, \beta)$, hiszen γ kifejezhető α-val és β-val. Olyan k számot keresünk, amikor itt egyenlőség áll, vagyis amelyre $K(\alpha, \beta) \subseteq M$.

Jelölje az α minimálpolinomját K fölött s, a β minimálpolinomját t. A β gyöke a $t(x) \in K[x] \subseteq M[x]$ és az $s(\gamma - kx) \in M[x]$ polinomoknak, és így e kettő $r(x) \in M[x]$ kitüntetett közös osztójának is. Ha (k alkalmas választásával) sikerül elérni, hogy r elsőfokú legyen, akkor $\beta \in M$, hiszen β az $r(x)$ elsőfokú polinom gyökeként az r együtthatóiból kifejezhető. De akkor $\alpha = \gamma - k\beta \in M = K(\gamma)$. Tehát $K(\alpha, \beta) \subseteq M$, és így γ eleget tesz a feltételeknek.

A $t(x)$ és az $s(\gamma - kx)$ polinomoknak a kitüntetett közös osztója a kanonikus alakjuk segítségével is meghatározható (3.1.20. Gyakorlat). Az eredmény akkor lesz elsőfokú, ha a két polinomnak csak egyetlen közös komplex gyöke van, és ez legalább az egyik polinomnak csak egyszeres gyöke.

A t polinomnak minden gyöke egyszeres, hiszen a tétel kimondása előtt meggondoltuk, hogy t irreducibilitása miatt t komplex gyökei páronként különbözők. Azt kell elérnünk,

hogy t többi komplex gyöke ne legyen gyöke $s(\gamma - kx)$-nek. Ehhez bontsuk az s és t polinomokat $\mathbb{C}$ fölött gyöktényezőkre:

$$s(x) = c(x - \alpha_1) \dots (x - \alpha_n) ,$$

ahol mondjuk $\alpha = \alpha_1$, és

$$t(x) = c(x - \beta_1) \dots (x - \beta_m) ,$$

ahol $\beta = \beta_1$. Az $s(\gamma - k\beta_i)$ akkor nulla, ha $\gamma - k\beta_i = \alpha_j$ alkalmas j-re. Mivel $\gamma = \alpha + k\beta$, azt kapjuk, hogy

$$(\alpha - \alpha_j) = k(\beta_i - \beta) .$$

Olyan k-t kell választanunk, amelyre ez az egyenlőség nem teljesül, semmilyen $\beta_i \neq \beta$ és semmilyen α_j esetén. De $\beta_i \neq \beta$ miatt k kifejezhető:

$$k = \frac{\alpha - \alpha_j}{\beta_i - \beta} .$$

Ez tényleg csak véges sok tilos k értéket jelent, hiszen az α_j és a β_i számok véges sokan vannak. □

Ha az Olvasó általánosítani akarja a fenti tételt, akkor érdemes összegyűjteni azokat a pontokat, ahol kihasználtuk, hogy $\mathbb{C}$ résztesteiről van szó. Először is az f és g polinomokat gyöktényezők szorzatára bontottuk. Ha tehát $\mathbb{C}$ nem áll rendelkezésre, akkor meg kell mutatni, hogy tetszőleges L testnek van olyan bővítése, amelyben bizonyos $L[x]$-beli polinomok gyöktényezőkre bomlanak. Ezt megtesszük majd a 6.4. Szakaszban.

Másodszor, kihasználtuk, hogy a K testnek végtelen sok eleme van. (Ez teljesül mindig, ha K karakterisztikája nulla, hiszen akkor prímteste $\mathbb{Q}$-val izomorf.) Ha a fenti bizonyítás nem is működik, maga az állítás, hogy minden véges bővítés egyszerű, a véges testekre is igaz (6.7.4. Állítás). Ez azon múlik, hogy véges test multiplikatív csoportja mindig ciklikus (4.3.16. Tétel).

Harmadszor, szükségünk volt arra, hogy az irreducibilis g polinomnak nincs többszörös gyöke K egyetlen bővítésében sem. Ezt fogalmazza meg a következő definíció.

6.3.9. Definíció. A *K tökéletes test*, ha egy K fölött irreducibilis polinomnak nem lehet többszörös gyöke K egyetlen bővítésében sem.

Azok a testek, amiket eddig vizsgáltunk, mind tökéletesek, az alábbi állítás szerint.

6.3.10. Állítás. *Minden nulla karakterisztikájú test, és minden véges test tökéletes.*

6.3.11. Tétel. *Tökéletes test minden véges bővítése egyszerű.*

Van egyáltalán nem tökéletes test? Noha könyvünkben a Galois-elmélet alkalmazásaihoz csak a $\mathbb{C}$ résztesteinek, illetve a véges testeknek a megértésére van szükség, az érdeklődő Olvasó számára lehetővé szeretnénk tenni, hogy a témát kicsit körüljárja. Most áttekintjük, hogy mindehhez mely feladatokat érdemes megoldania.

Azt, hogy minden nulla karakterisztikájú test tökéletes, a 6.3.16. Gyakorlatban bizonyítjuk. A 6.4.16. Gyakorlatban belátjuk, hogy végtelen tökéletes test minden véges bővítése egyszerű. Ezzel a nulla karakterisztikájú esetet teljesen el is intézzük.

A 6.4.22. Feladatban jellemezzük azokat az irreducibilis polinomokat, amelyeknek van többszörös gyöke egy alkalmas bővítésben. Ebből kiindulva a 6.4.23. Feladatban példát adunk nem tökéletes testre, sőt a 6.4.24. Feladatban jellemezzük is a tökéletes testeket. Speciális esetként kiderül, hogy minden véges test tökéletes (6.4.26. Gyakorlat). A 6.4.27. Feladatban megmutatjuk, hogy hogyan lehet tökéletes résztestet találni (vagyis orvosolni azt a problémát, hogy az alaptest esetleg nem tökéletes).

Végül megemlítünk néhány elnevezést, amit a szakirodalomban használnak. Az $f \in K[x]$ irreducibilis polinomot *szeparábilisnak* nevezzük, ha K egyetlen bővítésében sincs többszörös gyöke, különben *inszeparábilis*. A $K \leq L$ *szeparábilis bővítés*, ha L minden elemének K fölötti minimálpolinomja szeparábilis (vagyis egyetlen L-beli elem K fölötti minimálpolinomjának sincs többszörös gyöke a K egyetlen bővítésében sem). Tehát tökéletes test minden bővítése szeparábilis. Egy bővítés egy eleme akkor szeparábilis, ha a minimálpolinomja az.

Gyakorlatok, feladatok

6.3.12. Gyakorlat. Igazoljuk, hogy az $x^4 - 2$ polinom $\mathbb{Q}$ fölötti felbontási teste $\mathbb{Q}(\sqrt[4]{2}, i)$, és hogy ez $\mathbb{Q}$-nak nyolcadfokú bővítése.

6.3.13. Gyakorlat. Határozzuk meg az alábbi polinomok felbontási testének fokát $\mathbb{Q}$ fölött.

(1) $x^2 + 1$.
(2) $x^4 - 1$.
(3) $x^4 + 1$.
(4) $x^6 - 1$.
(5) $x^6 - 2$.
(6) $(x^2 - 2)(x^3 - 2)$.
(7) $(x^2 - 2)(x^2 - 3)$.

6.3.14. Gyakorlat. Mutassuk meg, hogy ha $K \leq L$ másodfokú bővítés, akkor normális, és ha K karakterisztikája nem 2, akkor $L = K(\sqrt{d})$ alkalmas $d \in K$ elemre (használjuk föl az 5.7.12. Gyakorlatot).

6.3.15. Feladat. Adjuk meg $\mathbb{Q}$-nak egy harmadfokú, normális bővítését.

6.3.16. Gyakorlat. Igazoljuk a 3.6.13. Feladat általánosításaként, hogy egy nulla karakterisztikájú K test fölötti irreducibilis polinomnak K egyetlen bővítésében sem lehet többszörös gyöke.

6.3.17. Gyakorlat. Mutassuk meg, hogy ha $K \leq L \leq M$ véges bővítés, és $K \leq M$ normális, akkor $L \leq M$ is normális.

6.3.18. Gyakorlat. Mutassuk meg, hogy ha $K \leq L$ véges normális bővítés, és $L \leq M$ egy $f \in K[x]$ polinom felbontási teste L fölött, akkor $K \leq M$ normális. Igaz-e, hogy normális bővítés normális bővítése is normális?

6.4. Testbővítések konstrukciója

Már korábban is pedzegettük, és a komplex számok példáján részben be is mutattuk, hogy faktorgyűrűk segítségével testbővítéseket lehet konstruálni. Ebben a szakaszban részletezzük ezt az eljárást. Ha az Olvasó gyorsan el akar jutni a Galois-elmélet főtételéig, és azon túl a fő alkalmazásokig, akkor ezt a fejezetet első olvasásra átugorhatja (annál is inkább, mert a most következők kicsit absztraktabbak az eddig megszokottnál). A kapott eredmények azonban szerepet játszanak a főtétel bizonyításában, és a véges testek konstrukciójában. Szó lesz az algebrailag zárt testek létezéséről is.

A most következők megértéséhez mindenképpen érdemes átismételni az 5.2. Szakaszban leírt módszert, amelynek segítségével faktorgyűrűben reprezentánsok segítségével számoltunk. Első állításunk az 5.2.8. Gyakorlatban szereplő $\mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}(\sqrt[3]{2})$ izomorfizmust általánosítja.

6.4.1. Tétel. *Legyen $K \leq L$ testbővítés és $\alpha \in L$ egy K fölött algebrai elem, melynek K fölötti minimálpolinomja s. Ekkor*

$$K[x]/(s) \cong K(\alpha)\,.$$

Ennél az izomorfizmusnál az α elemnek az $x+(s)$ mellékosztály, a $K \subseteq K(\alpha)$ test egy k elemének pedig a $k+(s)$ mellékosztály felel meg.

Bizonyítás. Tekintsük az „α behelyettesítése" nevű gyűrű-homomorfizmust (5.9.7. Gyakorlat), vagyis legyen $\varphi : K[x] \to L$ az a leképezés, amelyre tetszőleges $f \in K[x]$ esetén $\varphi(f) = f(\alpha)$. Ez nyilván műveletartó, és így a homomorfizmus-tétel miatt

$$K[x]/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)\,.$$

Itt $\operatorname{Ker}(\varphi)$ azokból az f polinomokból áll, amelyekre $f(\alpha) = 0$, vagyis amelyek a minimálpolinom többszörösei. Ezért $\operatorname{Ker}(\varphi) = (s)$. Az $\operatorname{Im}(\varphi)$ az $f(\alpha)$ alakú elemek halmaza, ahol $f \in K[x]$. Természetesen minden ilyen elem kifejezhető α-ból és K elemeivel összeadás és szorzás segítségével, és így benne van $K(\alpha)$-ban (hiszen $K(\alpha)$ test, amely K-t és α-t tartalmazza). Vagyis $\operatorname{Im}(\varphi) \subseteq K(\alpha)$.

Ha felhasználnánk a 6.1.13. Tételt, akkor látnánk, hogy $K(\alpha) \subseteq \operatorname{Im}(\varphi)$, és így az izomorfizmus bizonyításával készen lennénk. Mi azonban szeretnénk ezt a tételt is megkapni az új technikával, ezért inkább a következőképpen haladunk tovább.

Mivel α algebrai K fölött, az s minimálpolinom (nem a nullapolinom, hanem) irreducibilis K fölött. Így az 5.2.9. Tétel miatt $K[x]/(s)$ test. Ezért a vele izomorf $\operatorname{Im}(\varphi)$ is részteste L-nek. Ez a résztest tartalmazza K elemeit, és α-t is. Valóban, az $f(x) = x$ polinom φ-nél vett képe α, és $k \in K$ esetén a konstans $f(x) = k$ polinom képe k. Ezért $K(\alpha)$, ami a legszűkebb K-t és α-t tartalmazó részteste L-nek, része $\operatorname{Im}(\varphi)$-nek. Ezzel a tételbeli izomorfizmust beláttuk.

Tudjuk, hogy a homomorfizmustételben szereplő izomorfizmusnál az $f+(s)$ mellékosztály és a $\varphi(f)$ egymásnak felelnek meg (lásd a 4.5.15. Tétel bizonyítását). Ezért az előző bekezdésben írottak miatt α-hoz tényleg $x+(s)$, a $k \in K$-hoz pedig $k+(s)$ tartozik. □

6.4.2. Gyakorlat. A $K[x]/(s)$ faktorgyűrűben az 5.2. Szakaszban leírt reprezentánsrendszerrel számolva adjunk új bizonyítást a 6.1.13. Tételre, az egyértelműséget is beleértve.

Most megpróbáljuk megfordítani a fentieket, és adott s irreducibilis polinomhoz elkészíteni a K test egy olyan bővítését, amelyben s-nek már van gyöke. Erről is volt már szó korábban, amikor $K = \mathbb{R}$ és $s(x) = x^2 + 1$. Az 5.2. Szakaszban kiszámoltuk, hogy

$$(a + bx) + (x^2 + 1) \leftrightarrow a + bi$$

izomorfizmus $\mathbb{R}[x]/(x^2 + 1)$ és $\mathbb{C}$ között. Azt a komplex számok felhasználása nélkül is tudjuk, hogy ez a faktorgyűrű test, hiszen $x^2 + 1$ irreducibilis. Amit a komplex számok új bevezetéséhez még meg kell mutatni az az, hogy ennek a faktorgyűrűnek van $\mathbb{R}$-rel izomorf részteste, és hogy az $x^2 + 1$ polinomnak van benne gyöke. Természetesen az $a = a + 0i$ valós számot az $a + 0x = a$ konstans polinom mellékosztályának, az $i = 0 + 1 \cdot i$ számot pedig a $0 + 1 \cdot x = x$ polinom mellékosztályának akarjuk megfeleltetni. Mindez egybevág azzal, ami az előző tétel utolsó állításában szerepel.

6.4.3. Tétel. *Legyen K test, és s egy K fölött irreducibilis polinom. Ekkor létezik olyan L test, amelyben K résztest, és amelyben az s polinomnak már van gyöke.*

Bizonyítás. Tekintsük az $L = K[x]/(s)$ faktorgyűrűt, amely az 5.2.9. Tétel miatt test. A $k+(s)$ alakú elemek, ahol $k \in K$ a K-val izomorf K' résztestet alkotnak L-ben. Valóban, ezek az elemek páronként különbözők, hiszen ha $a + (s) = b + (s)$, ahol $a, b \in K$, akkor $a - b \in (s)$, vagyis $s \mid a - b$. De s nem konstans (hiszen irreducibilis), és így a konstans polinomok közül csak a nullapolinomnak osztója. Ezért $a - b = 0$, vagyis $a = b$. A faktorgyűrűben a szorzást reprezentánselemekkel definiáltuk, és ezért a $\psi(k) = k + (s)$ nyilván izomorfizmus K és K' között.

Legyen $\alpha = x + (s)$. Meg kellene mutatni, hogy α gyöke az s polinomnak.

Itt bizony bajba kerültünk, hiszen az α elemet be sem tudjuk helyettesíteni az s polinomba! Az α az L testnek eleme. Be tudjuk helyettesíteni $L[x]$-beli polinomokba. Az s azonban nem $L[x]$-ben, hanem $K[x]$-ben van, és K egyáltalán nem részhalmaza L-nek, hanem csak *izomorf* az L egy K' résztestével. Persze a K és a K' elemeit azonosítani szeretnénk amúgy is, és akkor a problémánk megoldódna. A bizonyítás érthetőbb lesz azonban, ha ezt az azonosítást most még nem végezzük el.

A $\psi : K \to K'$ izomorfizmust kiterjeszthetjük egy $K[x]$ és egy $K'[x]$ közötti izomorfizmussá: minden polinomnak az együtthatóira alkalmazhatjuk. Vagyis ha

$$f(x) = k_0 + k_1 x + \ldots + k_\ell x^\ell \in K[x]\,,$$

akkor legyen

$$\psi(f)(x) = \psi(k_0) + \psi(k_1)x + \ldots + \psi(k_\ell)x^\ell\,.$$

Ez már K' fölötti polinom, és $K' \subseteq L$. Ezért ebbe be lehet az L elemeit helyettesíteni, speciálisan az $\alpha = x + (s)$ elemet is. Végezzük el a helyettesítést. Mivel $\psi(k) = k + (s)$, ezért

$$\psi(k_i)\alpha^i = \big((k_i + (s)\big)\big((x + (s)\big)^i = k_i x^i + (s)\,,$$

hiszen a faktorgyűrűben reprezentánsokkal szorzunk. Az összeadást is ugyanígy elvégezve

$$\psi(f)(\alpha) = k_0 + k_1 x + \ldots + k_\ell x^\ell + (s) = f + (s)\,.$$

Speciálisan ha $f = s$, akkor

$$\psi(s)(\alpha) = s + (s) = 0 + (s)\,,$$

hiszen $s - 0 \in (s)$. Ez a K' nulleleme, vagyis beláttuk, hogy a $\psi(s)$ polinomnak gyöke az α. Mivel a K és K' elemeit a ψ mentén azonosítjuk, az s és a $\psi(s)$ polinomok is azonossá válnak, és ezzel a bizonyítást befejeztük. □

Ha az Olvasó precízen is látni szeretné ezt az azonosítási folyamatot, akkor egy lehetőség a következő. Az L testben a K' részhalmaz elemeit cseréljük ki a K elemeivel, így kapjuk az N halmazt. Tekintsük azt a $\theta : L \to N$ leképezést, amelyre $\psi(k)$-hoz k-t rendel, L többi (azaz K'-n kívüli elemeit) pedig helyben hagyja. A θ tehát bijekció L és N között. Ennek mentén a műveleteket definiálhatjuk N-en is úgy, hogy θ izomorfizmus legyen. A kapott N test már K-t tényleg tartalmazza (nem csak egy kópiáját), és a $\theta(\alpha)$ már tényleg s-nek (és nem $\psi(s)$-nek) lesz gyöke.

A 6.4.3. Tétel kívánt tulajdonságú algebrai bővítések létezését garantálja. Érdemes hozzátenni, hogy transzcendens bővítést is lehet konstruálni.

6.4.4. Állítás. *Legyen K test. Ekkor létezik egy $L = K(\alpha)$ test, ahol α transzcendens K fölött.*

Bizonyítás. A 6.1.18. Gyakorlat miatt L-nek megfelel a $K[x]$ polinomgyűrű $K(x)$ hányadosteste, vagyis a racionális törtfüggvények teste, ahol $\alpha = x$. □

Az előző tétel lehetővé teszi, hogy egy K testet úgy bővítsünk, hogy abban már egy f polinomnak egy gyöke benne legyen. Ezt ismételhetjük is, és így elérhetjük, hogy a bővítésben az f polinomnak az „összes" gyöke benne legyen, vagyis gyöktényezőkre bomoljon.

6.4.5. Következmény. *Ha K test, és $f \in K[x]$ nem nulla polinom, akkor létezik f-nek felbontási teste K fölött.*

Bizonyítás. Bontsuk f-et irreducibilis tényezőkre K fölött, és válasszunk ezek közül tetszőlegeset. Az előző tétel miatt van olyan $K \leq K(\alpha)$ bővítés, amelyben az α elem gyöke ennek az irreducibilis polinomnak, és így f-nek is. Ekkor $f(x) = (x - \alpha)g(x)$ alkalmas $g \in K(\alpha)[x]$ polinomra. A következő lépésben g egy gyökével bővítjük a $K(\alpha)$ testet, és így tovább. Mivel a kapott polinom foka egyre kisebb, az eljárás legfőljebb $\mathrm{gr}(f)$ lépésben véget ér. □

Az eljárást folytathatjuk, és így véges sok polinom gyökeit is hozzávehetjük K-hoz. De ugyanezzel a módszerrel algebrailag zárt testet is kaphatunk. Ehhez az összes polinom összes gyökét be kell venni, azaz végtelen sok lépésben bővíteni. Ez a probléma ismét nem algebrai, hanem halmazelméleti. A megoldására használt módszer azonban nem a

Zorn-lemma, mint a Krull-tétel esetében, hanem az úgynevezett *transzfinit indukció*. Ezt felhasználva, minden további algebrai nehézség nélkül bizonyítható az alábbi tétel.

6.4.6. Tétel. *Minden testnek van algebrailag zárt algebrai bővítése.*

Algebrailag zárt testre eddig két példát láttunk, a komplex számtestet, és az algebrai számok testét. A komplex számtestről még nem láttuk be, hogy algebrailag zárt (de be fogjuk, lásd 6.6.10. Tétel). Az algebrai számok testéről ezt igazoltuk, de közben kihasználtuk, hogy $\mathbb{C}$ algebrailag zárt. Ez utóbbi bizonyítás általánosításaként a 6.4.17. Feladatban megmutatjuk, hogy a K testhez elegendő a $K[x]$-beli polinomok gyökeit hozzávenni, ekkor már algebrailag zárt testet kapunk. Kicsit nehezebb igazolni, hogy elegendő minden irreducibilis polinomnak csak egy gyökét bevenni (6.4.19. Feladat). Ebből kiindulva az Olvasó transzfinit indukció helyett Krull tételére támaszkodva maga is beláthatja az algebrai lezárt létezését (6.4.20. Feladat).

Fölmerül a kérdés, hogy az algebrai lezárt (vagy akár egy polinom felbontási teste) izomorfia erejéig egyértelműen meg van-e határozva. A szakasz hátralévő részében ezt a problémát vizsgáljuk.

Első lépésként vizsgáljuk meg, hogy ha $\mathbb{Q}$-t az x^3-2 polinom két különböző gyökével bővítjük, akkor izomorf testeket kapunk-e. Legyenek ezek a gyökök $\sqrt[3]{2}$ és $\varepsilon\sqrt[3]{2}$, ahol $\varepsilon = \cos 120^\circ + i \sin 120^\circ$ primitív harmadik egységgyök. A két test elemei az

$$a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 \quad \text{illetve az} \quad a + b\varepsilon\sqrt[3]{2} + c\left(\varepsilon\sqrt[3]{2}\right)^2$$

alakú számok, ahol $a, b, c \in \mathbb{Q}$. Ezekkel azonban ugyanúgy kell számolni! Az összeadásra ez nyilvánvaló. A szorzást úgy végezzük el, hogy a disztributivitás alapján felbontjuk a zárójeleket, és az első esetben alkalmazzuk, hogy $\sqrt[3]{2}$ köbe kettő, a másodikban pedig azt, hogy $\varepsilon\sqrt[3]{2}$ köbe kettő. A két számolásban semmi különbség nem lesz (ha valaki véletlenül kicseréli a $\sqrt[3]{2}$ számot $\varepsilon\sqrt[3]{2}$-re, akkor azt észre sem vesszük). Ezért a két test izomorf.

Az előző bekezdésben leírtak megmagyarázzák, hogy a két test miért izomorf, de ez nem volt egy teljesen precíz bizonyítás. Vegyük azonban észre, hogy a 6.4.1. Tételt alkalmazhatjuk a $\sqrt[3]{2}$ és a $\varepsilon\sqrt[3]{2}$ számokra is. Mindkettő minimálpolinomja x^3-2, és ezért azt kapjuk, amit szeretnénk, hiszen

$$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}(\varepsilon\sqrt[3]{2})\,.$$

Sőt azt is tudjuk, hogy a $\sqrt[3]{2}$ számnak az első izomorfizmusnál $x+(x^3-2)$ felel meg, aminek a képe a másik izomorfizmusnál $\varepsilon\sqrt[3]{2}$. Ugyanakkor ha $q \in \mathbb{Q}$, akkor az első izomorfizmusnál ez $q+(x^3-2)$-be megy, és a másodiknál ez visszamegy q-ba. Vagyis létezik egy olyan $\varphi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\varepsilon\sqrt[3]{2})$ izomorfizmus, amelyre $\varphi(\sqrt[3]{2}) = \varepsilon\sqrt[3]{2}$, és $\varphi(q) = q$ minden $q \in \mathbb{Q}$ esetén.

Azonnal látjuk, hogy mindkét fenti gondolatmenet általánosítható a következőképpen. A $\mathbb{Q}$ helyett tetszőleges K testet vehetünk, x^3-2 helyett egy K fölött irreducibilis f polinomot, $\sqrt[3]{2}$ és $\varepsilon\sqrt[3]{2}$ helyett pedig f egy α és egy β gyökét.

6.4.7. Állítás. *Tegyük föl, hogy $K \leq L$ testbővítés, és az $\alpha, \beta \in L$ elemek K fölötti minimálpolinomja megegyezik. Ekkor van olyan $\varphi : K(\alpha) \to K(\beta)$ izomorfizmus, amely α-t β-ba, K elemeit pedig önmagukba viszi.*

A későbbi alkalmazások miatt még egy kicsit tovább kell ezt a helyzetet általánosítanunk. Ahelyett, hogy egy K testünk van, két izomorf testből kell kiindulnunk. Az előző tétel bizonyításában már használtuk azt a jelölést, hogy ha $\psi : K \to M$ izomorfizmus két test között, akkor ψ a $K[x]$-nek az $M[x]$-szel való izomorfizmusát adja: egy polinom képét úgy kapjuk, hogy minden együtthatójára alkalmazzuk a ψ-t. Az alábbi tételt csak annak érdemes megemésztenie, aki teljes egészében meg akarja érteni a felbontási test egyértelműségének és a Galois-elmélet főtételének a bizonyítását is.

6.4.8. Tétel [Izomorfizmus-kiterjesztési tétel]. *Legyen $K \leq L$ és $M \leq N$ két testbővítés, és $\psi : K \to M$ izomorfizmus. Tegyük föl, hogy $s \in K[x]$ egy irreducibilis polinom, és t a neki ψ-nél megfelelő irreducibilis polinom $M[x]$-ben. Legyen $\alpha \in L$ gyöke s-nek, és $\beta \in N$ gyöke t-nek. Ekkor létezik olyan*

$$\varphi : K(\alpha) \to M(\beta)$$

izomorfizmus, amelyre $\varphi(\alpha) = \beta$, és amely ψ-nek kiterjesztése, azaz tetszőleges $k \in K$ esetén $\varphi(k) = \psi(k)$.

Bizonyítás. A 6.4.1. Tételt kétszer alkalmazva

$$K(\alpha) \cong K[x]/(s) \quad \text{és} \quad M(\beta) \cong M[x]/(t)\,.$$

Az $f + (s) \leftrightarrow \psi(f) + (t)$ izomorfizmus $K[x]/(s)$ és $M[x]/(t)$ között (ezt beláthatjuk például úgy, hogy az $f \to \psi(f) + (t)$ leképezésre alkalmazzuk a homomorfizmus-tételt, de amúgy is nyilvánvaló, hiszen ha izomorf gyűrűket az izomorfizmusnál egymásnak megfelelő ideálokkal faktorizálunk, akkor a faktorok is nyilván izomorfak lesznek). A kapott izomorfizmusokat összekapcsolva (azaz kompozíciójukat véve) egy $K(\alpha)$ és $M(\beta)$ közötti φ izomorfizmust kapunk. Ha α-ból indulunk, akkor először $x + (s)$-et, innen $x + (t)$-t kapjuk (hiszen ψ a K egységelemét a M egységelemébe, és így az $x = 1 \cdot x \in K[x]$ polinomot $x \in M[x]$-be viszi), és végül az eredmény β lesz. Ha pedig $k \in K$, akkor ennek képe $k + (s)$, majd $\psi(k) + (t)$, végül $\psi(k)$. □

Most már be tudjuk bizonyítani, hogy a felbontási test is egyértelműen meghatározott.

6.4.9. Következmény. *Ha az $f \in K[x]$ polinomnak $K \leq L$ és $K \leq N$ is felbontási teste, akkor L és N izomorfak.*

A bizonyítás lényege nagyon egyszerű: az f gyökeit egyenként hozzávesszük K-hoz, és az izomorfizmust mindig tovább terjesztjük a kapott résztestre, amíg föl nem érünk L-ig. Ahhoz, hogy ez az eljárás működjön (és a későbbi alkalmazások miatt is), az állítást az előző tételhez hasonló általánosságban kell megfogalmaznunk.

6.4.10. Következmény. *Legyen $K \leq L$ és $M \leq N$ két testbővítés, és $\psi : K \to M$ izomorfizmus. Tegyük föl, hogy $f \in K[x]$ egy polinom, és g a neki ψ-nél megfelelő polinom $M[x]$-ben, továbbá hogy L felbontási teste f-nek K fölött, és N felbontási teste g-nek M fölött. Ekkor létezik olyan $\varphi : L \to N$ izomorfizmus, amely ψ-nek kiterjesztése.*

Bizonyítás. Az f fokszáma szerinti indukcióval bizonyítunk. Nulladfokú polinomra az állítás nyilvánvaló, hiszen ilyenkor $L = K$ és $N = M$, vagyis $\varphi = \psi$ megfelelő. Tegyük föl, hogy f foka n, és az ennél kisebb fokú polinomokra igaz a tétel. Legyenek f gyökei L-ben $\alpha_1, \ldots, \alpha_n$, ekkor $L = K(\alpha_1, \ldots, \alpha_n)$.

Vegyük az f polinom egy K fölött irreducibilis s tényezőjét. Ennek gyökei is az α_i elemek között vannak, az indexek átszámozásával feltehetjük, hogy s-nek α_1 gyöke. Természetesen $\psi(s)$ osztója a $g = \psi(f)$ polinomnak. Mivel az N az g polinom felbontási teste, a g itt gyöktényezőkre bomlik, és ezért a $\psi(s)$-nek is van egy β_1 gyöke N-ben. Az izomorfizmus-kiterjesztési tétel miatt ψ kiterjeszthető egy

$$\theta : K(\alpha_1) \to M(\beta_1)$$

izomorfizmussá.

Tekintsük a $h(x) = f(x)/(x - \alpha_1)$ polinomot. Ennek együtthatói a $K(\alpha_1)$ testből valók. Az L-et $K(\alpha_1)$ fölött már generálja $\alpha_2, \ldots, \alpha_n$, azaz h gyökei. Ezért L felbontási teste $K(\alpha_1)$ fölött az $n-1$-edfokú h polinomnak. Ugyanígy N felbontási teste lesz $M(\beta_1)$ fölött a $\theta(h)$ polinomnak. Valóban, $\theta(h) = g/(x - \beta_1)$, és N-et $K(\beta_1)$ fölött már generálják a g polinom β_1-től különböző gyökei. Az indukciós feltevés miatt ezért θ kiterjeszthető egy $L \to N$ izomorfizmussá. □

6.4.11. Gyakorlat. Mutassuk meg, hogy a $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ testnek van olyan önmagával való izomorfizmusa, amelynél $\sqrt[3]{2}$ képe $\varepsilon\sqrt[3]{2}$. (Itt ε primitív harmadik egységgyök.)

Ennek a gyakorlatnak a tanulságát fogalmazzuk meg általánosan is, mert később szükségünk lesz rá.

6.4.12. Következmény. *Tegyük föl, hogy $K \leq L$ véges normális bővítés, és az $\alpha, \beta \in L$ elemek K fölötti minimálpolinomja megegyezik. Ekkor van olyan $\varphi : L \to L$ izomorfizmus, amely α-t β-ba, K elemeit pedig önmagukba viszi.*

Bizonyítás. A 6.4.7. Állítás miatt van olyan $\psi : K(\alpha) \to K(\beta)$ izomorfizmus, amely K elemeit önmagukba viszi, és melyre $\psi(\alpha) = \beta$. A 6.3.7. Gyakorlat szerint L egy alkalmas $f \in K[x]$ polinom felbontási teste K fölött. Ekkor ugyanennek az f polinomnak L felbontási teste $K(\alpha)$ és $K(\beta)$ fölött is. A ψ az f polinomot önmagába viszi, hiszen K elemeit fixálja. Ezért az előző 6.4.10. Következmény miatt ψ kiterjeszthető egy $L \to L$ izomorfizmussá. □

Az algebrailag zárt bővítés egyértelműsége ugyanígy bizonyítható, csak az izomorfizmust végtelen sok lépésben, transzfinit módszerekkel kell kiterjeszteni.

6.4.13. Tétel. *Ha a K testnek L és N is algebrailag zárt algebrai bővítése, akkor L és N izomorfak, sőt K minden automorfizmusa kiterjeszthető egy $L \to N$ izomorfizmussá.*

6.4.14. Definíció. A K test (egyértelműen meghatározott) algebrailag zárt algebrai bővítését a *K algebrai lezártjának* nevezzük.

Például a racionális számok testének algebrai lezártja az algebrai számok teste, a valós számokénak pedig a komplex számtest.

Gyakorlatok, feladatok

6.4.15. Gyakorlat. Tegyük föl, hogy $K \leq L$ véges bővítés. Mutassuk meg, hogy van olyan $L \leq M$ test, hogy $K \leq M$ véges normális bővítés.

6.4.16. Gyakorlat. Igazoljuk, hogy végtelen elemszámú tökéletes test minden véges bővítése egyszerű.

6.4.17. Feladat. Tegyük föl, hogy $K \leq L$ algebrai bővítés, és minden nem konstans $K[x]$-beli polinom gyöktényezők szorzatára bomlik L-ben. Mutassuk meg, hogy L algebrailag zárt.

6.4.18. Gyakorlat. Mutassuk meg, hogy ha egy testnek van algebrailag zárt bővítése, akkor van algebrailag zárt algebrai bővítése is.

6.4.19. Feladat. Tegyük föl, hogy $K \leq L$ algebrai bővítés, amelyben minden irreducibilis $K[x]$-beli polinomnak van gyöke. Mutassuk meg, hogy L algebrailag zárt.

6.4.20. Feladat. Legyen K test. Minden irreducibilis $f \in K[x]$ polinomhoz vegyünk föl egy x_f határozatlant, és legyen I a $K[\ldots, x_f, \ldots]$ polinomgyűrűben az összes $f(x_f)$ polinomok által generált ideál. Mutassuk meg, hogy van I-t tartalmazó maximális ideál, és a szerinte vett faktor olyan algebrailag zárt test, amelynek van K-val izomorf részteste.

6.4.21. Feladat. Igazoljuk, hogy ha $K \leq L$ testbővítés, és K-t végtelen sok olyan polinom gyökével bővítjük, amelynek az összes gyöke L-ben van, akkor normális bővítést kapunk. Megfordítva, igazoljuk, hogy minden normális bővítés megkapható ilyen módon.

Ez a feladat tehát azt mutatja, hogy a normális bővítések pontosan a polinomhalmazok felbontási testei. A most következő feladatok a szeparábilis bővítések és tökéletes testek témakörét járják körül.

6.4.22. Feladat. Igazoljuk, hogy ha K test, akkor az $f \in K[x]$ irreducibilis polinomnak akkor és csak akkor van többszörös gyöke a K egy alkalmas bővítésében, ha K karakterisztikája egy p prímszám, és f az x^p polinomjaként írható (vagyis az x^i együtthatója nulla minden p-vel nem osztható i esetén).

6.4.23. Feladat. Legyen α transzcendens elem $\mathbb{Z}_p$ fölött. Mutassuk meg, hogy $x^p - \alpha$ irreducibilis $\mathbb{Z}_p(\alpha)$ fölött, de van többszörös gyöke egy alkalmas bővítésben (vagyis ez a polinom inszeparábilis).

6.4.24. Feladat. Mutassuk meg, hogy a $p \neq 0$ karakterisztikájú K test akkor és csak akkor tökéletes, ha minden eleméből vonható p-edik gyök.

6.4.25. Feladat. Igazoljuk, hogy tökéletes test minden véges bővítése is tökéletes.

6.4.26. Gyakorlat. Igazoljuk, hogy az $x \mapsto x^p$ Frobenius-endomorfizmus minden p karakterisztikájú véges testben automorfizmus, és ezért minden véges test tökéletes.

6.4.27. Feladat. Tegyük föl, hogy L algebrailag zárt bővítése a K testnek. Mutassuk meg, hogy a K elemeinek p-hatványadik gyökei L-ben egy K-t tartalmazó tökéletes testet alkotnak.

6.4.28. Feladat. Mutassuk meg, hogy ha $K \leq L$ tetszőleges testbővítés, akkor L szeparábilis elemei résztestet alkotnak.

6.5. Szimmetriák és közbülső testek

A Galois-elmélet alkalmazásai során általában az a feladat, hogy adott egy $K \leq L$ testbővítés, és meg kell találnunk a *közbülső* $K \leq T \leq L$ testeket. Ezek ismerete dönt el olyan problémákat, mint például a geometriai szerkeszthetőség. A közbülső testeket a $K \leq L$ úgynevezett *szimmetriáinak* segítségével találhatjuk meg (úgy, hogy a *fixpontjaikat* tekintjük). Ebben a szakaszban példákon keresztül próbáljuk megérteni ezeket a fogalmat. Fontos, hogy az Olvasó ezeket a példákat ne ugorja át.

A komplex számok esetében a konjugálás fogalma alapvető eszköznek bizonyult. Például beláttuk, hogy egy valós együtthatós polinom minden komplex gyökének a konjugáltja is gyök, és ennek segítségével meg tudtuk határozni az irreducibilis polinomokat is $\mathbb{R}$ fölött. A konjugálás azért hatásos, mert „jó” tulajdonságokkal rendelkezik: összeg- és szorzattartó. Tudjuk azt is, hogy bijektív, továbbá egy szám konjugáltja akkor és csak akkor önmaga, ha az a szám valós.

Hasonlóan hasznos a $\mathbb{Q}(\sqrt{2})$ testen a

$$\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$$

képlettel értelmezett függvény. Könnyen látható, hogy ez is izomorfizmus, és pont a $\mathbb{Q}$ elemeit hagyja fixen. Ezt a φ leképezést felfoghatjuk úgy is, mint $\mathbb{Q}(\sqrt{2})$ egy szimmetriáját, ami azt mutatja, hogy ebben a testben $\sqrt{2}$ és $-\sqrt{2}$ szerepe azonos.

6.5.1. Definíció. Egy $K \leq L$ testbővítés szimmetriájának, vagy *relatív automorfizmusának* (ritkán konjugálásának) az olyan $\varphi : L \to L$ izomorfizmusokat nevezzük, amelyek K minden elemét fixen hagyják, azaz $k \in K$ esetén $\varphi(k) = k$. Ezek halmazát $G(L/K)$ jelöli.

6.5.2. Kérdés. Hogyan lehet meghatározni a $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$ bővítés összes szimmetriáit?

Ha φ ilyen, akkor

$$\Big(\varphi(\sqrt{2})\Big)^2 = \varphi(\sqrt{2}) \cdot \varphi(\sqrt{2}) = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(2) = 2\,,$$

hiszen $\mathbb{Q}$ elemei fixen maradnak. Viszont olyan szám, amelynek a négyzete 2, még $\mathbb{C}$-ben is csak kettő van: a $\pm\sqrt{2}$ (hiszen ezek az x^2-2 polinomnak a gyökei). Ha $\varphi(\sqrt{2}) = -\sqrt{2}$, akkor

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a - b\sqrt{2}\,,$$

hiszen a és b is racionális számok, tehát fixen maradnak. Vagyis φ a fenti leképezés. Hasonlóan láthatjuk, hogy ha $\varphi(\sqrt{2}) = \sqrt{2}$, akkor φ az identitás. Ennek a bővítésnek tehát két szimmetriája van.

Hasonlóan láthatjuk be, hogy az $\mathbb{R} \leq \mathbb{C}$ bővítésnek is két szimmetriája van, a komplex konjugálás és önmaga. Ehhez az $x^2 - 2$ helyett az $x^2 + 1$ polinomot kell használni.

Az eddigi számolásban két ötletünk volt. Az elsővel meghatároztuk, hogy a bővítést generáló elem (példánkban a $\sqrt{2}$ szám) hová mehet csak (az $x^2 - 2$ polinomnak, azaz a minimálpolinomjának a többi gyökébe). A másik ötlet pedig, hogy ennek az elemnek a képe már az egész szimmetriát meghatározza. Most ezeket általában is megfogalmazzuk.

6.5.3. Állítás. *Ha φ relatív automorfizmusa a $K \leq L$ testbővítésnek, akkor φ minden $f \in K[x]$ polinom L-beli gyökeit permutálja, vagyis ha $f(\alpha) = 0$, akkor $f\big(\varphi(\alpha)\big) = 0$ tetszőleges $\alpha \in L$-re.*

Bizonyítás. Az állítás részben a 3.3.6 Lemmát általánosítja, és a bizonyítása is hasonló. Legyen $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. Ennek gyöke az α, tehát

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0\,.$$

Alkalmazzuk φ-t mindkét oldalra. Mivel φ összeg- és szorzattartó, az eredmény ez lesz:

$$\varphi(a_0) + \varphi(a_1)\,\varphi(\alpha) + \ldots + \varphi(a_n)\,\varphi(\alpha)^n = \varphi(0)\,.$$

Mivel $0 \in K$ és $a_j \in K$ minden j-re, ezért $\varphi(0) = 0$ és $\varphi(a_j) = a_j$. Így a bal oldalon $f\big(\varphi(\alpha)\big)$ áll, a jobb oldalon 0, tehát $\varphi(\alpha)$ tényleg gyöke f-nek.

Az f polinomnak L-ben csak véges sok gyöke van. Mivel φ bijekció L-en, ezért injektív a gyökök véges halmazán is, és így szürjektív is itt, azaz permutáció. □

6.5.4. Állítás. *Ha a $K \leq K(\alpha)$ véges bővítésnek φ egy szimmetriája, akkor a $\varphi(\alpha)$ elem a φ-t már az egész bővítésen meghatározza.*

Bizonyítás. Legyen $\varphi(\alpha) = \beta$. A $K(\alpha)$ elemei

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

alakúak, ahol $a_0, \ldots, a_n \in K$. Ennek az elemnek a képe φ-nél

$$a_0 + a_1\beta + \ldots + a_n\beta^n\,,$$

hiszen minden relatív automorfizmus művelettartó, és az $a_j \in K$ elemeket fixálja. □

Az előző állítást több generátorelemre is általánosíthatjuk. Azt javasoljuk az Olvasónak, hogy a következő gyakorlatot ne a fenti módon közvetlen számolással, hanem a 4.4.28. Gyakorlat mintájára oldja meg.

6.5.5. Gyakorlat. Legyen $K \leq L$ testbővítés, és $L = K(\alpha_1, \ldots, \alpha_m)$. Igazoljuk, hogy ha $\varphi \in G(L/K)$, és ismerjük a $\varphi(\alpha_1), \ldots, \varphi(\alpha_m)$ elemeket, akkor ez φ-t már egyértelműen meghatározza az L minden elemén.

Ha egy bővítés szimmetriáit néha konjugálásoknak hívják, akkor célszerű egy elem képeit a konjugáltjainak nevezni.

6.5.6. Definíció. Legyen $K \leq L$ bővítés és $\alpha \in L$. Ekkor az $\varphi(\alpha)$ alakú elemeket, ahol $\varphi \in G(L/K)$, az α elem K fölötti *konjugáltjainak* nevezzük.

Egy komplex szám fenti értelemben vett konjugáltjai tehát önmaga és a komplex konjugáltja. Hogyan lehet a konjugáltakat általában meghatározni? A 6.5.3. Állítás szerint egy elem konjugáltjai gyökei a minimálpolinomjának. Például a $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ bővítésben az $x^3 - 2$ polinom egyetlen gyöke a $\sqrt[3]{2}$, hiszen a polinom másik két gyöke nem valós szám, a $\mathbb{Q}(\sqrt[3]{2})$-nek viszont minden eleme valós. Ezért ebben a bővítésben a $\sqrt[3]{2}$ számnak csak egyetlen konjugáltja van, önmaga, és így az egyetlen szimmetria az identitás. Megjavul a helyzet, ha bevesszük az $x^3 - 2$ polinom másik két gyökét is, vagyis az $x^3 - 2$ felbontási testét vizsgáljuk. A 6.3.1. Gyakorlat szerint ez $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, ami hatodfokú normális bővítése $\mathbb{Q}$-nak, és itt már elegendően sok automorfizmus lesz. A 6.4.11. Gyakorlat szerint például van olyan szimmetria, ami $\sqrt[3]{2}$-t $\varepsilon\sqrt[3]{2}$-be viszi.

6.5.7. Állítás. *Ha $K \leq L$ véges normális bővítés, akkor az $\alpha \in L$ elem K fölötti konjugáltjai pontosan a K fölötti minimálpolinomjának a gyökei.*

Bizonyítás. Az, hogy a konjugáltak gyökei a minimálpolinomnak, a 6.5.3. Állításból következik. A megfordítás pontosan a 6.4.12. Következmény állítása. □

Az előző bizonyítás meglehetősen lakonikus, de csak azért, mert a munkát már elvégeztük a 6.4. Szakaszban, amikor izomorfizmusokat terjesztettünk ki. Az Olvasónak érdemes mindezt átismételni (főleg a 6.4.7. Állítás előtti példát), ha mögé akar látni ennek a bizonyításnak.

Az $x^3 - 2$ polinom felbontási testének hat automorfizmusa van (vagyis $x^3 - 2$ gyökeinek minden permutációja megvalósul egy alkalmas automorfizmus segítségével). Ezt a legegyszerűbb úgy megmutatni, hogy a $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ testet $\mathbb{Q}(\alpha)$ alakban írjuk föl alkalmas α számra, vagyis egyszerű bővítésként. (A 6.3.8. Tételben beláttuk, hogy ez lehetséges.) Ekkor az α szám $\mathbb{Q}$ fölötti s minimálpolinomja hatodfokú, és ennek mindegyik gyöke, vagyis az α összes $\mathbb{Q}$ fölötti konjugáltja benne van a $\mathbb{Q}(\alpha)$ testben, hiszen ez $\mathbb{Q}$-nak normális bővítése. Legyenek ezek a konjugáltak $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_6$. Az eddig bizonyított állítások miatt minden $1 \leq j \leq 6$ esetén pontosan egy olyan szimmetriája van ennek a bővítésnek, amely α-t α_j-be viszi. Ez a gondolatmenet általában is mutatja, hogy egy n-edfokú normális bővítésnek n szimmetriája lesz (6.6.1. Állítás).

6.5.8. Definíció. A $K \leq L$ testbővítés *közbülső testei* a $K \leq T \leq L$ testek, vagyis az L azon résztestei, amelyek K-t tartalmazzák.

6.5.9. Gyakorlat. Legyen φ relatív automorfizmusa a $K \leq L$ testbővítésnek. Mutassuk meg, hogy a φ fixpontjainak a halmaza, vagyis a

$$T = \{\alpha \in L \,:\, \varphi(\alpha) = \alpha\}$$

halmaz részteste L-nek, amely a K testet tartalmazza, és így közbülső test.

Mielőtt általános eredményeket bizonyítanánk, egy konkrét példán bemutatjuk, hogy hogyan kapcsolódnak össze a szimmetriák és a közbülső testek. Az x^4-2 polinomot fogjuk megvizsgálni $\mathbb{Q}$ fölött. A 6.3.12. Gyakorlat szerint az x^4-2 polinom $\mathbb{Q}$ fölötti felbontási teste $\mathbb{Q}(\sqrt[4]{2}, i)$, és ez $\mathbb{Q}$-nak nyolcadfokú bővítése. A fenti gondolatmenet szerint tehát 8 szimmetria van. Egy φ szimmetria megadásához a $\sqrt[4]{2}$ és az i elemek φ-nél képeit kell megtalálnunk (ez már meghatározza φ-t a 6.5.5. Gyakorlat szerint). Ezek a képek a két elem konjugáltjai, vagyis az x^4-2 és az x^2+1 polinom gyökei közül kerülnek ki, tehát

$$\varphi(\sqrt[4]{2}) \in \left\{\sqrt[4]{2},\ -\sqrt[4]{2},\ i\sqrt[4]{2},\ -i\sqrt[4]{2}\right\} \quad \text{és} \quad \varphi(i) \in \{i, -i\}\,.$$

Ez $4 \cdot 2$ lehetőséget ad φ-re. Mivel tudjuk, hogy nyolc szimmetria van, a felsorolt nyolc lehetőség tényleg meg is valósul egy-egy alkalmas φ automorfizmussal.

Ahhoz, hogy egy ilyen automorfizmus fixpontjait meghatározzuk, föl kell írnunk a bővítés egy általános elemét, vagyis egy bázist kell keresni a bővítésben. Tekintsük a

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt[4]{2}) \leq \mathbb{Q}(\sqrt[4]{2}, i)$$

testláncot. Az első bővítésben az

$$1\,, \quad \sqrt[4]{2}\,, \quad \left(\sqrt[4]{2}\right)^2 = \sqrt[4]{4} = \sqrt{2}\,, \quad \left(\sqrt[4]{2}\right)^3 = \sqrt[4]{8} = \sqrt[4]{2}\sqrt{2}$$

alkot bázist (6.1.13. Tétel), a másodikban pedig az 1 és az i. A „nagy" bővítés egy bázisát a szorzástétel (6.2.3. Következmény) bizonyítása szerint úgy kaphatjuk, hogy e két bázis elemeit egymással minden lehetséges módon összeszorozzuk. Tehát $\mathbb{Q}(\sqrt[4]{2}, i)$ elemei egyértelműen felírhatók

$$\beta = a + b\sqrt[4]{2} + c\left(\sqrt[4]{2}\right)^2 + d\left(\sqrt[4]{2}\right)^3 + ei + fi\sqrt[4]{2} + gi\left(\sqrt[4]{2}\right)^2 + hi\left(\sqrt[4]{2}\right)^3$$

alakban, ahol $a, b, c, d, e, f, g, h \in \mathbb{Q}$.

Példaként számítsuk ki annak a φ automorfizmusnak a fixpontjait, amelyre

$$\varphi(\sqrt[4]{2}) = i\sqrt[4]{2} \quad \text{és} \quad \varphi(i) = -i\,.$$

Ahhoz, hogy β képét kiszámíthassuk, mind a nyolc báziselem képét tudnunk kell. A φ művelettartása miatt például

$$\varphi\left(\left(\sqrt[4]{2}\right)^2\right) = \left(\varphi\left(\sqrt[4]{2}\right)\right)^2 = \left(i\sqrt[4]{2}\right)^2 = -\sqrt{2}\,,$$

és hasonlóan

$$\varphi\left(i\sqrt[4]{2}\right) = \varphi(i)\varphi\left(\sqrt[4]{2}\right) = (-i)\left(i\sqrt[4]{2}\right) = \sqrt[4]{2}\,.$$

A többi báziselem képét is kiszámolva, majd φ összegtartását, és azt felhasználva, hogy $\mathbb{Q}$ elemeit helyben hagyja

$$\varphi(\beta) = a + bi\sqrt[4]{2} - c\big(\sqrt[4]{2}\big)^2 - di\big(\sqrt[4]{2}\big)^3 - ei + f\sqrt[4]{2} + gi\big(\sqrt[4]{2}\big)^2 - h\big(\sqrt[4]{2}\big)^3 =$$
$$= a + f\sqrt[4]{2} - c\big(\sqrt[4]{2}\big)^2 - h\big(\sqrt[4]{2}\big)^3 - ei + bi\sqrt[4]{2} + gi\big(\sqrt[4]{2}\big)^2 - di\big(\sqrt[4]{2}\big)^3$$

adódik. Az utolsó sorban a báziselemek már ugyanolyan sorrendben vannak, ahogy β eredeti felírásában. Ezért a felírás egyértelműsége miatt $\varphi(\beta) = \beta$ akkor és csak akkor teljesül, ha a kapott kifejezés β-val együtthatóról együtthatóra megegyezik, azaz

$$a = a\,, \quad b = f\,, \quad c = -c\,, \quad d = -h\,, \quad e = -e\,, \quad f = b\,, \quad g = g\,, \quad h = -d\,.$$

Ez egy nyolcismeretlenes, nyolc egyenletből álló lineáris egyenletrendszer, amit azonban triviális megoldani: a, b, d, g tetszőleges, $c = e = 0$, és $f = b$, $h = -d$. Ezért a φ fixpontjai pontosan az

$$a + b(1+i)\sqrt[4]{2} + d(1-i)\big(\sqrt[4]{2}\big)^3 + gi\big(\sqrt[4]{2}\big)^2$$

alakú elemek, vagyis a

$$\mathbb{Q}\left((1+i)\sqrt[4]{2},\ (1-i)\big(\sqrt[4]{2}\big)^3,\ i\big(\sqrt[4]{2}\big)^2\right) = \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})$$

résztest, mert könnyű látni, hogy a $\gamma = (1+i)\sqrt[4]{2}$ segítségével (első lépésben négyzetre emelve) a másik két generátorelem kifejezhető. Még egyszer négyzetre emelve kapjuk, hogy $\gamma/2$ gyöke a $2x^4 + 1$ polinomnak, ami a fordított Schönemann-Eisenstein kritérium miatt irreducibilis $\mathbb{Q}$ fölött. Ezért a φ fixpontjainak teste, vagyis $\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})$ a $\mathbb{Q}$-nak negyedfokú bővítése (és így valódi résztest, vagyis $\mathbb{Q}(\sqrt[4]{2}, i)$-től különbözik).

Ha valakit arra kérnénk, hogy mondjon közbülső testeket a most vizsgált bővítésben, akkor biztos eszébe jutna a $\mathbb{Q}(\sqrt[4]{2})$, a $\mathbb{Q}(i)$, és valószínűleg a $\mathbb{Q}(i\sqrt[4]{2})$, valamint a $\mathbb{Q}(\sqrt{2})$ is. A most kapott testre nem valószínű, hogy gondolna számolás nélkül.

Ennél azonban sokkal fontosabb, hogy az elméletet fordított irányban is használhatjuk majd: nemcsak résztestek megtalálására, hanem éppen annak bizonyítására, hogy csak nagyon kevés résztest van. Ehhez egy olyan tételt fogunk belátni, hogy minden közbülső test megkapható automorfizmusok fixpontjainak segítségével (6.6.3. Következmény).

Az nem igaz, hogy minden közbülső test előáll egy alkalmas automorfizmus fixponthalmazaként. A legegyszerűbb példa ebben a bővítésben a $\mathbb{Q}$ alaptest, amely nem áll így elő (ez a későbbiekből következik), de nem áll így elő például a $\mathbb{Q}(i\sqrt{2})$ közbülső test sem. Ez a test előáll azonban két fixponthalmaz metszeteként: az imént vizsgált φ mellett azt a ψ automorfizmust is tekinteni kell, amelyre

$$\psi(\sqrt[4]{2}) = -\sqrt[4]{2} \quad \text{és} \quad \psi(i) = i\,.$$

Az Olvasónak ajánljuk, gyakorlásul számítsa ki, hogy ψ fixponthalmaza $\mathbb{Q}(i, \sqrt{2})$, és hogy φ és ψ közös fixpontjainak halmaza $\mathbb{Q}(i\sqrt{2})$.

Általában is igaz, hogy a szimmetriák fixponthalmazaként kapott közbülső testek metszeteként már minden közbülső test előáll. Már ez is jelentős eredmény, hiszen például

következik belőle, hogy csak véges sok közbülső test lehet. De ha n darab automorfizmus van, akkor ezek fixponttestét az összes lehetséges módon, azaz 2^n-féleképpen el kellene hogy metsszük egymással ahhoz, hogy az összes közbülső testet megkapjuk. Ennél hatékonyabb eljárást szeretnénk.

Vegyük észre, hogy a $\mathbb{Q}(i\sqrt{2})$ test elemeit nemcsak φ és ψ hagyja fixen, hanem nyilvánvalóan a $\varphi \circ \psi$ kompozíció is. Általában ha T közbülső test, akkor a T elemeit fixáló szimmetriák halmaza (vagyis $G(L/T)$) zárt a kompozícióra. Ez azt sugallja, hogy a szimmetriákat csoportként érdemes kezelni, és a közbülső testeket nem tetszőleges részhalmazok, hanem a részcsoportok jelölik majd ki. Az nyilvánvaló, hogy szimmetriák kompozíciója és inverze is szimmetria, vagyis egy csoportot kapunk.

6.5.10. Definíció. A $K \leq L$ bővítés relatív automorfizmusainak csoportját a kompozíció műveletére a bővítés *Galois-csoportjának* nevezzük (és szintén $G(L/K)$-val jelöljük).

Példaként számítsuk ki a $\varphi \circ \varphi$ kompozíciót. Az eddigi számolásokat felhasználva

$$\varphi\big(\varphi(\sqrt[4]{2})\big) = \varphi(i\sqrt[4]{2}) = \sqrt[4]{2} \quad \text{és} \quad \varphi\big(\varphi(i)\big) = \varphi(-i) = i\,.$$

Tehát $\varphi \circ \varphi$ fixálja a $\mathbb{Q}(\sqrt[4]{2}, i)$ generátorait, és így az identikus leképezés. Vagyis a φ automorfizmus rendje 2, és így $\{\varphi, id\}$ egy kételemű részcsoport. Persze φ és id közös fixpontjai ugyanazok, mint φ fixpontjai, vagyis $\mathbb{Q}(\sqrt[4]{2}+i\sqrt[4]{2})$ elemei. Érdemes észrevenni, hogy a

$$\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) \leq \mathbb{Q}(\sqrt[4]{2}, i)$$

bővítésnek a foka $8/4 = 2$ a szorzástétel miatt. Vagyis azt sejthetjük, hogy ha a T test a H részcsoporthoz tartozik, akkor $|L : T|$ a H rendje lesz.

Most értsük meg a $\mathbb{Q} \leq \mathbb{Q}(\sqrt[4]{2}, i)$ bővítés G Galois-csoportját izomorfia erejéig. Mivel 8 szimmetria van, a G csoport nyolcelemű. Emlékezzünk rá, hogy $\mathbb{Q}(\sqrt[4]{2}, i)$ az $x^4 - 2$ felbontási testeként keletkezett. E polinom gyökeit a rövidség kedvéért jelölje

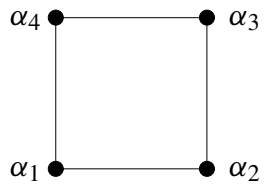
$$\alpha_1 = \sqrt[4]{2}\,, \quad \alpha_2 = i\sqrt[4]{2}\,, \quad \alpha_3 = -\sqrt[4]{2}\,, \quad \alpha_4 = -i\sqrt[4]{2}\,.$$

Mind a nyolc szimmetria ezeket permutálja, és ha ezt a permutációt ismerjük, akkor már meg van adva a szimmetria is, hiszen ez a négy szám generálja a bővítést. Ez azt jelenti, hogy a G Galois-csoport elemeit e négyelemű halmaz permutációinak is képzelhetjük. Az imént vizsgált φ szimmetria kicseréli α_1-et α_2-vel és α_3-at α_4-gyel. Ezt a permutációknál tanult ciklusos jelöléssel úgy írhatjuk, hogy $(\alpha_1\alpha_2)(\alpha_3\alpha_4)$.

Egy négyelemű halmaznak összesen 24 permutációja van, melyik nyolc az, amelyik itt megvalósul? A kulcsot az adja, hogy

$$\alpha_1 + \alpha_3 = 0 \quad \text{és} \quad \alpha_2 + \alpha_4 = 0\,.$$

Ezért az α_1, α_3 pár csak olyan elemekbe mehet, amelyek összege szintén nulla. Vagyis ha lerajzoljuk ezt a négy számot egy négyzet négy csúcsába,



akkor az előző észrevétel azt mondja, átló képe átló kell, hogy legyen. Persze akkor oldal csak oldalba mehet, és így minden relatív automorfizmus ennek a négyzetnek is szimmetriája lesz, vagyis a D_4 diédercsoportnak eleme. Ennek a csoportnak is nyolc a rendje, vagyis a négyzet minden szimmetriáját megkapjuk egy relatív automorfizmusból. Beláttuk tehát, hogy az $x^4 - 2$ felbontási testének Galois-csoportja a D_4 diédercsoporttal izomorf.

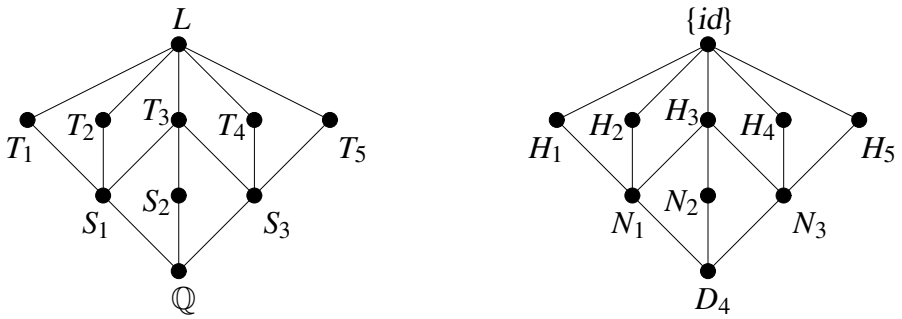
Most megadjuk a D_4 csoport összes részcsoportját, és a hozzájuk tartozó közbülső testeket. A részcsoportokat Lagrange tétele segítségével határozhatjuk meg (a 4.4.33. Gyakorlatban látott módon), a hozzájuk tartozó fixpont-testeket pedig a fentiekhez hasonló számolással. A permutációk megadásakor az α-kat lehagyjuk, vagyis például $(\alpha_1\alpha_2)(\alpha_3\alpha_4)$ helyett (12)(34)-et írunk.

$$
\begin{aligned}
\mathbb{Q}(i, \sqrt[4]{2}) = L \quad &\longleftrightarrow \quad \{id\} \\
\mathbb{Q}(i\sqrt[4]{2}) = T_1 \quad &\longleftrightarrow \quad H_1 = \{id, (13)\} \\
\mathbb{Q}(\sqrt[4]{2}) = T_2 \quad &\longleftrightarrow \quad H_2 = \{id, (24)\} \\
\mathbb{Q}(i, \sqrt{2}) = T_3 \quad &\longleftrightarrow \quad H_3 = \{id, (13)(24)\} \\
\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) = T_4 \quad &\longleftrightarrow \quad H_4 = \{id, (12)(34)\} \\
\mathbb{Q}(\sqrt[4]{2} - i\sqrt[4]{2}) = T_5 \quad &\longleftrightarrow \quad H_5 = \{id, (14)(23)\} \\
\mathbb{Q}(\sqrt{2}) = S_1 \quad &\longleftrightarrow \quad N_1 = \{id, (13), (24), (13)(24)\} \\
\mathbb{Q}(i) = S_2 \quad &\longleftrightarrow \quad N_2 = \{id, (1234), (13)(24), (1432)\} \\
\mathbb{Q}(i\sqrt{2}) = S_3 \quad &\longleftrightarrow \quad N_3 = \{id, (12)(34), (14)(23), (13)(24)\} \\
\mathbb{Q} = K \quad &\longleftrightarrow \quad D_4
\end{aligned}
$$

A részcsoportokat növekvő elemszám szerint rendeztük. A másodrendű részcsoportokhoz tartozó bővítések negyedfokúak a három negyedrendű részcsoporthoz tartozó három bővítés viszont másodfokú $\mathbb{Q}$ fölött. Ez további alapot ad annak a korábbi sejtésünknek, hogy ha a T test a H részcsoporthoz tartozik, akkor $|L : T|$ a H rendje, $|T : K|$ pedig a H indexe G-ben. Azt is láthatjuk, hogy nagyobb testhez kisebb részcsoport tartozik, vagyis ha $T \geq S$, akkor a hozzájuk tartozó részcsoportokra $H \leq N$. Még azt is érdemes észrevenni, hogy a normálosztókhoz ($\{id\}$, H_3, N_1, N_2, N_3, D_4) tartozó közbülső testek pont

azok, amelyek a $\mathbb{Q} = K$ alaptestnek normális bővítései. Mindezt általánosan belátjuk majd a Galois-elmélet főtételében (6.6.7. Tétel).

A fenti táblázat jobban áttekinthető, ha egy rajzot készítünk róla. Ha $S < T$ két közbülső test, akkor S-et lejjebb rajzoljuk, T-t följebb, és ha nincs közben más test, akkor egy vonallal összekötjük őket. A részcsoportoknál ugyanezt a rajzot fordítva csináljuk, és így az egyelemű részcsoport lesz legfelül. Ekkor a közbülső testek és a részcsoportok diagrammja ugyanaz lesz. A kapott rajzokat hálóknak nevezzük. A hálók algebrai struktúrák is, a 8. Fejezetben vizsgáljuk majd őket.



6.1. Ábra. Az $x^4 - 2$ felbontási testének közbülső testei, és a megfelelő részcsoportok.

Végül két megjegyzést teszünk. Az első, hogy módszerünkkel nem normális véges bővítések közbülső testeit is megkaphatjuk. A 6.4.15. Gyakorlat miatt ugyanis ezek kibővíthetők normális bővítéssé. Például a fenti diagramból látjuk, hogy a $\mathbb{Q} \leq \mathbb{Q}(\sqrt[4]{2})$ bővítés egyetlen nemtriviális közbülső teste a $\mathbb{Q}(\sqrt{2})$.

A másik megjegyzés arra vonatkozik, ahogy a Galois-csoportot az előbbi példában származtattuk. Ha f egy n-edfokú polinom akkor felbontási teste a 6.3.3. Gyakorlat szerint legföljebb $n!$ fokú lehet. Ez meg is valósul például az $x^3 - 2$ esetében, és összhangban van azzal, hogy a Galois-csoport elemeit úgy is felfoghatjuk, mint az f gyökeinek permutációit. Egy n-edfokú irreducibilis polinom Galois-csoportja tehát az S_n csoport részcsoportja. Az $x^4 - 2$ példájában a Galois-csoport csak D_4 volt, az S_4 szimmetrikus csoport valódi részcsoportja. Ennek oka az, hogy a gyökök között nemtriviális összefüggés van (két gyök összege nulla). A Galois-csoport tehát annál kisebb, minél több ilyen összefüggés van a polinom gyökei között.

Gyakorlatok, feladatok

6.5.11. Gyakorlat. Mennyiben változnak meg az itt leírt számítások, ha az $x^4 - 2$ polinom helyett az $x^4 - 5$ polinom felbontási testét vizsgáljuk?

6.5.12. Gyakorlat. Mutassuk meg, hogy az $x^4 - 2$, az $x^4 + 2$ és az $x^8 - 4$ polinomok felbontási teste ugyanaz, és a fenti $T_4 = \mathbb{Q}\left(\sqrt[4]{2} + i\sqrt[4]{2}\right)$ test az $x^4 + 2$ polinom egyik gyökével is generálható.

Az előző gyakorlat állítása nem marad érvényben, ha az x^4-2 helyett az x^4-5 polinomot tekintjük, lásd 6.6.13. Gyakorlat.

6.5.13. Gyakorlat. Igaz-e a 6.5.3. Állítás feltételei mellett, hogy α és $\varphi(\alpha)$ az f polinomnak ugyanannyiszoros gyökei?

6.6. A Galois-elmélet főtétele

Az előző szakaszban tárgyalt példa alapján most kimondjuk és bebizonyítjuk a Galois-elmélet főtételét. Alkalmazásként belátjuk, hogy a komplex számok teste algebrailag zárt.

Azt szeretnénk, hogy a most következőket minden Olvasónk megértse, azok is, akik nem mélyedtek el a korábbi anyagrészek egyes technikai részleteiben. Amit ebben a szakaszban vizsgálni fogunk, az egy $K \leq L$ normális bővítés. Ahhoz, hogy a bizonyítások működjenek, szükség lesz arra, hogy a szereplő bővítések mind egyszerűek legyenek, és hogy az irreducibilis polinomoknak ne legyen többszörös gyöke a bővítésekben sem. Ennek megfelelően az Olvasó az alábbi lehetőségek közül választhat.

- A legegyszerűbb, ha fölteszi, hogy a $\mathbb{C}$ résztesteiről van szó. Ebben az esetben a 6.3.8. Tétel biztosítja, hogy a szereplő bővítések egyszerűek legyenek.
- Ehelyett elegendő, ha a szereplő testek karakterisztikája nulla, vagy pedig végesek, a 6.3.10. Állítás, és a 6.3.11. Tétel együtt biztosítja az egyszerűséget.
- Valójában arra van szükség, hogy a K alaptest tökéletes legyen. Ekkor a 6.4.25. Feladat szerint a véges bővítései is azok, tehát a 6.3.11. Tétel ismét biztosítja, hogy minden szereplő bővítés egyszerű.

Röviden szólva: az állításokban szerepelni fog az a feltétel, hogy K tökéletes test, de az Olvasó ezt úgy is kiolvashatja, hogy részteste $\mathbb{C}$-nek.

6.6.1. Állítás. *Legyen L a K tökéletes test véges normális bővítése. Ekkor a bővítés relatív automorfizmusainak a száma pont a bővítés foka, azaz $|L:K|$.*

Bizonyítás. A K tökéletes, ezért a $K \leq L$ bővítés egyszerű, vagyis van olyan $\alpha \in L$ elem, melyre $L = K(\alpha)$. Legyen s az α minimálpolinomja K fölött. Mivel $K \leq L$ normális bővítés, az s gyökténye zőkre bomlik L-ben. A gyökök mind egyszeresek, hiszen K tökéletes, jelölje őket $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, ezek tehát az α konjugáltjai. Az n megegyezik az s fokával, ami ugyanaz, mint az α elem foka K fölött. Ez a fokszám viszont $L = K(\alpha)$ miatt $|L:K|$.

A 6.5.7. Állításban már beláttuk, hogy minden j-re van olyan φ_j relatív automorfizmus, ami $\alpha = \alpha_1$-et α_j-be viszi. (Megjegyezzük, hogy ez az egyszerűbben bizonyítható 6.4.7. Állításból is adódik). Ezek az automorfizmusok persze páronként különbözők. A 6.5.5. Gyakorlat miatt az α elem képe az automorfizmust már meghatározza, és így az automorfizmusok száma n. □

Most azt kezdjük el bizonyítani, hogy minden közbülső test megkapható automorfizmusok fixpontjainak segítségével.

6.6.2. Állítás. *Legyen L a K tökéletes test véges normális bővítése. Ha egy $\alpha \in L$ elem a bővítés minden relatív automorfizmusának fixpontja, akkor $\alpha \in K$.*

Bizonyítás. Legyenek $\varphi_1, \ldots, \varphi_n$ a $K \leq L$ bővítés összes automorfizmusai (ahol tehát $n = |L : K|$), és jelölje T a $\varphi_1, \ldots, \varphi_n$ közös fixpontjainak halmazát. Ez nyilván közbülső teste a $K \leq L$ bővítésnek (hiszen az egyes automorfizmusokhoz tartozó fixpont-testek metszete).

A $T \leq L$ is normális bővítés (6.3.17. Gyakorlat), és T is tökéletes test (6.4.25. Feladat). Ezért a $T \leq L$ bővítésnek is annyi szimmetriája van, amennyi a bővítés foka (6.6.1. Állítás). De a φ_i mindegyike relatív automorfizmusa a $T \leq L$ bővítésnek, hiszen T elemeit fixen hagyja. Ezért $n \leq |L : T|$, és a szorzástétel miatt

$$|T : K| = \frac{|L : K|}{|L : T|} \leq \frac{n}{n} = 1\,.$$

Így T egydimenziós K fölött, vagyis $T = K$ (6.1.16. Gyakorlat). □

6.6.3. Következmény. *Legyen L a K tökéletes test véges normális bővítése. Ekkor minden közbülső test előáll néhány $G(L/K)$-beli automorfizmus közös fixpontjainak a halmazaként. Pontosabban, ha $K \leq T \leq L$, akkor T azoknak az automorfizmusoknak a közös fixpontjaiból áll, amelyek T elemeit fixálják. Ezek az automorfizmusok a $G(L/T)$ Galois-csoport elemei, amely $G(L/K)$-nak részcsoportja.*

Bizonyítás. A T elemeit fixáló automorfizmusok a $T \leq L$ bővítés relatív automorfizmusai, vagyis tényleg a $G(L/T)$ csoport elemei. Az előző állítást K helyett T-re alkalmazva kapjuk, hogy ezek közös fixpontjainak a halmaza pont T (és nem nagyobb). □

Tehát minden közbülső test megkapható egy részcsoportból, a közös fixpontok halmazaként. Nemsokára belátjuk, hogy különböző részcsoportokhoz különböző közbülső testek tartoznak. Ennek lényege a következő állítás.

6.6.4. Állítás. *Legyen L a K tökéletes test véges normális bővítése, H valódi részcsoportja a $G(L/K)$ Galois-csoportnak (azaz $H \neq G(L/K)$), és T a H-beli szimmetriák közös fixpontjainak a halmaza. Ekkor $T \neq K$.*

Bizonyítás. Legyen $\alpha \in L$, és

$$h(x) = \prod_{\varphi \in H} \big(x - \varphi(\alpha)\big)\,.$$

Megmutatjuk, hogy ez a polinom T-beli együtthatós.

Soroljuk föl a H elemeit: $\varphi_1, \ldots, \varphi_m$. Hogy a bizonyítást megértsük, vizsgáljuk először a h polinomban az x^{m-1}-es tag együtthatóját, ami a gyökök és együtthatók összefüggése miatt

$$-\varphi_1(\alpha) - \ldots - \varphi_m(\alpha)\,.$$

Ha erre φ_j-t alkalmazzuk, akkor az eredmény az összegtartás miatt

$$-\varphi_j\big(\varphi_1(\alpha)\big) - \ldots - \varphi_j\big(\varphi_m(\alpha)\big)\,.$$

Mivel H részcsoport a kompozícióra, a $\varphi_j \circ \varphi_1, \ldots, \varphi_j \circ \varphi_m$ ismét a H összes eleme, csak esetleg más sorrendben. Ezért a fenti összegnek a tagjai csak cserélődtek, de maga az összeg nem változott. Ugyanígy bizonyíthatjuk, hogy h többi együtthatója is fixen marad φ_j-nél, hiszen azok is (elemi) szimmetrikus kifejezések. Ezért h együtthatói közös fixpontjai a H elemeinek, és ezért T definíciója miatt T-ben vannak. Ezzel beláttuk, hogy h tényleg T-beli együtthatós.

A gondolatmenetet elmondhattuk volna úgy is, hogy a $\varphi_j : L \to L$ leképezést a polinomok együtthatóira alkalmazva kiterjesztjük egy $L[x] \to L[x]$ izomorfizmussá, amit szintén φ_j-vel jelölünk. Ekkor

$$\varphi_j(h)(x) = \big(x - \varphi_j\big(\varphi_1(\alpha)\big)\big)\ldots\big(x - \varphi_j\big(\varphi_m(\alpha)\big)\big) = \big(x - \varphi_1(\alpha)\big)\ldots\big(x - \varphi_m(\alpha)\big) = h(x)\,,$$

hiszen a tényezők csak permutálódnak. Ezért $\varphi_j(h) = h$, ami azt jelenti, hogy h együtthatói fixen maradnak φ_j-nél.

Az állítás bizonyításához tegyük föl, hogy $T = K$, és válasszuk az $\alpha \in L$ elemet úgy, hogy $K(\alpha) = L$ legyen (ilyen van, mert K tökéletes test). Az ehhez készített m-edfokú $h \in K[x]$ polinomnak α gyöke (itt m a H elemszáma). Ezért az α elem K fölötti minimálpolinomjának foka legföljebb m. Ennek a minimálpolinomnak a foka $|L : K|$, hiszen $L = K(\alpha)$. Ezért $|L : K| \leq m$. De $|L : K|$ a $G(L/K)$ Galois-csoport rendje (a 6.6.1. Állítás miatt), és így H nem lehet valódi részcsoport. □

Az előző bizonyításban szereplő h polinom felhasználható arra is, hogy a 6.5.7. Állításra egy új bizonyítást adjunk (6.6.17. Gyakorlat).

Most már ki tudjuk mondani fő eredményünket. A bonyolult fogalmazást elkerülendő, jelölést vezetünk be a H részcsoporthoz tartozó közbülső testre.

6.6.5. Definíció. Legyen L a K tökéletes test véges normális bővítése, és $G = G(L/K)$ a bővítés Galois-csoportja. Ha $K \leq T \leq L$ közbülső test, akkor legyen $T^\sharp = G(L/T)$ azoknak az automorfizmusoknak a részcsoportja G-ben, amelyek a T elemeit fixen hagyják. Megfordítva, ha $H \leq G$ részcsoport, akkor legyen $H^\flat$ az a közbülső test, amely a H-beli elemek közös fixpontjaiból áll.

6.6.6. Gyakorlat. Mutassuk meg, hogy az előző definícióban szereplő megfeleltetés *rendezésfordító*, vagyis $T_1 \leq T_2$ esetén $T_1^\sharp \supseteq T_2^\sharp$ és $H_1 \geq H_2$ esetén $H_1^\flat \subseteq H_2^\flat$.

6.6.7. Tétel [A Galois-elmélet főtétele]. *Legyen L a K tökéletes test véges normális bővítése, és $G = G(L/K)$ a bővítés Galois-csoportja. Ekkor a $T \mapsto T^\sharp$ és a $H \mapsto H^\flat$ kölcsönösen egyértelmű, rendezésfordító megfeleltetést létesít a $K \leq T \leq L$ közbülső testek és a G Galois-csoport H részcsoportjai között, melyek egymás inverzei. Ha a T közbülső test a H részcsoportnak felel meg, akkor*

(1) $|L : T| = |H|$ *és* $|T : K| = |G : H|$;

(2) *a $K \leq T$ bővítés akkor és csak akkor normális, ha H normálosztó G-ben, és ekkor Galois-csoportja izomorf a G/H faktorcsoporttal.*

Bizonyítás. A (2) kivételével csaknem az összes állítást bebizonyítottuk már. Ha T közbülső test, akkor a 6.6.3. Következmény azt mondja ki, hogy $T^{\sharp\flat} = T$.

Legyen $H \leq G$ és $M = H^{\flat}$. Alkalmazzuk a 6.6.4. Állítást az $M \leq L$ bővítésre. Persze H részcsoportja a $G(L/M)$ Galois-csoportnak, hiszen H elemei fixen hagyják M-et. Ugyanakkor a H-beli elemek közös fixpontjainak halmaza, amit a lemmában T-vel jelöltünk, az M definíciója szerint maga M. Ezért ebből az állításból azt kapjuk, hogy $H = G(L/M) = M^{\sharp} = H^{\flat\sharp}$. Ezzel beláttuk, hogy a $\sharp$ és $\flat$ leképezések egymás inverzei. Azt hogy a megfeleltetés rendezésfordító, tudjuk a 6.6.6. Gyakorlatból.

Tegyük most föl, hogy a T közbülső test és a H részcsoport egymásnak felel meg. Ekkor a $T \leq L$ bővítés Galois-csoportja H, és így H rendje egyenlő a bővítés fokával, vagyis $|L : T|$-vel (6.6.1. Állítás). Persze G rendje $|L : K|$, és így a szorzástétel, valamint Lagrange tétele miatt

$$|T : K| = \frac{|L : K|}{|L : T|} = \frac{|G|}{|H|} = |G : H| .$$

Ezért (1) is igaz. A (2) állítást erősebb formában igazoljuk a most következőkben. A bizonyításnak ez a része absztraktabb és nehezebb az eddigieknél, az Olvasó elsőre nyugodtan átugorhatja.

A csoportelméletben tanultunk konjugálásról, ez az $x \to gxg^{-1}$ leképezés volt. Hogyan kapcsolódik ez a most tanult konjugáltság fogalmához? Egy $K \leq L$ bővítés α és β elemei akkor konjugáltak, ha egy alkalmas szimmetria az egyiket a másikba viszi. Persze akkor a $K(\alpha)$ és $K(\beta)$ résztestek is egymásba mennek ennél a szimmetriánál (szokás őket konjugált résztesteknek nevezni). Megmutatjuk, hogy ez akkor történik, amikor az ezekhez tartozó részcsoportok konjugált részcsoportok a Galois-csoportban.

A konjugált elemeket persze felfoghatjuk úgy is, hogy a Galois-csoportnál egy orbitban vannak. Az α elem stabilizátora pedig nem más, mint a $K(\alpha)$-hoz tartozó részcsoport. Tehát nem véletlen a hasonlóság a 4.6.37. Gyakorlat és a következő állítás között.

6.6.8. Állítás. *Legyen L a K tökéletes test véges normális bővítése, T közbülső test, és H a hozzá tartozó részcsoport. Ekkor tetszőleges $\varphi \in G$ esetén a $\varphi(T)$ közbülső testhez a $\varphi H \varphi^{-1}$ részcsoport tartozik (vagyis H-nak a φ-vel vett konjugáltja).*

Bizonyítás. Tetszőleges $\psi \in G$ esetén $\psi \in \varphi(T)^{\sharp}$ akkor és csak akkor, ha minden $\alpha \in T$-re $\psi\big(\varphi(\alpha)\big) = \varphi(\alpha)$. De ez azzal ekvivalens, hogy $\varphi^{-1}\psi\varphi(\alpha) = \alpha$, vagyis hogy $\varphi^{-1}\psi\varphi \in H$. Átrendezve $\psi \in \varphi H \varphi^{-1}$. □

Speciálisan H akkor és csak akkor normálosztó, ha minden konjugáltja önmaga, vagyis ha $\varphi(T) = T$ minden $\varphi \in G$-re.

6.6.9. Állítás. *Legyen L a K tökéletes test véges normális bővítése. Ekkor egy T közbülső test akkor és csak akkor normális bővítése K-nak, ha zárt a konjugáltságra, vagyis minden $\varphi \in G(L/K)$-ra $\varphi(T) = T$.*

Bizonyítás. Tegyük föl, hogy $K \leq T$ normális bővítés. Ha $\alpha \in T$, akkor $\beta = \varphi(\alpha) \in L$ ennek egy konjugáltja. E két elem K fölötti s minimálpolinomja megegyezik a 6.5.7. Állítás miatt. Az $s \in K[x]$ irreducibilis polinom, amelynek $\alpha \in T$ gyöke. Ezért s-nek az összes gyöke T-ben van, speciálisan β is, hiszen $K \leq T$ normális. Beláttuk tehát, hogy $\varphi(T) \subseteq T$. Ugyanezt φ inverzére alkalmazva $\varphi^{-1}(T) \subseteq T$, azaz $T \subseteq \varphi(T)$.

Megfordítva, ha T zárt mindegyik φ-re, akkor legyen $\alpha \in T$ olyan, hogy $K(\alpha) = T$. Ekkor T-ben benne vannak α konjugáltjai is, és persze generálják is K fölött. Ezért T az α minimálpolinomjának felbontási teste K fölött, és így K-nak normális bővítése. □

A főtétel bizonyításából most már csak annak megmutatása van hátra, hogy ha $K \leq T$ normális bővítés (és így a megfelelő H részcsoport normálosztó a $G = G(L/K)$-ban), akkor $G(T/K) \cong G/H$. Szorítsuk meg G minden φ elemét T-re, azaz ha $\varphi \in G$, akkor legyen $\tau(\varphi)$ az a függvény, amely T-n van értelmezve, de minden helyen ugyanazt az értéket veszi föl, mint φ. Mivel beláttuk, hogy $\varphi(T) = T$, ez a megszorítás a $G(T/K)$ csoportnak egy eleme lesz. Más szóval

$$\tau : G \to G(T/K)$$

egy leképezés. Ez nyilván tartja a kompozíciót, vagyis csoport-homomorfizmus. Ezért a homomorfizmus-tétel miatt

$$\mathrm{Im}(\tau) \cong G/\mathrm{Ker}(\tau)\,.$$

A τ magja azokból a $\varphi \in G$ automorfizmusokból áll, amelyek megszorítása T-re az identitás (vagyis $G(T/K)$ egységeleme). Ezek tehát pont a $H = G(L/T)$ elemei. Megmutatjuk, hogy τ képe az egész $G(T/K)$ (és így $G(T/K) \cong G/H$ adódik, azaz készen leszünk a bizonyítással).

Azt kell belátni, hogy minden $\psi \in G(T/K)$ automorfizmus egy alkalmas $\varphi \in G$ megszorítása T-re. Ez a felbontási test egyértelműségéből, azaz a 6.4.10. Következményből adódik, hiszen a $T \leq L$ bővítés normális és egyszerű, ezért egy alkalmas polinom felbontási teste (6.3.7. Gyakorlat). Ezzel a Galois-elmélet főtételét bebizonyítottuk. □

Az elmélet első alkalmazásaként belátjuk az algebra alaptételét (2.5.4. Tétel). Előrebocsátjuk, hogy a komplex számok testében minden másodfokú polinomnak van gyöke, és így nem lehet irreducibilis. Ezt kiszámoltuk az 1.3.13. Feladatban, de adódik a másodfokú egyenlet megoldóképletéből is, hiszen $\mathbb{C}$-ben a gyökvonás elvégezhető (lásd 5.7.12. Gyakorlat).

6.6.10. Tétel. *A komplex számok teste algebrailag zárt.*

Bizonyítás. Legyen $f \in \mathbb{C}[x]$ irreducibilis polinom, meg kell mutatnunk, hogy elsőfokú. Bővítsük $\mathbb{C}$-t ennek egy gyökével (6.4.3. Tétel). Ekkor egy véges $\mathbb{C} \leq K$ bővítést kapunk, amelynek foka $\mathrm{gr}(f)$. Ezért elegendő megmutatni, hogy minden $\mathbb{C} \leq K$ véges bővítés elsőfokú.

Tekintsük az $\mathbb{R} \leq \mathbb{C} \leq K$ bővítést, ez is véges a szorzástétel miatt. Ezért a 6.4.15. Gyakorlat miatt van olyan $K \leq L$ bővítés, hogy $\mathbb{R} \leq L$ már normális, de még mindig véges.

Legyen a Galois-csoportja G, és H ennek a 2-Sylow részcsoportja. A H-hoz tartozó közbülső T testnek a foka $\mathbb{R}$ fölött $|G : H|$, ezért páratlan.

Ha $\alpha \in T$, ekkor ez is páratlan fokú $\mathbb{R}$ fölött, és így az s minimálpolinomja is páratlan fokú, és irreducibilis $\mathbb{R}$ fölött. Az elemi analízissel bizonyított A.3.4. Tétel miatt s-nek azonban van valós gyöke, és így csak akkor lehet irreducibilis, ha elsőfokú. Ezért $\alpha \in \mathbb{R}$. Ezzel beláttuk, hogy $T = \mathbb{R}$, vagyis $H = G$, más szóval, hogy az $\mathbb{R} \leq L$ bővítés Galois-csoportja 2-csoport.

Az $\mathbb{R} \leq \mathbb{C} \leq L$ közbülső testnek a G Galois-csoportban egy 2 indexű N részcsoport felel meg. Ha N nem egyelemű, akkor a 4.10.8. Tétel miatt van benne egy kettő indexű M részcsoport. Az ehhez tartozó S közbülső test tehát $\mathbb{C}$-nek másodfokú bővítése. Ilyen azonban nincs, mert akkor tetszőleges $\beta \in S - \mathbb{C}$ minimálpolinomja másodfokú és irreducibilis lenne $\mathbb{C}$ fölött. Ez az ellentmondás bizonyítja, hogy N elemszáma 1, vagyis G elemszáma 2, és ezért $L = \mathbb{C}$. De akkor $\mathbb{C} \leq K \leq L$ is $\mathbb{C}$-vel egyenlő, és ezzel az állítást igazoltuk. □

Gyakorlatok, feladatok

6.6.11. Gyakorlat. Adjuk meg az $x^3 - 2$ polinom $\mathbb{Q}$ fölötti felbontási testének összes részтestét.

6.6.12. Gyakorlat. Adjuk meg a 6.3.13. Gyakorlatban szereplő bővítések Galois-csoportját és a közbülső testeket.

6.6.13. Gyakorlat. Mutassuk meg, hogy $x^4 - 5$ és $x^4 + 5$ felbontási teste különböző (vö. 6.5.12. Gyakorlat). Számítsuk ki az $x^4 + 5$ polinom felbontási testének Galois-csoportját, és közbülső testeit.

6.6.14. Gyakorlat. Mutassuk meg, hogy ha $K \leq L \leq \mathbb{C}$, és $K \leq L$ negyedfokú bővítés, akkor kettő, három, vagy öt közbülső teste lehet.

6.6.15. Feladat. Bizonyítsuk be, hogy az $x^5 - 4x + 2$ polinom $\mathbb{Q}$ fölötti felbontási testének Galois-csoportja az ötödfokú szimmetrikus csoport.

6.6.16. Gyakorlat. Igazoljuk, hogy ha K tökéletes test, akkor a $K \leq L$ véges bővítés közbülső testeinek száma akkor is véges, ha ez a bővítés nem normális.

6.6.17. Gyakorlat. Legyen L a K tökéletes test véges normális bővítése. Mutassuk meg, hogy ha $\alpha \in K$, akkor

$$\prod_{\varphi \in G(L/K)} \big(x - \varphi(\alpha)\big) = s(x)^m \,,$$

ahol s az α elem K fölötti minimálpolinomja, és $m = |K : L|/\mathrm{gr}_k(\alpha)$. Vezessük le ebből, hogy a konjugáltak pontosan a minimálpolinom gyökei.

6.6.18. Gyakorlat. Legyen L az $f \in K[x]$ polinom felbontási teste a K tökéletes test fölött. Mutassuk meg, hogy a $G(L/K)$ Galois-csoport az f gyökein ható szimmetrikus csoport egy részcsoportjával izomorf, és f akkor és csak akkor irreducibilis K fölött, akkor ez a részcsoport tranzitív.

6.6.19. Gyakorlat. Legyen α transzcendens elem $\mathbb{Z}_p$ fölött. Határozzuk meg az $x^p - \alpha$ polinom felbontási testének Galois-csoportját $\mathbb{Z}_p(\alpha)$ fölött (vö. 6.4.23. Feladat).

6.6.20. Feladat. Tegyük föl, hogy α és β komplex számok, melyek $\mathbb{Q}$ fölötti foka relatív prím. Bizonyítsuk be, hogy $\alpha + \beta$ foka α és β fokainak szorzata.

6.7. Véges testek

Ebben a szakaszban leírjuk a véges testeket izomorfia erejéig: minden q prímhatványra izomorfia erejéig pontosan egy q elemű test van, és más véges test nincs. Belátjuk, hogy egy véges test véges bővítése mindig normális, és a Galois-csoport ciklikus. Végül igazoljuk Wedderburn tételét, mely szerint minden véges ferdetest kommutatív.

Kiindulópontunk egy lineáris algebrai észrevétel, amely a véges vektorterek elemszámát állapítja meg.

6.7.1. Állítás. *Egy K véges test fölötti n-dimenziós vektortérnek $|K|^n$ eleme van, ahol $|K|$ a K elemszáma.*

Bizonyítás. A V elemei egyértelműen

$$k_1 b_1 + \ldots + k_n b_n$$

alakban írhatók, ahol $b_1, \ldots, b_n$ bázis. Mindegyik $k_i \in K$ elem egymástól függetlenül $|K|$-féleképpen választható. □

6.7.2. Következmény. *Minden véges test elemszáma prímhatvány.*

Bizonyítás. Legyen K véges test. A K karakterisztikája csakis egy p prímszám lehet (hiszen nincs végtelen rendű eleme az összeadásra). Ezért a K test P prímteste $\mathbb{Z}_p$-vel izomorf (5.7.7. Tétel). Ennek K véges, mondjuk n-edfokú bővítése. Ekkor K egy n-dimenziós vektortér P fölött, és így elemszáma p^n. □

6.7.3. Gyakorlat. Igazoljuk, hogy ha K egy p^n elemű test, akkor additív csoportja izomorf a $(\mathbb{Z}_p^+)^n$ direkt hatvánnyal.

A csoportelméleti részben már beláttuk, hogy *minden véges test multiplikatív csoportja ciklikus* (4.3.16. Tétel). Ebből azonnal adódik, hogy

6.7.4. Állítás. *Véges test minden véges bővítése egyszerű.*

Bizonyítás. Tegyük föl, hogy $K \leq L$ véges bővítés, ahol K véges. Persze ekkor L is véges (elemszáma $|K|^{|L:K|}$). Legyen $\alpha \in L$ egy olyan elem, amely generálja L multiplikatív csoportját. Ekkor $L = K(\alpha)$, hiszen L minden nem nulla eleme α-nak hatványa. □

6.7.5. Gyakorlat. Igazoljuk, hogy az 5.2.10. Gyakorlatban talált négyelemű test mindegyik eleme gyöke az $x^4 - x$ polinomnak.

6.7.6. Tétel. *Minden p^n prímhatványra létezik $q = p^n$ elemű test, mégpedig izomorfia erejéig egyféle. Ez a test az $x^q - x$ polinom felbontási teste $\mathbb{Z}_p$ fölött.*

Bizonyítás. Legyen p prím és $q = p^n$. Ha K egy q elemű test, akkor multiplikatív csoportja $q - 1$ elemű. Lagrange tételének egy következménye, hogy e csoport minden elemének $q - 1$-edik hatványa az egységelem (4.4.16. Következmény). Vagyis a K nem nulla elemei gyökei az $x^{q-1} - 1$ polinomnak, és így az $x^q - x$-nek már K minden eleme gyöke lesz, a nulla is. Ennek a polinomnak az együtthatói 0, 1, -1, amik benne vannak a K test P prímtestében. Ezért K az $x^q - x \in P[x]$ polinom felbontási teste $P \cong \mathbb{Z}_p$ fölött (hiszen e polinom gyökei nemcsak generálják, hanem egyenesen felsorolják K összes elemét). Ez minden p^n elemű testre igaz, és így a felbontási test egyértelműsége (6.4.9. Következmény) miatt bármely két p^n elemű test izomorf.

Az előző bekezdésben elmondottak elárulják azt is, hogy hogyan érdemes elindulni, ha $q = p^n$ elemű testet akarunk készíteni. A 6.4.5. Következményben beláttuk, hogy minden polinomnak minden test fölött van felbontási teste. Legyen speciálisan K felbontási teste az $x^q - x \in \mathbb{Z}_p[x]$ polinomnak $\mathbb{Z}_p$ fölött. Megmutatjuk, hogy K elemszáma p^n.

Az $x^q - x$ összes gyöke K-ban van (azaz lineáris tényezők szorzatára bomlik), és a gyökök K-t generálják. Belátjuk, hogy ezek a gyökök résztestet alkotnak (és így K az $x^q - x$ gyökeinek a halmaza). Ez közvetlen számolással adódik abból, hogy K-ban érvényes az $(x + y)^q = x^q + y^q$ azonosság (az 5.7.4. Tétel miatt, hiszen q hatványa K karakterisztikájának), és a nyilvánvaló $(xy)^q = x^q y^q$ azonosság is.

Egyszerűbb azonban a 6.4.26. Gyakorlatra hivatkozni, mely szerint a $\varphi(x) = x^p$ leképezés K-nak automorfizmusa. Ezért a φ-t n-szer alkalmazva a kapott $\varphi^n(x) = x^{p^n}$ leképezés is az. De az $x^q - x$ gyökei ennek a fixpontjai, és így résztestet alkotnak.

Tehát $x^q - x$ lineáris tényezőkre bomlik K-ban, és K e gyökök halmaza. Ahhoz, hogy K elemszáma q, már csak azt kell belátni, hogy ezek a gyökök mind különbözők, vagyis hogy az $x^q - x$ polinomnak nincs többszörös gyöke K-ban. Ha lenne, akkor ez gyöke lenne a deriváltjának is (a 3.6.5. Következmény miatt). De a derivált

$$qx^{q-1} - 1 = p^n x^{q-1} - 1 = -1\,,$$

hiszen $K[x]$ karakterisztikája is p, vagyis minden elemének p-szerese nulla. A -1 polinomnak nincs gyöke, és így $x^q - x$-nek tényleg nincs többszörös gyöke K-ban. Ezzel az állítást beláttuk. □

6.7.7. Gyakorlat. Hol a hiba a következő kijelentésben? „A $\mathbb{Z}_2$ fölött az $x^3 - x$ polinom gyökei (e polinom felbontási testében) résztestet alkotnak, ezért ez egy háromelemű test”.

6.7.8. Definíció. A $q = p^n$ elemű testet GF(q)-val jelöljük.

A GF a *Galois Field* elnevezésre utal. Ehelyett gyakori az $\mathbb{F}_q$ jelölés is. Mi az előbbit használjuk, egyrészt a Galois iránt érzett tiszteletből, másrészt azért, mert a GF(2^m) képletben az m kitevő jobban olvasható, mint $\mathbb{F}_{2^m}$ esetében.

Ha ténylegesen számolni akarunk a GF(p^n) testben, akkor a most leírt megadási mód nem praktikus, mert a felbontási test konstrukciójakor sok egyszerű bővítést végzünk egymás után. Jobb, ha csak egyetlen egyszerű bővítést hajtunk végre. Ez azt jelenti, hogy keresni kell egy n-edfokú irreducibilis f polinomot $\mathbb{Z}_p$ fölött, és ekkor GF(p^n) $\cong \mathbb{Z}_p[x]/(f)$ (6.4.1. Tétel). Ilyen irreducibilis f biztosan létezik, hiszen $\mathbb{Z}_p \leq$ GF(p^n) egyszerű bővítés, és bármely generátorelemének a minimálpolinomja n-edfokú lesz. Persze minden ilyen elem gyöke az $x^{p^n} - x$ polinomnak is, tehát f-et ennek osztói között kell keresnünk.

Példaként nézzük azt az esetet, amikor $p = 2$ és $n = 3$. Ekkor $\mathbb{Z}_2$ fölött

$$x^8 - x = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)\,,$$

ahol a tényezők a 3.3.17. Gyakorlat miatt már irreducibilisek $\mathbb{Z}_2$ fölött. A két harmadfokú irreducibilis polinom bármelyikével dolgozhatunk, a kapott faktorgyűrű nyolcelemű test lesz. Ennek elemei az $x^8 - x$ polinom összes gyökei. Az x és az $x - 1$ gyökei a 0 és az 1, vagyis a prímtest elemei. A fennmaradó hat elem közül három az $x^3 + x + 1$-nek, a másik három az $x^3 + x^2 + 1$-nek lesz gyöke. Látható, hogy hat darab harmadfokú elem van, amelyek közül hárman-hárman konjugáltak. Ez összecseng azzal, hogy a $\mathbb{Z}_2 \leq$ GF(8) bővítés harmadfokú, és ezért minden $\mathbb{Z}_2$-n kívüli elemének a foka is három.

Ha ezekre az elemekre konkrétan is kíváncsiak vagyunk, akkor ezt a testet úgy érdemes felfognunk, mint a

$$K = \mathbb{Z}_2[x]/(x^3 + x + 1)$$

faktorgyűrűt. Az 5.2. Szakaszban leírtuk azt a módszert, amelynek segítségével az ilyen faktorgyűrűkben reprezentánsok segítségével számolhatunk. Ahelyett azonban, hogy mellékosztályokkal és reprezentánsokkal számolnánk, egyszerűbb ezt a K testet (a 6.4.3. Tétel alapján) úgy tekinteni, hogy $K = \mathbb{Z}_2(\alpha)$, ahol az α elem minimálpolinomja x^3+x+1. Ezért K elemeit nem az $a + bx + cx^2$ alakú polinomok mellékosztályainak, hanem $a + b\alpha + c\alpha^2$ alakú kifejezéseknek tekintjük, ahol $\alpha^3 + \alpha + 1 = 0$ és $a, b, c \in \mathbb{Z}_2$ (természetesen α-t az $x + (x^3 + x + 1)$ mellékosztályként kaptuk). Az $a + b\alpha + c\alpha^2$ kifejezésben az a, b, c együtthatók egyértelműen meghatározottak, ez egy harmadfokú egyszerű bővítés. Az α elem minimálpolinomja tehát $x^3 + x + 1$ a $P = \{0, 1\}$ prímtest fölött.

Határozzuk meg a K többi elemének a minimálpolinomját is P fölött. Nézzük meg, hogy az $1+\alpha$ elemnek is x^3+x+1-e a minimálpolinomja. Az $\alpha^3+\alpha+1 = 0$ egyenletből $\alpha^3 = \alpha + 1$ hiszen kettő karakterisztikában $-y = y$. Ezért

$$(1+\alpha)^3 + (1+\alpha) + 1 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 + 1 + \alpha + 1 = \alpha^2 + \alpha\,,$$

ami nem a nullelem. Ezért az $1+\alpha$ minimálpolinomja csakis x^3+x^2+1 lehet. Hasonlóan a többi elemet is elintézhetnénk. A következő bizonyítás után megmutatjuk, hogyan lehet mindezt gyorsabban és elegánsabban kiszámítani.

6.7.9. Tétel. *Legyen $K \leq L$ testbővítés, ahol L véges. Ekkor ez a bővítés normális, és a Galois-csoportja az $n = |L : K|$ rendű ciklikus csoport. A közbülső testek az n osztóinak felelnek meg kölcsönösen egyértelműen.*

Speciálisan a $\mathrm{GF}(p^d)$ *akkor és csak akkor részteste* $\mathrm{GF}(p^n)$*-nek, ha* $d \mid n$*, és ilyenkor ez a résztest azokból az* $\alpha \in \mathrm{GF}(p^n)$ *elemekből áll, melyekre* $\alpha^{p^d} = \alpha$*.*

Bizonyítás. Legyen p a K karakterisztikája, P a prímteste. Láttuk, hogy L az $x^{|L|} - x$ polinom felbontási teste P fölött. Persze akkor ugyanennek a polinomnak a felbontási teste K fölött is, és ezért a $K \leq L$ bővítés felbontási test, vagyis normális. A véges testek tökéletesek (6.4.26. Gyakorlat), ezért a Galois-elmélet főtétele alkalmazható erre a bővítésre.

Ugyanebből a gyakorlatból tudjuk, hogy a $\varphi(x) = x^p$ Frobenius-endomorfizmus automorfizmusa L-nek. Legyen $|K| = p^m$, ekkor $|L| = (p^m)^n = p^{mn}$. Megmutatjuk, hogy a $\psi = \varphi^m$ elem generálja a $K \leq L$ bővítés Galois-csoportját. A ψ eleme ennek a csoportnak, vagyis fixálja K elemeit, hiszen ha $k \in K$, akkor $|K| = p^m$ miatt k gyöke az $x^{p^m} - x$ polinomnak, és így $\varphi^m(k) = k^{p^m} = k$.

Azt kell még megmutatni, hogy ψ rendje n (hiszen a főtétel miatt a Galois-csoport n elemű). Persze n rendű csoportban ψ^n az egységelem, vagyis csak azt kell belátni, hogy $i < n$ esetén ψ^i nem az identitás L-en. Legyen β az L multiplikatív csoportjának a generátoreleme. A β rendje tehát $|L| - 1 = p^{mn} - 1$. Ekkor

$$\psi^i(\beta) = \varphi^{mi}(\beta) = \beta^{p^{mi}}.$$

Ez nem lehet β, mert ha az lenne, akkor β-nak a $p^{mi} - 1$-edik hatványa 1 lenne, de $p^{mi} - 1$ kisebb a β rendjénél, ami $p^{mn} - 1$.

Ezzel beláttuk, hogy a Galois-csoport ciklikus. A főtétel miatt így a közbülső testek a $\mathbb{Z}_n^+$ ciklikus csoport részcsoportjainak felelnek meg, vagyis n minden osztójához egyetlen ilyen részcsoport van (4.3.21. Állítás). Ebből következik, hogy a $K \leq T \leq L$ közbülső testek pontosan a $\mathrm{GF}(p^{md})$ testek, ahol $d \mid n$. Valóban, minden $d \mid n$ esetén egyetlenegy n/d rendű H részcsoport van $G(L/K)$-ban, amelyhez tartozó T közbülső testre a főtétel szerint $|T : K| = d$, vagyis T elemszáma p^{md}, és mivel több részcsoport nincs, más közbülső test sincs. Ezt a H részcsoportot ψ^d generálja, és ezért T azokból az $\alpha \in L$ elemekből áll, amelyekre $\alpha = \psi^d(\alpha) = \alpha^{p^{md}}$.

A $\mathrm{GF}(p^n)$ résztestei mind tartalmazzák a P prímtestet, ezért a $P \leq \mathrm{GF}(p^n)$ közbülső testei. Így az előző bekezdésben bizonyított állítás $m = 1$ esetéből megkapjuk $\mathrm{GF}(p^n)$ összes résztesteit. □

Térjünk vissza a nyolcelemű test félbehagyott példájára. Most már tudjuk, hogy a $P \leq K$ bővítés relatív automorfizmusai a $\varphi(x) = x^2$ leképezés hatványai. Mivel α minimálpolinomja $x^3 + x + 1$, a konjugáltjainak, vagyis a $\varphi(\alpha) = \alpha^2$, és a $\varphi^2(\alpha) = \alpha^4$ elemeknek is ugyanez a minimálpolinomja. Az α^4-t még át kell alakítani $a + b\alpha + x\alpha^2$ alakba

(igazából x^4-t kellene maradékosan osztani x^3+x+1-gyel). Tudjuk, hogy $\alpha^3 = \alpha+1 = 0$, ezért

$$\alpha^4 = \alpha(\alpha+1) = \alpha^2+\alpha\,.$$

Így az α harmadik konjugáltja $\alpha^2+\alpha$. Az $\alpha+1$ konjugáltjai $(\alpha+1)^2 = \alpha^2+1$ (hiszen tagonként lehet négyzetre emelni, φ automorfizmus), és $(\alpha+1)^4 = \alpha^4+1 = \alpha^2+\alpha+1$, ezek minimálpolinomja x^3+x^2+1.

Az eddigi példák azt sugallhatják, hogy egy K véges test fölött az azonos fokú (mondjuk n-edfokú) irreducibilis polinomok „egyenlőnek születtek", hiszen mindegyik felbontási teste ugyanaz a $|K|^n$ elemű test lesz. Ez mégsincs egészen így, a következő definíció szerint.

6.7.10. Definíció. Legyen K véges test. Egy $f \in K[x]$ irreducibilis polinomot *primitív polinomnak* nevezünk, ha a K fölötti L felbontási testének mindegyik gyöke generálja az L multiplikatív csoportját.

Vigyázzunk, ne keverjük össze a $\mathbb{Z}[x]$-beli primitív polinom fogalmát (3.4.1. Definíció) a most definiált fogalommal. (Egy egész együtthatós polinom akkor primitív, ha együtthatóinak legnagyobb közös osztója 1. Ennek a fogalomnak véges test fölött nem lenne haszna, hiszen itt minden nem nulla elem egység.) A primitív szó itt a számelméleti „primitív gyök" fogalmára utal. Ehhez kapcsolódva néha egy általános ciklikus csoport generátorelemét (és így egy test multiplikatív csoportjának generátorelemét) is primitív elemnek nevezik.

Primitív polinomokkal a 6.7.14. és a 6.7.23. Gyakorlatban foglalkozunk, de a kódelméletről szóló 9. Fejezetben is szükség lesz rájuk.

6.7.11. Tétel [Wedderburn tétele]. *Minden véges ferdetest kommutatív.*

Bizonyítás. A tétel bizonyításához az eddig tanultakon kívül föl kell még használnunk elemi lineáris algebrai ismereteket ferdetest fölötti „vektorterekről". A lényeg az, hogy ezek a testek fölötti vektorterekhez teljesen hasonlóan viselkednek a bázis és a dimenzió szemszögéből. Ez könnyen ellenőrizhető állítás, de be is fogjuk bizonyítani a modulusokról szóló fejezetben. A 7.2.20. Feladat és a 7.2.15. Tétel nyilvánvaló következménye, hogy egy véges K ferdetest fölötti véges V „vektortér" elemszáma az K elemszámának hatványa (ahogy ezt kommutatív F esetében a 6.7.1. Állításban beláttuk). Speciálisan ha $K \leq L$, ahol K és L ferdetestek, akkor L tekinthető „vektortérnek" K fölött (pontosan ugyanúgy, ahogy a kommutatív esetben), és így igaz a következő.

6.7.12. Állítás. *Ha a K ferdetest rész-ferdeteste a véges L ferdetestnek, akkor $|L| = |K|^n$ alkalmas n egészre.*

Egy másik fogalom, amit a csoportelméletből kölcsönzünk, a centrum és a centralizátor fogalma. Ezek most szintén ferdetestek lesznek.

6.7.13. Állítás. *Legyen K ferdetest és $k \in K$. Ekkor a k-val (szorzásra) felcserélhető elemek egy $C(k)$ rész-ferdetestet alkotnak K-ban, amelyet k centralizátorának nevezünk. Az összes elemek centralizátorainak metszete, vagyis a K ferdetest $Z(K)$ centruma (amely*

az összes K-beli elemekkel felcserélhető elemekből áll), szintén rész-ferdeteste K-nak. Ezek mind tartalmazzák az egységelemet.

A triviális bizonyítást az Olvasóra hagyjuk. Legyen K ferdetest, és $G = K - \{0\}$ a K multiplikatív csoportja. Ekkor a $g \in G$ centralizátora a G csoportban pontosan $C(g) - \{0\}$, a G centruma pedig $Z(K) - \{0\}$. Ezért ha felírjuk a G csoport osztályegyenletét:

$$|G| = |Z(G)| + |K_1| + \ldots + |K_m|\,,$$

ahol K_i a nem egyelemű konjugált osztályok, akkor $|G| = |K| - 1$ és $|Z(G)| = |Z(K)| - 1$. Válasszunk $k_i \in K_i$ elemeket minden i-re, ekkor a K_i elemszáma a k_i centralizátorának az indexe (4.7.10. Következmény). Ezt beírva a fenti egyenlet a következőképpen alakul.

$$|K| - 1 = \big(|Z(K)| - 1\big) + \frac{|K| - 1}{|C(k_1)| - 1} + \ldots + \frac{|K| - 1}{|C(k_m)| - 1}\,.$$

Most ezt az egyenletet átírjuk úgy, hogy a szereplők elemszámát kiszámítjuk. Legyen K karakterisztikája a p prímszám. A $Z(K)$ véges kommutatív test, és így elemszáma p-nek egy q hatványa. A K elemszáma ekkor q^n alakban írható, hiszen K nyilván vektortér $Z(K)$ fölött a szokásos műveletekre (de hivatkozhatunk a 6.7.12. Állításra is, vagyis $Z(K)$ kommutativitása sem fontos). Ugyanígy $C(k_i)$ elemszáma q^{n_i} alkalmas n_i-re, mert $Z(K)$ ezeknek részteste. Végül $C(k_i)$ részteste K-nak. Ezért a 6.7.12. Állítás miatt K elemszáma, vagyis q^n, hatványa $C(k_i)$ elemszámának, vagyis q^{n_i}-nek. Ez azt jelenti, hogy $n_i \mid n$ minden i-re, és persze valódi osztó, mert K_i nem egyelemű konjugált osztály. Az egyenletünk most így fest:

$$q^n - 1 = (q - 1) + \frac{q^n - 1}{q^{n_1} - 1} + \ldots + \frac{q^n - 1}{q^{n_m} - 1}\,.$$

Ebben már benne lapul az ellentmondás, csak még nem látszik. Hogy előjöjjön, vegyük elő a $\Phi_n(x)$ körosztási polinomot. Tudjuk, hogy

$$\prod_{d \mid n} \Phi_d(x) = x^n - 1$$

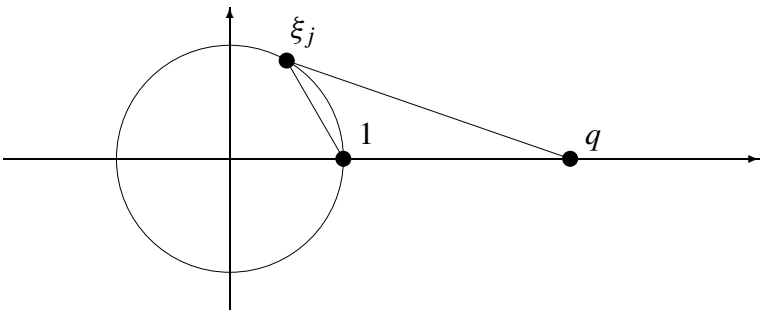
(3.9.5. Lemma). Ezt a képletet alkalmazzuk n-re és n_i-re is. Azt kapjuk, hogy $\Phi_n(x)$ osztója mindegyik

$$\frac{x^n - 1}{x^{n_i} - 1}$$

polinomnak, hiszen a számlálóban szerepel, a nevezőben nem (és $n_i \mid n$ miatt a nevezőből minden tényező kiegyszerűsödik). Természetesen $\Phi_n(x)$ osztója $x^n - 1$-nek is. Az x helyébe q-t helyettesítve a fenti egyenlet mindegyik tagjáról látjuk, hogy $\Phi_n(q)$-val osztható, kivéve a $q - 1$-et. Ezért az egyenlet miatt $q - 1$ is osztható vele, vagyis beláttuk, hogy

$$\Phi_n(q) \mid q - 1\,.$$

A q szám prímhatvány, ezért $q \geq 2$. Megmutatjuk, hogy ez az oszthatóság csak $n = 1$ esetén lehetséges. Ezzel készen is leszünk, mert ebben az esetben $|K| = q^n = q = |Z(K)|$, vagyis $K = Z(K)$ és ezért K kommutatív.



6.2. Ábra. A Wedderburn-tétel bizonyításának a vége.

A körosztási polinom definíciója miatt

$$\Phi_n(q) = (q - \xi_1) \dots (q - \xi_{\varphi(n)}) ,$$

ahol $\xi_1, \dots, \xi_{\varphi(n)}$ az összes primitív n-edik egységgyök. Ha $n > 1$, akkor az 1 nem szerepel a ξ_j számok között, ezért valamennyi ξ_j szám valós része 1-nél kisebb (ezek az egységkörön helyezkednek el). Így a ξ_j, az 1 és a q pontok alkotta háromszögben az 1 pontnál tompaszög van. Ezért ennek a háromszögnek a leghosszabb oldala az 1-gyel szemközti, vagyis

$$|q - \xi_j| > |q - 1| = q - 1 \geq 1 .$$

Az egyenlőtlenségeket összeszorozva $|\Phi_n(q)| > q - 1$ adódik, ami ellentmond annak, hogy $\Phi_n(q) \mid q - 1$. Ez az ellentmondás bizonyítja Wedderburn tételét. □

Véleményünk szerint ez a könyvben szereplő legszebb bizonyítás, hiszen a körosztási polinomok összefognak a geometriával, a csoportelmélettel és a lineáris algebrával is, hogy egy gyűrűelméleti állítást megmutathassanak, igazi, interdiszciplináris módon.

Gyakorlatok, feladatok

6.7.14. Gyakorlat. A 3.3.17. Gyakorlatban leírtuk a kételemű test fölötti negyedfokú irreducibilis polinomokat, $m(x) = x^4 + x^3 + 1$ ezek egyike. Legyen $\alpha = x + (m)$ eleme az $L = \mathbb{Z}_2[x]/(m)$ testnek.

(1) Írjuk fel α összes hatványát $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ alakban, ahol $a_i \in \mathbb{Z}_2$. A kapott táblázat alapján mutassuk meg, hogy az α generálja az L multiplikatív csoportját.
(2) Adjuk meg L összes elemének minimálpolinomját a prímtest fölött. Melyek lesznek ezek közül primitívek?

6.7.15. Gyakorlat. Mutassuk meg, hogy minden véges test fölött minden $n > 0$ egészre létezik n-edfokú irreducibilis polinom.

6.7.16. Gyakorlat. Mutassuk meg, hogy ha p prím, akkor $x^{p^n} - x$ az összes olyan $\mathbb{Z}_p$ fölött irreducibilis polinom szorzata, melyek foka n-nek osztója.

6.7.17. Gyakorlat. Hány négyzet- illetve köbelem van a 27-elemű testben? Hány gyöke van a ebben a testben az $x^4+x^3+x^2+x+1$, illetve az x^2-x+1 polinomnak?

6.7.18. Gyakorlat. Határozzuk meg a 17 elemű test fölött az x^2+1 és az x^2-3 polinomok felbontási testét.

6.7.19. Feladat. Határozzuk meg x^2+x+1 felbontási testét GF(121) és GF(125) fölött.

6.7.20. Feladat. Határozzuk meg az $x^{11}-1$ polinom felbontási testét $\mathbb{Z}_2$ fölött. Hogyan lehetne a kapott eredményt általánosítani?

6.7.21. Feladat. Hány nyolcad- illetve 12-edfokú irreducibilis polinom van $\mathbb{Z}_2$ fölött?

6.7.22. Feladat. Legyenek p és q prímek és n pozitív egész. Bizonyítsuk be, hogy $\mathbb{Z}_p$ fölött a q^n-edfokú irreducibilis polinomok száma $(p^{q^n}-p^{q^{n-1}})/q^n$.

6.7.23. Gyakorlat. Mutassuk meg, hogy ha K véges test, és L az $f\in K[x]$ polinom felbontási teste, akkor f gyökeinek ugyanaz a rendje L multiplikatív csoportjában. Speciálisan tehát f akkor és csak akkor primitív polinom, ha van olyan gyöke, ami L multiplikatív csoportját generálja.

6.7.24. Feladat. Legyen α a $K=\mathrm{GF}(p^n)$ multiplikatív csoportjának generátoreleme, ahol p prím. Igazoljuk, hogy a $\beta=\alpha^i$ elem $\mathbb{Z}_p$ fölötti minimálpolinomjának a foka éppen a p rendje modulo m, ahol $m=(p^n-1)/(p^n-1,i)$ a h elem multiplikatív rendje. Igazoljuk, hogy ez a fok pontosan akkor n, ha i nem osztható $(p^n-1)/(p^d-1)$-gyel semmilyen $d<n$ esetén. Következik-e ebből, hogy β rendje p^n-1?

6.7.25. Feladat. Mutassuk meg, hogy a 16 csúcsú teljes gráf élei kiszinezhetők három színnel úgy, hogy ne keletkezzen egyszínű háromszög, de a 17 csúcsú teljes gráf élei már nem.

6.8. Geometriai szerkeszthetőség

A geometriai szerkeszthetőség elméletéről csak nagyon vázlatosan lesz szó. Egy apparátust adunk az Olvasó kezébe amellyel (kellő geometriai tudás és ötletesség birtokában) a szerkesztési feladatokról eldöntheti, hogy megoldhatóak-e. Alkalmazásként néhány nevezetes és klasszikus problémát tárgyalunk (körnégyszögesítés, kockakettőzés, szögharmadolás, szabályos sokszögek szerkeszthetősége), a feladatokban pedig két háromszög-szerkesztési alkalmazás is szerepel. Nagyon melegen ajánljuk Czédli Gábor és Szendrei Ágnes [**7**] könyvét, amely a precíz felépítés mellett széles kitekintést ad a témáról, geometriai szemszögből is.

Hogyan lehet egy olyan állítást bizonyítani, hogy például nem szerkeszthető szabályos hétszög körzővel és vonalzóval? Az elvet a következő kérdés kapcsán érthetjük meg.

6.8.1. Kérdés. Adott egy négyzethálós papír, és egy vonalzó. Meg tudjuk-e szerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög harmadik csúcsát?

Ha a válasz igenlő lenne, akkor elég lenne megadni egy eljárást. Sajnos azonban a válasz nemleges, és ezért pontosan meg kell fogalmazni, mit értünk szerkesztésen. Ha csak vonalzónk van, akkor kétféle dolgot tehetünk: két, már meglévő ponton át egyenest húzhatunk, vagy pedig kijelölhetjük két, már meglévő egyenes metszéspontját. Ezeket a lépéseket ismételgethetjük.

Ha felveszünk egy koordinátarendszert úgy, hogy az origó és az $(1, 0)$ pont egy kis négyzet szomszédos csúcsaiba kerüljön, akkor a négyzetrácsban adott pontok éppen azok, amelyek koordinátái egészek. Ha két ilyen pontot összekötő egyenes egyenletét felírjuk, akkor a kapott együtthatókat a négy alapművelet segítségével számolhatjuk ki, és ezért racionális számokat kapunk. Két ilyen egyenes metszéspontjának ismét racionális számok lesznek a koordinátái.

A szerkesztési eljárás tehát csak racionális koordinátájú pontot adhat. A keresett pont koordinátái azonban $(1/2, \sqrt{3}/2)$, és így a 6.8.1. Kérdésre nemleges a válasz.

Ha megengedünk körzőt is, akkor a racionális számok mellett a négyzetgyökvonást tartalmazó kifejezések is szerkeszthetővé válnak. A nevezetes feladatok szerkeszthetetlensége azon fog múlni, hogy a szerkesztendő pontok koordinátái ilyen négyzetgyökös kifejezéssel sem írhatók föl.

Az egyszerűség kedvéért úgy képzeljük, hogy pontok vannak megadva, és a szerkesztendő objektumok is pontok. Ez nem jelent megszorítást, mert ha például egy szakasz van megadva, akkor azt a két végpontja meghatározza, ha pedig mondjuk egy kört kell szerkeszteni, akkor elegendő megszerkeszteni a középpontját és még egy pontját.

6.8.2. Definíció. Adottak a síkon pontok, legalább két darab. A következő lépéseket engedjük meg.

(1) Két adott vagy megszerkesztett ponton át egyenes húzása.
(2) Két megszerkesztett egyenes metszéspontjának meghatározása.
(3) Két adott vagy megszerkesztett pont körzőnyílásba vétele, és ezzel a sugárral egy adott vagy megszerkesztett pont körüli kör rajzolása.
(4) Megszerkesztett kör és egyenes metszéspontjainak kijelölése.
(5) Két megszerkesztett kör metszéspontjainak kijelölése.

Azt mondjuk, hogy egy P pont a kiindulási pontokból *euklideszi szerkesztéssel* megkapható, ha a fenti lépések alkalmas véges sorozatának az eredménye.

Nem szokás megengedni, hogy kör és egyenes metszéspontját akkor is kijelöljük, ha az érintési pont. (Ennek oka az, hogy a szerkesztés ettől pontatlanabbá válhat, hiszen minél „meredekebben” metszi egymást két görbe, annál könnyebb pontosan kijelölni a metszéspontot.) Meg lehet azonban mutatni elemi geometriai eszközökkel, hogy az érintési pont két egyenes metszéspontjaként is megkapható, és így akár megengedjük az érintési pont kijelölését, akár nem, ugyanazok az objektumok lesznek szerkeszthetők. Az ilyesfajta problémák diszkussziójával nem foglalkozunk.

Vegyünk föl egy koordinátarendszert *úgy, hogy az origó, vagyis a* $(0,0)$ *pont és az* $(1,0)$ *pont is adott (vagy megszerkeszthető) legyen.* Rendkívül fontos, hogy a koordinátarendszert csak így szabad fölvenni, lásd a 6.8.22. Gyakorlatot. A megadott pontok koordinátáival generáljunk egy testet $\mathbb{Q}$ fölött, így egy $\mathbb{Q} \leq K_0$ testbővítést kapunk. A K_0 neve *az alapadatok által generált test*.

Amikor a szerkesztési lépéseket végezzük, akkor írjuk föl minden újonnan kapott pontnak a koordinátáit, és minden új egyenesnek és körnek az egyenletét. A pontokat tehát (p,q) számpárok adják meg. A körök esetében egy

$$(x-p)^2+(y-q)^2=r^2$$

alakú egyenletet írhatunk föl, ahol (p,q) a kör középpontja, és r a sugara. Az egyenesekkel azonban kicsit vigyázni kell: az $y=ax+b$ típusú egyenlet ugyanis nem működik a függőleges, vagyis az $x=c$ egyenlettel megadható egyenesekre. Ezért az egyenesek egyenletét

$$ax+by+c=0$$

alakban írjuk (ahol a és b nem egyszerre nulla). Ez az alak nem egyértelmű, mert ha egy nem nulla konstanssal beszorzunk, akkor ugyanannak az egyenesnek az egyenletét kapjuk. Erre a későbbiekben figyelnünk kell. Az egységes fogalmazás kedvéért a fenti képletekben szereplő p, q, r, a, b, c számokat kissé pongyolán a megfelelő alakzatok (pontok, körök, egyenesek) koordinátáinak fogjuk nevezni.

6.8.3. Lemma. *Tegyük föl, hogy a szerkesztés egy pillanatában megadott vagy megszerkesztett pontok, körök, egyenesek koordinátái mind egy* $K \leq \mathbb{R}$ *testben vannak. Ha az euklideszi szerkesztés ötféle lépésének bármelyikét végrehajtjuk, akkor az újonnan kapott alakzat koordinátái mindig benne vannak a* K*-ban, vagy* K *egy olyan másodfokú bővítésében, amely része* $\mathbb{R}$*-nek. Az egyenesek esetében ezt úgy kell érteni, hogy az újonnan kapott egyenesnek* **van** *ilyen egyenlete.*

Bizonyítás. Az állítás bizonyítása az a számolás, amit középiskolában már megismertünk koordinátageometriából. Az (1) lépésben két ponton átmenő egyenes egyenletét kell fölírni, ez a négy alapművelettel lehetséges a két pont koordinátáiból, vagyis ilyenkor K-ban maradunk. A (2) esetben két egyenes metszéspontjának meghatározásához lineáris egyenletrendszert kell megoldani, a megoldások most is a négy alapművelettel kaphatók. Ennél a két lépésnél tehát K nem is bővül (összhangban azzal, amit a csak vonalzós szerkesztésekről írtunk a szakasz elején).

A (3) lépésnél az újonnan keletkező kör sugara két korábbi pont távolsága. Ezt a koordinátákból Pitagorasz tételével számíthatjuk ki. Ezért a kör sugara a $K(\sqrt{d})$ legföljebb másodfokú bővítésnek lesz az eleme, ahol $d \in K$.

A (4) lépésnél a kör és egyenes metszéspontjának kiszámítása másodfokú egyenletre vezet (az egyenes egyenletéből az egyik ismeretlent kifejezve). Ezért a metszéspontok koordinátái a megoldóképlet segítségével kaphatók, vagyis ismét egy $K(\sqrt{d})$ típusú test keletkezik.

Végül az (5) lépésben, két kör metszéspontjának kiszámításakor azt érdemes észrevenni, hogy a két köregyenlet kivonásakor kiesik az x^2 és az y^2, és ezért elsőfokú egyenlet, vagyis egy egyenes egyenlete keletkezik, amelynek koordinátái a négy alapművelettel kaphatók:

$$(x - p_1)^2 + (y - q_1)^2 = {r_1}^2$$
$$(x - p_2)^2 + (y - q_2)^2 = {r_2}^2$$

különbsége

$$2(p_2 - p_1)x + 2(q_2 - q_1)y + (p_1^2 - p_2^2 + q_1^2 - q_2^2 - r_1^2 + r_2^2) = 0\,.$$

A két kör metszéspontjai ugyanazok, mint ennek az egyenesnek és az egyik körnek a metszéspontjai. Ezért a metszéspontok koordinátái a már elintézett (4) típusú lépéssel is megkaphatók, vagyis szintén egy másodfokú bővítésben vannak. □

Az előző állításban másodfokú bővítésekről beszéltünk, de látszólag erősebbet bizonyítottunk, hiszen $K(\sqrt{d})$ típusú bővítéseket kaptunk. Ez mindegy, $\mathbb{C}$ résztestei esetében minden másodfokú bővítés egy négyzetgyökkel való bővítéssel kapható (a másodfokú egyenlet megoldóképlete miatt, lásd 6.3.14. Gyakorlat).

Az Olvasó joggal hiányolhatja a diszkussziót. Honnan tudjuk, hogy a két egyenes nem párhuzamos-e? Hogy a két kör metszi-e egymást? A válasz a következő. A fenti lemma arról szól, hogy *ha* valakinek sikerült megszerkesztenie egy pontot, *akkor* a kapott pont koordinátái milyen testben vannak benne. Ha az a két kör nem metszi egymást, akkor a szerkesztés nem is működik. Ha metszi egymást (ami a szerkesztő szemszögéből a legjobb eset), akkor is biztosak lehetünk abban, hogy az illető *csak* olyan pontokat kaphat, bármilyen ügyesen szerkeszt is, amelyek koordinátái az adott testbővítésben vannak. Ez a lemma tehát negatív eredmények bizonyítására való: ha a szerkesztendő pont koordinátái nincsenek benne ezekben a bővítésekben, akkor biztosan nem végezhető el a szerkesztés.

6.8.4. Állítás. *Legyen K_0 egy szerkesztési feladat alapadatai által generált test. Ha a (p, q) pont szerkeszthető, akkor van olyan n és egy*

$$K_0 < K_1 < \ldots < K_n \leq \mathbb{R}$$

testlánc, melyre $p, q \in K_n$, és mindegyik $K_i \leq K_{i+1}$ bővítés foka kettő. Így a $K_0 \leq K_n$ bővítés foka 2-hatvány, p és q algebrai K_0 fölött, és a fokuk szintén 2-hatvány.

Bizonyítás. Ez az előző lemmából nyilvánvaló. Minden egyes szerkesztési lépés során egy első vagy másodfokú bővítésben benne vannak az új objektum koordinátái, így kapjuk a K_i testeket. A szerkesztés végén kapott pont koordinátái az utolsó bővítésben vannak. A szorzástétel (6.2.3. Következmény) miatt $|K_n : K_0| = 2^n$. Mivel elem foka osztója a bővítés fokának, és véges bővítés minden eleme algebrai (6.2.4. Állítás), ezért p és q tényleg 2-hatvány fokú algebrai elemek K_0 fölött. □

Kényelmesebb lesz a következőkben a szerkeszthető pontok koordinátáit szerkeszthető számoknak nevezni. Nyilvánvaló, hogy a (p, q) pont akkor és csak akkor szerkeszthető,

ha $(p, 0)$ és $(q, 0)$ is szerkeszthető. Ha pedig egy r hosszú szakaszt sikerült szerkeszteni, akkor ezt fölmérhetjük az origóból kiindulva, és így $(r, 0)$ szerkeszthető pont.

6.8.5. Definíció. Az $r \in \mathbb{R}$ *szerkeszthető szám*, ha $(r, 0)$ szerkeszthető pont (adott pontokból kiindulva).

A szerkeszthető számok tehát algebraiak és 2-hatvány fokúak az alapadatok által generált test fölött. Ez már elegendő néhány híres negatív eredmény bizonyítására.

6.8.6. Probléma. A *kockakettőzés* problémája az, hogy szerkesszünk egy megadott élű kockához egy olyan másik kockát (illetve ennek az élét), amelynek a térfogata az első kocka térfogatának kétszerese.

Alapadatunk tehát az első kocka éle, egy szakasz (pontosabban ennek két végpontja). A koordinátarendszert máshogy nem is vehetjük föl, mint hogy az egyik végpont a $(0, 0)$, a másik az $(1, 0)$ legyen. Az alapadatok által generált test tehát a $\mathbb{Q}$. Az első kocka élhossza 1, térfogata 1 köbegység. A második kocka térfogata tehát 2, vagyis élhossza $\sqrt[3]{2}$. Így a feladat az, hogy $\sqrt[3]{2}$ hosszú szakaszt kell szerkeszteni. Az előző következmény szerint ha ez megtehető, akkor $\sqrt[3]{2}$ (algebrai és) 2-hatvány fokú $\mathbb{Q}$ fölött. Ez ellentmondás, hiszen $\sqrt[3]{2}$ foka 3 (ezt láttuk a 6.1. Szakaszban: gyöke a harmadfokú $x^3 - 2$ polinomnak, amely a Schönemann-Eisenstein kritérium miatt irreducibilis). Ez az ellentmondás bizonyítja, hogy a kockakettőzés nem végezhető el euklideszi szerkesztéssel.

6.8.7. Probléma. A *körnégyszögesítés* problémája az, hogy szerkesszünk egy megadott sugarú körrel egyenlő területű négyzetet (illetve ennek az oldalát).

Ami adott, az a kiinduló kör sugara, vagyis egy szakasz. Az előzőhöz hasonlóan felvéve a koordinátarendszert ismét $\mathbb{Q}$ lesz az alaptest. Így a kör sugara 1, területe π, és a szerkesztendő négyzet oldala $\sqrt{\pi}$. Ha ez szerkeszthető lenne, akkor az előző következmény szerint $\sqrt{\pi}$ algebrai $\mathbb{Q}$ fölött. Mivel az algebrai számok testet alkotnak (6.2.10. Következmény), π is algebrai lenne $\mathbb{Q}$ fölött.

Ez azonban nem igaz. Lindemann igen nevezetes és mély tétele, amit 1882-ben Hermite eredményeire támaszkodva bizonyított, hogy a π szám transzcendens. Emiatt a nehéz tétel miatt tudjuk tehát (a fentieket is figyelembe véve), hogy a körnégyszögesítés nem végezhető el körzővel és vonalzóval.

6.8.8. Probléma. A *szögharmadolás* problémája az, hogy szerkesszük meg egy megadott szög harmadát.

A szögharmadolás szintén nem végezhető el euklideszi szerkesztéssel. Valóban, ha lenne egy ilyen általános eljárás, akkor annak konkrétan a 60 fokos szög esetében is működnie kellene. Megmutatjuk, hogy már a 60 fokos szög sem harmadolható. Mivel egy tetszőleges szakaszból kiindulva tudunk szabályos háromszöget, és így 60 fokos szöget is szerkeszteni, egy 60 fokos szög megadása valójában csak azt jelenti, hogy megadtunk két pontot, és így alaptestünk továbbra is a $\mathbb{Q}$. Ha a 20 fokos szög megszerkeszthető, akkor ebből 1 átfogójú

derékszögű háromszöget, és így $\cos 20^\circ$ hosszúságú szakaszt is szerkeszthetünk. Ahhoz, hogy ez nem végezhető el, elég megmutatni, hogy a $\cos 20^\circ$ számnak a foka nem 2-hatvány. Ezt később általánosabban is belátjuk, az Olvasónak azonban ajánljuk, hogy oldja meg a következő gyakorlatot, hogy fölmérhesse a kérdéssel kapcsolatos nehézségeket.

6.8.9. Gyakorlat. Az 1.5.23. Feladatban igazolt $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ összefüggés alapján adjuk meg $\cos 20^\circ$ minimálpolinomját $\mathbb{Q}$ fölött, és mutassuk meg, hogy ez egy harmadfokú szám.

6.8.10. Probléma. A *szabályos sokszögek szerkeszthetőségének* problémája az, hogy milyen n egészekre lehet szabályos n-szöget szerkeszteni.

Most is adva van az egységszakasz. Szabályos n-szöget akkor tudunk szerkeszteni, ha meg tudjuk szerekszteni azt a szöget, amely alatt a sokszög középpontjából az egyik oldal látszik. Ez a szög $2\pi/n$, vagyis a kérdés az, hogy $\cos(2\pi/n)$ hosszú szakaszt tudunk-e szerkeszteni. (A 20 fokos szög szerkeszthetősége tehát a szabályos $360/20 = 18$-szög szerkeszthetőségével ekvivalens.) Már a $\cos 20^\circ$ fokának a megállapítása sem volt nyilvánvaló, a $\cos(2\pi/n)$ minimálpolinomjának felírása (főleg az irreducibilitás ellenőrzése) pedig eléggé reménytelennek tűnik. A megoldás az, hogy ehelyett vizsgáljuk az

$$\varepsilon = \cos(2\pi/n) + i\sin(2\pi/n)$$

komplex számot, vagyis az egyik primitív n-edik egységgyököt, mert ennek könnyű kiszámítani a fokát (egy korábban bizonyított, nehéz tétel birtokában, vö. 6.8.25. Gyakorlat).

6.8.11. Állítás. *Mindegyik n-edik primitív egységgyök foka $\mathbb{Q}$ fölött $\varphi(n)$ (itt φ az Euler-függvény).*

Bizonyítás. Az n-edik egységgyökök gyökei a $\Phi_n(x)$ körosztási polinomnak, amely irreducibilis $\mathbb{Q}$ fölött (3.9.8. Tétel). E polinom foka pedig $\varphi(n)$. □

Mi a kapcsolat $\cos(2\pi/n)$ és ε foka között? Nyilván

$$\varepsilon \in \mathbb{Q}\big(\cos(2\pi/n)\big)\big(i\sin(2\pi/n)\big)\,,$$

és

$$\big(i\sin(2\pi/n)\big)^2 = -\sin^2(2\pi/n) = \cos^2(2\pi/n) - 1 \in \mathbb{Q}\big(\cos(2\pi/n)\big)\,.$$

Ezért ε foka $\mathbb{Q}\big(\cos(2\pi/n)\big)$ fölött 2 vagy 1. Ha tehát $\cos(2\pi/n)$ foka $\mathbb{Q}$ fölött 2-hatvány, akkor ε is benne van egy 2-hatvány fokú bővítésben, és így foka, vagyis $\varphi(n)$ is 2-hatvány. Beláttuk tehát a következő állítást.

6.8.12. Állítás. *Ha $\cos(2\pi/n)$ foka 2-hatvány $\mathbb{Q}$ fölött, akkor a $\varphi(n)$ szám 2-hatvány.*

Ha tehát szerkeszthető szabályos n-szög, akkor $\varphi(n)$ biztosan 2-hatvány. Speciálisan $n = 18$ esetén $\varphi(n) = 6$ nem 2-hatvány, és így sem szabályos 18-szög, sem 20 fokos szög nem szerkeszthető. A most bizonyított állítás megfordítása is igaz.

6.8.13. Tétel. *Akkor és csak akkor szerkeszthető szabályos n-szög körzővel és vonalzóval, ha a $\varphi(n)$ szám 2-hatvány (ahol φ a számelméletből ismert Euler-függvény). Ez akkor és csak akkor igaz, ha*

$$n = 2^m p_1 p_2 \dots p_r ,$$

ahol $m \geq 0$, és a p_i számok páronként különböző Fermat-prímek (vagyis $2^{2^k} + 1$ alakú prímszámok).

A fenti tétel Gausstól származik, és olyan híressé vált, hogy Gauss sírkövén egy szabályos 17-szög látható. A $17 = 2^{2^2} + 1$ a harmadik Fermat-prím. Nem nehéz megmutatni, hogy az első öt $2^{2^k} + 1$ alakú szám prímszám (ezek tehát 3, 5, 17, 257, 65537). A

$$2^{2^5} + 1 = 4294967297$$

szám már nem prím, Eulernek sikerült belátnia (egy szellemes, matematikai bizonyítással, tehát nem számolással), hogy osztható 641-gyel. Egy mai számítógép persze azonnal kiírja, hogy a fenti szám prímtényezős felbontása $641 \cdot 6700417$.

A nagyobb Fermat-számokkal azonban a számítógép is egyre nehezebben birkózik meg. Híres megoldatlan probléma, hogy van-e a felsorolt öt számon kívül még Fermat-prím. Erről a problémáról a [**11**] könyvben olvashatunk többet.

6.8.14. Gyakorlat. Mutassuk meg a $\varphi(n)$ függvény explicit képlete (lásd A.4.2. Tétel) segítségével, hogy $\varphi(n)$ akkor és csak akkor 2-hatvány, ha n az előző tételben leírt alakú szám.

Ahhoz, hogy az előző tétel megfordítását is belássuk, tovább kell fejlesztenünk eddigi elméletünket, olyan tételt bizonyítani, amely algebrai feltételek segítségével a szerkeszthetőséget biztosítja. Első lépésünk, hogy megmutatjuk a 6.8.4. Állítás első részének megfordítását.

6.8.15. Tétel. *Legyen K_0 egy szerkesztési feladat alapadatai által generált test. Ekkor egy $r \in \mathbb{R}$ szám akkor és csak akkor szerkeszthető, ha van olyan n és egy*

$$K_0 < K_1 < \ldots < K_n \leq \mathbb{R}$$

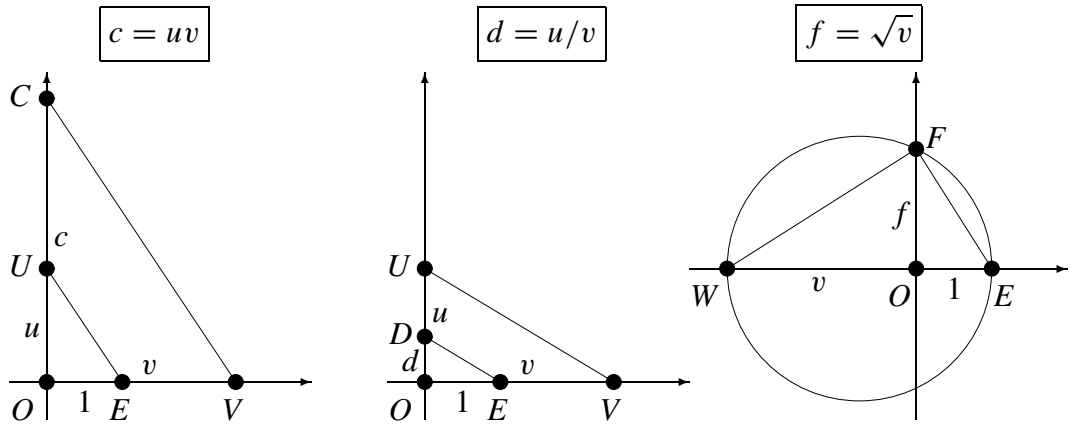
testlánc, melyre $r \in K_n$, és mindegyik $K_i \leq K_{i+1}$ bővítés foka kettő.

Bizonyítás. Elég megmutatni, hogy ha u és v szerkeszthető számok, akkor $u + v$, $u - v$, uv és $v \neq 0$ esetén u/v, továbbá $v \geq 0$ esetén $\sqrt{v}$ is szerkeszthető (vagyis a szerkeszthető számok egy résztestet alkotnak $\mathbb{R}$-ben, amely zárt a négyzetgyökvonásra is). Valóban, tegyük föl, hogy ezt már tudjuk. Ekkor az 1 szám szerkeszthető (hiszen (1, 0) adott pont, így vettük föl a koordinátarendszert). Ezért az általa generált résztest, azaz $\mathbb{Q}$ minden eleme is szerkeszthető. A K_0 test elemeit a megadott pontok (szerkeszthető) koordinátái generálják $\mathbb{Q}$ fölött, és így a négy alapművelettel megkaphatók, tehát ezek is szerkeszthetők. Tegyük föl, hogy K_i-ről már tudjuk, hogy minden eleme szerkeszthető. Mivel K_{i+1} ennek másodfokú bővítése, a 6.3.14. Gyakorlat szerint $K_{i+1} = K_i(\sqrt{v})$ alkalmas $v \neq 0$ elemre.

Itt $v \geq 0$, mert $K_i \leq \mathbb{R}$. De akkor feltevésünk szerint $\sqrt{v}$, és ezért K_{i+1} minden eleme is szerkeszthető. Így végül K_n elemei is szerkeszthetők.

Tegyük föl tehát, hogy u és v szerkeszthető, vagyis az $(u, 0)$ és a $(v, 0)$ pontok szerkeszthetők. Mivel 0 is szerkeszthető (hiszen $(0, 0)$ megadott pont), a megfelelő szakaszokat triviálisan egymás mellé mérhetjük körzővel, ahonnan látszik, hogy $(u \pm v, 0)$ is szerkeszthető. Speciálisan ellentettet is tudunk szerkeszteni, és ezért a továbbiakban feltehetjük, hogy u és v pozitívak.

Ahhoz, hogy uv és u/v hosszúságú szakaszokat tudjunk szerkeszteni, szükség van egy egység hosszúságú szakaszra is, szerencsére ez rendelkezésre áll, hiszen $(0, 0)$ és $(1, 0)$ adott pontok. Hasonló háromszögeket építünk a következőképpen. Legyen $U = (0, u)$ és $V = (v, 0)$, továbbá $O = (0, 0)$ és $E = (1, 0)$.



6.3. Ábra. Szorzat, hányados és négyzetgyök szerkesztése.

Húzzunk párhuzamost az UE egyenessel a V ponton keresztül, és jelölje $C = (0, c)$ ennek az egyenesnek a metszéspontját az y-tengellyel. Az OUE és az OCV háromszögek hasonlóak, és ezért $u/1 = c/v$, vagyis $c = uv$. Így szorzatot tudunk szerkeszteni.

Most húzzunk párhuzamost az UV egyenessel az E-n keresztül, és jelölje $D = (0, d)$ ennek az egyenesnek a metszéspontját az y-tengellyel. Az OUV és az ODE háromszögek is hasonlóak, és ezért $u/v = d/1$, vagyis hányadost is tudunk szerkeszteni.

Végül a v négyzetgyökének szerkesztéséhez tekintsük az $E = (1, 0)$ és a $W = (-v, 0)$ pontokat. Rajzoljunk erre a szakaszra egy Thalész-kört, vagyis a felezőpontja körül egy olyan kört, amely átmegy az E és W pontokon. Ez a kör messe az y-tengely pozitív felét az $F = (0, f)$ pontban. Ekkor az EFW szög derékszög, és FO ennek a derékszögű háromszögnek az átfogóhoz tartozó magassága. A magasságtétel (vagyis a WOF és az FOE háromszögek hasonlósága) miatt $f = \sqrt{1 \cdot v}$, és így négyzetgyököt is sikerült szerkesztenünk. □

Az előző tétel nagyon fontos, mert a geometriai problémát algebraira vezeti vissza. De nem oldja meg, mert azt nem könnyű eldönteni, hogy van-e a tételben megkívánt testlánc.

Az sajnos nem igaz, hogy minden 2-hatvány fokú bővítésben van ilyen testlánc (lásd a 6.10.10. Gyakorlatot). A Galois-elmélet segítségével azonban meg tudjuk oldani a problémát. Ehhez az kell, hogy a szereplő bővítések normálisak legyenek, amit a következő lemma biztosít.

6.8.16. Lemma. *Tegyük föl, hogy $K \leq L \leq \mathbb{C}$ véges normális bővítés, és*

$$L \leq L_1 = L(\sqrt{\alpha}) \leq \mathbb{C}\,,$$

ahol $\alpha \in L$. Ekkor van olyan

$$L_1 \leq \ldots \leq L_k = M \leq \mathbb{C}$$

testlánc, hogy mindegyik $L_i \leq L_{i+1}$ bővítés első, vagy másodfokú, és $K \leq M$ már normális bővítés.

Bizonyítás. Jelölje s az $\alpha \in L$ elem minimálpolinomját K fölött. Mivel $K \leq L$ normális bővítés, az s gyöktényezőkre bomlik L fölött, legyenek $\alpha_1 = \alpha, \ldots, \alpha_k$ az s gyökei (vagyis az α szám K fölötti konjugáltjai). Bővítsük L-et sorban az α_i számok négyzetgyökével. Minden lépésben első- vagy másodfokú bővítést kapunk. Így elérkezünk egy $M = L_k \leq \mathbb{C}$ testhez, amelyet L fölött ezek a négyzetgyökök generálnak. Megmutatjuk, hogy a $K \leq M$ bővítés normális.

Ehhez a 6.3.18. Gyakorlat miatt elég belátni, hogy M egy alkalmas $K[x]$ fölötti polinom felbontási teste L fölött. Az $s(x^2)$ ilyen polinom, hiszen ennek gyökei pontosan a $\pm\sqrt{\alpha_i}$ számok. □

A fentieket úgy kell elképzelni, hogy ha mondjuk $K = \mathbb{Q}$ és $L = \mathbb{Q}(\sqrt{2})$, amit tovább bővítünk a $\sqrt{1+\sqrt{2}}$ számmal, akkor a kapott L_1 test nem normális bővítése $\mathbb{Q}$-nak, ehhez be kell venni a $\sqrt{1-\sqrt{2}}$ számot is (vagyis az $(x^2-1)^2-2$ polinom összes gyökét). Persze ez a szám nem valós, de ez minket nem zavar, mint ahogy nem zavart akkor sem, amikor az n-szögek szerkesztése kapcsán komplex egységgyökök jöttek elő, hiszen ezeket a komplex számokat nem akarjuk megszerkeszteni, hanem csak algebrai segédeszközként fölhasználni.

6.8.17. Tétel. *Legyen K_0 egy szerkesztési feladat alapadatai által generált test. Ekkor egy $r \in \mathbb{R}$ szám akkor és csak akkor szerkeszthető, ha benne van K_0 egy 2-hatvány fokú* ***normális*** *bővítésében. Ezzel ekvivalens, hogy az r szám K_0 fölötti minimálpolinomjának felbontási teste K_0-nak 2-hatvány fokú bővítése.*

Bizonyítás. Tegyük föl először, hogy r szerkeszthető, tehát van olyan

$$K_0 < K_1 < \ldots < K_n \leq \mathbb{R}$$

testlánc, hogy $K_{i+1} = K_i(\sqrt{d_i})$ alkalmas $d_i \in K_i$ elemre, és $r \in K_n$. Megmutatjuk, hogy vannak olyan

$$K_0 = M_0 \leq M_1 \leq \ldots \leq M_n \leq \mathbb{C}$$

testek, hogy mindegyik $K_0 \leq M_i$ bővítés normális, 2-hatvány fokú, és $K_i \leq M_i$. Lentről fölfelé haladunk. Ha M_i már megvan ezekkel a feltételekkel, akkor alkalmazzuk az előző

lemmát abban a szereposztásban, hogy $K = K_0$, $L = M_i$ és $\alpha = d_i$. A kapott M test megfelelő lesz M_{i+1}-nek. Valóban, $M_i \geq K_i$ miatt $M_{i+1} \geq M_i(\sqrt{d_i}) \geq K_i(\sqrt{d_i}) = K_{i+1}$. Az $M = M_{i+1}$ a lemma szerint normális bővítése a K_0 alaptestnek. Végül M_{i+1} foka M_i fölött a lemma szerint 2-hatvány, és így a szorzástétel miatt $|M_{i+1} : K_0|$ is az.

Tehát $r \in K_n \leq M_n$, ami K_0-nak egy 2-hatvány fokú normális bővítése, és ezzel a tétel egyik irányát beláttuk. Természetesen az r szám K_0 fölötti minimálpolinomjának a felbontási teste része M_n-nek, és így az is egy 2-hatvány fokú normális bővítés.

A megfordítás igazolásához a 6.8.15. Tétel szerint azt kell megmutatni, hogy ha $K_0 \leq M$ egy 2-hatvány fokú normális bővítés, akkor minden $r \in \mathbb{R}$ eleme elérhető egy olyan testlánc segítségével, amelyben minden bővítés másodfokú, és *amely végig valósban marad.* Ennek kulcsa a Galois-elmélet főtétele, és a csoportelméletben tanult 4.10.8. Tétel, amely szerint egy 2-hatvány rendű csoportban minden maximális részcsoport (normálosztó, és ezért) indexe 2.

Legyen G a $K_0 \leq M$ bővítés Galois-csoportja. Ennek a csoportnak a rendje a bővítés foka, vagyis 2-hatvány (más szóval ez egy 2-csoport). Jelölje T a $K_0(r) \leq \mathbb{R}$ testet, és legyen H az ehhez tartozó részcsoport. A keresett K_0-tól T-ig tartó testlánc megadásához tehát olyan $G = H_0 > H_1 > \ldots > H_m = H$ részcsoportokat kell találni, ahol minden lépésnél az index 2, vagyis $|H_i : H_{i+1}| = 2$ mindegyik i-re.

Legyen H_1 egy olyan maximális részcsoportja G-nek, amely H-t tartalmazza. Az imént idézett 4.10.8. Tétel miatt H_1 indexe G-ben 2. Most H_2 legyen a H-t tartalmazó maximális részcsoportja H_1-nek. Az eljárást folytatva előbb-utóbb H-ig jutunk. □

A konkrét szerkesztési feladatok sokszor harmad- vagy negyedfokú egyenletre vezetnek. A most bizonyított tétel segítségével eldönthetjük, hogy ezek megoldhatóak-e. A harmadfokú egyenletnél egyszerű a helyzet: ha irreducibilis polinomot kapunk, akkor a gyökök nem szerkeszthetők, különben igen. Az, hogy egy negyedfokú polinom gyökei mikor szerkeszthetők, azon múlik, hogy a harmadfokú rezolvense irreducibilis-e, vagy sem (6.10.10. Gyakorlat).

A szabályos sokszögek szerkeszthetőségének vizsgálatához még annyit kell tudnunk, hogy egy komplex egységgyökkel való bővítés mindig normális.

6.8.18. Definíció. A $\mathbb{Q}(\varepsilon)$ testet, ahol ε egy n-edik komplex primitív egységgyök, az n-edik *körosztási testnek* nevezzük.

6.8.19. Tétel. *Legyen ε egy n-edik komplex primitív egységgyök. Ekkor a $\mathbb{Q} \leq \mathbb{Q}(\varepsilon)$ egy $\varphi(n)$ fokú normális bővítés, és a Galois-csoportja a $\mathbb{Z}_n^\times$ csoporttal izomorf.*

Bizonyítás. A 6.8.11. Állítás miatt e bővítés foka $\varphi(n)$, hiszen ε minimálpolinomja a $\Phi_n(x)$ körosztási polinom. A ε hatványaiként az összes többi primitív n-edik egységgyök előáll, és így $\mathbb{Q}(\varepsilon)$ a $\Phi_n(x)$ felbontási teste, tehát normális.

Ha ψ eleme a $\mathbb{Q} \leq \mathbb{Q}(\varepsilon)$ bővítés G Galois-csoportjának, akkor $\psi(\varepsilon)$ is gyöke $\Phi_n(x)$-nek, vagyis $\psi(\varepsilon) = \varepsilon^j$ egy n-hez relatív prím j egészre. Mivel ε generálja a bővítést, ez a j egyértelműen meghatározza a ψ szimmetriát, amit ψ_j-vel jelölünk. Nyilván

$$\psi_j\psi_k(\varepsilon) = \psi_j(\varepsilon^k) = \big(\psi_j(\varepsilon)\big)^k = (\varepsilon^j)^k = \varepsilon^{jk}\,,$$

azaz $\psi_j \circ \psi_k = \psi_{jk}$. Így a $j \leftrightarrow \psi_j$ megfeleltetés izomorfizmus G és $\mathbb{Z}_n^\times$ között. □

Most már be tudjuk látni a szabályos sokszögek szerkeszthetőségéről szóló 6.8.13. Tétel hiányzó irányát is.

Bizonyítás. Tegyük föl, hogy a $\varphi(n)$ szám 2-hatvány, és legyen

$$\varepsilon = \cos(2\pi/n) + i\,\sin(2\pi/n)\,.$$

Ekkor

$$1/\varepsilon = \cos(2\pi/n) - i\,\sin(2\pi/n) \in \mathbb{Q}(\varepsilon)\,,$$

ezért

$$\cos(2\pi/n) = \frac{\varepsilon + (1/\varepsilon)}{2} \in \mathbb{Q}(\varepsilon)\,.$$

Így $\cos(2\pi/n)$ benne van egy 2-hatvány fokú normális bővítésben, tehát szerkeszthető. □

6.8.20. Feladat. Írjuk föl az ötödik és a tizenhetedik primitív egységgyököket négyzetgyökvonások segítségével.

A 6.9.10. Következményben belátjuk majd, hogy minden komplex egységgyököt föl lehet írni gyökvonások segítségével. Ahhoz, hogy ezeket a képleteket konkrétan is megkaphassuk, az előző feladat megoldását kell általánosítani. Ez a *Gauss-ciklusok* fogalmához vezet, amelyekről Fried Ervin [**13**] könyvének 8.12. Szakaszában olvashatunk (ott a tizenharmadik egységgyökök példája is ki van dolgozva).

Gyakorlatok, feladatok

6.8.21. Gyakorlat. Az alábbi szerkesztési feladatok mindegyikében határozzuk meg a K alaptestet, a $K(\alpha)$ bővítés fokát K fölött, az α minimálpolinomja felbontási testének fokát K fölött, és döntsük el, hogy a szerkesztés elvégezhető-e.

(1) Adott az egységszakasz, szerkesztendő $\alpha = \sqrt[5]{2}$.
(2) Adott az egységszakasz, szerkesztendő $\alpha = \sqrt[4]{2}$.
(3) Adott az egységszakasz és egy $\sqrt[3]{2}$ hosszú szakasz, szerkesztendő $\alpha = \sqrt[6]{2}$.
(4) Adott az egységszakasz és egy $\sqrt[3]{2}$ hosszú szakasz, szerkesztendő $\alpha = \sqrt[5]{2}$.
(5) Adott $(0, 0)$, $(0, 1)$, $(0, \pi)$, a feladat az egységsugarú kör négyszögesítése.
(6) Adott egy szabályos 9-szög, szerkesztendő egy szabályos 18-szög.

6.8.22. Gyakorlat. Hol a hiba a következő gondolatmenetben? Az egységszakaszból akarunk π hosszú szakaszt szerkeszteni. Vegyük föl a koordinátarendszert úgy, hogy a síkon adott egységszakasz két végpontja a $(0, \pi)$ és az $(1, \pi)$ pontokba kerüljön. Ekkor az alapadatok által generált test $K = \mathbb{Q}(0, 1, \pi)$, amelynek a szerkesztendő szám eleme. Tehát ez a szerkesztés elvégezhető.

6.8.23. Gyakorlat. Szerkeszthető-e a háromszög, ha adott két oldalának és az egyikhez tartozó szögfelezőnek a hossza? Válaszoljunk az alábbiak megoldásával. Jelölje (a szokásos módon) az oldalakat a, b, c, a hozzájuk tartozó szögfelezőket f_a, f_b, f_c, a szemköztes szögeket α, β, γ.

(1) Mutassuk meg, hogy $f_a = \big(2bc\,\cos(\alpha/2)\big)/(b+c)$.
(2) Mutassuk meg, hogy $\cos(\alpha/2) = \sqrt{(1+\cos\alpha)/2}$.
(3) Vizsgáljuk azt az esetet, amikor a megadott adatok értéke $a = 1$, $b = 1$, $f_a = 1$. Ha ez nem szerkeszthető, mi a helyzet az általános feladattal?
(4) Fejezzük ki ebben az esetben $\cos\alpha$-t az oldalak segítségével.
(5) A c-re kapott egyenletből milyen érték adódik c fokára $\mathbb{Q}$ fölött?

6.8.24. Gyakorlat. Mutassuk meg, hogy nem szerkeszthető egyenlő szárú háromszög a szárából és a beírt kör sugarából.

6.8.25. Gyakorlat. A körosztási polinom irreducibilitásának bizonyítása nem volt könnyű. Ugyanakkor a Schönemann-Eisenstein kritériumból adódott, hogy minden prímhatvány indexű körosztási polinom irreducibilis (3.9.23. Gyakorlat). Mutassuk meg csak ennek a felhasználásával, hogy ha egy szabályos n-szög szerkeszthető, akkor a $\varphi(n)$ szám 2-hatvány.

6.8.26. Gyakorlat. Milyen n egészekre szerkeszthető n fokos szög?

6.8.27. Feladat. Határozzuk meg $\cos(2\pi/n)$ és $\sin(2\pi/n)$ fokát $\mathbb{Q}$ fölött.

6.8.28. Feladat. Legyen p prímszám és K egy p karakterisztikájú test. Definiáljuk a K fölötti n-edik Φ_n körosztási polinomot ugyanazzal a rekurzióval, mint $\mathbb{Z}$ fölött.

(1) Tegyük föl, hogy $n = p^k m$, ahol már $p \nmid m$. Mutassuk meg, hogy $\Phi_n = \Phi_m^{\varphi(p^k)}$.
(2) Igazoljuk, hogy ha $p \nmid m$, akkor Φ_m gyökei K-ban pontosan a K multiplikatív csoportjának n rendű elemei.
(3) Igazoljuk, hogy ha $p \nmid m$, akkor Φ_m felbomlik $o_m(p)$ fokú, a K prímteste fölött irreducibilis polinomok szorzatára.
(4) Hogyan kaphatjuk meg a K fölött irreducibilis tényezők fokszámát?

6.9. Egyenletek gyökjelekkel való megoldhatósága

Ebben a szakaszban megvizsgáljuk, hogy mely polinomok gyökei írhatók föl az együtthatókból kiindulva a négy alapművelet és gyökvonások segítségével, azaz *gyökkifejezésként*. A célunk elsősorban az, hogy az Olvasó megértse a fő gondolatokat. Ezért mindent a lehető legegyszerűbben tárgyalunk, például komplex együtthatós polinomokra szorítkozunk. Aki az általános esetre, vagy a pontos finomságokra kíváncsi, érdemes elolvasnia Fried Ervin [**13**] könyvében is ezt az anyagrészt.

A legföljebb negyedfokú polinomok esetében megmutattuk a 3.8. Szakaszban, hogy minden gyökük gyökkifejezés. Fő eredményünk a 6.9.7. Tétel, miszerint a legalább ötödfokú polinomok gyökeire nincs ilyen általános „gyökképlet”.

Az, hogy egy polinom gyökökkel megoldható-e, a polinomtól függ. Például az $x^5 - 2$ polinom gyökei kifejezhetők gyökvonás segítségével. Be fogjuk látni, hogy *egy polinom gyökei akkor és csak akkor gyökkifejezések, ha a felbontási testének Galois-csoportja feloldható* (6.9.4. és 6.9.11. Tétel). A következő szakaszban tudásunkat a harmad- és negyedfokú egyenlet vizsgálatára alkalmazzuk.

A 6.5. Szakasz végén (illetve a 6.6.18. Gyakorlatban) megbeszéltük, hogy egy n-edfokú irreducibilis polinom felbontási testének Galois-csoportja valójában a polinom gyökein ható permutációcsoport, az S_n szimmetrikus csoport részcsoportja. A Galois-csoport annál „kisebb", minél több összefüggés van a polinom gyökei között. Jó példa erre az n-edik körosztási polinom, amelynek gyökei egymásból hatványozással kifejezhetők, és a Galois-csoport olyan kicsi, amilyen csak lehet, vagyis rendje a polinom fokával egyezik meg (6.8.19. Tétel).

Ha véletlenszerűen választunk egy polinomot, annak a gyökei között nem lesz összefüggés, és ezért a Galois-csoport a teljes szimmetrikus csoport, ami $n \geq 5$ esetén nem feloldható (4.12.8. Tétel). Például az $x^5 - 4x + 2$ polinom Galois-csoportja S_5 (lásd 6.9.5. Következmény). Így a polinomok többségére nem létezik gyökképlet, és egy legalább ötödfokú polinom gyökeinek gyökvonásokkal történő meghatározására csak akkor van esélyünk, ha valamilyen összefüggést fölfedezünk a gyökök között. Ilyenek például a reciprok polinomok (3.8.12. Feladat).

A Galois-csoport kiszámítható akkor is, ha a polinom gyökeit nem ismerjük (lásd a [**13**] könyvben a 8.46/A. Tételt), és így az egyenletekről elvileg el tudjuk dönteni, hogy vannak-e ilyen rejtett összefüggések, és hogy gyökjelekkel megoldhatók-e.

A most következő elmélet nagyon hasonló ahhoz, amiről az előző szakaszban a geometriai szerkeszthetőség kapcsán szó volt. Annyi a különbség, hogy ott csak négyzetgyököket vonhattunk, most viszont tetszőleges gyökvonást tudnunk kell kezelni. Emiatt a technikai nehézségek kissé megnövekszenek. Általános n-edik gyökvonás helyett elég a p-edik gyökvonást megengedni a gyökképletben, ahol p prím, hiszen ilyenek egymásutánjával minden n-edik gyökvonás előállítható.

Vegyünk egy f polinomot, amelynek valamelyik gyöke egy gyökvonást és a négy alapműveletet használó képlettel írható föl a polinom együtthatóiból. Induljunk ki az együtthatók által generált K testből, és ahogy a képlet fölépül, bővítsük a testet is megfelelően. Például ha a képlet

$$\sqrt[6]{\sqrt{5} - \sqrt[5]{2 + \sqrt[7]{4}}},$$

akkor első lépésben $\sqrt[7]{4}$-gyel bővítünk, a másodikban a kapott testet $\sqrt[5]{2 + \sqrt[7]{4}}$-gyel, a harmadikban $\sqrt{5}$-tel, végül a $\sqrt[6]{\ }$ kiszámításához még két bővítés tartozik: először négyzetgyököt, majd köbgyököt kell vonni (hiszen csak prímedik gyökvonást engedélyeztünk).

Be fogjuk látni, hogy minden egyes p-edik gyökvonás (alkalmas feltételek mellett) egy p-edfokú normális bővítést eredményez. Ennek a Galois-csoportban egy p indexű normálosztó felel meg. Ha tehát egy gyököt föl lehet építeni gyökvonások segítségével, akkor a Galois-csoportban egy normállánc keletkezik, és így a Galois-csoport feloldható lesz. Megfordítva, megmutatjuk, hogy egy p indexű normálosztóhoz egy p-edik gyökkel való bővítés

tartozik (szintén alkalmas feltételek mellett), és így kiderül, hogy ha a Galois-csoport feloldható, akkor a polinom gyökei gyökkifejezések. Az „alkalmas feltételek" arról szólnak, hogy az alaptestnek tartalmaznia kell a p-edik egységgyököket.

Az előző bekezdésben leírt tervet kicsit pontosítani kell. Ahhoz, hogy Galois-csoportról beszélhessünk, ügyelni kell arra, hogy ne csak az egyes bővítések legyenek normálisak, hanem az együttes bővítés is. A szerkeszthetőségnél bizonyított 6.8.16. Lemma megmutatja, hogyan lehet ezen a problémán úrrá lenni: ha $\sqrt[p]{\alpha}$-val bővítünk, akkor mindig be kell venni a $\sqrt[p]{\alpha_i}$ elemeket is, ahol az α_i elemek befutják az α konjugáltjait az alaptest fölött.

Első feladatunk tehát az, hogy megértsük a $K \leq K(\sqrt[p]{\alpha})$ alakú bővítéseket, ahol $\alpha \in K$. Példaként vegyük elő a már sokszor tárgyalt $x^3 - 2$ polinomot.

(1) Ez a polinom a Schönemann-Eisenstein kritérium miatt irreducibilis $\mathbb{Q}$ fölött, és így egyik gyökével, például a valós $\sqrt[3]{2}$-vel bővítve harmadfokú bővítést kapunk, ami azonban nem normális, mert a polinom másik két gyökét nem tartalmazza.

(2) Az x^3-2 polinom felbontási teste $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, ahol $\varepsilon = \cos 120^\circ + i \sin 120^\circ$ primitív harmadik egységgyök. Ez egy normális bővítése $\mathbb{Q}$-nak, de nem harmad-, hanem hatodfokú.

(3) Ha $K = \mathbb{Q}(\varepsilon)$, akkor $K(\sqrt[3]{2})$ foka K fölött három, és ez a bővítés normális is.

Az (1) állításban használt Schönemann-Eisenstein kritérium általában nem áll rendelkezésre, és így nem tudjuk, hogy $x^p - \alpha$ mikor lesz irreducibilis. Ha egy K test tartalmazza is az ε számot, miért ne lehetne $\sqrt[3]{2}$ mondjuk másodfokú K fölött? A válasz az, hogy ebben az esetben $x^3 - 2$ egy másod- és elsőfokú polinom szorzatára bomolna K fölött, és az elsőfokú tényezőnek lenne gyöke K-ban. Ez a gyök akár $\varepsilon\sqrt[3]{2}$, akár $\varepsilon^2\sqrt[3]{2}$, az $\varepsilon \in K$ miatt $\sqrt[3]{2} \in K$, és így $\sqrt[3]{2}$ elsőfokú (és nem másodfokú) K fölött.

Azt hihetnénk, hogy ez a gondolatmenet csak harmadfokú polinomra működik. Hiszen miért ne fordulhatna elő, hogy $x^5 - 2$ egy másod- és egy harmadfokú irreducibilis polinom szorzatára bomlik egy K test fölött. A következő állítás mutatja, hogy ez nem lehetséges.

6.9.1. Lemma. *Legyen $K \leq \mathbb{C}$ test, $\alpha \in K$, és p prímszám. Ekkor az $x^p - \alpha$ polinom vagy irreducibilis K fölött, vagy van gyöke K-ban.*

Bizonyítás. Feltehető, hogy $\alpha \neq 0$. Jelölje β a $\sqrt[p]{\alpha}$ tetszőleges értékét, tudjuk, hogy ekkor $\sqrt[p]{\alpha}$ többi értékét úgy kapjuk, hogy a β számot megszorozzuk a p-edik egységgyökökkel. Ezért $x^p - \alpha$ gyöktényezős alakja

$$x^p - \alpha = x^p - \beta^p = \prod_{j=1}^{p} (x - \varepsilon_j \beta)\,,$$

ahol $\varepsilon_1, \ldots, \varepsilon_p$ az összes p-edik egységgyök.

Tegyük föl, hogy $x^p - \alpha$ nem irreducibilis K fölött, azaz $x^p - \alpha = f(x)g(x)$ alkalmas $f, g \in K[x]$ normált polinomokra, ahol $0 < n = \mathrm{gr}(f) < p$. Ekkor f gyökei is az $\varepsilon^j\beta$ számok közül kerülnek ki. A gyökök és együtthatók összefüggése miatt f konstans tagja

(ami K egy eleme) az f gyökeinek a szorzata, és így felírható $\pm\xi\beta^n$, alakban, ahol ξ is p-edik egységgyökök (hiszen p-edik egységgyökök szorzata is p-edik egységgyök).

Oldjuk meg az $nu + pv = 1$ lineáris diofantikus egyenletet u-ra és v-re. Ez megtehető, mert $0 < n < p$, és így $(n, p) = 1$. Ekkor

$$K \ni (\xi\beta^n)^u\alpha^v = \xi^u\beta^{nu+pv} = \xi^u\beta\,.$$

A kapott szám azonban gyöke $x^p - \alpha$-nak, hiszen $\xi^p = 1$. □

Előfordulhat, hogy $x^p - \alpha$-nak csak egy gyöke van K-ban, például ez a helyzet az $x^3 - 8$ polinom esetében, ha $K = \mathbb{Q}$. Könnyű megmutatni, hogy ha $x^p - \alpha$-nak legalább két gyöke van K-ban, akkor itt gyöktényezőkre bomlik (mert a két gyök hányadosa primitív p-edik egységgyök, amelynek hatványaiként az összes p-edik egységgyök előáll).

Megjegyezzük, hogy ez a bizonyítás (és a továbbiak is) általánosabban is elmondhatók lennének. Semmi erőfeszítést nem kellene tennünk annak érdekében, hogy mondjuk a $\mathbb{Q}(x)$ hányadostest fölötti polinomokra is érvényes legyen. Ez fontos lesz később, amikor „általános" megoldóképleteket vizsgálunk majd.

6.9.2. Következmény. *Legyen $K \leq \mathbb{C}$ test, $\alpha \in K$, és p prímszám. Ha K tartalmazza a p-edik egységgyököket, akkor $K \leq K(\sqrt[p]{\alpha})$ normális bővítés (mindegy, hogy $\sqrt[p]{\alpha}$ melyik értékét vesszük, ugyanazt a bővítést kapjuk), és foka 1 vagy p. Ez utóbbi esetben $x^p - \alpha$ irreducibilis K fölött.*

Bizonyítás. Legyen β a $\sqrt[p]{\alpha}$ bármelyik értéke. A $K(\beta)$ bővítésben benne vannak az $x^p - \alpha$ többi gyökei is, hiszen azok $\varepsilon\beta$ alakúak, ahol ε befutja a p-edik egységgyököket, és ezek elemei K-nak. Tehát $K(\beta)$ az $x^p - \alpha$ felbontási teste K fölött, és így normális bővítése K-nak. Ha $x^p - \alpha$ irreducibilis K fölött, akkor a bővítés foka p. Ha nem, akkor az előző állítás szerint valamelyik $\varepsilon\beta$ gyöke eleme K-nak. De akkor $\varepsilon \in K$ miatt $\beta \in K$, és ezért a bővítés elsőfokú. □

Ezek szerint ha be akarjuk bizonyítani a Galois-csoport feloldhatóságát a megadott terv szerint, akkor azzal célszerű kezdeni, hogy az alaptestet először a megfelelő egységgyökökkel bővítjük. Ez nem fogja elrontani a csoport feloldhatóságát, mert ez a bővítés a 6.8.19. Tétel miatt egy Abel-féle Galois-csoportot eredményez.

6.9.3. Gyakorlat. Legyen $K \leq \mathbb{C}$ test, és ε primitív n-edik egységgyök. Mutassuk meg, hogy a $K \leq K(\varepsilon)$ bővítés normális, és a Galois-csoportja a $\mathbb{Z}_n^\times$ csoport egy részcsoportjával izomorf.

6.9.4. Tétel. *Legyen $K \leq \mathbb{C}$ test, és $f \in K[x]$ egy irreducibilis polinom. Ha f valamelyik (komplex) gyöke felírható egy olyan képlettel, amely f együtthatóiból a négy alapművelettel és gyökvonásokkal keletkezik, akkor az f polinom K fölötti felbontási testének Galois-csoportja feloldható csoport.*

Az alábbiakban a bizonyítást csak vázoljuk, a részletek kidolgozását az Olvasóra bízzuk.

Bizonyítás. Feltehetjük, hogy a képletben csak prímedik gyökvonások szerepelnek. Szorozzuk össze az összes ilyen prímet, az eredmény legyen n. Bővítsük K-t először egy primitív n-edik ε egységgyökkel. Az előző gyakorlat miatt a $K \leq K(\varepsilon)$ bővítés normális, és a Galois-csoportja kommutatív, vagyis feloldható. A $K(\varepsilon)$ persze tartalmazza a p-edik egységgyököket is minden $p \mid n$-re.

Végezzük el sorban a gyökképletből adódó, $\sqrt[p]{\alpha}$ elemekkel való bővítéseket. Minden ilyen bővítésnél vegyük be a $\sqrt[p]{\alpha'}$ elemet is, ahol α' az α elem K fölötti konjugáltjain fut végig (a 6.8.16. Lemma bizonyításához hasonlóan). Ekkor a (6.9.2. Következmény miatt) minden lépésben p-edfokú, vagy elsőfokú normális bővítést kapunk, a végeredmény pedig egy olyan $K(\varepsilon) \leq M$ test lesz, amely K-nak normális bővítése, és f egyik gyökét tartalmazza.

Jelölje G a $K \leq M$ bővítés Galois-csoportját, és legyen N a $K(\varepsilon)$-hoz a Galois-elmélet főtétele szerint tartozó részcsoport (amely normálosztó, hiszen $K \leq K(\varepsilon)$ normális bővítés). Mivel $K(\varepsilon)$-tól M-ig eljutottunk prímfokú normális bővítésekkel, a főtétel szerint N-től le tudunk jutni $\{id\}$-ig úgy, hogy mindig egy prímindexű normálosztóra lépünk (ezek N-nek nem feltétlenül normálosztói). Ezért N feloldható. A G/N faktorcsoport viszont Abel-féle, mert ez a $K \leq K(\varepsilon)$ bővítés Galois-csoportja a főtétel miatt. Mivel a feloldható csoportok osztálya bővítésre zárt (4.12.20. Feladat), ezért G is feloldható.

A $K \leq M$ normális bővítés, amelyben az irreducibilis f polinomnak van gyöke, ezért f összes gyöke M-ben van. Jelölje L az ezek által K fölött generált résztestet (vagyis f felbontási testét), és legyen H a megfelelő részcsoport G-ben. Mivel $K \leq L$ normális bővítés (hiszen L felbontási test), H normálosztó, és $G(L/K) \cong G/H$. De feloldható csoport faktorcsoportja is feloldható (4.12.19. Feladat), ezért $G(L/K)$ tényleg feloldható. □

Most már meg tudjuk mutatni, hogy az ötödfokú egyenletre nincs gyökképlet. Sőt, megadunk egy konkrét polinomot, amelynek egyik gyöke sem gyökkifejezés.

6.9.5. Következmény. *Az $x^5 - 4x + 2$ polinom egyik gyöke sem gyökkifejezés $\mathbb{Q}$ fölött.*

Bizonyítás. E polinom $\mathbb{Q}$ fölötti felbontási testének Galois-csoportja a 6.6.15. Feladat szerint az ötödfokú szimmetrikus csoport (azaz S_5), ami nem feloldható csoport. □

Az eddigiekben azt vizsgáltuk, hogy egy konkrét polinom konkrét gyöke felírható-e gyökkifejezésként. A megoldóképletet azonban nem egészen így szokás érteni. Például az $x^2 + bx + c = 0$ másodfokú egyenlet megoldóképlete

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

úgy értendő, hogy *bármely* b és c esetén működik. Ezt algebrailag úgy kezelhetjük, hogy b-t és c-t határozatlanoknak képzeljük, vagyis a $\mathbb{Q}[b, c]$ polinomgyűrű hányadostestéből indulunk ki, mint alaptestből.

Az eddigi bizonyításokban az egyszerűség kedvéért feltettük ugyan, hogy $\mathbb{C}$ résztesteiről van szó, de nulla karakterisztikában minden ugyanúgy működik, és az egységgyökökről is ugyanúgy beszélhetünk. Ezért az ilyen általános együtthatós polinomok esetében is igaz,

hogy akkor és csak akkor létezik gyökképlet, ha a felbontási test Galois-csoportja feloldható. Az általános együtthatós polinom esetében azonban mindig a teljes szimmetrikus csoportot fogjuk kapni.

6.9.6. Tétel. *Legyenek $y_1, \ldots, y_n$ határozatlanok, K a $\mathbb{Q}[y_1, \ldots, y_n]$ hányadosteste, és*

$$f(x) = x^n + y_1 x^{n-1} + \ldots + y_{n-1}x + y_n \in K[x]\,.$$

Ekkor az f polinom K fölötti felbontási testének a Galois-csoportja az S_n szimmetrikus csoport.

A bizonyítást csak vázoljuk. Azt fogjuk megmutatni, hogy e polinom gyökei között nincsenek „rejtett összefüggések", a gyökök „olyanok, mint ha határozatlanok lennének". Ennek a kulcsa pedig a szimmetrikus polinomok alaptételének egyértelműségi állítása.

Bizonyítás. Válasszunk $x_1, \ldots, x_n$ határozatlanokat, ezek (pontosabban az ellentettjeik) fognak majd megfelelni f gyökeinek, ezért tekintsük a

$$g(x) = (x + x_1) \ldots (x + x_n)$$

polinomot. Ezt beszorozva, a gyökök és együtthatók összefüggése alapján

$$g(x) = x^n + \sigma_1 x^{n-1} + \ldots + \sigma_{n-1}x + \sigma_n\,.$$

Az itt szereplő σ_j elemi szimmetrikus polinomokat szeretnénk megfeleltetni az f polinom y_j együtthatóinak. Azaz legyen $F \in \mathbb{Q}[y_1, \ldots, y_n]$ esetén

$$\psi : F(y_1, \ldots, y_n) \mapsto F(\sigma_1, \ldots, \sigma_n)\,.$$

A ψ leképezés tehát egy $\mathbb{Q}[y_1, \ldots, y_n]$-beli polinomhoz egy $\mathbb{Q}[x_1, \ldots, x_n]$-beli polinomot rendel, ugyanúgy, mint a szimmetrikus polinomok alaptételében (2.7.3. Tétel). Ez a leképezés nyilván összeg- és szorzattartó, és az alaptétel egyértelműségi állítása miatt injektív is. A ψ képe pedig a szimmetrikus polinomokból álló részgyűrű $\mathbb{Q}[x_1, \ldots, x_n]$-ben.

A ψ leképezést persze polinomok hányadosain is értelmezhetjük (a jóldefiniáltságot ellenőrizni kell az 5.6.4. Tétel mintájára). Ezért egy ψ izomorfizmust kapunk a $\mathbb{Q}[y_1, \ldots, y_n]$ hányadosteste (vagyis a K test), és a $\mathbb{Q}[x_1, \ldots, x_n]$ gyűrű $\mathbb{Q}(x_1, \ldots, x_n)$ hányadostestének egy S részteste között. Az S pontosan a szimmetrikus polinomok hányadosaiból áll. Ennél az izomorfizmusnál az f polinomnak a fenti g polinom felel meg. Ezért ezentúl K és f helyett S-sel és g-vel foglalkozunk.

A g polinom felbontási teste S fölött a $\mathbb{Q}(x_1, \ldots, x_n)$ hányadostest! Valóban, g gyökei a $-x_i$ határozatlanok, amelyek ezt a testet generálják (már $\mathbb{Q}$ fölött is). Az pedig nyilvánvaló, hogy a $\{-x_1, \ldots, -x_n\}$ halmaz minden permutációja a $\mathbb{Q}(x_1, \ldots, x_n)$ test egy automorfizmusa, ami a szimmetrikus kifejezéseket, azaz S elemeit fixen hagyja. Ezért a keresett Galois-csoport tényleg S_n. □

6.9.7. Tétel. *Az általános n-edfokú egyenletre $n \geq 5$ esetén nem létezik gyökképlet.*

Bizonyítás. Az előző tételből tudjuk, hogy az általános n-edfokú polinom felbontási testének Galois-csoportja S_n. A 4.12.8. Tétel miatt ez a csoport $n \geq 5$ esetén nem feloldható. Ezért a 6.9.4. Tétel (kellően általános verziója) szerint az általános n-edfokú polinom egyik gyöke sem gyökkifejezés. □

A szakasz hátralévő részében a 6.9.4. Tétel megfordításával foglalkozunk, vagyis annak megmutatásával, hogy ha a Galois-csoport feloldható, akkor az egyenlet gyökeire van megoldóképlet. Továbbra is $\mathbb{C}$ résztesteire szorítkozunk.

Az eddigiekhez képest az a változás, hogy most nekünk kell a gyökképletet megkonstruálni. Ezért pontosabban kell tisztáznunk, hogy mit is értünk gyökkifejezés alatt. A fő problémát az okozza, hogy a gyökvonás nem egyértékű művelet. Például ha valaki felírja, hogy $\sqrt[3]{2}$, akkor a három közül melyik értékére gondol? Megengedjük-e, hogy ha a képletben két helyen is szerepel $\sqrt[3]{2}$, akkor azok különböző értékei legyenek? Leírhatjuk-e a $\cos 120^\circ + i \sin 120^\circ$ számot úgy, hogy $\sqrt[3]{1}$? Emlékezzünk vissza, hogy a Cardano-képletnél az ilyet nem engedtük meg, még azt is megadtuk, hogy a köbgyökvonásnál mely értékek tartoznak össze.

A 6.9.4. Tétel bizonyítása még az ilyesfajta szabadosságok megengedésekor is működött. Amikor azonban a gyökképletet konstruáljuk, akkor ki szeretnénk zárni ezeket a trükköket, hiszen ez szinte lehetetlenné tenné a képlet használatát. Például az $\varepsilon = \cos 120^\circ + i \sin 120^\circ$ számot

$$\varepsilon = \frac{-1 + i\sqrt{3}}{2}$$

alakban akarjuk megadni (ami mindenki számára elfogadhatóan tényleg gyökkifejezés, az $i = \sqrt{-1}$-et is annak tekintve).

A problémát teljes részletességében nem tárgyaljuk, csak a leglényegesebb pontot kezeljük le. A $\sqrt[3]{1}$ kifejezéssel az a baj, hogy az $x^3 - 1$ polinom nem irreducibilis, és így az 1 szám „szebb" gyöke, mint a másik kettő. Azok egy másodfokú bővítést generálnak, ami már „igazából" nem köbgyökvonás, hanem négyzetgyökvonás: a $\sqrt{-3}$ négyzetgyökkel kell bővíteni. Ezért a $\sqrt[p]{\alpha}$ számot csak akkor fogjuk megengedni a képletben, ha $x^p - \alpha$ a korábbi testek fölött irreducibilis. Meg fogjuk látni, hogy speciálisan a komplex egységgyökök mindegyike felírható ilyenfajta gyökvonásokkal is.

6.9.8. Definíció. Legyen $K_0 \leq \mathbb{C}$ test. Az $r \in \mathbb{C}$ szám akkor és csak akkor K_0 fölötti *gyökkifejezés*, ha van olyan n és egy

$$K_0 < K_1 < \ldots < K_n \leq \mathbb{C}$$

testlánc, melyre $r \in K_n$, és mindegyik i-re $K_{i+1} = K_i(\sqrt[p_i]{\alpha_i})$, ahol $\alpha_i \in K_i$, a p_i prímszám, és az $x^{p_i} - \alpha_i$ polinom irreducibilis K_i fölött.

Ahogy az előző irány nemtriviális matematikai ötlete a 6.9.1. Lemma állítása volt, úgy most is kiemeljük az ennek megfelelő, leglényegesebb ötletet.

6.9.9. Lemma. *Tegyük föl, hogy a $K \leq \mathbb{C}$ test tartalmazza a p-edik egységgyököket, ahol p prímszám. Ha $K \leq L$ egy p-edfokú normális bővítés, akkor van olyan $\alpha \in K$, hogy L az $x^p - \alpha \in K[x]$ irreducibilis polinom felbontási teste K fölött.*

Az L tehát egy olyan p-edik gyök hozzávételével keletkezik, ami az előző definícióban is megengedett. Más szóval, ha K minden eleme gyökkifejezés egy K_0 test fölött, akkor L minden eleme is az.

Bizonyítás. Olyan $\beta \in L$ elemet keresünk, amelynek a p-edik hatványa K-ban van, de maga nincs K-ban. Ha találtunk egy ilyet, akkor készen vagyunk a 6.9.2. Következmény miatt.

A $G(L/K)$ Galois-csoport prímrendű, tehát ciklikus, legyen ψ egy (p rendű) generátor-eleme. Ekkor $\psi^p = id$, és ψ lineáris transzformációja az L vektortérnek K fölött, mert összegtartó, és $k \in K$, $\gamma \in L$ esetén

$$\psi(k\gamma) = \psi(k)\psi(\gamma) = k\psi(\gamma)\,,$$

hiszen ψ fixálja K elemeit. A $\psi^p = id$ azt jelenti, hogy a ψ transzformáció gyöke az $x^p - 1$ polinomnak, vagyis s minimálpolinomja osztója $x^p - 1$-nek. Emiatt s gyökei bizonyos p-edik egységgyökök, mindegyik egyszeres (és mindegyik K-ban van). Ezek között van egy $\varepsilon \neq 1$ szám is, mert különben $s(x) = x - 1$ lenne, ami azt jelentené, hogy ψ maga az identitás. Tudjuk lineáris algebrából, hogy a minimálpolinom minden gyöke sajátérték, ezért van olyan $0 \neq \beta \in L$ (a hozzá tartozó sajátvektor), hogy $\psi(\beta) = \varepsilon\beta$. Persze $\beta \notin K$, hiszen ψ fixálja K elemeit, és $\varepsilon \neq 1$. De akkor

$$\psi(\beta^p) = \psi(\beta)^p = (\varepsilon\beta)^p = \varepsilon^p\beta^p = \beta^p\,.$$

Mivel ψ fixponthalmaza K, ezért $\beta^p \in K$. □

A most használt lineáris algebrai tételt, nevezetesen, hogy a minimálpolinom gyökei mind sajátértékek, a Cayley-Hamilton tételből szokás levezetni (erről szó is lesz később a könyvben, lásd 7.6.6. Tétel). Valójában azonban van egy rövid, egyszerű bizonyítása is (6.9.16. Feladat).

Az előző lemmát az úgynevezett *Lagrange-rezolvens* segítségével elemi számolással is lehet bizonyítani. Ezt a 6.9.17. Feladatban mutatjuk be. A következő szakaszban meglátjuk, hogy a Lagrange-rezolvens konkrét gyökképletek, például a Cardano-képlet megtalálásában is segítséget nyújt.

Most már be tudjuk látni, hogy minden komplex egységgyök $\mathbb{Q}$ fölött gyökkifejezés.

6.9.10. Következmény. *Legyen $K \leq \mathbb{C}$ test, amelynek minden eleme gyökkifejezés egy $K_0 \leq K$ test fölött. Ha ε primitív n-edik egységgyök, akkor $K(\varepsilon)$ minden eleme is gyökkifejezés K_0 fölött.*

Bizonyítás. Indukcióval bizonyítunk n szerint, vagyis föltehetjük, hogy az állítást már igazoltuk az összes m-edik egységgyökre, ahol $m < n$, és minden olyan testre, amelynek minden eleme gyökkifejezés K_0 fölött.

A $\varphi(n) < n$ szám minden p prímosztójára bővítsük K-t egy p-edik primitív egységgyökkel. A kapott L test elemei az indukciós föltevés miatt gyökkifejezések K_0 fölött.

Tudjuk, hogy az $L \leq L(\varepsilon)$ bővítés G Galois-csoportja $\mathbb{Z}_n^\times$-nek részcsoportja (6.9.3. Gyakorlat), vagyis kommutatív (így feloldható), és rendje osztója $\varphi(n)$-nek. Vegyük G egy kompozícióláncát, és tekintsük a hozzá tartozó

$$L = L_0 < L_1 < \ldots < L_\ell = L(\varepsilon)$$

testláncot. Az itt szereplő bővítések fokai olyan p prímek, amik $\varphi(n)$-nek osztói, és így a p-edik egységgyökök már benne vannak L-ben. Így az előző 6.9.9. Lemma segítségével ezen a láncon végighaladva látjuk, hogy mindegyik L_i elemei is gyökkifejezések K_0 fölött. Így végül $K(\varepsilon) \leq L(\varepsilon)$ elemei is azok. □

A 6.9.4. Tétel megfordításának áhított bizonyítása lényegében ugyanaz, mint ami most elhangzott, csak $\mathbb{Z}_n^\times$ helyett tetszőleges Galois-csoport fog benne szerepelni. Az előző következmény lehetővé teszi, hogy a szükséges egységgyököket bevegyük.

6.9.11. Tétel. *Legyen $K \leq \mathbb{C}$ test, és $K \leq L$ egy olyan véges normális bővítés, amelynek a Galois-csoportja feloldható. Ekkor L minden eleme gyökkifejezés K fölött.*

A bizonyítás most is kicsit vázlatos lesz, mint a 6.9.4. Tétel esetében.

Bizonyítás. Legyen $n = |L : K|$, és ε primitív n-edik egységgyök. Ekkor a $K \leq L(\varepsilon)$ bővítés a 6.3.18. Gyakorlat szerint szintén normális, hiszen a $\Phi_n \in K[x]$ felbontási teste L fölött. Legyen G ennek a Galois-csoportja. Ez szintén feloldható. Valóban, ha N jelöli az L közbülső testhez tartozó normálosztót, akkor G/N a $K \leq L$ Galois-csoportja, ami a feltétel szerint feloldható, N pedig az $L \leq L(\varepsilon)$ Galois-csoportja, ami része $\mathbb{Z}_n^\times$-nek, és így szintén feloldható. Ezért G is feloldható a 4.12.20. Feladat miatt.

Az előző következmény miatt a $K(\varepsilon)$ elemei gyökkifejezések K fölött. Jelölje H a G csoport $K(\varepsilon)$-hoz tartozó részcsoportját, ez is feloldható (4.12.19. Feladat). Belátjuk, hogy H rendje osztója n-nek. Mivel a $K(\varepsilon)$ és L testek együtt generálják $L(\varepsilon)$-t, ezért e két testet $L(\varepsilon)$ résztestei közül csak L tartalmazza. Ez a főtétel szerint azt jelenti, hogy G-nek az egyetlen részcsoportja, ami H-nak és N-nek is része, az egyelemű részcsoport. Más szóval $H \cap N = \{id\}$. Az első izomorfizmus-tétel miatt

$$H \cong H/(H \cap N) \cong HN/N \leq G/N\,.$$

Vagyis H izomorf G/N egy részcsoportjával. De akkor H rendje osztója G/N rendjének, ami n.

Vegyük a H egy kompozícióláncát, és az ennek megfelelő testláncot $K(\varepsilon)$ és $L(\varepsilon)$ között. A szereplő bővítések foka csupa olyan p prímszám, amely osztója H rendjének, tehát n-nek is. Ezért $K(\varepsilon)$ tartalmazza a p-edik egységgyököket, és így a 6.9.9. Lemma segítségével ezen a testláncon végighaladva azt kapjuk, hogy a szereplő testek mindegyik eleme gyökkifejezés K fölött. Speciálisan $L \leq L(\varepsilon)$ minden eleme is az. □

6.9.12. Következmény. *Ha az $f \in K[x]$ irreducibilis polinom egyik gyöke gyökkifejezés K fölött, akkor mindegyik gyöke az.*

Bizonyítás. Az f felbontási testének Galois-csoportja feloldható a 6.9.4. Tétel miatt. Így a most bizonyított tétel szerint ennek a testnek minden eleme gyökkifejezés, az f többi gyöke is. □

Az előző bizonyításban az egységgyökök hozzávétele nemcsak a bizonyítást segítő ötlet, hanem kényszer, a Casus irreducibilis jelensége! Ezt a következő szakaszban fogjuk megérteni.

Gyakorlatok, feladatok

6.9.13. Gyakorlat. Igazoljuk, hogy az $x^5 - 15x - 3$, $x^5 - 35x + 5$, $x^5 - 15x^4 + 6$ polinomok egyike sem oldható meg gyökjelekkel.

6.9.14. Gyakorlat. Legyen p prím, és K nulla karakterisztikájú test, ami nem tartalmazza egyik p-edik primitív egységgyököt sem. Mutassuk meg, hogy ha $a \in K$, akkor $x^p - a$ vagy irreducibilis K fölött, vagy pontosan egy gyöke van K-ban. Mi lesz a Galois-csoportja ebben a második esetben?

6.9.15. Gyakorlat. Legyen K test és $a \in A$. Mutassuk meg, hogy az $x^n - a$ polinom felbontási testének Galois-csoportja mindig feloldható (függetlenül a K karakterisztikájától, és attól, hogy K milyen egységgyököket tartalmaz).

6.9.16. Feladat. Mutassuk meg (a Cayley-Hamilton tétel fölhasználása nélkül), hogy ha A lineáris transzformáció egy T test fölötti véges dimenziós vektortéren, akkor a minimálpolinomjának minden $\lambda \in T$ gyöke sajátérték.

6.9.17. Feladat. Legyen p prímszám, és jelölje $\varepsilon_1, \ldots, \varepsilon_p = 1$ a p-edik komplex egységgyököket. Tegyük föl, hogy ezek elemei a K testnek, és $K \leq L$ egy p-edfokú normális bővítés, melynek Galois-csoportját egy ψ elem generálja. Ha $\gamma \in L$, akkor legyen

$$(\varepsilon_j, \gamma) = \gamma + \psi(\gamma)/\varepsilon_j + \ldots + \psi^{p-1}(\gamma)/\varepsilon_j^{p-1} = \sum_{\ell=0}^{p} \psi^\ell(\gamma)\varepsilon_j^{-\ell}$$

(ezt a kifejezést hívjuk *Lagrange-rezolvensnek*). Mutassuk meg, hogy a $\beta = (\varepsilon_j, \gamma)$ számra $\psi(\beta) = \varepsilon_j\beta$, és hogy γ és j megválasztható úgy, hogy $\beta \notin K$ legyen. Adjunk ennek segítségével új bizonyítást a 6.9.9. Lemmára.

6.10. A legfeljebb negyedfokú egyenletek

Ebben a szakaszban a harmad- és negyedfokú egyenleteknek a 3.8. Szakaszban megismert megoldási módszereit vizsgáljuk meg a Galois-elmélet szemszögéből, és megértjük a Casus irreducibilis jelenségét.

Elsőként megmutatjuk, miért kell a gyökképlet vizsgálatakor az alaptestbe bevenni a megfelelő egységgyököket. Egy példával kezdjük: elkészítjük $\mathbb{Q}$-nak egy harmadfokú, valós, normális bővítését.

6.10.1. Gyakorlat. Legyen $\varepsilon = \cos 40^\circ + i \sin 40^\circ$ egy kilencedik primitív egységgyök. Mutassuk meg, hogy $\mathbb{Q}(\varepsilon)$ valós elemei egy L résztestet alkotnak, amely $\mathbb{Q}$-nak harmadfokú normális bővítése. Igazoljuk azt is, hogy L az $x^3 - 3x + 1$ polinom felbontási teste $\mathbb{Q}$ fölött, és hogy ennek a polinomnak a gyökei $2\cos 40^\circ$, $2\cos 80^\circ$ és $2\cos 160^\circ$. Írjuk föl $\cos 40^\circ$-ot gyökkifejezésként.

Az előző gyakorlatban szereplő a $\mathbb{Q} \leq L$ harmadfokú bővítés nem kapható meg egy köbgyök hozzávételével. Ha ugyanis $L = \mathbb{Q}(\sqrt[3]{d})$ lenne, akkor, mivel $\mathbb{Q} \leq L$ normális bővítés, az $x^3 - d$ (irreducibilis) polinom többi gyöke is benne lenne L-ben. Ez nem igaz, hiszen ezek a gyökök nem is valós számok. Ugyanakkor L elemei gyökkifejezések, hiszen $L \subseteq \mathbb{Q}(\varepsilon)$. Sőt, Cardano képlete segítségével fel is írhatnánk ezeket a kifejezéseket. Ekkor azonban kilépünk a valós számok közül!

A geometriai szerkeszthetőségnél nem lép fel a Casus irreducibilis jelensége: a 6.8.17. Tétel magában foglalja azt az állítást, hogy ha $K_0 \leq L$ normális, 2-hatvány fokú bővítés, és K egy közbülső test, akkor a K maga is elérhető K_0-ból másodfokú bővítések sorozatával. Ennek két oka van. Az első ok a 2-csoportok szép szerkezete (lásd a tétel bizonyítását). Ez önmagában még nem lenne elég, hiszen a fenti példában szereplő $\mathbb{Z}_9^\times \cong \mathbb{Z}_6^+$ Galois-csoport is „szép". A másik ok az, hogy a szerkeszthetőségnél második egységgyökökre van szükség, és a ± 1 minden testben benne van. A fenti $\mathbb{Q} \leq L$ bővítés hiába harmadfokú és normális, a harmadik egységgyökök hiányában nem kapható meg egy köbgyök adjungálásával.

A Casus irreducibilis általánosabb annál, amit a most vizsgált példa mutat. A valósban maradva $\cos 40^\circ$ nemcsak egy köbgyökvonással, hanem ennél bonyolultabb módon sem írható föl gyökképletként.

6.10.2. Tétel [A Casus irreducibilis tétele]. *Legyen $f \in \mathbb{Q}[x]$ harmadfokú irreducibilis polinom, amelynek mindegyik gyöke valós. Ekkor f egyik gyöke sem írható föl olyan gyökkifejezéssel, amelynél mindegyik gyökvonás a valósban marad.*

Bizonyítás. Tegyük föl, hogy f-nek az egyik gyöke valósban maradó gyökkifejezés. Ekkor létezik a 6.9.8. Definícióban megadott típusú

$$\mathbb{Q} = K_0 < K_1 < \ldots < K_n \leq \mathbb{R}$$

testlánc, hogy K_n-ben f-nek van gyöke. Válasszuk ezt a testláncot úgy, hogy n a lehető legkisebb legyen. Ekkor f-nek nem lehet gyöke K_{n-1}-ben, és ezért (harmadfokú lévén) irreducibilis K_{n-1} fölött. Legyen $\beta \in K_n$ gyöke f-nek. Mivel a $K_{n-1} \leq K_n$ bővítés foka egy p prímszám, $K_n = K_{n-1}(\beta)$, és így $p = 3$. A definíció szerint $K_n = K_{n-1}(\sqrt[3]{\alpha})$, ahol $\alpha \in K_{n-1}$ és $x^3 - \alpha$ irreducibilis K_{n-1} fölött.

Legyen L az f felbontási teste K_{n-1} fölött. Ekkor $L \leq \mathbb{R}$, mert f gyökei valósak. A $K_{n-1} \leq L$ normális bővítés tartalmazza az irreducibilis $x^3 - \alpha$ polinom egyik gyökét, és ezért az összeset tartalmazza. De akkor $L \leq \mathbb{R}$-ben benne lennének a harmadik komplex egységgyökök, amik nem valós számok. □

A legfeljebb negyedfokú egyenletek Galois-csoportjának vizsgálatához igen hasznos eszköz az alábbi állítás.

6.10.3. Lemma. *Tegyük föl, hogy f egy n-edfokú polinom a K nulla karakterisztikájú test fölött, melynek nincs többszörös gyöke a felbontási testében. Ekkor f Galois-csoportja akkor és csak akkor része az f gyökein ható alternáló csoportnak, ha f diszkriminánsa egy K-beli elem négyzete.*

Bizonyítás. Legyen $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$, ahol az $\alpha_1, \dots, \alpha_n$ gyökök az f polinom K fölötti felbontási testét generálják. A 3.7.6. Tétel szerint, ha

$$d = c^{n-1} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)\,,$$

akkor az f diszkriminánsa d^2. Mivel f-nek nincs többszörös gyöke, ezért $d \neq 0$. A d^2 akkor és csak akkor egy K-beli elem négyzete, ha $d \in K$ (hiszen d^2 két négyzetgyöke d és $-d$, és ha az egyik K-beli, akkor a másik is).

Ha az f polinom G Galois-csoportjának egy φ elemét alkalmazzuk a fenti kifejezésre, akkor az eredmény d illetve $-d$, attól függően, hogy φ páros vagy páratlan permutáció az f gyökeinek halmazán. Mivel $d \neq -d$, a G pontosan akkor része a gyökök halmazán ható alternáló csoportnak, ha G minden eleme fixen hagyja a d elemet, vagyis ha $d \in K$. □

E lemmát és a Lagrange-rezolvenst (6.9.17. Feladat) először a másodfokú polinomok nagyon egyszerű esetén illusztráljuk, mert ez mintát szolgáltat a magasabb fokú polinomok vizsgálatához is. Tudjuk a 6.6.18. Gyakorlatból, hogy egy f polinom Galois-csoportja akkor és csak akkor tranzitív az f gyökeinek a halmazán, ha f irreducibilis. Ha tehát f másodfokú, és nincs többszörös gyöke, akkor két eset lehetséges. Ha f diszkriminánsa egy K-beli elem négyzete, akkor f Galois-csoportja triviális, az f nem irreducibilis, hanem két elsőfokú polinom szorzata. Ha f diszkriminánsa nem négyzetelem, akkor viszont az f Galois-csoportja a kételemű csoport, és f irreducibilis. Mindez persze a másodfokú egyenlet megoldóképletéből is nyilvánvaló.

Legyen $f(x) = x^2 + px + q$ másodfokú irreducibilis, normált polinom K fölött, és α_1, α_2 az f gyökei (a felbontási testében). A Galois-csoport egyetlen nemtriviális ψ automorfizmusa megcseréli ezeket a gyököket. A

$$d = (-1, \alpha_1) = \alpha_1 - \psi(\alpha_1) = \alpha_1 - \alpha_2$$

Lagrange-rezolvensre $\psi(d) = -d$, vagyis $d^2 \in K$. Ez a d ugyanaz, mint a 6.10.3. Lemma bizonyításában szereplő d elem, vagyis d^2 az f diszkriminánsa. A gyökök és együtthatók összefüggéséből $\alpha_1 + \alpha_2 = -p$, és a lineáris egyenletrendszert megoldva $\alpha_1 = (-p+d)/2$, továbbá $\alpha_2 = (-p-d)/2$ adódik. A Lagrange-rezolvens segítségével tehát a másodfokú egyenlet gyökképletét is megkaptuk (a $d = p^2 - 4q$ értékét már kiszámoltuk determinánsok segítségével a 3.7.10. Gyakorlatban). Ugyan föltettük, hogy f irreducibilis, de ha a 6.9.6. Tétel mintájára a p és q elemeket határozatlannak tekintjük, akkor ez automatikusan teljesül.

6.10.4. Gyakorlat. Igazoljuk, hogy ha $c \neq 0$ és d a K test elemei, akkor az $f \in K[x]$ polinom Galois-csoportja ugyanaz, mint az $f(cx+d)$ polinomé (vagyis a lineáris helyettesítés nem változtat a Galois-csoporton).

Az előző gyakorlat szerint a harmadfokú egyenletek vizsgálatakor föltehetjük, hogy az egyenletben nem szerepel x^3-ös tag. Legyen tehát $f(x) = x^3 + px + q$ harmadfokú *irreducibilis* polinom a nulla karakterisztikájú K test fölött, L az f felbontási teste K fölött, és G ennek a Galois-csoportja. Ha D jelöli a Cardano-képletben a négyzetgyökjel alatti kifejezést, akkor f diszkriminánsa $-108D = -27q^2 - 4p^3$ (3.7.11. Gyakorlat). A G az f gyökein ható permutációcsoport, és mivel f irreduciblis, ez a hatás tranzitív (6.6.18. Gyakorlat). Így G-re csak két lehetőség van: $G = A_3$ (az alternáló csoport), vagy $G = S_3$. A két esetet az különbözteti meg, hogy az f polinom $-108D$ diszkriminánsa négyzetelem-e K-ban vagy sem (6.10.3. Lemma).

Ha $-108D$ négyzetelem K-ban, akkor a Cardano-képletben a négyzetgyökvonás már K-ban elvégezhető, és a $K_0 \leq L$ bővítés harmadfokú. Ha K tartalmazza a primitív harmadik egységgyököket, akkor f gyökei egy köbgyök adjungálásával kaphatók, különben viszont nem. Ha $-108D$ nem négyzetelem K-ban, akkor $G = S_3$, és $K(\sqrt{-108D})$ másodfokú bővítés, amely a Galois-csoportban egy kettő indexű normálosztónak, vagyis az A_3 részcsoportnak felel meg. Az f gyökei egy-egy harmadfokú bővítést generálnak, amelyek megfelelnek az S_3 kételemű részcsoportjainak. Ezzel az összes közbülső testet áttekintettük, hiszen S_3-nak nincs több nemtriviális részcsoportja.

6.10.5. Gyakorlat. Legyen L az $f(x) = x^3 + px + q \in K[x]$ irreducibilis polinom felbontási teste a nulla karakterisztikájú K test fölött, $\alpha_1, \alpha_2, \alpha_3 \in L$ az f gyökei, G az L/K bővítés Galois-csoportja, végül

$$s = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 \quad \text{és} \quad t = \alpha_1^2\alpha_3 + \alpha_3^2\alpha_2 + \alpha_2^2\alpha_1 .$$

Igazoljuk az alábbiakat.

(1) $s + t = 3q \in K$.
(2) $s - t = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$, és így $(s-t)^2 = -108D = -27q^2 - 4p^3$ az f diszkriminánsa.
(3) Az s és t fixen marad G minden harmadrendű eleménél, és így $K(s) = K(t)$ az $A_3 \leq G$ részcsoporthoz tartozó résztest.
(4) Az s és t kicserélődik G minden másodrendű eleménél (ha van ilyen G-ben).

Adjunk ennek felhasználásával új bizonyítást arra, hogy ha f diszkriminánsa nem négyzetelem K-ban, akkor $G \cong S_3$, különben pedig $G \cong A_3$.

A Cardano-képletet is megkaphatjuk a Lagrange-rezolvensből a következő módon. Tegyük föl, hogy $f(x) = x^3 + px + q$ általános együtthatós a $K = \mathbb{Q}(\varepsilon)$ fölött, ahol ε primitív harmadik egységgyök. Ekkor a $d^2 = -108D \in K$ diszkrimináns nem négyzetelem K-ban (mert ha az lenne, akkor minden konkrét polinom esetében is az lenne), és f irreducibilis is (mert ha lenne felbontása, akkor minden konkrét polinom esetében egy felbontást kapnánk). Ezért a Galois-csoport S_3. Jelölje f gyökeit α_1, α_2 és α_3. Legyen ψ az

a harmadrendű automorfizmus, amely ezeket körbepermutálja: $\psi : \alpha_1 \to \alpha_2 \to \alpha_3 \to \alpha_1$, és φ az az automorfizmus, amely a α_2 és α_3 gyököket kicseréli, az α_1 elemet pedig fixen hagyja. A φ a d elemet nem fixálhatja, mert a másodfokú d és a harmadfokú α_1 generálja az egész bővítést, és φ nem az identitás. De $d^2 \in K$ fixen marad φ-nél, és így $\varphi(d) = -d$. Legyen

$$u = (\alpha_1, \varepsilon) = \alpha_1 + \alpha_2/\varepsilon + \alpha_3/\varepsilon^2$$

a Lagrange-rezolvens. A 6.9.17. Feladat szerint $\psi(u) = \varepsilon u$ és $u^3 \in K(d)$. Továbbá

$$v = \varphi(u) = \alpha_1 + \alpha_3/\varepsilon + \alpha_2/\varepsilon^2 .$$

A gyökök és együtthatók összefüggése miatt $\alpha_1 + \alpha_2 + \alpha_3 = 0$, és így az ε-ra vonatkozó elemi összefüggéseket ($\varepsilon^{-1} + \varepsilon^{-2} = -1$) is felhasználva adódik, hogy

$$u + v = 2\alpha_1 - \alpha_2 - \alpha_3 = 3\alpha_1 .$$

Innen $\alpha_1 = (u + v)/3$ adja az egyenlet egyik gyökét. Az S_3 csoportban $\psi\varphi = \varphi\psi^2$, ahonnan $\psi(v) = \varphi\psi^2(u) = \varphi(\varepsilon^2 u) = \varepsilon^2 v$. Így ψ-t kétszer alkalmazva $\alpha_2 = (\varepsilon u + \varepsilon^2 v)/3$ és $\alpha_3 = (\varepsilon^2 u + \varepsilon v)/3$ adódik, azaz u és v segítségével (két köbgyök összegeként) megkaptuk az egyenlet három gyökét. Azt, hogy $u/3$ és $v/3$ tényleg a Cardano-képletben szereplő két köbgyök, az Olvasó például úgy ellenőrizheti, hogy elvégzi a gyökök és együtthatók összefüggése alapján az

$$uv = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 = -3p$$

és

$$u^3 + v^3 = (u + v)\big((u + v)^2 - 3uv\big) = 27(\alpha_1^3 + \alpha_1 p) = -27q$$

számolásokat. A lényeg azonban az, hogy kiderült, miért kézenfekvő az ismeretlent két köbgyök összegének formájában keresni.

Ennél egyszerűbb heurisztika azt mondani, hogy mivel az ismeretlen $K(d)$ fölött harmadfokú, kereshetjük $a_0 + a_1 u + a_2 u^2$ formában, ahol u egy $K(d)$-beli elem köbgyöke. Abból, hogy a gyökök összege nulla, könnyű látni, hogy $a_0 = 0$, és így az ismeretlen tényleg két köbgyök összege. A fenti számolás azonban azt is mutatja, miért jogos a 13. oldalon található gondolatmenetben az (1.3) egyenletrendszer megoldására áttérni.

A negyedfokú egyenlet Galois-csoportjának kiszámítását feladatsorozat formájában mutatjuk be. Itt is *irreducibilis* polinomra szorítkozunk (az irreducibilitás a 3.8.9. Feladat segítségével ellenőrizhető, melynek megoldása tetszőleges nulla karakterisztikájú test fölött érvényben marad). A diszkrimináns mellett a harmadfokú rezolvenst is használni fogjuk (lásd a 3.8.4. Tétel bizonyítását).

6.10.6. Feladat. Legyen K nulla karakterisztikájú test, $f \in K[x]$ negyedfokú irreducibilis polinom, melynek harmadfokú rezolvense g. Igazoljuk az alábbi állításokat.

(1) Ha g irreducibilis K fölött, akkor az f Galois-csoportja A_4, illetve S_4 attól függően, hogy az f diszkriminánsa négyzetelem-e K-ban, vagy sem.
(2) Ha g elsőfokú tényezőkre bomlik K fölött, akkor az f Galois-csoportja a Klein-csoport, és f diszkriminánsa négyzetelem K-ban.

(3) Ha g egy első- és egy másodfokú irreducibilis polinom szorzatára bomlik K fölött, akkor az f Galois-csoportja vagy a D_4 diédercsoporttal, vagy a $\mathbb{Z}_4^+$ ciklikus csoporttal izomorf, és f diszkriminánsa biztosan *nem* négyzetelem K-ban.

Tehát már csak azt kell eldönteni, hogy az előző feladat (3) esetében a Galois-csoport ciklikus-e, vagy pedig a diédercsoport. Azért, hogy egyszerűbb képleteket kapjunk, föltesszük, hogy a polinomban nem szerepel x^3-ös tag (ez egy $x \mapsto x + c$ alakú helyettesítéssel érhető el). Elsőként azokat a polinomokat vizsgáljuk meg, amelyekben nincs x-es tag sem. Ezek irreducibilitását a 3.8.10. Gyakorlat segítségével ellenőrizhetjük.

6.10.7. Feladat. Legyen $f(x) = x^4 + bx^2 + d \in K[x]$ irreducibilis polinom, ahol K nulla karakterisztikájú test. Mutassuk meg a következő állításokat.

(1) Ha d négyzetelem K-ban, akkor f Galois-csoportja a Klein-csoport.
(2) Ha d nem négyzetelem K-ban, akkor f Galois-csoportja $\mathbb{Z}_4^+$, illetve D_4, attól függően, hogy $d(b^2 - 4d)$ négyzetelem-e K-ban, vagy sem.

A másik eset, amikor az f polinomban van x-es tag. Ekkor az irreducibilitás ellnőrzéséhez a 3.8.9. Feladatot használhatjuk.

6.10.8. Feladat. Legyen $f(x) = x^4 + bx^2 + cx + d \in K[x]$ irreducibilis polinom, ahol K nulla karakterisztikájú test és $c \neq 0$. Tegyük föl, hogy az f polinom g harmadfokú rezolvensének u az egyetlen gyöke K-ban. Mutassuk meg, hogy ha $(2u-b)(2u+b)^2 - 4c^2$ négyzetelem K-ban, akkor f Galois-csoportja $\mathbb{Z}_4^+$, különben pedig D_4.

Gyakorlatok, feladatok

6.10.9. Gyakorlat. Igaz-e a $\mathbb{Z}_3$ test fölött, hogy minden harmadfokú polinomból eltüntethető a másodfokú tag egy lineáris helyettesítéssel? Megoldható-e minden $x^3 + px + q = 0$ alakú egyenlet $\mathbb{Z}_3$ fölött a Cardano-képlet módszerével? Megkaphatók-e a harmadfokú egyenletek megoldásai gyökkifejezésként?

6.10.10. Gyakorlat. Legyen $K \subseteq \mathbb{R}$ egy szerkesztési feladatban az alapadatok által generált test és $f \in K[x]$ negyedfokú irreducibilis polinom. Igazoljuk, hogy az alábbiak ekvivalensek.

(1) Az f valamelyik gyöke szerkeszthető.
(2) Az f összes gyöke szerkeszthető.
(3) Az f harmadfokú rezolvensének van gyöke K-ban.

6.11. Összefoglaló

III. rész

A modern algebra néhány fejezete

7. MODULUSOK

Követném egy pólus ívét
Simuló-sík formájában,
Szimmetrikus tenzor ízét
Éreznénk bit alakjában,

Megszámlálnám tagjaidat
— Vajha volnék rá alkalmas! —
És mátrixszá rendeznélek,
Gyönyörű végtelen halmaz!

Stanisław Lem: *Kiberiáda*
(Murányi Beatrix fordítása)

Az algebrán belül a modulusok elsődleges haszna az, hogy segítségükkel felderíthetjük a gyűrűk szerkezetét. Híres geometriai és topológiai tételek bizonyítására is alkalmazzák a modulusokat, az úgynevezett homológiaelmélet keretében. A fizikával való kapcsolatot a tenzorszorzat vizsgálata fogja jelenteni.

A modulusok témakörét éppen csak érintjük. Néhány alapvető fogalommal való megismerkedés után egyetlen komoly tételt látunk be, a véges Abel-csoportok alaptételének, és a Jordan-féle normálalakról szóló lineáris algebrai tételnek közös általánosítását.

7.1. Részmodulusok, homomorfizmusok

Amikor a modulusokkal először találkozunk, úgy érdemes gondolni rájuk, mint a vektorterekre, ahol azonban a skalárok nem testet, hanem csak gyűrűt alkotnak.

7.1.1. Definíció. Azt mondjuk, hogy M bal oldali *modulus* az R gyűrű fölött, ha M Abel-csoport a $+$ és $-$ műveletekre, és minden $r \in R$ és $m \in M$ esetén értelmezve van az $rm \in M$ szorzat, a vektortereknél megszokott azonosságokkal. Vagyis tetszőleges $r, s \in R$, $m, n \in M$ esetén

(1) $r(m+n) = rm + rn$;
(2) $(r+s)m = rm + sm$;
(3) $(rs)m = r(sm)$.

Ha R egységelemes, és $m \in M$ esetén

(4) $1m = m$

is teljesül, akkor M-et *unitér* modulusnak nevezzük. ***Ebben a könyvben minden modulusról föltesszük, hogy unitér*** (hacsak nem állítjuk az ellenkezőjét).

A fenti axiómákból $0m = 0 = r0$ és $(-r)m = -(rm) = r(-m)$ következik tetszőleges $r \in R$ és $m \in M$ esetén (vö. 2.2.20. Feladat). Modulusra nemcsak a vektorterek szolgáltatnak példát, hanem az Abel-csoportok is, mint a $\mathbb{Z}$ gyűrű fölötti modulusok.

7.1.2. Gyakorlat. Mutassuk meg, hogy tetszőleges A Abel-csoport modulus lesz az egész számok $\mathbb{Z}$ gyűrűje fölött, ha az ng szorzatot a $g \in A$ elem szokásos egész számszorosaként értelmezzük.

A harmadik főpéldánk modulusra egy lineáris transzformáció hatását írja le egy vektortéren. Ez a modulus szokatlanabb az első két példánál, és ezért azt javasoljuk, hogy az Olvasó elsősorban vektortereket és Abel-csoportot képzeljen maga elé, amikor a bizonyításokat tanulmányozza. Az alábbi modulussal több gyakorlat megoldása során ismerkedünk majd meg közelebbről. A 7.1.9. Gyakorlatban további példákat láthatunk modulusra.

7.1.3. Definíció. Legyen V vektortér egy T test fölött, és A egy lineáris transzformáció V-n. Definiáljuk az $M = M(A, V)$ modulust a $T[x]$ polinomgyűrű fölött úgy, hogy alaphalmaza V, összeadása V összeadása legyen, és $f \in T[x]$, $v \in V$ esetén $fv = \big(f(A)\big)(v)$. Ugyanígy beszélünk $M(A, V)$-ről akkor is, ha $A \in T^{n\times n}$ egy $n \times n$-es mátrix, és $V = T^n$, ekkor is $fv = \big(f(A)\big)(v)$.

Amikor egy új struktúrával ismerkedünk meg, akkor elsőnek mindig érdemes felderíteni, mit mondhatunk a részstruktúrákról és a generálásról, a homomorfizmusokról és magjaikról, a direkt szorzatokról, és hogy vannak-e, és hogyan írhatók le a szabadok a struktúráink között. Ezt a programot követjük most is. Látszólag a lineáris algebra elemi részeit ismételjük át, de azért új jelenségekkel is szembesülünk.

Első lépésként egy fokkal precízebbé kell tenni a modulus definícióját. Az eddigi algebrai struktúrákban (csoportokban, gyűrűkben) csak egy alaphalmaz volt, most azonban kettő van: R és M. Ha tehát részmodulusról akarunk beszélni, akkor melyiknek vegyük egy részhalmazát? Esetleg mindkettőnek? Az a megközelítés bizonyult szerencsésnek, amikor csak M-nek vesszük egy részét, az R változatlan marad. Ennek oka talán az, hogy általában egy adott R gyűrű szerkezetének a megértése a cél, és ezt a fölötte vett összes modulus együttes vizsgálatával érhetjük el. A lineáris algebrában, amikor altérről beszéltünk, szintén változatlanul hagytuk a skalárok testét.

Technikailag ezt a következőképpen valósíthatjuk meg. Az rm szorzatot tekinthetnénk kétváltozós műveletnek is. Jobb azonban, ha minden $r \in R$ esetén az r-rel való szorzást az M halmazon értelmezett egyváltozós műveletnek tekintjük, amely m-hez rm-et rendel. Ebben az esetben a megszokott fogalmak (rész, homomorfizmus, direkt szorzat) tökéletesen működnek majd: például ha részmodulust tekintünk, akkor az R gyűrű nem változhat meg, hiszen a résznek *ugyanazokra a műveletekre* kell modulusnak lennie, mint az egésznek.

7.1.4. Definíció. Ha M egy bal oldali R-modulus, akkor az $N \subseteq M$ halmazt *részmodulusnak* nevezzük, ha maga is R-modulus az M műveleteire nézve. Jelölés: $N \leq M$. A $\{0\}$ és az M az M modulus *triviális részmodulusai*.

Mivel a modulus-axiómák is azonosságok, a 2.2.24. Feladat megoldásához hasonlóan láthatjuk, hogy ha M egy R-modulus, akkor az $N \subseteq M$ akkor és csak akkor részmodulus, ha részcsoport, és zárt az R elemeivel való szorzásra, azaz $r \in R$ és $n \in N$ esetén $rn \in N$.

A részmodulusokhoz kapcsolódik a *generált részmodulus* fogalma. Az eddig látott generálás-fogalmakhoz hasonlóan ha $X \subseteq M$, akkor az X által generált részmodulus az a legszűkebb részmodulusa M-nek, amely X-et tartalmazza, jele $\langle X \rangle_R$, vagy csak egyszerűen $\langle X \rangle$. Ha az X által generált részmodulus az egész M, akkor X-et *generátorrendszernek* nevezzük.

A generált részmodulus mindig létezik, mert az egyetlen ilyen részmodulus az X-et tartalmazó részmodulusok metszete. Elemeit a lineáris algebrában megszokott lineáris kombinációk segítségével kaphatjuk meg.

7.1.5. Gyakorlat. Igazoljuk, hogy az X által generált részmodulus az összes olyan

$$r_1 x_1 + \ldots + r_k x_k$$

lineáris kombinációkból áll, ahol $r_i \in R$, $x_i \in X$, a k pedig nemnegatív egész szám.

Speciálisan ha $m \in M$, akkor az M által generált részmodulus az rm alakú elemekből áll, ahol r befutja R-et. A csoportelméleti komplexusszorzás mintájára ezt a halmazt néha Rm-nek is írjuk. Általában legyen

$$rX = \{rm \,:\, m \in X\} \quad \text{és} \quad Ym = \{rm \,:\, r \in Y\},$$

ahol $r \in R$, $X \subseteq M$, $m \in M$ és $Y \subseteq R$.

Amikor modulusok között homomorfizmust, azaz művelettartó leképezést akarunk értelmezni, akkor ehhez ismét az szükséges, hogy a két modulusnak „ugyanazok" legyenek a műveletei, tehát *ugyanazon gyűrű fölötti modulusok legyenek* (miként lineáris leképezést is csak ugyanazon test fölötti vektorterek között értelmezünk).

7.1.6. Definíció. Legyen R gyűrű, és M, N bal oldali R-modulusok. Azt mondjuk, hogy a $\varphi : M \to N$ leképezés modulus-homomorfizmus (vagy R-homomorfizmus), ha művelettartó, azaz tetszőleges $r \in R$ és $m_1, m_2, m \in M$ esetén

(1) $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$ (összegtartás);
(2) $\varphi(rm) = r\varphi(m)$ (az r-rel szorzás tartása).

Az M-ből N-be menő R-homomorfizmusok halmazát $\mathrm{Hom}_R(M, N)$ jelöli.

Érdemes külön is meggondolni, hogy a (2) tulajdonság mit fejez ki: mindegy, hogy először a műveletet (az r-rel szorzást) alkalmazzuk, és utána a homomorfizmust (a φ-t), vagy pedig fordítva. A csoportokhoz hasonlóan értelmezzük egy φ homomorfizmus *képét*

$$\mathrm{Im}(\varphi) = \{\varphi(m) \,:\, m \in M\} \leq N$$

és *magját*:

$$\mathrm{Ker}(\varphi) = \{m \in M \,:\, \varphi(m) = 0\} \leq M\,.$$

A kép tetszőleges részmodulus lehet. Amikor csoportokat vizsgáltunk, akkor a mag speciális részcsoport volt, így kaptuk a normálosztó fogalmát. A gyűrűk esetében az ideálokat kaptuk. Most egyszerűbb a helyzet: a homomorfizmusok magjai pontosan a részmodulusok. A bizonyításhoz a *faktormodulus* fogalmát kell bevezetnünk.

7.1.7. Gyakorlat. Mutassuk meg, hogy tetszőleges modulushomomorfizmus magja részmodulus. Megfordítva, ha N részmodulusa M-nek, akkor definiáljuk az M/N faktormodulust úgy, hogy az M/N faktorcsoport elemein az R elemeivel való szorzást az

$$r(m + N) = rm + N$$

képlettel (azaz reprezentánsokkal) értelmezzük. Mutassuk meg, hogy ez a szorzás jóldefiniált, és M/N bal oldali R-modulus lesz. Igazoljuk, hogy az

$$m \mapsto m + N$$

leképezés R-homomorfizmus, melynek magja N (ezt most is *természetes homomorfizmusnak* nevezzük).

7.1.8. Gyakorlat. Fogalmazzuk meg, és bizonyítsuk be modulusokra is a homomorfizmustételt, és a két izomorfizmus-tételt. Adjuk meg a kapcsolatot a faktormodulus részmodulusai, és az eredeti modulusnak a magot tartalmazó részmodulusai között.

Egy csoportot, gyűrűt akkor nevezünk egyszerűnek, ha csak triviális homomorfizmusai voltak. Mivel a homomorfizmusok magjai a részmodulusok, *egyszerű modulusnak* az olyan modulusokat hívjuk, amelyeknek pontosan két részmodulusa van: a triviális részmodulusok ($\{0\}$, és az egész modulus). Az egyszerű modulusokat sokszor *irreducibilis modulusoknak*, és néha *minimális modulusoknak* is nevezik.

Gyakorlatok, feladatok

7.1.9. Gyakorlat. Mutassuk meg, hogy az alábbi struktúrák mind unitér modulusok, kivéve az elsőt, amely modulus ugyan, de nem unitér.

(1) Egy tetszőleges Abel-csoport egy tetszőleges gyűrű fölött, ahol a modulusszorzást azonosan nullának értelmezzük.
(2) Ha T test, akkor T^n a $T^{n\times n}$ mátrixgyűrű fölött a mátrix-vektor szorzásra.
(3) Az $M(A, V)$ modulus (lásd 7.1.3. Definíció).
(4) Egy m exponensű A Abel-csoport $\mathbb{Z}_m$ fölött, ahol na jelentése a szokásos.
(5) Ha S részgyűrűje R-nek, akkor R az S fölött, ahol az összeadás az R-beli összeadás, és sr az R-beli szorzat.
(6) Ha J balideálja R-nek, akkor J az R fölött, ahol az összeadás a J-beli összeadás, és rs az R-beli szorzat. Ezt a modulust ${}_RJ$-vel szokás jelölni.

7.1.10. Gyakorlat. Igazoljuk, hogy az előző 7.1.9. Gyakorlat (2) pontjában szereplő modulus egyszerű.

7.1.11. Gyakorlat. Legyen V vektortér a T test fölött, $A \in \mathrm{Hom}(V)$ és $M = M(A, V)$.

(1) Ha $t \in T$ és $v \in M$, akkor a tv szorzatot úgy is érthetjük, hogy a t skalárral szorozzuk a v vektort, de úgy is, hogy a t konstans polinommal szorozzuk a v moduluselemet. Mutassuk meg, hogy mindkét esetben ugyanazt az eredményt kapjuk.
(2) Igazoljuk, hogy az $M(A, V)$ modulus részmodulusai éppen a V vektortér A-invariáns alterei (vagyis azok a W alterek, amelyekre $w \in W$ esetén $A(w) \in W$).

7.1.12. Gyakorlat. Tegyük $\mathbb{R}$ additív csoportját modulussá $\mathbb{R}[x]$ fölött kétféleképpen. Az első modulus szorzása $fr = f(1)r$, a másodiké $fr = f(2)r$. Izomorf modulusokat kaptunk-e?

7.1.13. Gyakorlat. Legyenek M_i $(i \in I)$ az M modulus részmodulusai. Mutassuk meg, hogy az ezek által generált részmodulus ugyanaz, mint az általuk generált részcsoport (vagyis a komplexusösszegük: az elemeikből képzett véges összegek halmaza).

7.1.14. Gyakorlat. Tegyük föl, hogy $E \subseteq F$ bal oldali R-modulusok, és $\varphi_0 : F \to K$ egy R-homomorfizmus. Mutassuk meg, hogy ha $E \subseteq \mathrm{Ker}(\varphi_0)$, akkor a $\varphi(f + E) = \varphi_0(f)$ megfeleltetés jóldefiniált, és modulus-homomorfizmus lesz F/E-ből K-ba.

7.2. Direkt összeg és függetlenség

Modulusok *direkt szorzatát* az alaphalmazok direkt szorzataként értelmezzük, ahol a műveleteket komponensenként végezzük. Vagyis ha M_i modulusok R fölött (ahol i egy I indexhalmazt fut végig), akkor a

$$\prod_{i \in I} M_i$$

Abel-csoport R-modulussá válik, ha az $r \in R$-rel szorzást az

$$r(\ldots, m_i, \ldots) = (\ldots, rm_i, \ldots)$$

képlettel definiáljuk (minden komponenst r-rel szorzunk).

7.2.1. Definíció. Az R gyűrű fölötti M_i modulusok *direkt összege* (más néven *diszkrét direkt szorzata)* a direkt szorzatuk azon elemeiből áll, amelyek komponensei véges sok kivétellel nullával (pontosabban a megfelelő M_i modulus nullelemével) egyenlőek. A direkt összegre a

$$\bigoplus_{i \in I} M_i$$

jelölést alkalmazzuk.

Véges sok tényező esetén a direkt összeg és a direkt szorzat ugyanaz. A direkt összeg fogalmát nemcsak Abel-csoportok, hanem modulusok esetén is jobban megérthetjük, ha a kategóriákról szóló 8.8. Szakaszt elolvassuk (lásd a 8.8.7. Feladat utáni megjegyzéseket).

Csoportok esetében a direkt összeget belsőleg is jellemeztük. Az analóg állítást gyakorlat formájában fogalmazzuk meg.

7.2.2. Gyakorlat. Tegyük föl, hogy az M modulus az M_i modulusok direkt összege. Jelölje M_i^* az M azon elemeinek halmazát, amelyeknek az i-edik esetleges kivételével minden komponense nulla. Igazoljuk, hogy ekkor

(1) az M_i^* halmazok részmodulusok, amelyek generálják M-et (vagyis az összegük M, lásd 7.1.13. Gyakorlat);
(2) Bármelyik M_i^* részmodulusnak a többi M_j^* részmodulusok generátumával vett metszete nulla.

Megfordítva, mutassuk meg, hogy ha M_i^* részmodulusai az M modulusnak, melyek rendelkeznek ezzel a két tulajdonsággal, akkor M izomorf az M_i^* modulusok direkt összegével.

Ha az iménti gyakorlatban fölsorolt feltételek teljesülnek, akkor azt úgy is fogalmazhatjuk, hogy M az M_i^* ***rész***modulusainak a direkt összege. A következő gyakorlat állítása szerint a direkt összeg szoros kapcsolatban áll a lineáris algebrából ismert lineáris függetlenség fogalmával.

7.2.3. Gyakorlat. Legyenek M_i részmodulusai az M modulusnak, amelyek együttvéve generálják M-et. Igazoljuk, hogy az alábbi állítások ekvivalensek.

(1) Az M az M_i részmodulusainak a direkt összege.
(2) Ha $m_1, m_2, \ldots, m_k$ csupa különböző (indexű) M_i részmodulusnak az elemei, és

$$m_1 + \ldots + m_k = 0\,,$$

akkor $m_1 = \ldots = m_k = 0$.
(3) Ha $m_1, m_2, \ldots, m_k$ csupa különböző (indexű) M_i részmodulusnak az elemei, és

$$r_1 m_1 + \ldots + r_k m_k = 0$$

valamilyen $r_1, \ldots, r_k$ gyűrűelemekre, akkor $r_1 m_1 = \ldots = r_k m_k = 0$.

Ez a gyakorlat lehetővé teszi, hogy a függetlenség fogalmát részmodulusokra általánosítsuk (lásd a 7.3.23. Feladat előtti definíciót). Még általánosabban, a moduláris hálók nyelvén is vizsgálhatjuk a függetlenséget (8.6.34. Feladat). Ebben a szakaszban csak közvetlenebb általánosításra, elemek függetlenségére lesz szükségünk.

7.2.4. Definíció. Azt mondjuk, hogy az M modulusban X *gyengén független* rendszer, ha X-beli elemek egy (véges) lineáris kombinációja csak úgy lehet nulla, ha a kombináció valamennyi *tagja* nulla. Az X *független*, ha X-beli elemek egy (véges) lineáris kombinációja csak úgy lehet nulla, ha a kombináció valamennyi *együtthatója* nulla. Egy modulus (gyenge) bázisának a (gyengén) független generátorrendszereit nevezzük.

Vagyis ha m_i az X elemei, és $r_1m_1 + \ldots + r_km_k = 0$, akkor ebből gyengén független X esetében az következik, hogy mindegyik $r_im_i = 0$, független X esetében pedig az, hogy mindegyik $r_i = 0$. Egy gyengén független rendszerbe a nullát akárhányszor betehetjük, gyengén független marad, míg független rendszerben a nulla egyáltalán nem szerepelhet. Ha vektortérről van szó, akkor a két fogalom csak a nullák esetleges jelenléte miatt tér el.

7.2.5. Gyakorlat. Mutassuk meg, hogy ha R test, és M egy R-modulus (azaz vektortér R fölött), akkor egy rendszer akkor és csak akkor gyengén független, ha a nullával egyenlő elemeit elhagyva független lesz.

Ha kilépünk a vektorterek közül, akkor más különbség is lehet a két függetlenségi fogalom között.

7.2.6. Gyakorlat. Mutassuk meg, hogy a $\mathbb{Z}_6^+$ csoportban, mint $\mathbb{Z}$-modulusban, az $\{1\}$ halmaz is, és a $\{3, 4\}$ halmaz is egy-egy gyenge bázis. Van-e ennek a modulusnak bázisa?

7.2.7. Gyakorlat. Betehető-e a 6 elem a $\mathbb{Z}_{12}^+$ egy gyenge bázisába?

7.2.8. Gyakorlat. Mutassuk meg, hogy egy M modulusban az m_i ($i \in I$) akkor és csak akkor gyenge bázis, ha

$$M = \bigoplus_{i \in I} \langle m_i \rangle \, .$$

Lineáris algebrában (vagy a modulusok elméletében) sokszor generátor*rendszerről*, független *rendszerről* beszélünk, ezért tisztáznunk kell, milyen értelemben használjuk itt a „rendszer" szót. Egy halmaz elemeinek nincsen sorrendje, és minden elem csak egyszer szerepelhet. Egy sorozatban számít a sorrend, és ugyanaz az elem többször is szerepelhet. A „rendszer" a kettő között van: az elemek sorrendje nem számít, de ugyanaz az elem többször is szerepelhet. A rendszerek természetes módon adódnak: ha például egy mátrix rangját vizsgáljuk, akkor az oszlopaiból (vagy a soraiból) álló vektorrendszert érdemes tekinteni, és semmi sem zárja ki, hogy a mátrix két oszlopa egyenlő legyen. Hasonlóképpen az az állítás, hogy „generátorrendszer képe szürjektív lineáris leképezésnél generátorrendszer lesz" igaz, de az eredeti generátorrendszer elemeinek képei között egybeesések is előfordulhatnak.

A rendszer fogalmát tehát nem kerülhetjük meg, de óvatosan kell vele bánni. Mit értünk például egy rendszer elemeinek egy lineáris kombinációján? Nyilván egy $r_1m_1 + \ldots + r_km_k$ kifejezést, ahol $m_1, \ldots, m_k$ elemei a rendszernek. Ha ezek például egy mátrix oszlopvektorai, akkor előfordulhat, hogy mondjuk $m_3 = m_5$. Azt azonban már nem tekintjük lineáris kombinációnak, hogy $rm_1 + sm_1$ (ha az ilyet megengednénk, akkor minden rendszer lineárisan összefüggő lenne). Ugyanazt az elemet többször a kombinációban tehát csak akkor használhatjuk föl, ha a rendszerben is többször szerepel. Kicsit pontosabban fogalmazva egy

lineáris kombinációban szereplő vektorok a rendszer különböző *indexű* elemei kell, hogy legyenek. Hasonló óvatossággal kell megfogalmazni a lineáris algebra kicserélési tételét is (lásd 7.2.19. Gyakorlat). Szerencsére a rendszerek egyenlő elemeitől általában meg lehet szabadulni. Például a generált részmodulus nem változik meg, ha a generátorok közül néhányat kevesebbszer (vagy többször) írunk le, ha meg egy vektorrendszerben van két egyenlő elem, akkor az biztosan lineárisan összefüggő lesz.

Egy egyelemű rendszer mindig gyengén független. Ugyanakkor vegyünk egy A Abel-csoportot, mint $\mathbb{Z}$-modulust (lásd 7.1.2. Feladat), mondjuk a $\mathbb{Z}_3^+$ csoportot. Ebben $3 \cdot 1 = 0$, tehát az 1 elem önmagában sem független, de nem is nulla! Általában, ha A egy Abel-csoport, és $g \in A$, akkor ahhoz, hogy $\{g\}$ független legyen, az kell, hogy $ng = 0$-ból $n = 0$ következzen. Másképp fogalmazva: a g elem rendje végtelen kell, hogy legyen. Ez viszont akkor és csak akkor igaz, ha a $\langle g \rangle$ részcsoport izomorf $\mathbb{Z}^+$-szal, vagyis az alapgyűrűvel, mint Abel-csoporttal. Ezeket az állításokat szeretnénk modulusokra is kimondani.

7.2.9. Definíció. Legyen M bal oldali R-modulus, és $m \in M$. Azt mondjuk, hogy az m rendje nulla, ha tetszőleges $r \in R$ esetén $rm = 0$-ból $r = 0$ következik.

Miért hívjuk az ilyen m elemet végtelen helyett nulla rendűnek? Ezt részben már megindokoltuk az 5.7.2. Definíció utáni megjegyzésben: pontosan a nulla többszörösei azok, amik az m-et nullába szorozzák, és így egységesen kezelhetjük a véges és végtelen rend fogalmát (ezt meg is tesszük majd a 7.3.1. Definícióban). Van azonban még egy indok, ami miatt a „végtelen" jelző általában nem lenne megfelelő.

Ha egy Abel-csoportban g végtelen rendű elem, akkor sokkal többet tudunk annál, mint hogy g-nek végtelen sok különböző többszöröse van: azt is tudjuk, hogy ezek páronként különbözők! Vagyis hogy az $n \mapsto ng$ megfeleltetés injektív. Másképp: g-nek annyi többese van, ahány egész szám. Mindez modulusokra is elmondható. Nyilván $rm = sm$ pontosan akkor teljesül, ha $(r-s)m = 0$. Ha tehát m rendje nulla, akkor a $\varphi : r \mapsto rm$ leképezés bijekció lesz az R gyűrű, és az m többszöröseinek a halmaza (vagyis az $\langle m \rangle$ részmodulus) között. Végtelen rendről tehát már csak azért sem lenne érdemes beszélni, mert nem tudhatjuk, hogy R-nek végtelen sok eleme van-e.

7.2.10. Gyakorlat. Mutassuk meg, hogy egy rendszer akkor és csak akkor független, ha gyengén független, és mindegyik elemének nulla a rendje.

Az $n \mapsto ng$ leképezés csoportok esetén nyilván összegtartó. Érdemes észrevenni, hogy ennek általánosítása, vagyis az R-et M-be képző $\varphi : r \mapsto rm$ is az. Megmutatjuk, hogy ez a leképezés R-homomorfizmus is lesz. Ehhez azonban R-ről mint bal oldali R-modulusról, és nem mint gyűrűről kell tudnunk beszélni. Lineáris algebrában (és a Galois-elméletben) az alaptestet gyakran képzeltük egydimenziós vektortérnek önmaga fölött (vö. 5.9.4. Gyakorlat). Ennek általánosításaként az R-et önmaga fölötti modulusnak képzeljük, amelynek összeadása az R gyűrű összeadása, és R egy elemével (skalárnak képzelve) R egy elemét (mint moduluselemet) úgy kell megszorozni, hogy az R gyűrűben összeszorozzuk őket. Az így kapott modulust ${}_R R$ jelöli.

7.2.11. Gyakorlat. Igazoljuk, hogy az ${}_R R$ modulus részmodulusai az R balideáljai.

7.2.12. Gyakorlat. Mutassuk meg, hogy ha M bal oldali R-modulus, és $m \in M$ tetszőleges elem, akkor a $\varphi : r \mapsto rm$ leképezés R-homomorfizmus ${}_RR$ és M között.

Ha tehát $\{m\}$ független, akkor a φ leképezés R-izomorfizmus lesz ${}_RR$ és $\langle m \rangle$ között. Ezt az állítást kiterjeszthetjük többelemű rendszerekre is, ilyenkor az ${}_RR$ modulus egy diszkrét direkt hatványát kapjuk. Ezt tehát egy struktúratételnek is fölfoghatjuk, ami az olyan modulusokat írja le, melyeknek van bázisa.

7.2.13. Lemma. *Legyen M egy bal oldali R-modulus. Ekkor M-nek pontosan akkor van bázisa, ha izomorf az ${}_RR$ modulus néhány példányban vett direkt összegével.*

Bizonyítás. Ha m_i $(i \in I)$ bázis M-ben, akkor a 7.2.8 gyakorlat szerint M az $\langle m_i \rangle$ részmodulusainak direkt összege. A függetlenség miatt mindegyik $\langle m_i \rangle$ izomorf ${}_RR$-rel.

A megfordításhoz azt kell belátni, hogy az ${}_RR^k$ modulusnak van bázisa. Ez a modulus ismerős lineáris algebrából, csak ott k magas oszlopvektornak írtuk az elemeit. A szokásos bázis analógiájára tekintsük az

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in R^k$$

elemeket, ahol az 1-es az i-edik komponensben van. Könnyű kiszámolni, hogy ezek tényleg bázist alkotnak, amit most is a *szokásos bázisnak* nevezünk. A gondolatmenet akkor is igaz marad, ha ${}_RR^k$-nak végtelen sok példányban vett direkt összegét tekintjük. □

7.2.14. Gyakorlat. Mutassuk meg, hogy az $e_1, \ldots, e_k$ elemek bázist alkotnak ${}_RR^k$-ban. Általánosítsuk ezt az állítást végtelen sok tagú direkt összegre is.

A lineáris leképezések előírhatósági tétele azt mondta ki, hogy ha egy M vektortér egy bázisának elemeit bárhogyan leképezzük egy N vektortérbe, akkor ez egyértelműen kiterjeszthető egy M-ből N-be menő homomorfizmussá. Ez a tulajdonsága a fenti $e_1, \ldots, e_k$ bázisnak is megvan. Hiszen ha N tetszőleges modulus, és $\varphi(e_i) = n_i \in N$ elő van írva, akkor

$$\varphi\big((r_1, \ldots, r_k)\big) = \varphi(r_1e_1 + \ldots + r_ke_k) = r_1\varphi(e_1) + \ldots + r_k\varphi(e_k) = r_1n_1 + \ldots + r_kn_k$$

lehet csak, és könnyű ellenőrizni, hogy az $(r_1, \ldots, r_k) \mapsto r_1n_1 + \ldots + r_kn_k$ leképezés tényleg modulushomomorfizmus.

A most vizsgált tulajdonság a csoportelméletben a szabad csoportok vizsgálatakor jött elő. Egy X generátorrendszer akkor szabad, ha semmilyen „fölösleges” összefüggés nincs az elemei között (csak azok, amiknek a csoportaxiómák miatt muszáj teljesülniük). Ezt az intuitív fogalmat úgy tettük precízzé, hogy a következő tulajdonságot követeltük meg: ha X elemeit bárhogyan leképezzük egy másik csoportba, akkor ez a leképezés legyen (egyértelműen) kiterjeszthető egy csoporthomomorfizmussá (4.9.1 Definíció). Hasonlóképpen definiálhatjuk a szabad generátorrendszert bármely más struktúrára is (8.3.24. Definíció). A fenti állítás tehát azt fejezi ki, hogy az $e_1, \ldots, e_k$ szabad generátorrendszere az ${}_RR^k$ modulusnak. Sőt általában az ${}_RR$ modulus akárhány példányának direkt összege is szabad.

Mindez összevág a szabadságról alkotott intuitív fogalmunkkal is. Modulusok esetében csakis $r_1x_1 + \ldots + r_nx_n$ típusú kifejezéseket írhatunk föl (hiszen bárhogy is végzünk műveleteket, az eredmény ilyen alakra hozható, lásd 8.3.6. Gyakorlat). Egy „fölösleges" összefüggés tehát $r_1x_1 + \ldots + r_nx_n = s_1x_1 + \ldots + s_nx_n$ alakú lesz, ahol nem mindegyik r_i egyenlő a megfelelő s_i-vel. Vagyis a szabad generátorrendszer várhatóan a bázissal lesz azonos.

7.2.15. Tétel. *Az M modulus egy generátorrendszere akkor és csak akkor szabad generátorrendszer, ha bázis. Az X halmaz által generált szabad modulus izomorf az ${}_RR$ modulusnak $|X|$ példányban vett direkt összegével (ahol $|X|$ az X elemszáma).*

Bizonyítás. Az egyszerűbb jelölés kedvéért az állítást csak véges generátorrendszerre látjuk be, az általánosítást az Olvasóra bízzuk. Tegyük föl tehát, hogy $b_1, \ldots, b_k$ bázis. Ekkor

$$M = \langle b_1 \rangle \oplus \ldots \oplus \langle b_k \rangle ,$$

és az $r \mapsto rb_i$ leképezés izomorfizmus ${}_RR$ és $\langle b_i \rangle$ között (7.2.13. Lemma). Ezért az

$$(r_1, \ldots, r_k) \mapsto r_1b_1 + \ldots + r_kb_k$$

izomorfizmus az ${}_RR^k$ és M között, ahol a szokásos bázis e_i elemének b_i felel meg. Mivel $e_1, \ldots, e_k$ szabad generátorrendszer, $b_1, \ldots, b_k$ is az.

Megfordítva, ha $x_1, \ldots, x_k$ szabad generátorrendszer, akkor az $x_i \mapsto e_i$ megfeleltetés kiterjeszthető egy $\varphi : M \to {}_RR^k$ homomorfizmussá. Ennél

$$\varphi(r_1x_1 + \ldots + r_kx_k) = r_1e_1 + \ldots + r_ke_k = (r_1, \ldots, r_k) .$$

Ha tehát $r_1x_1 + \ldots + r_kx_k = 0$, akkor $(r_1, \ldots, r_k) = 0$, vagyis minden komponense nulla. Így $x_1, \ldots, x_k$ független. □

Gyakorlatok, feladatok

7.2.16. Gyakorlat. Gyenge bázist alkot-e a $\mathbb{Z}_2^+ \times \mathbb{Z}_4^+$ csoportban $\{(1, 2), (1, 1)\}$?

7.2.17. Gyakorlat. Bázist alkot-e a $\mathbb{Z}^+ \times \mathbb{Z}^+$ csoportban $\{(1, 0), (1, 1)\}$? Adjunk meg ebben a csoportban végtelen sok különböző bázist.

7.2.18. Gyakorlat. Mutassuk meg, hogy ha az M modulus az M_i részmodulusainak direkt összege, és mindegyik M_i részmodulusban veszünk egy (gyenge) $\mathbf{b}_i$ bázist, akkor ezek a bázisok a nullelemtől eltekintve páronként diszjunktak, és uniójuk (gyenge) bázisa lesz az M modulusnak. Megfordítva, mutassuk meg, hogy ha $\mathbf{b}$ gyenge bázisa egy M modulusnak, amely a $\mathbf{b}_i$ páronként diszjunkt halmazok uniója, akkor a $\mathbf{b}_i$ által generált M_i modulusok direkt összege M.

7.2.19. Gyakorlat. A lineáris algebra kicserélési tétele azt mondja ki, hogy ha F független rendszer egy V vektortérben, és F függ egy G rendszertől, akkor F minden f eleméhez van olyan $g \in G$, hogy F-ből f-et elhagyva és g-t hozzávéve újra független rendszert kapunk (lásd [**10**], 4.5.5. Lemma). Magyarázzuk el, miért szükséges a megfogalmazásban rendszereket használni. Ha rendszer helyett halmazt mondanánk, milyen kiegészítő feltételre lenne szükség?

7.2.20. Feladat. Mutassuk meg, hogy egy ferdetest fölötti végesen generált modulusnak mindig van bázisa, és a bázis elemszáma egyértelműen meghatározott.

7.2.21. Feladat. Legyen V a sík, mint $\mathbb{R}$ fölötti vektortér, A az $y = x$ egyenesre való tükrözés, és $M = M(A, V)$ (azaz a sík, mint $\mathbb{R}[x]$-modulus, lásd 7.1.3. Definíció). Bontsuk föl ezt a modulust két nemtriviális részmodulusának direkt összegére. Választhatunk-e a tükrözés helyett egy olyan lineáris transzformációt a síkon, amely esetében ilyen felbontás nem lehetséges?

7.3. Elem rendje modulusban

Ha G egy csoport, és $g \in G$, akkor a g elem jó kitevőinek hívtuk azokat az n egészeket, melyekre $g^n = 1$. Megmutattuk, hogy n akkor és csak akkor jó kitevő, ha g rendjének többszöröse, és ez az állítás akkor is igaz marad, ha g rendje nulla (amit a csoportok esetében végtelennek mondtunk): ilyenkor csak a nulla lesz jó kitevő. Ha mindezt egy modulus tetszőleges elemére akarjuk általánosítani, akkor most is a „jó együtthatók" halmazát érdemes tekinteni.

7.3.1. Definíció. Legyen M bal oldali R-modulus, és $m \in M$. Ekkor az

$$O(m) = \{r \in R \,:\, rm = 0\}$$

halmazt az m elem *rendjének* nevezzük. Ha van olyan $o \in O(m)$ elem, hogy $O(m)$ pontosan az o többszöröseiből áll (vagyis ha $O(m)$ főideál):

$$O(m) = \{ro \,:\, r \in R\}\,,$$

akkor az o elemet is az m rendjének nevezzük, és $o(m)$-mel jelöljük.

Az $O(m)$ halmaz könnyen láthatóan balideálja R-nek. Tegyük föl, hogy R (kommutatív) főideálgyűrű (5.5.2. Definíció). Ekkor $o(m)$ mindig létezik, és fennáll az egységgyököknél, csoportoknál tanult, jól ismert összefüggés is:

$$\boxed{rm = sm \iff o(m) \mid r - s, \quad \text{speciálisan} \quad rm = 0 \iff o(m) \mid r.}$$

Fontos megjegyeznünk azonban, hogy *az $o(m)$ elemrend* (miként például két elem legnagyobb közös osztója is) *csak asszociáltság erejéig van meghatározva.*

7.3.2. Gyakorlat. Legyen $\varphi : M_1 \to M_2$ modulus-izomorfizmus. Mutassuk meg, hogy $m \in M_1$ esetén m és $\varphi(m)$ rendje ugyanaz.

Főideálgyűrűben érvényes marad a hatvány rendjének képlete (4.3.2. Gyakorlat, (4) állítás), és a bizonyítás is ugyanaz, mint régen, hiszen főideálgyűrűben érvényes a számelmélet alaptétele (5.5.8. Következmény).

7.3.3. Gyakorlat. Ha R főideálgyűrű, M egy R-modulus, $r \in R$ és $m \in M$, akkor igazoljuk, hogy

$$\boxed{o(rm) \sim \frac{o(m)}{(o(m), r)}}.$$

Itt $(o(m), r)$ legnagyobb közös osztót, a $\sim$ pedig asszociáltságot jelöl.

Érdemes az elemrend fogalmát általánosítani a következőképpen.

7.3.4. Definíció. Ha M egy R-modulus és $X \subseteq M$, akkor az X *annullátora* a következő:

$$\operatorname{ann}(X) = \{r \in R : rX = 0\}$$

(vagyis azon r gyűrűelemek halmaza, amelyek X minden elemét nullába szorozzák).

Az m elem $O(m)$ rendje tehát az $\{m\}$ egyelemű halmaz annullátora. Másik speciális esetként a gyűrűknél szerepelt bal oldali annullátor fogalmához jutunk (5.3.6. Definíció). Ha ugyanis R-et bal oldali modulusnak tekintjük önmaga fölött, akkor a kapott ${}_R R$ modulusban egy X részhalmaz annullátora nyilván $\ell(X)$ lesz. Ezért a következő gyakorlat az 5.3.7. Lemmát általánosítja.

7.3.5. Gyakorlat. Mutassuk meg, hogy tetszőleges részhalmaz annullátora balideál, részmodulus annullátora pedig kétoldali ideál.

Csoportoknál szó esett az exponens fogalmáról is (4.8.5. Definíció). Ezt az elemek rendjeinek legkisebb közös többszöröseként definiáltuk.

Problémát okozott azonban, hogy az exponens nemcsak pozitív egész szám lehet, hanem végtelen is. Ez nemcsak akkor fordul elő, ha a csoportnak van végtelen rendű eleme, hanem akkor is, ha a véges rendű elemek rendjei nem korlátosak. Az a konvenció, hogy a végtelen rend helyett nullát mondunk, az exponens esetében is hasznos lesz, amit a következő definíció utáni gyakorlat mutat.

7.3.6. Definíció. Ha R főideálgyűrű, és M egy R-modulus, akkor M *exponensének* nevezzük az $\operatorname{ann}(M)$ ideál (egyik) generátorelemét.

7.3.7. Gyakorlat. Igazoljuk, hogy főideálgyűrű fölött egy modulus exponense az elemek rendjeinek legkisebb közös többszöröse, illetve nulla, ha ez a legkisebb közös többszörös nem létezik.

A csoportelméleti elemrend fogalmához szorosan kapcsolódott a ciklikus csoportok fogalma. Véletlen-e az, hogy a lehetséges elemrendek $(1, 2, \ldots, \infty)$ éppen ugyanazok, mint a ciklikus csoportok lehetséges rendjei? Igaz-e általában is, hogy egy „ciklikus" modulus struktúráját a generátor rendje határozza meg egyértelműen? Általánosítható-e az az észrevétel, hogy a ciklikus csoportok izomorfia erejéig pont a $\mathbb{Z}^+$ csoport faktorai? Hogy ciklikus része is ciklikus?

Egy modulust akkor nevezünk *ciklikusnak*, ha egy elemmel generálható. A fenti állításokat a jobb érthetőség kedvért csak főideálgyűrű fölötti modulusokra általánosítjuk. A további általánosítás lehetőségét a 7.3.21. Feladat tárgyalja.

7.3.8. Feladat. Legyen R főideálgyűrű. Igazoljuk az alábbi állításokat.

(1) Egy R-modulus, akkor és csak akkor ciklikus, ha az ${}_RR$ egy faktormodulusával izomorf. Egy ciklikus modulusban bármelyik generátorelemnek (asszociáltság erejéig) ugyanaz a rendje. Két ciklikus modulus akkor és csak akkor izomorf, ha generátorelemük rendje ugyanaz (pontosabban asszociált).
(2) Az R bármelyik r eleméhez van olyan ciklikus modulus, ahol a generátorelem rendje r. Ilyen modulus például ${}_RR/(r)$.
(3) Ciklikus modulus minden homomorf képe ciklikus.
(4) Ciklikus modulus minden részmodulusa is ciklikus, és a részmodulusok kölcsönösen egyértelmű megfeleltetésben állnak a modulust generáló elem rendjének osztóival (ha az asszociált osztókat egyformának tekintjük).
(5) Ciklikus modulus exponense ugyanaz, mint a (generátorelem) rendje.

Ha R főideálgyűrű és $r \in R$, akkor tehát ugyanúgy beszélhetünk „az" r rendű ciklikus modulusról, ahogy csoportelméletben beszéltünk „a" hatodrendű ciklikus csoportról. Most is fontos megvizsgálnunk, hogy ciklikus modulusok direkt szorzata mikor ciklikus (vö. 4.8.4. Állítás és 4.8.7. Következmény).

7.3.9. Gyakorlat. Mutassuk meg a következő állításokat, amelyek egy R főideálgyűrű fölötti modulusokról szólnak.

(1) R-modulusok direkt szorzatában egy elem rendje a komponensei rendjeinek legkisebb közös többszöröse.
(2) R-modulusok direkt szorzatának és direkt összegének exponense egyaránt a tényezők exponenseinek legkisebb közös többszöröse.
(3) Ha egy M modulus m elemének rendje uv, ahol u és v relatív prímek, akkor
$$\langle m\rangle = \langle um\rangle \oplus \langle vm\rangle\,,$$
ahol $o(vm) = u$ és $o(um) = v$.
(4) Ha egy M modulus m elemének rendje $u = u_1 \dots u_k$, ahol $u_1, \dots, u_k$ páronként relatív prímek, és $v_i = u/u_i$ akkor
$$\langle m\rangle = \langle v_1 m\rangle \oplus \dots \oplus \langle v_k m\rangle\,,$$
ahol $o(v_i m) = u_i$.
(5) Ha $r, s \in R$, akkor az r rendű és az s rendű ciklikus modulus direkt szorzata pontosan akkor ciklikus, ha r és s relatív prímek. Általánosítsuk ezt az észrevételt kettőnél több, de véges sok tényezőre.

A nullának bármely r elemmel vett legnagyobb közös osztója r, és bármely elemmel vett legkisebb közös többszöröse nulla. Emiatt az előző gyakorlat (5) állítása akkor is igaz, ha r és s valamelyike (vagy akár mindkettő) nullával egyenlő, míg a csoportelméleti speciális esetben csak véges ciklikus csoportokra vizsgáltuk a kérdést. Az a konvenció tehát, hogy a végtelen rend helyett nulla rendről beszélünk, most is hasznosnak bizonyult.

Az elemrend segítségével definiálhatunk néhány fogalmat, melyekre szükség lesz a következőkben.

7.3.10. Definíció. Legyen M egy R főideálgyűrű fölötti modulus. Az M *torzió-részmodulusa* az M nem nulla rendű elemeinek a halmaza. Az M *torziómodulus*, ha nincs nulla rendű eleme, és *torziómentes*, ha minden nem nulla elemének rendje nulla.

7.3.11. Gyakorlat. Mutassuk meg, hogy a torzió-részmodulus tényleg részmodulus, és a szerinte vett faktor torziómentes.

7.3.12. Definíció. Legyen R tetszőleges gyűrű, M egy R-modulus, és $r \in R$. Ekkor

$$M[r] = \{m \in M \,:\, rm = 0\} \quad \text{és} \quad rM = \{rm \,:\, m \in M\}$$

az M modulus r*-talpa*, illetőleg r-szerese.

7.3.13. Gyakorlat. Melyik csoporttal izomorf $\mathbb{Z}_n^+[m]$, illetve $\mathbb{Z}_n^+ / m\,\mathbb{Z}_n^+$?

7.3.14. Gyakorlat. Mutassuk meg, hogy ha R kommutatív, akkor $M[r]$ és rM részmodulusok, melyekre $r(M[r]) = 0$, és $r(M/rM) = 0$.

Az, hogy $rM = 0$, főideálgyűrű fölött úgy fogalmazható, hogy M minden elemének rendje osztója r-nek.

7.3.15. Gyakorlat. Mutassuk meg, hogy ha M modulus egy R főideálgyűrű fölött, melynek exponense osztja az $r \in R$ elemet (azaz $rM = 0$), akkor M modulusnak tekinthető az $R/(r)$ faktorgyűrű fölött, ha a szorzást a következőképpen értelmezzük:

$$\big(s + (r)\big)m = sm\,.$$

Igazoljuk, hogy a gyenge függetlenség ugyanazt jelenti R és $R/(r)$ fölött, és a részmodulusok is ugyanazok.

Gyakorlatok, feladatok

Az első három gyakorlatban újra a 7.1.3. Definícióban szereplő $M = M(A, V)$ modulust vizsgáljuk, ahol V vektortér egy T test fölött, és $A \in \mathrm{Hom}(V)$ (vagy $A \in T^{n\times n}$).

7.3.16. Gyakorlat. Legyen V a sík $\mathbb{R}$ fölött, és A az $y = x$ egyenesre való tükrözés. Számítsuk ki az $M(A, V)$ modulus elemeinek rendjeit, és a modulus exponensét is. Ciklikus ez a modulus? A sík mely A transzformációira kapunk ciklikus modulust?

7.3.17. Gyakorlat. Legyen $V = \mathbb{R}^3$ az $\mathbb{R}$ fölött,

$$u = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \qquad \text{és} \qquad A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Igazoljuk, hogy u generálja $M = M(A, V)$-t, határozzuk u rendjét, és a részmodulusok számát.

7.3.18. Gyakorlat. Mutassuk meg, hogy ha V véges dimenziós, akkor $M(A, V)$ egyik elemének sem lehet nulla a rendje, és $M(A, V)$ exponense az A minimálpolinomja.

7.3.19. Gyakorlat. Legyen R főideálgyűrű, $p \in R$ prím, és M egy R-modulus. Mutassuk meg, hogy ha $b \in M$, akkor $b + M[p]$ rendje az $M/M[p]$ faktormodulusban $o(b)/p$, ha $o(b)$ osztható p-vel, és $o(b)$ egyébként.

7.3.20. Gyakorlat. Legyen M torziómodulus az R főideálgyűrű fölött, $p \in M$ prím, és M_p az M azon elemeinek halmaza, melyek rendje p-hatvány. Mutassuk meg, hogy M_p részmodulus, és

$$M = \bigoplus_p M_p \,,$$

ahol p befutja R prímelemeit (asszociált prímeket csak egyszer szerepeltetve). Az M_p-t az M *p-komponensének* nevezzük.

7.3.21. Gyakorlat. Legyen R tetszőleges (egységelemes) gyűrű. Lássuk be az alábbiakat.

(1) Egy R-modulus pontosan akkor ciklikus, ha az ${}_R R$ egy faktorával izomorf.
(2) Ha J részmodulusa ${}_R R$-nek (azaz balideálja R-nek), akkor az R/J modulus $1 + J$ generátorának a rendje J (tehát a ciklikus modulusok generátorainak a lehetséges rendjei pontosan az R balideáljai).
(3) Ciklikus modulus minden homomorf képe ciklikus.

7.3.22. Feladat. Legyen T test és $R = T^{n\times n}$ (a teljes mátrixgyűrű). Bontsuk föl az ${}_R R$ modulust n darab egyszerű részmodulusának direkt összegére. Izomorfak lesznek ezek a részmodulusok?

Az alábbiakban néhány nehezebb feladat következik (valójában egy olyan témából adunk ízelítőt, amit terjedelmi okok miatt részletesebben nem tudunk tárgyalni). Rögzítsünk egy (egységelemes) R gyűrűt. Egy R-modulust *teljesen reducibilisnek* nevezünk, ha irreducibilis (azaz egyszerű) részmodulusainak összege. Az M modulus M_i ($i \in I$) részmodulusait akkor nevezzük *függetlennek*, ha összegük direkt összeg, azaz bármelyiknek a többi összegével vett metszete csak a nullából áll. (Az elnevezést a 7.2.3. Gyakorlat állítása indokolja.) Az M egy N részmodulusát akkor nevezzük *direkt összeadandónak*, ha van olyan $K \leq M$ részmodulus, hogy $M = N \oplus K$.

7.3.23. Feladat. Legyen az M modulus az M_i ($i \in I$) egyszerű részmodulusainak összege, és N egy részmodulusa M-nek. Mutassuk meg, hogy van olyan $I' \subseteq I$, hogy M_i ($i \in I'$) függetlenek, és ha (direkt) összegüket K jelöli, akkor $M = N \oplus K$.

7.3.24. Gyakorlat. Legyen M az M_i ($i \in I$) egyszerű részmodulusainak összege. Bizonyítsuk be, hogy

(1) M minden részmodulusa és faktormodulusa is teljesen reducibilis, és M minden részmodulusa direkt összeadandó;
(2) M minden egyszerű részmodulusa és minden egyszerű faktormodulusa izomorf valamelyik M_i modulussal.

7.3.25. Gyakorlat. Mutassuk meg, hogy ha az ${}_RR$ modulus teljesen reducibilis, akkor minden R-modulus az.

7.3.26. Feladat. Legyen R egyszerű gyűrű, melynek van egy J minimális balideálja. Igazoljuk, hogy ${}_RR$ teljesen reducibilis modulus, és minden egyszerű R-modulus izomorf ${}_RJ$-vel (lásd 7.1.9 Gyakorlat (6)).

7.3.27. Feladat. Legyen az R gyűrű k darab ferdetest fölötti teljes mátrixgyűrű direkt szorzata. Mutassuk meg, hogy R fölött pontosan k darab nem izomorf egyszerű modulus van.

7.3.28. Feladat. Mutassuk meg, hogy ha ${}_RR$ minden részmodulusa direkt összeadandó, akkor ${}_RR$ (és így minden R-modulus) teljesen reducibilis.

Meg lehet mutatni a Wedderburn–Artin-tétel (5.12.4. Tétel) felhasználásával, hogy ha minden R-modulus teljesen reducibilis, akkor R izomorf véges sok, ferdetest fölötti teljes mátrixgyűrű direkt szorzatával (lásd [**13**], 10.22. Tétel). Ezek az állítások a véges csoportok reprezentációelméletének kiindulópontját képezik.

7.4. Végesen generált modulusok

Fő célunk a főideálgyűrűk fölötti végesen generált modulusokról szóló struktúratétel bizonyítása. Speciális eseteként kapjuk a véges Abel-csoportok alaptételét (4.8.14. Tétel), és a Jordan-normálalakról szóló tételt (7.6.5. Tétel).

7.4.1. Tétel [A főideálgyűrű fölötti modulusok alaptétele]. *Tegyük föl, hogy R főideálgyűrű, és M egy végesen generált R-modulus. Ekkor M felbontható véges sok ciklikus modulus direkt összegére, ahol mindegyik összeadandó rendje prímhatvány, vagy nulla. A felbontásban szereplő tényezők (generátorelemeinek) rendjei a sorrendtől eltekintve egyértelműen meghatározottak.*

Az egyértelműség pontosabban azt jelenti, hogy ha az M modulust kétféleképpen is felbontottuk prímhatványrendű, illetve nulla rendű ciklikus modulusok direkt összegére, akkor bárhogy is veszünk egy $r \in R$ elemet, amely prímhatvány vagy nulla, a két felbontásban ugyanannyi r rendű (pontosabban r-rel asszociált rendű) ciklikus összeadandó lesz. Konkrét példákért érdemes visszalapozni a 4.8.14. Tétel utáni megjegyzéshez, és a 4.8.21, valamint a 4.8.22. Gyakorlatokhoz.

7.4.2. Tétel. *Főideálgyűrű fölötti végesen generált modulus minden részmodulusa is végesen generált.*

Ezt a két tételt párhuzamosan látjuk be, és a bizonyítást a jobb érthetőség kedvéért csak euklideszi gyűrűre (5.5.1. Definíció) mondjuk el. A 7.4.14-től 7.4.17-ig számozott gyakorlatokban és feladatokban azonban megmutatjuk, hogyan vihető át a bizonyítás főideálgyűrűre. Mostantól tehát R euklideszi gyűrűt jelöl. Az egyértelműséget a következő szakaszban főideálgyűrűkre bizonyítjuk.

A bizonyítás ötlete a következő. Minden végesen generált M modulus megkapható úgy, mint egy szabad modulus (azaz ${}_RR^k$) homomorf képe. Jelölje K ennek a homomorfizmusnak a magját. Így az $R^k/K \cong M$ modulust kell megértenünk. Képzeljük egy pillanatra R-et testnek, ekkor K altere az R^k vektortérnek, ami azonban egy „nagyon ferde" sík is lehet. Egy olyan „bázistranszformációt" fogunk végrehajtani R^k-n Gauss-elimináció segítségével, hogy az új bázis már „közelebb kerüljön" a K-hoz.

Például ha a $K \leq \mathbb{Z}^+ \times \mathbb{Z}^+$ részmodulust a $(2,0)$ és a $(0,3)$ elemek generálják, akkor nagyon könnyű megmutatni, hogy

$$(\mathbb{Z}^+ \times \mathbb{Z}^+)/K \cong \big(\mathbb{Z}^+/(2)\big) \times \big(\mathbb{Z}^+/(3)\big) \cong \mathbb{Z}_2^+ \times \mathbb{Z}_3^+$$

(7.4.7. Lemma). Ha viszont az L részmodulust a $(2,2)$ és a $(2,5)$ elemek generálják, akkor közvetlenül nem látjuk, hogy mivel izomorf az L szerinti faktor, pedig az szintén $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ lesz. Ennek megmutatásához a Gauss-elimináció egy módosított változatát használjuk.

7.4.3. Gyakorlat. Mutassuk meg, hogy ha egy modulus tetszőleges bázisában az egyik báziselemhez egy másik báziselem tetszőleges skalárszorosát (azaz gyűrűelem-szeresét) hozzáadjuk, akkor ismét bázist kapunk. Igazoljuk az analóg állítást generátorrendszerekre is. Adjunk példát, ami azt mutatja, hogy az állítás gyenge bázisra nem marad érvényben.

Legyen R gyűrű, és $K \leq {}_RR^k$. Hogyan lehetne megadni K elemeit? A lineáris algebrában mátrix segítségével adtunk meg leképezéseket, és ez az eszköz most is hasznos lesz. Válasszunk egy $b_1, \ldots, b_k$ bázist R^k-ban (a következő szakaszban belátjuk majd, hogy minden bázis k elemű), és egy tetszőleges, akár végtelen g_i $(i \in I)$ generátorrendszert K-ban (jobb híján bevehetjük akár K összes elemét is). Ekkor minden g_i fölírható a báziselemek lineáris kombinációjaként:

$$g_i = r_{i1}b_1 + \ldots + r_{ik}b_k\,.$$

Az r_{ij} elemeket tegyük be egy mátrixba, amelynek tehát k oszlopa van, és annyi sora, ahány elemű a generátorrendszer (esetleg végtelen sok). Vizsgáljuk meg, hogyan változik a mátrix, ha eliminációs lépéseket hajtunk végre.

7.4.4. Gyakorlat. Igazoljuk a most definiált mátrixra az alábbi állításokat.

(1) Ha b_i helyett $b_i + rb_j$-t írunk (ahol $i \neq j$ és $r \in R$), akkor a mátrix j-edik oszlopából kivonódik az i-edik oszlop r-szerese.
(2) Ha g_i helyett $g_i + rg_j$-t írunk (ahol $i \neq j$ és $r \in R$), akkor a mátrix i-edik sorához hozzáadódik a j-edik sor r-szerese.
(3) Ha két b_i-t kicserélünk, akkor a mátrix megfelelő két oszlopa is kicserélődik.
(4) Ha két g_i-t kicserélünk, akkor a mátrix megfelelő két sora is kicserélődik.

Ez és az előző gyakorlat azt mutatja, hogy mátrixunkra a szokásos eliminációs lépéseket alkalmazhatjuk, és ilyenkor új bázis illetve K új generátorrendszere keletkezik. A mátrixot minél szebb alakra szeretnénk hozni. Vigyáznunk kell azonban: a szokásos eliminációs eljárásban szabad volt osztani a mátrix elemeivel, és ez tette lehetővé elemek „kinullázását".

Most a mátrix elemei csak egy gyűrűből valók, tehát ügyesebben kell számolnunk. De a végeredmény most is „diagonális” mátrix lesz.

7.4.5. Lemma. *Legyen R euklideszi gyűrű. Ekkor tetszőleges, R fölötti, k oszlopot tartalmazó $((r_{ij}))$ mátrix az imént leírt négyféle eliminációs lépéssel olyan $((s_{ij}))$ alakra hozható, amelyben minden elem nulla, kivéve esetleg a „főátlóban” álló $s_{11}, s_{22}, \ldots, s_{kk}$ elemeket, ezekre viszont teljesül, hogy*

$$s_{11} \mid s_{22} \mid \ldots \mid s_{kk} ,$$

vagyis ezek az elemek egymás osztói.

A lemmában leírt alakot a mátrix *normálalakjának* hívjuk. A bizonyítás egyben eljárást is szolgáltat a normálalak kiszámítására.

Bizonyítás. Ha a mátrix csupa nullából áll, akkor már normálalakban van, és semmit nem kell tennünk. Ha nem, akkor tekintsük a nem nulla elemeket. Mivel R euklideszi gyűrű, ezek mindegyikének van egy euklideszi normája, ami nemnegatív egész szám. Az eljárás első lépése az, hogy a legkisebb normájú elemet becseréljük a bal felső sarokba (két sor, majd két oszlop cseréjével).

Az eljárás második lépése során megpróbáljuk kinullázni a mátrix első sorában álló többi elemet. Ehhez a bal felső sarokban álló r_{11} elemmel osszuk el maradékosan az első sor egy tetszőleges másik elemét:

$$r_{1j} = r_{11}q + r ,$$

ahol $r = 0$, vagy r már r_{11}-nél kisebb normájú. Vonjuk ki az első oszlop q-szorosát a j-edik oszlopból. Ekkor az első sor j-edik helyére r kerül. Ha $r = 0$, akkor a kinullázás sikerrel járt. Ha nem, akkor viszont a mátrixban keletkezett egy új elem (az r), ami az r_{11}-nél kisebb normájú. Ekkor az eljárást kezdjük újra az első lépéssel.

Mivel a normák nemnegatív egészek, ilyen újrakezdés csak véges sokszor lehetséges (a bal felső sarokban ugyanis egyre kisebb normájú elem áll). Így előbb-utóbb az első sor kinullázása sikerülni fog. Ugyanígy kinullázhatjuk az első oszlop elemeit is.

Az eljárás harmadik lépése során elérjük, hogy a mátrix bal felső sarkában álló r_{11} elem ossza a mátrix összes többi elemét. Tegyük föl, hogy ez még nincs így, mert van egy r_{ij} elem, ami nem osztható r_{11}-gyel (az r_{ij} nem lehet az első sorban vagy oszlopban, mert azokat már kinulláztuk). Ekkor

$$r_{ij} = r_{11}q + r ,$$

ahol $r \neq 0$, de a normája kisebb, mint r_{11} normája. Adjuk hozzá az első sort az i-edikhez. Mivel az első oszlop már ki volt nullázva, az i-edik sor első eleme r_{11} lesz. Ezután a j-edik oszlopból vonjuk ki az első oszlop q-szorosát. Így a mátrixba bekerül az r, aminek a normája kisebb, mint r_{11} normája. Ekkor az egész eljárást ismét kezdjük legelölről, az első lépéssel. Ilyenfajta újrakezdés is csak véges sokszor lehetséges. Előbb-utóbb tehát elérjük azt az állapotot, amikor az első sor és oszlop ki van nullázva, és a bal felső sarokban álló s_{11} elem osztja a mátrix összes elemét.

Ezután hagyjuk el a mátrix első sorát és oszlopát, majd ismételjük az eljárást. Mivel véges sok oszlop van, előbb-utóbb a mátrix a kívánt alakú lesz. □

Ha az eljárást végrehajtjuk, akkor az R^k modulusban egy új $c_1, \ldots, c_k$ bázis, a K részmodulusban pedig egy új generátorrendszer keletkezik, amit az új mátrix ír le. E mátrix alakjából látjuk, hogy K-t az $s_{11}c_1, \ldots, s_{kk}c_k$ elemek generálják (a csupa nulla soroknak ugyanis a nulla generátorelem felel meg, ami minden generátorrendszerből elhagyható).

7.4.6. Következmény. *Ha K részmodulusa az R^k modulusnak, akkor van olyan $c_1, \ldots, c_k$ bázis R^k-ban, és olyan $s_1 \mid s_2 \mid \ldots \mid s_k$ elemek R-ben, hogy*

$$K = \langle s_1c_1, \ldots, s_kc_k \rangle .$$

Speciálisan R^k minden részmodulusa végesen generált.

7.4.7. Lemma. *Az előző következmény jelöléseit használva*

$$R^k/K = \langle u_1 \rangle \oplus \ldots \oplus \langle u_k \rangle ,$$

ahol az $u_i = c_i + K$ elem rendje s_i.

Bizonyítás. A 7.2.8. Gyakorlat szerint elég belátni, hogy az $u_1, \ldots, u_k$ elemek gyenge bázist alkotnak ebben a faktorban, és hogy u_i rendje s_i. Ez utóbbi állítással kezdjük. Vizsgáljuk meg, milyen $r \in R$ elemekre lesz $ru_i = 0$. Mivel faktormodulusban reprezentánsokkal végezzük a műveleteket, és a nullelem a K részmodulus, $0 = ru_i$ azt jelenti, hogy

$$K = ru_i = r(c_i + K) = rc_i + K ,$$

azaz $rc_i \in K$. Tehát rc_i fölírható a K generátorrendszerével:

$$rc_i = r_1s_1c_1 + \ldots + r_ks_kc_k$$

alkalmas $r_1, \ldots, r_k \in R$ elemekre. Mivel $c_1, \ldots, c_k$ bázis, innen $r = r_is_i$ következik, azaz $s_i \mid r$. Megfordítva, ha $s_i \mid r$, akkor $s_ic_i \in K$ miatt $rc_i \in K$, tehát $ru_i = 0$. Beláttuk, hogy $ru_i = 0$ akkor és csak akkor, ha $s_i \mid r$, és ezért u_i rendje tényleg s_i.

Annak igazolásához, hogy $u_1, \ldots, u_k$ gyenge bázis R^k/K-ban, tegyük föl, hogy

$$r_1u_1 + \ldots + r_ku_k = 0 .$$

Ez azt jelenti, hogy $r_1c_1 + \ldots + r_kc_k \in K$, tehát fölírható K generátorrendszerével:

$$r_1c_1 + \ldots + r_kc_k = t_1s_1c_1 + \ldots + t_ks_kc_k$$

alkalmas $t_1, \ldots, t_k \in R$ elemekre. Mivel $c_1, \ldots, c_k$ bázis, innen $r_i = t_is_i$ következik, és így $r_ic_i = t_i(s_ic_i) \in K$, vagyis $r_iu_i = 0$. Tehát $u_1, \ldots, u_k$ gyengén független. □

Most már összerakhatjuk a 7.4.1. Tétel bizonyítását. Tegyük föl, hogy M végesen generált R-modulus: $M = \langle d_1, \ldots, d_k \rangle$. Tekintsük az R^k (szabad) modulus szokásos e_i bázisát, és képezzük le e_i-t d_i-re. Ezt a leképezést kiterjeszthetjük egy $\varphi : R^k \to M$ homomorfizmussá, ami szürjektív, hiszen $d_1, \ldots, d_k$ generátorrendszer. A homomorfizmus-tétel miatt

$$M = \operatorname{Im}\varphi \cong R^k / \operatorname{Ker}\varphi .$$

Legyen $K = \operatorname{Ker}\varphi$. Az előző lemma szerint R^k/K izomorf ciklikus modulusok direkt összegével. Azt kell még elérnünk, hogy a direkt összeadandóink rendje nulla, vagy prímhatvány legyen.

Legyen egy ilyen direkt összeadandó rendje $0 \neq s \in R$. Mivel R alaptételes, s előáll prímhatványok szorzataként. A 7.3.9. Gyakorlat miatt tehát ez a direkt összeadandó szétbontható prímhatványrendű ciklikus modulusok direkt összegére. Ezzel a 7.4.1. Tétel első állítását bebizonyítottuk. Az alábbi állítás lehetővé teszi, hogy a normálalakra hozandó mátrixot a szabad modulusokra való hivatkozás nélkül fölírjuk.

7.4.8. Állítás. *Az $M = \langle d_1, \ldots, d_k \rangle$ modulushoz készítsük el az összes olyan $(r_1, \ldots, r_k)$ együtthatósorozatot, melyre*

$$r_1 d_1 + \ldots + r_k d_k = 0\,.$$

Tegyük ezeket a sorozatokat egy mátrix soraiba. Ha ezt a mátrixot normálalakra hozzuk, és a főátlóban $s_1 \mid s_2 \mid \ldots \mid s_k$ szerepel, akkor M izomorf az $s_1, \ldots, s_k$ rendű ciklikus modulusok direkt összegével.

Bizonyítás. Tekintsük ismét azt a $\varphi : R^k \to M$ szürjektív homomorfizmust, mely e_i-t d_i-be viszi, és legyen ennek magja K. A K összes eleme nyilván generátorrendszert alkot K-ban, és így az ehhez tartozó mátrixot is használhatjuk a bizonyításban. Megmutatjuk, hogy ez ugyanaz a mátrix, mint amiről a most bizonyítandó állításban szó van. Valóban,

$$r_1 e_1 + \ldots + r_k e_k = (r_1, \ldots, r_k) \in K$$

akkor és csak akkor igaz, ha φ-t alkalmazva

$$r_1 d_1 + \ldots + r_k d_k = 0\,.$$

Azaz mindkét szóban forgó mátrix soraiba pont a K elemeit tesszük. □

7.4.9. Következmény. *Az előző állításban szereplő M modulus exponense s_k.*

Bizonyítás. A 7.3.9. Gyakorlat szerint direkt összeg exponense a tényezők exponenseinek legkisebb közös többszöröse, és az s_i rendű ciklikus modulus exponense s_i. Így M exponense az $s_1, \ldots, s_k$ legkisebb közös többszöröse. Mivel $s_1 \mid s_2 \mid \ldots \mid s_k$, ez tényleg s_k. □

7.4.10. Gyakorlat. Mutassuk meg, hogy a 7.4.8. Állításban szereplő M modulus akkor és csak akkor ciklikus, ha $s_1, \ldots, s_{k-1}$ egység.

A 7.4.2. Tétel bizonyításához meg kell mutatnunk, hogy egy (euklideszi gyűrű fölötti) végesen generált M modulus minden részmodulusa is végesen generált. Legyen $N \leq M$. Vegyük N teljes inverz képét a φ homomorfizmusnál. Így egy $L \leq R^k$ részmodulust kapunk. Azt már beláttuk, hogy R^k minden részmodulusa végesen generált, így L is. De L-nek N homomorf képe, tehát N is végesen generált. Így ezt a tételt is beláttuk.

Érdemes észrevenni, hogy ez a tétel közvetlenül is leolvasható a mátrix normálalakját adó lemmából. Tegyük föl, hogy az M modulust generálják a $d_1, \ldots, d_n$ elemek, és legyen N részmodulusa M-nek. Írjuk föl az N elemeit a d_i elemek lineáris kombinációjaként, készítsük

el az ehhez tartozó mátrixot, és hozzuk normálalakra. Ekkor a véges sok nem nulla sor egy véges generátorrendszert szolgáltat N-ben.

Gyakorlatok, feladatok

7.4.11. Gyakorlat. Az alábbi M modulusok megadott $X = \{d_1, \ldots, d_k\}$ generátorrendszeréhez készítsük el az alaptétel bizonyításában használt mátrixot, hozzuk ezt normálalakra, és ennek alapján bontsuk föl M-et ciklikus modulusok direkt összegére.

(1) $M = \mathbb{Z}_6^+$ a $\mathbb{Z}$ fölött, $X = \{2, 3\}$.
(2) $M = \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ a $\mathbb{Z}$ fölött, $X = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.
(3) $M = \mathbb{Z}_{16}^\times$ a $\mathbb{Z}$ fölött, $X = \{3, 5\}$.

7.4.12. Gyakorlat. Az alább felsorolt L mátrixok mindegyikéből készítsük el az $L - xI$ mátrixot (amelynek elemei tehát racionális együtthatós polinomok, I a megfelelő méretű egységmátrixot jelöli). Számítsuk ki a kapott mátrixoknak a normálalakját.

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & -2 \\ 1 & 1 & -2 \\ 1 & 1 & -2 \end{bmatrix}$$

Egy főideálgyűrű fölötti (akár végtelen sok sorból álló) L mátrix i-edik *determinánsosztójának* nevezzük, és $\Delta_i(L)$-lel jelöljük az L összes $i \times i$ méretű aldeterminánsainak kitüntetett közös osztóját (és $\Delta_0(L) = 1$). Az L mátrix i-edik *elemi osztója* $\Delta_i(L)/\Delta_{i-1}(L)$, illetve nulla, ha $\Delta_{i-1}(L) = 0$.

7.4.13. Feladat. Hogyan olvashatók le a determinánsosztók és az elemi osztók egy mátrix normálalakjából? Mutassuk meg, hogy az elimináció végrehajtásakor használt elemi átalakítások során a determinánsosztók (asszociáltság erejéig) nem változnak, és ezért a normálalak egyértelmű.

A most következő feladatokban azt fogjuk végiggondolni, hogy egy (nem feltétlenül euklideszi) főideálgyűrű fölött hogyan lehet egy mátrixot normálalakra hozni.

7.4.14. Feladat. Igazoljuk, hogy ha R alaptételes gyűrű, és $L \in R^{k\times k}$ egy $k \times k$-as mátrix, akkor L-nek pontosan akkor van inverze az $R^{k\times k}$-ban, ha determinánsa R-nek egysége.

7.4.15. Feladat. Tegyük föl, hogy R alaptételes gyűrű, M egy R-modulus, és $b_1, \ldots, b_k$ generátorrendszer M-ben. Legyen $L = ((r_{ij})) \in R^{k\times k}$, melynek determinánsa R-nek egysége. Mutassuk meg, hogy akkor a k darab

$$c_i = r_{i1}b_1 + \ldots + r_{ik}b_k \quad (i = 1, \ldots, k)$$

elem szintén generátorrendszert alkot M-ben. Igazoljuk azt is, hogy ha $b_1, \ldots, b_k$ bázis volt, akkor az új elemek is bázist alkotnak.

7.4.16. Gyakorlat. Tegyük föl, hogy R alaptételes gyűrű, $su + tv = 1$, ahol $s, t, u, v \in R$, és M egy R-modulus. Adott $b_1, b_2 \in M$ elemekre legyen

$$c_1 = sb_1 + tb_2 \quad \text{és} \quad c_2 = -vb_1 + ub_2\,.$$

(1) Fejezzük ki c_1 és c_2 segítségével a b_1 és b_2 elemeket.
(2) Mutassuk meg, hogy egy független rendszer független marad, ha a benne szereplő b_1, b_2 elemeket c_1, c_2-re cseréljük.

7.4.17. Gyakorlat. Tegyük föl, hogy R főideálgyűrű, $b_1, \ldots, b_k$ bázis ${}_RR^k$-ban, és g_i generátorrendszere a $K \leq R^k$ részmodulusnak. Legyen

$$g_i = r_{i1}b_1 + \ldots r_{ik}b_k\,,$$

és készítsük el az $r_{ij} \in R$ elemekből a szokásos mátrixot.

(1) Tegyük föl, hogy a mátrix r_{11} és r_{12} elemeinek kitüntetett közös osztója d. Írjuk föl a d elemet $r_{11}u + r_{12}v$ alakban, ahol $u, v \in R$. Hajtsuk végre az előző feladatban leírt helyettesítést az $s = r_{11}/d,\ t = r_{12}/d,\ u,\ v$ elemeket használva. Mutassuk meg, hogy a kapott új bázishoz tartozó mátrix bal felső sarkába d, mellé 0 került.
(2) Tegyük föl, hogy a mátrix r_{11} és r_{21} elemeinek kitüntetett közös osztója d. Változtassuk meg a g_1 és g_2 elemeket az előző pontban látotthoz hasonló eljárással úgy, hogy újra K generátorrendszerét kapjuk, és az új generátorrendszerhez tartozó mátrix bal felső sarkába d, alá pedig 0 kerüljön.
(3) Tervezzünk egy stratégiát, amellyel ezeket az újfajta lépéseket felhasználva a mátrix normálalakra hozható.

7.5. A felbontás egyértelműsége

Ez a szakasz is az első olvasásra átugorhatóak közé tartozik, nem mintha a most következő bizonyítás olyan trükkös lenne, hanem mert bizonyos algebrai érettséget igényel. A végesen generált modulusok alaptételének (vagyis a 7.4.1. Tételnek) az egyértelműségi állítását akarjuk belátni. Rögzítsünk tehát egy végesen generált M modulust az R gyűrű fölött. Ebben a szakaszban elég azt feltennünk, hogy R főideálgyűrű.

A bizonyítás menetét egy hasonlattal próbáljuk meg érzékeltetni. Egy zsákban futó verseny résztvevői törpék, emberek és óriások. Mindannyian beszálltak egy liftbe. Mi, akik a lépcsőházban állunk, meg akarjuk számolni, hogy hány törpe, hány ember, és hány óriás van. Ezt megtehetjük úgy, hogy egy résen át bekukucskálunk. Amikor a lift elhalad lefelé a szemünk előtt, akkor először az összes zsákot látjuk a lift alján. Ha ezeket megszámoljuk, már tudjuk, hogy összesen hány törpe, ember és óriás van. Amikor a lift továbbhaladt, és már minden törpe feje a látóterünk alá ért, akkor megint megszámoljuk, hogy hány zsákot látunk, ez az emberek és óriások együttes száma. Végül, amikor már az emberek is eltűntek a szemünk elől, akkor csak az óriásokat tartalmazó zsákokat látjuk. Ezeket megszámolva az emberek illetve a törpék számát is megkapjuk, egyszerű kivonással.

Hogyan lehet ezzel a módszerrel ciklikus direkt összeadandókat megszámolni? Tekintsük például az $A = \mathbb{Z}_2^4 \times \mathbb{Z}_4^2 \times \mathbb{Z}_8^3$ Abel-csoportot. A törpék a $\mathbb{Z}_2$-knek, az emberek a $\mathbb{Z}_4$-eknek,

az óriások a $\mathbb{Z}_8$-aknak felelnek meg. A „rés”, amin át bekukucskálunk, csak „két egység magas”. Ezért először csak a csoportunknak az „alját”, vagyis az $A[2]$ részcsoportot látjuk (azokat az elemeket, amelyek kétszerese nulla). Ennek az elemszáma 2^{4+2+3} lesz, vagyis ehhez mindegyik direkt tényező hozzájárul. Valóban, az A csoport egy

$$(r_1, r_2, r_3, r_4, s_1, s_2, t_1, t_2, t_3)$$

eleme akkor és csak akkor van $A[2]$-ben, ha mindegyik t_i nulla vagy 4, mindegyik s_i nulla vagy 2, és mindegyik r_1 nulla vagy 1. Ilyen elem tényleg 2^{4+2+3}-féle van.

A lift lefelé haladása annak felel meg, hogy A-t faktorizáljuk $A[2]$-vel. Ki fogjuk számolni, hogy ilyenkor a tényezők mindegyike „eggyel kisebb lesz”, azaz

$$B = A/A[2] \cong \mathbb{Z}_1^4 \times \mathbb{Z}_2^2 \times \mathbb{Z}_4^3 \ .$$

Itt persze elhagyhatjuk a $\mathbb{Z}_1$-es tényezőket. Ha most ismét belenézünk a liftbe, azaz kiszámítjuk a $B[2]$ elemszámát, akkor az előző érvelés szerint 2^{2+3} adódik. Az eljárást még egyszer megismételve az eredeti $\mathbb{Z}_4$-ek is eltűnnek, és ezért a $\mathbb{Z}_8$-cal izomorf tényezők számát kapjuk.

Az van csak hátra, hogy ezt a gondolatot megfelelő technikai köntösbe öltöztessük. A bizonyítás során külön fogjuk megszámolni a nulla rendű ciklikus tényezőket (egy új ötlet segítségével), majd a fenti gondolatot külön-külön alkalmazzuk minden egyes prímhez tartozó prímhatványokra.

Tegyük föl, hogy az M modulusnak adott egy felbontása prímhatványrendű és nulla rendű ciklikus részmodulusok direkt összegére. Először a nulla rendű ciklikus direkt összeadandókat akarjuk megszámolni, és ezért ezt a felbontást a következő alakban írjuk fel:

$$M = \langle a_1 \rangle \oplus \ldots \oplus \langle a_k \rangle \oplus \langle b_1 \rangle \oplus \ldots \oplus \langle b_\ell \rangle \ ,$$

ahol az $a_1, \ldots, a_k$ elemek rendje nulla, a $b_1, \ldots, b_\ell$ elemek rendje nem nulla.

7.5.1. Gyakorlat. Igazoljuk, hogy M torzió-részmodulusa $T = \langle b_1, \ldots, b_k \rangle$. Mutassuk meg azt is, hogy az $a_i + T$ elemek bázist alkotnak M/T-ben, és így $M/T \cong {}_R R^k$. (A torzió-részmodulus fogalmával a 7.3.10. Definícióban és a 7.3.11. Gyakorlatban találkoztunk.)

Meg akarjuk mutatni, hogy a nulla rendű generátorok száma (az iménti felbontásban szereplő k szám) nem függ attól, hogy melyik felbontást tekintjük. Ha vesszük a modulusnak egy másik felbontását ciklikus modulusok direkt összegére, akkor a torzió-részmodulusa (és így a szerinte vett faktor) ugyanaz a modulus lesz mindkét felbontás esetén, hiszen a torzió-részmodulus fogalmát mindenféle direkt felbontástól függetlenül definiáltuk. Ha a másik felbontásban n darab nulla rendű ciklikus direkt összeadandó van, akkor M/T izomorf R^n-nel is. Ezért elég belátni a következőt.

7.5.2. Lemma. *Ha R^k és R^n izomorf R-modulusok, akkor $k = n$.*

Bizonyítás. Az állítást lineáris algebrára vezetjük vissza. Legyen $\varphi : R^k \to R^n$ egy R-izomorfizmus, és ψ az inverze. Vegyük R^k szokásos $e_1, \ldots, e_k$ bázisát, és írjuk be a $\varphi(e_i)$ elemeket, amiket n magas oszlopvektoroknak képzelünk, egy mátrix oszlopaiba. Ez tehát ugyanaz az eljárás, mint amikor egy φ lineáris leképezés mátrixát írjuk föl. Ily módon egy A mátrixot kapunk, melynek n sora, k oszlopa van, és elemei R-beliek. Ugyanezt az eljárást a ψ-re elvégezve egy $k \times n$-es B mátrix adódik.

Az, hogy φ és ψ egymás inverzei, úgy fejezhető ki, hogy mindkét sorrendben vett kompozíciójuk az identitás. Ahogy lineáris algebrában kiszámoltuk, hogy a kompozíciónak mátrix-szorzás felel meg, úgy most is azt kapjuk, hogy az A és B mátrixok mindkét sorrendben vett szorzata az egységmátrix, az egyik $n \times n$-es, a másik $k \times k$-as.

Ezt a két mátrixot az R hányadosteste fölötti mátrixnak tekinthetjük, ami már test, tehát szabad alkalmaznunk a lineáris algebrai tételeket. Tudjuk, hogy szorzatmátrix rangja nem nagyobb, mint bármelyik tényező rangja. Ezért A rangja legalább k és legalább n. Másrészt A rangja legfeljebb k és legfeljebb n, hiszen n sora és k oszlopa van. Ezért A rangja k-val is és n-nel is megegyezik, és így $k = n$. □

A 7.8.26. Feladatban megmutatjuk, hogy az előző gondolatmenet hogyan mondható el elegánsabban a tenzorszorzat fölhasználásával.

Beláttuk tehát, hogy M felbontásában a nulla rendű ciklikus direkt összeadandók száma egyértelműen meghatározott. Most megmutatjuk ugyanezt az p^α rendű direkt összeadandók számáról is, ahol $p \in R$ egy rögzített prím. Ehhez új jelölést alkalmazunk: most a p-hatvány rendű ciklikus összeadandókat választjuk külön. Legyen

$$M = \langle c_1 \rangle \oplus \ldots \oplus \langle c_n \rangle \oplus \langle d_1 \rangle \oplus \ldots \oplus \langle d_m \rangle \,,$$

ahol a $c_1, \ldots, c_n$ nem nulla elemek rendje (asszociáltság erejéig) p-hatvány, a $d_1, \ldots, d_m$ elemek rendje pedig nem osztható p-vel. A szakasz elején bemutatott eljárást szeretnénk alkalmazni, ezért tekintsük az $M[p]$ részmodulust (7.3.12. Definíció). Ennek elemeit nem mindig tudjuk megszámolni (például lehet végtelen sok eleme is). Ezért még egy gondolatra szükség van.

Amikor azt mondjuk, hogy az $A[2]$ csoport rendje 2^n, akkor ezt nemcsak úgy láthatjuk be, hogy megszámoljuk az elemeit, hanem úgy is, hogy megmutatjuk: izomorf $\mathbb{Z}_2^n$-nel. Ha az elemeket nem szabad megszámolni, akkor honnan tudjuk, hogy nem lehet izomorf $\mathbb{Z}_2^k$-nal is egyúttal? Képzeljük ezt az $A[2]$ csoportot vektortérnek a $\mathbb{Z}_2$ test fölött! Ennek a vektortérnek az első esetben n, a másodikban k a dimenziója, ezért szükségképpen $n = k$. (Természetesen nem minden csoportot lehet vektortérnek tekinteni $\mathbb{Z}_2$ fölött, hanem csak azokat, amelyekben mindegyik elem kétszerese nulla, lásd 4.8.29. Feladat).

7.5.3. Gyakorlat. Tegyük föl, hogy a fenti felbontásban $o(c_i) = p^{\alpha_i}$ (ahol $\alpha_i \geq 1$, mert $c_i \neq 0$). Mutassuk meg, hogy a $c_i'' = p^{\alpha_i - 1} c_i$ nem nulla elemek gyenge bázist alkotnak $M[p]$-ben.

Ezek szerint $M[p]$-nek van egy n darab nem nulla elemből álló gyenge bázisa. Ha egy másik felbontást veszünk, amelyben a p-hatvány rendű ciklikus direkt összeadandók száma nem n, hanem k, akkor abból az adódik, hogy $M[p]$-nek van egy k darab nem nulla elemből álló gyenge bázisa is. Mint az előbb, most is meg kellene mutatni, hogy $n = k$. Ebben ismét a lineáris algebra fog segíteni: az $M[p]$ modulusról megmutatjuk, hogy vektortér R egy faktorgyűrűje fölött.

Mivel p prím, a (p) maximális ideál R-ben, és ezért $R/(p)$ test lesz (5.5.9. Tétel). A 7.3.15. Feladatban beláttuk, hogy $M[p]$ vektortér az $R/(p)$ test fölött, és ugyanebből

a feladatból következik, hogy a $c_1'', \ldots, c_k''$ elemek gyenge bázist alkotnak $R/(p)$ fölött is. De most már vektortérben vagyunk, és ebben a gyenge bázisban a nulla nem szerepel, ezért ez bázis is (lásd 7.2.5. Gyakorlat). Beláttuk tehát, hogy *M tetszőleges felbontásában a p-hatványrendű ciklikus direkt összeadandók száma egyértelműen meghatározott, mint $M[p]$ dimenziója $R/(p)$ fölött.*

Most küldjük a liftet egy emelettel lejjebb, azaz faktorizáljunk $M[p]$-vel. A most következő gyakorlat megoldása nagyon hasonló a 7.4.7. Lemma bizonyításához.

7.5.4. Gyakorlat. Mutassuk meg, hogy az $M/M[p]$ modulusban gyenge bázist alkotnak a

$$c_1' = c_1 + M[p], \ldots, c_n' = c_n + M[p], \quad d_1' = d_1 + M[p], \ldots, d_m' = d_m + M[p]\,,$$

elemek, továbbá $o(c_i') = o(c_i)/p = p^{\alpha_i - 1}$ és $o(d_j') = o(d_j)$.

Az $M[p]$-vel való faktorizálással tehát sikerült eggyel csökkenteni mindegyik p-hatvány rendű generátor rendjében a p kitevőjét. Speciálisan ha eredetileg c_i rendje p volt, akkor a faktorban c_i' nulla lesz, ezeket a tényezőket elhagyhatjuk. Ha $N = M/M[p]$ jelöli az új modulusunkat, akkor tehát $N[p]$ dimenziója $R/(p)$ fölött azt mondja meg, hogy hány olyan p-hatvány rendű ciklikus direkt összeadandó van az M eredeti felbontásában, melynek rendje legalább p^2 (pontosabban rendje p^α, ahol α legalább 2). Az eljárást folytatva meg tudjuk számolni minden α esetén a legalább p^α rendű ciklikus direkt összeadandókat az M eredeti felbontásában. A számoláskor csupa olyan fogalomra hivatkozunk (például $(M/M[p])[p]$ dimenziója), amely független attól, hogy M melyik felbontásából indultunk ki. Ezért az eredmény mindegyik felbontásban ugyanaz lesz, és így a végesen generált modulusok alaptételének bizonyítását befejeztük.

Gyakorlatok, feladatok

7.5.5. Gyakorlat. Legyen V vektortér egy T test fölött, $A \in \mathrm{Hom}(V)$, és $M = M(A, V)$. Tekintsük a $p(x) = x - \lambda$ polinomot, ahol $\lambda \in T$.

(1) Hogyan hívtuk az $M[p]$ alteret lineáris algebrában?
(2) Mutassuk meg, hogy az M modulus p-komponensének az elemei pontosan a λ-hoz tartozó úgynevezett *általánosított sajátvektorok*, vagyis azok a $v \in M$ elemek, melyekre $(A - \lambda I)^m(v) = 0$ alkalmas m egészre. (A p-komponens fogalmát a 7.3.20. Gyakorlatban definiáltuk.)

7.5.6. Gyakorlat. Tegyük föl, hogy M egy főideálgyűrű fölötti modulus, és $p \in R$ egy prím. Legyen $N = M/M[p]$, és tekintsük az $N[p]$ részmodulus teljes inverz képét az M modulusban (a természetes homomorfizmusnál). Mutassuk meg, hogy ez pontosan az $M[p^2]$ részmodulus.

7.5.7. Gyakorlat. Tegyük föl, hogy $b_1, \ldots, b_k$ bázis az R főideálgyűrű fölötti M modulusban, és $p \in R$ egy prím. Legyen $N = M/pM$, mint $R/(p)$ fölötti vektortér (lásd

7.3.15. Gyakorlat). Mutassuk meg, hogy ennek a vektortérnek a dimenziója k. Megmutathattuk volna ennek felhasználásával is, hogy egy szabad modulusban a bázis elemszáma egyértelmű?

7.5.8. Gyakorlat. Tegyük föl, hogy M egy főideálgyűrű fölötti modulus, $p \in R$ egy prím, és

$$M = \langle c_1 \rangle \oplus \ldots \oplus \langle c_n \rangle ,$$

ahol $o(c_i) = p^{\alpha_i}$ és $c_i \neq 0$.

(1) Legyen $N = M/pM$, mint $R/(p)$ fölötti vektortér (lásd 7.3.15. Feladat). Mutassuk meg, hogy ennek a vektortérnek a dimenziója n.
(2) Igazoljuk, hogy a pc_i elemek bázist alkotnak pM-ben, és $o(pc_i) = p^{\alpha_i - 1}$.
(3) Ezeknek az észrevételeknek a felhasználásával adjunk az alaptétel egyértelműségi részére egy új bizonyítást (amikor a lift lentről felfelé halad, tehát először a tetejét látjuk meg).

7.6. A Jordan-féle normálalak

Ebben a szakaszban megmutatjuk, hogy a Jordan-féle normálalakról szóló lineáris algebrai tétel következik a főideálgyűrű fölötti végesen generált modulusok alaptételéből. A tétel durván azt mondja ki, hogy egy komplex elemű négyzetes mátrix bázistranszformációval egy viszonylag szép, „majdnem diagonális" alakra hozható, és ez az alak ráadasul lényegében egyértelmű is. A pontos állítás elolvasható például Freud Róbert lineáris algebra tankönyvében ([**10**], 6.6.4. Tétel), de kiderül majd az alábbiakból is.

A tétel bizonyításához olyan modulust kell tekintenünk, amely egy V vektortér egy A lineáris transzformációjának a viselkedését fogja meg. A modulus M alaphalmaza maga a V vektortér lesz. Az R gyűrű elemeivel való szorzásnak az A hatását kellene leírniuk.

Az első ötlet az lenne, hogy az A transzformációt vegyük be az R gyűrűbe, és az Av modulusszorzatot $A(v)$-nek definiáljuk. Ekkor az R gyűrűt választhatnánk az A (és az identitás) által generált R részgyűrűnek $\mathrm{Hom}(V)$-ben. A 5.1.2. Állításhoz hasonlóan beláthatjuk, hogy az R elemei az A polinomjai lesznek, mert az A hatványai egymással fölcserélhetők. Technikailag kényelmesebb (és lényegében ekvivalens megközelítés) azonban, ha ehelyett a még ismeretlen gyűrű helyett inkább magát a polinomgyűrűt választjuk R-nek, és egy f polinommal egy v vektort úgy szorzunk, hogy a $f(A)(v)$ elemet tekintjük, vagyis a már többször látott $M(A, V)$ modulust vizsgáljuk (7.1.3. Definíció). Mivel test fölötti polinomgyűrű euklideszi, alkalmazhatjuk az előző két szakaszban bizonyított tételt.

Rögzítsünk tehát egy V véges dimenziós vektorteret egy T test fölött, egy A lineáris transzformációt V-n, és legyen $M = M(A, V)$. Ha $d_1, \ldots, d_k$ bázis a V vektortérben, akkor ez nyilván generátorrendszere M-nek (a 7.1.11. Gyakorlat szerint már a konstans polinomok is elegendőek ahhoz, hogy M elemeit generáljuk velük), és ugyanebben a gyakorlatban azt is beláttuk, hogy M részmodulusai pontosan a V vektortér A-invariáns alterei.

Alkalmazni szeretnénk az M modulusra az alaptételt (7.4.1. Tétel). Az M modulusnak nincs nulla rendű eleme (lásd 7.3.18. Gyakorlat), és ezért M felbomlik prímhatványrendű ciklikus modulusok direkt összegére. A célunk az, hogy egy olyan vektortér-bázist válasszunk ki V-ben ennek a felbontásnak a segítségével, amelyben az A transzformációnak „szép" a mátrixa.

Először azt tisztázzuk, hogy az M modulus direkt összegre való felbontása segítségével hogyan lehet az A mátrixát diagonális blokkokra felbontani. Ez egy egyszerű lineáris algebrai állítás, a részletek kidolgozását az Olvasóra hagyjuk (vö. 7.2.18. Gyakorlat).

7.6.1. Állítás. *Legyen V egy vektortér, és A egy lineáris transzformáció V-n. Tegyük föl, hogy V felbomlik az A-invariáns U és W alterek direkt összegére. Legyen* **b** *bázisa U-nak, és* **c** *bázisa W-nek. Ekkor e két bázis* **b**, **c** *egyesítése bázisa lesz V-nek, és ebben az A mátrixa*

$$\begin{bmatrix} K & O_1 \\ O_2 & L \end{bmatrix}$$

alakú lesz, ahol K az A (U-ra vett megszorításának a) mátrixa a **b** *bázisban, L az A (W-re vett megszorításának a) mátrixa a* **c** *bázisban, és az O_1, O_2 mátrixok csupa nullából állnak. Megfordítva, ha A mátrixa valamilyen* **b**, **c** *bázisban ilyen alakú, akkor* **b** *és* **c** *egy-egy A-invariáns alteret generál, melyek direkt összege V.*

Most azt tisztázzuk, hogy ha az M felbontásában az egyik prímhatványrendű ciklikus direkt összeadandó a $W = \langle c \rangle$, akkor a W altérben hogyan választhatunk olyan bázist, amelyben az A mátrixa „szép" lesz. Jelölje c rendjét p^m, ahol $p \in T[x]$ egy prímelem, vagyis egy irreducibilis polinom. Tegyük föl, hogy T a komplex számtest (elég annyi is, hogy T algebrailag zárt). Ekkor a p polinom elsőfokú, és mivel moduluselem rendjét csak asszociáltság erejéig definiáltuk, feltehető, hogy p normált, vagyis $p(x) = x - \lambda$.

7.6.2. Lemma. *Legyen $c \in M$ olyan elem, melyre $p^m c = 0$, és*

$$c_1 = c\,, \quad c_2 = pc\,, \quad \ldots\,. c_m = p^{m-1}c\,.$$

Ekkor

$$\langle c \rangle_{T[x]} = \langle c_1, \ldots, c_m \rangle_T\,,$$

ahol a bal oldalon $T[x]$ fölötti modulus-generálás, a jobb oldalon pedig T fölötti vektortér-generálás szerepel. Ha c rendje p^m, akkor $c_1, \ldots, c_m$ független T fölött.

Bizonyítás. A bal oldal elemei az fc vektorok, ahol $f \in T[x]$. A 2.4.16. Feladat szerint f (egyértelműen) fölírható $x - \lambda$ polinomjaként, azaz

$$f(x) = t_0 + t_1(x - \lambda) + \ldots + t_n(x - \lambda)^n$$

alakban. Nulla együtthatókat beírva feltehető, hogy $n \geq m-1$. Ekkor

$$fc = t_0c + t_1(x-\lambda)c + \ldots + t_n(x-\lambda)^n c = t_0c + t_1(pc) + \ldots + t_{m-1}(p^{m-1}c)\,.$$

Itt azért elég csak m tagot kiírni, mert $p^m c = 0$ (és így $p^{m+1}c$, $p^{m+2}c$, ... is nulla). Ezzel a lemma „generálós" összefüggését beláttuk.

Tegyük föl, hogy c rendje p^m és hogy $t_0c_1 + t_1c_2 + \ldots + t_{m-1}c_m = 0$ valamilyen $t_i \in T$ elemekre. Ekkor

$$0 = t_0c_1 + t_1c_2 + \ldots + t_{m-1}c_m = t_0c + t_1(pc) + \ldots + t_{m-1}(p^{m-1}c) = fc\,,$$

ahol $f(x) = t_0 + t_1(x-\lambda) + \ldots + t_{m-1}(x-\lambda)^{m-1}$. Mivel $fc = 0$, a c rendje osztója f-nek, tehát $p^m \mid f$. De p^m foka m, az f polinom pedig legfeljebb $m-1$-edfokú, ezért $f = 0$. A 2.4.16. Feladat egyértelműségi része miatt ebből következik, hogy mindegyik $t_i = 0$, vagyis $c_1, \ldots, c_m$ lineárisan független T fölött. □

7.6.3. Gyakorlat. Mutassuk meg, hogy ha az előző lemmában c rendje nem p^m, akkor $c_1, \ldots, c_m$ lineárisan összefügg T fölött.

Most számítsuk ki az A mátrixát a $c_1, \ldots, c_m$ bázisban. Legyen $B = A - \lambda I$, ahol I az identikus transzformáció. Ekkor $p(A) = A - \lambda I = B$, és így

$$B(c_i) = B(p^{i-1}c) = B\big(B^{i-1}(c)\big) = B^i(c) = p^i c\,.$$

Ezért $B(c_i) = c_{i+1}$ ha $i < m$ és $B(c_m) = p^m c = 0$. Így $A = B + \lambda I$ miatt a W altér $c_1, \ldots, c_n$ bázisában

$$[B] = \begin{bmatrix} 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix} \quad \text{ahonnan} \quad [A] = \begin{bmatrix} \lambda & 0 & \ldots & 0 & 0 \\ 1 & \lambda & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & \lambda \end{bmatrix},$$

azaz egy λ-hoz tartozó $m \times m$-es *Jordan-blokk* (ahol tehát a főátlóban csupa λ van, az alatta levő „ferde sorban" csupa 1-es, és a mátrix többi eleme nulla).

7.6.4. Gyakorlat. Tegyük föl, hogy $c_1, \ldots, c_m$ egy bázis W-ben, melyben A mátrixa az iménti Jordan-blokk. Mutassuk meg, hogy $c = c_1$ generálja W-t mint $T[x]$-modulust, és c rendje ebben a modulusban p^m lesz.

7.6.5. Tétel [Jordan-féle normálalak]. *Egy algebrailag zárt T test fölötti véges dimenziós V vektortéren minden A lineáris transzformációhoz van olyan bázisa V-nek, hogy ebben a transzformáció mátrixa a diagonálisra helyezett Jordan-blokkokból tevődik össze, a mátrix többi eleme pedig nulla (ez a Jordan-féle normálalak). Ez az alak egyértelmű is abban az értelemben, hogy tetszőleges $\lambda \in T$, és m egész szám esetén a mátrixban a bázis választásától függetlenül mindig ugyanannyi $m \times m$-es, λ-hoz tartozó Jordan-blokk lesz. (Vagyis az A transzformáció Jordan alakú mátrixai csak a blokkok sorrendjében térhetnek el).*

Bizonyítás. Bontsuk föl az $M = M(A, V)$ modulust prímhatványrendű ciklikus modulusok direkt összegére, és válasszuk mindegyik így kapott A-invariáns altérben a 7.6.2. Lemmában megadott bázist. Ekkor (az 7.6.1. Állítást és a fenti számolást is felhasználva) azt kapjuk, hogy A mátrixa alkalmas bázisban a kívánt alakú.

Az egyértelműség bizonyításához tegyük föl, hogy A mátrixa egy alkalmas bázisban Jordan-alakú. A 7.6.1. Állítás segítségével bontsuk fel a teret a Jordan-blokkoknak megfelelő invariáns alterek (azaz részmodulusok) direkt összegére. A 7.6.4. Gyakorlat szerint mindegyik direkt összeadandó prímhatványrendű ciklikus modulus: egy $\lambda \in T$-hez tartozó $m \times m$-es blokkból egy $(x - \lambda)^m$ rendű ciklikus összeadandót kapunk. A végesen generált modulusok alaptételének egyértelműségi állítása tehát pontosan azt adja, amit a tétel egyértelműségi állításában megköveteltünk. □

Fontos tudnunk, hogy a most adott bizonyítás eljárást is ad a Jordan-alak meghatározására. A „konyhaszabályokat" a következő tétel foglalja össze.

7.6.6. Tétel. *Legyen A lineáris transzformáció a T test fölötti véges dimenziós V vektortéren, és $d_1, \ldots, d_k$ egy vektortér-bázis V-ben T fölött. Írjuk föl az A mátrixát ebben a bázisban, és legyen L ennek a mátrixnak a transzponáltja. Tekintsük az $L - xI$ úgynevezett* karakterisztikus mátrixot *(amelynek elemei T fölötti polinomok), hozzuk ezt normálalakra a 7.4.5. Lemma bizonyításában leírt eljárással, és jelölje $s_1 \mid s_2 \mid \ldots \mid s_k$ a főátlóban kapott polinomokat. Ekkor a következők teljesülnek.*

(1) *Az $s_1 s_2 \ldots s_k$ polinom az A karakterisztikus polinomja, előjeltől eltekintve.*

(2) *Az s_k polinom az A minimálpolinomjának konstansszorosa. Speciálisan a minimálpolinom osztója a karakterisztikus polinomnak (ez a lineáris algebrából ismert Cayley-Hamilton-tétel). Az s_k minimálpolinom az $M(A, V)$ modulusnak az exponense, és van olyan vektor V-ben, melynek rendje pont ez a polinom.*

(3) *Tegyük föl, hogy mindegyik s_i polinom gyöktényezőkre bomlik T fölött. Legyen $\lambda \in T$, és m_i a λ gyök multiplicitása az s_i polinomban (ami lehet nulla is). Ekkor az A normálalakjában a λ-hoz tartozó Jordan-blokkok mérete $m_1, \ldots, m_k$. Speciálisan tehát annyi λ-hoz tartozó blokk van, ahány s_i polinomnak λ gyöke.*

Néha szükségünk van egy olyan bázisra, amelyben a mátrix Jordan-alakúvá válik. Ilyen bázist általában úgynevezett általánosított sajátértékek segítségével keresnek. Mi most egy ettől kissé eltérő eljárást mutatunk, amelynek helyessége az eddigiekből könnyen következik. Miközben az $L - xI$ mátrixot normálalakra hozzuk, kövessük nyomon (a 7.4.4. Gyakorlat felhasználásával), hogy hogyan változik a $d_1, \ldots, d_k$ vektorrendszer. A végeredményt jelölje $u_1, \ldots, u_k$, ahol u_i rendje az főátlóban szereplő s_i polinom. (Ez általában nem vektortérbázis, hiszen tipikus esetben az s_i polinomok közül az első néhány a konstans 1 lesz, és így a hozzá tartozó $u_i = 0$). Ha az s_i polinom gyöktényezős alakja

$$s_i(x) = (x - \lambda_1)^{k_1} \ldots (x - \lambda_\ell)^{k_\ell} ,$$

ahol mindegyik $k_j > 0$, akkor az u_i-ből $k_1 + \ldots + k_\ell$ darab vektort készítünk a következőképpen. Legyen $g_j(x) = s_i(x)/(x - \lambda_j)^{k_j}$ és $c_j = g_j(A)(u_i)$. Ekkor vektoraink

$$c_j,\ (A - \lambda_j I)c_j,\ (A - \lambda_j I)^2 c_j,\ \ldots\ , (A - \lambda_j I)^{k_j - 1} c_j ,$$

ahol $j = 1, 2, \ldots, \ell$. Ezt az eljárást mindegyik u_i-re elvégezve a kapott összes vektor bázist alkot, melyben a mátrix Jordan-alakú lesz. Az, hogy ez az eljárás helyes, automatikusan következik a most következő bizonyításban leírt gondolatokból, és a 7.3.9. Gyakorlatból.

Bizonyítás. Az első kérdés az, hogy miért pont az $L - xI$ mátrixot kell normálalakra hozni. Ennek megmutatásához a 7.4.8. Állításból indulunk ki. Eszerint a normálalakra hozandó (nagy) mátrixba az olyan $(p_1, \ldots, p_k)$ polinomsorozatokat kell tennünk, amelyekre

$$p_1 d_1 + \ldots + p_k d_k = 0\,.$$

Az $L - xI$ mátrix mindegyik sora ilyen polinomsorozat. Valóban, mivel az A mátrixa L transzponáltja, ha $L = ((t_{ij}))$, akkor

$$Ad_i = t_{i1} d_1 + \ldots + t_{ik} d_k\,,$$

ahonnan átrendezéssel

$$t_{i1} d_1 + \ldots + (t_{ii} - x) d_i + \ldots + t_{ik} d_k = 0$$

adódik. Elegendő megmutatni, hogy a többi $(p_1, \ldots, p_k)$ polinomsorozat már fölösleges, azaz megkapható az $L - xI$ mátrix soraiból (polinomegyütthatós) lineáris kombináció segítségével. Ekkor ugyanis a „nagy" mátrixban az eliminációt kezdhetjük úgy, hogy ezeket a $(p_1, \ldots, p_k)$ sorokat az $L - xI$ sorai segítségével kinullázzuk, és akkortól kezdve ezek már nem játszanak szerepet.

Az, hogy az $L - xI$ sorai már minden szükséges információt tartalmaznak, azon múlik, hogy már e sorok ismeretében is tudjuk, hogy

$$xd_i = t_{i1} d_1 + \ldots + t_{ik} d_k\,,$$

és így ezek a sorok teljesen leírják, hogy hogyan kell x-szel szorozni V elemeit, vagyis meghatározzák az $M(A, V)$ modulust.

Tegyük föl, hogy a „nagy" mátrixnak egy olyan $(p_1, p_2, \ldots, p_k)$ sora, ami mégsem állítható elő $L - xI$ sorainak lineáris kombinációjaként, és legyen p_i a(z egyik) legnagyobb fokú polinom a $p_1, \ldots, p_k$ között. Ha p_i nem konstans, és főtagja tx^ℓ, akkor a

$$(t_{i1}, \ldots, t_{ii} - x, \ldots, t_{ik})$$

sor $tx^{\ell-1}$-szeresét adjuk hozzá $(p_1, p_2, \ldots, p_k)$-hoz. Ekkor ismét a „nagy" mátrix egy sorát kapjuk. Ebben már eggyel kevesebb ℓ-edfokú polinom van, mint eredetileg volt, és az új sor szintén nem áll elő az $L - xI$ sorainak lineáris kombinációjaként (különben az eredeti $(p_1, p_2, \ldots, p_k)$ is előállna). Az eljárást ismételgetve az összes ℓ-edfokú polinomot eltüntethetjük. Ezután folytassuk a sor $\ell - 1$-edfokú polinomjaival, és így tovább. Végül a „nagy" mátrix egy csupa konstans polinomokból álló $(t_1, \ldots, t_k)$ sorát kapjuk, amely még mindig nem áll elő az $L - xI$ sorainak lineáris kombinációjaként. Mivel ez sora a mátrixnak,

$$t_1 d_1 + \ldots + t_k d_k = 0\,,$$

és így a $d_1, \dots, d_k$ függetlensége miatt valamennyi $t_i = 0$. Ez ellentmondás, mert az azonosan nulla sor előáll, mint $L - xI$ sorainak lineáris kombinációja. Beláttuk tehát, hogy tényleg elegendő az $L - xI$ mátrixot normálalakra hozni.

Legyen $M = M(A, V)$. A 7.4.7. Lemma szerint tehát

$$M = \langle u_1 \rangle \oplus \dots \oplus \langle u_k \rangle ,$$

ahol u_i rendje s_i (a normálalak főátlójában szereplő polinom). Már láttuk, hogy M egyik elemének a rendje sem nulla (7.3.18. Gyakorlat), ezért $s_i \neq 0$. Ha

$$s_i(x) = (x - \lambda_1)^{k_1} \dots (x - \lambda_\ell)^{k_\ell} ,$$

akkor a 7.3.9. Gyakorlatban leírt módon $\langle u_i \rangle$ szétbontható prímhatványrendű ciklikus modulusok direkt összegére, ahol a szereplő prímhatványok pontosan az $(x - \lambda_j)^{k_j}$ polinomok lesznek. Tudjuk, hogy mindegyik ilyen összeadandóhoz egy $k_j \times k_j$ méretű Jordan-blokk tartozik, amelyben a λ_j szerepel. Ezzel a 7.6.6. Tétel (3)-as állítását beláttuk.

A tétel (1) állítása azért igaz, mert az A karakterisztikus polinomja $\det(L - xI)$ (figyelembe véve, hogy transzponáláskor a determináns nem változik). Ha az eliminációt végrehajtjuk, akkor a determinánsnak csak az előjele változhat meg. Az eljárás végén kapott mátrix determinánsa viszont $s_1 s_2 \dots s_k$. Végül a (2) állítás abból következik, hogy az s_k elem az $M(A, V)$ modulus exponense (7.4.9. Következmény), ami ugyanaz, mint az A minimálpolinomja a 7.3.18. Gyakorlat miatt. □

7.6.7. Feladat. Mutassuk meg, hogy egy mátrixnak és a transzponáltjának ugyanaz a minimálpolinomja és a Jordan-alakja, sőt a karakterisztikus mátrixuk normálalakja is.

Gyakorlatok, feladatok

7.6.8. Gyakorlat. Számítsuk ki a 7.4.12. Gyakorlatban szereplő mátrixok transzponáltjainak minimálpolinomját és Jordan-alakját.

7.6.9. Gyakorlat. Számítsuk ki az alábbi mátrixokhoz tartozó karakterisztikus mátrix normálalakját, és ennek alapján adjuk meg minimálpolinomjukat és Jordan-alakjukat.

$$\begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \begin{pmatrix} -3 & -4 & 1 \\ 6 & 9 & -2 \\ 15 & 24 & -5 \end{pmatrix} \qquad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

7.6.10. Gyakorlat. Az alábbiakban megadjuk egy-egy komplex elemű (ismeretlen) L mátrix esetében az $L - xI$ normálalakjában a főátlóban szereplő polinomokat. Adjuk meg e mátrix minimálpolinomját és a Jordan-féle normálalakját.

(1) $\{1, x^2\}$.
(2) $\{x, x, x\}$.
(3) $\{1, 1, x^3\}$.
(4) $\{1, 1, 1, 1, 1, 1, x, x(x-1)^2, x^3(x-1)^2\}$.

7.6.11. Gyakorlat. Számítsuk ki egy Jordan-blokk karakterisztikus mátrixának normálalakját.

7.6.12. Feladat. Igazoljuk, hogy végtelen test fölött egy lineáris transzformációnak akkor és csak akkor van véges sok invariáns altere, ha minimálpolinomjának foka megegyezik a tér dimenziójával. Hány invariáns altér van ilyenkor?

7.7. Homomorfizmusok csoportjai

A lineáris algebrában két vektortér közötti lineáris leképezések halmazán is értelmeztünk műveleteket, és ilyenkor vektorteret kaptunk. Modulusok esetében a $\mathrm{Hom}_R(M, N)$ halmaz szintén Abel-csoporttá, és kommutatív R esetén bal oldali R-modulussá is tehető. Tanulmányozni fogjuk az így kapott modulusok közötti homomorfizmusokat is.

7.7.1. Definíció. Legyenek M és N bal oldali R-modulusok, és $\varphi, \psi \in \mathrm{Hom}_R(M, N)$ (lásd 7.1.6. Definíció). Ekkor a *pontonkénti összegüket* a

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m)$$

képlet definiálja (ez szintén R-homomorfizmus lesz). Ha $r \in R$, akkor legyen

$$(r\varphi)(m) = r\varphi(m)\,.$$

Az $r\varphi$ ***csak kommutatív R esetén lesz R-homomorfizmus*** (lásd 7.7.3. Gyakorlat).

7.7.2. Gyakorlat. Mutassuk meg, hogy a most definiált összeadásra $\mathrm{Hom}_R(M, N)$ csoport, és ha R kommutatív, akkor a fent definiált skalárral szorzásra R-modulus is. Mi ennek a csoportnak a nulleleme? Igazoljuk, hogy egy homomorfizmus ellentettje ugyanaz, mint a -1-szerese. Végül ellenőrizzük, hogy R-homomorfizmusok kompozíciója is R-homomorfizmus.

Az ${}_RR$ bal oldali moduluson az r-rel való jobbszorzás mindig R-homomorfizmus az R asszociativitása miatt, az r-rel való balszorzás azonban általában nem.

7.7.3. Gyakorlat. Legyen R tetszőleges gyűrű és $r \in R$. Értelmezzük a $\psi_r : R \to R$ leképezést a $\psi_r(x) = xr$ képlettel (ez az r-rel való jobbszorzás). Mutassuk meg, hogy $\psi_r \in \mathrm{Hom}_R({}_RR, {}_RR)$. Speciálisan $\psi_1 = id_R$. Igazoljuk, hogy ha minden $r \in R$ esetén $r id_R$ (ami az r-rel való balszorzás) is R-homomorfizmus, akkor R kommutatív.

A $\mathrm{Hom}_R(M, N)$ kiszámítása nem mindig egyszerű feladat. Ennek érzékeltetésére néhány példát mutatunk az Abel-csoportok (vagyis $\mathbb{Z}$-modulusok) esetében.

7.7.4. Kérdés. Melyik ismert csoporttal izomorf a $\mathrm{Hom}(\mathbb{Z}_2^+, \mathbb{Z}_3^+)$ Abel-csoport?

Ha egy g csoportelem képét vesszük egy homomorfizmusnál, akkor annak rendje a g rendjének osztója lesz (4.3.12. Gyakorlat). Az $1 \in \mathbb{Z}_2$ elem rendje 2, ezért $\varphi(1)$ rendje 1 vagy 2 tetszőleges $\varphi \in \mathrm{Hom}(\mathbb{Z}_2^+, \mathbb{Z}_3^+)$ homomorfizmusnál. Lagrange tétele szerint a 2 nem lehetséges, hiszen $2 \nmid 3$. Ezért $\varphi(1)$ rendje 1, vagyis $\varphi(1) = 0$. Ezért $\varphi = 0$, vagyis $\mathrm{Hom}(\mathbb{Z}_2^+, \mathbb{Z}_3^+)$ csak a nullelemből áll.

7.7.5. Gyakorlat. Mutassuk meg, hogy ha m és n relatív prím pozitív egészek, akkor $\mathrm{Hom}(\mathbb{Z}_m^+, \mathbb{Z}_n^+) = 0$.

7.7.6. Kérdés. Melyik ismert csoporttal izomorf a $\mathrm{Hom}(\mathbb{Z}_4^+, \mathbb{Z}_4^+)$ Abel-csoport?

Legyen $\varphi \in \mathrm{Hom}(\mathbb{Z}_4^+, \mathbb{Z}_4^+)$, és $b = \varphi(1)$. Ekkor persze $\varphi(2) = \varphi(1+1) = b + b = 2b$ és $\varphi(3) = \varphi(2+1) = \varphi(2) + \varphi(1) = 2b + b = 3b$. Vagyis φ a $\mathbb{Z}_4$ minden elemét a b-szeresébe viszi, jelöljük ezt a leképezést φ_b-vel. A b értéke 0, 1, 2 vagy 3 lehet, és φ_b mindegyik esetben nyilván homomorfizmus. Ezért

$$\mathrm{Hom}(\mathbb{Z}_4^+, \mathbb{Z}_4^+) = \{\varphi_0, \varphi_1, \varphi_2, \varphi_3\}\,.$$

Melyik négyelemű csoporttal izomorf ez a csoport? Vegyük észre, hogy

$$(\varphi_b + \varphi_c)(1) = \varphi_b(1) + \varphi_c(1) = b + c\,,$$

és ezért $\varphi_b + \varphi_c = \varphi_{b+c}$. Vagyis a $b \leftrightarrow \varphi_b$ leképezés művelettartó (és kölcsönösen egyértelmű) $\mathrm{Hom}(\mathbb{Z}_4^+, \mathbb{Z}_4^+)$ és $\mathbb{Z}_4^+$ között.

7.7.7. Gyakorlat. Mutassuk meg, hogy $\mathrm{Hom}(\mathbb{Z}_n^+, \mathbb{Z}_n^+) \cong \mathbb{Z}_n^+$.

7.7.8. Kérdés. Melyik ismert csoporttal izomorf a $\mathrm{Hom}(\mathbb{Z}_4^+, \mathbb{Z}_6^+)$ Abel-csoport?

Az előző gondolatmenet szerint haladunk, legyen $\varphi \in \mathrm{Hom}(\mathbb{Z}_4^+, \mathbb{Z}_6^+)$, és $b = \varphi(1)$. Most is ugyanúgy látszik, hogy $\varphi(x) = xb$ minden $x \in \mathbb{Z}_4$ esetén, jelöljük ezt a leképezést φ_b-vel. Az előző esettől eltérően azonban nem minden $b \in \mathbb{Z}_6$ esetén lesz φ_b homomorfizmus, ehhez ugyanis

$$\varphi_b(x +_4 y) = \varphi_b(x) +_6 \varphi_b(y)\,,$$

azaz $(x +_4 y)b = xb +_6 yb$ szükséges. Innen $x = y = 2$ helyettesítéssel $6 \mid 4b$ adódik, vagyis b csak 0 és 3 lehet. (Ez összevág azzal, hogy $b = \varphi(1)$ rendje osztója kell, hogy legyen 4-nek és 6-nak is.) Könnyű megmutatni, hogy φ_0 és φ_3 tényleg homomorfizmusok, és így $\mathrm{Hom}(\mathbb{Z}_4^+, \mathbb{Z}_6^+) \cong \mathbb{Z}_2^+$.

7.7.9. Gyakorlat. Mutassuk meg, hogy $\mathrm{Hom}(\mathbb{Z}_m^+, \mathbb{Z}_n^+) \cong \mathbb{Z}_{(m,n)}^+$ (ahol (m, n) az m és n pozitív egészek legnagyobb közös osztója).

A most elhangzott gondolatmenet még egyszerűbb abban az esetben, ha a $\mathrm{Hom}(\mathbb{Z}^+, B)$ csoportot akarjuk kiszámítani. Ha φ ennek eleme, és $\varphi(1) = b$, akkor, mivel φ az ellentettképzést is tartja, $\varphi(x) = xb$ minden $x \in \mathbb{Z}$-re. Az így kapott φ_b leképezés mindig homomorfizmus. Ezt már beláttuk sokkal általánosabban is (7.2.12. Gyakorlat): ez jelenti azt, hogy ${}_{\mathbb{Z}}\mathbb{Z}$ az 1 elemmel generált szabad $\mathbb{Z}$-modulus. Ezért a $b \leftrightarrow \varphi_b$ leképezés

izomorfizmus lesz $\mathrm{Hom}(\mathbb{Z}^+, B)$ és B között. A következő gyakorlat ezt az észrevételt általánosítja.

7.7.10. Gyakorlat. Igazoljuk, hogy tetszőleges R gyűrű és M bal oldali R-modulus esetén $\mathrm{Hom}_R({}_RR, M) \cong M$ (kommutatív R esetén mint R-modulusok, általános R esetén mint Abel-csoportok lesznek izomorfak).

Speciálisan $\mathrm{Hom}_R({}_RR, {}_RR) \cong {}_RR$. Ha R test, akkor lineáris algebrából tudjuk, hogy a $\mathrm{Hom}_R(M, N)$ vektortér dimenziója az M és N vektorterek dimenzióinak szorzata (és ez izomorfia erejéig egyértelműen meghatározza a szerkezetét). Speciális (szabad) modulusok esetében ez tetszőleges R gyűrűre általánosítható.

7.7.11. Feladat. Legyenek M, N, K tetszőleges bal oldali R-modulusok. Igazoljuk, hogy

$$\mathrm{Hom}_R(M \times N, K) \cong \mathrm{Hom}_R(M, K) \times \mathrm{Hom}_R(N, K)\,,$$

és

$$\mathrm{Hom}_R(K, M \times N) \cong \mathrm{Hom}_R(K, M) \times \mathrm{Hom}_R(K, N)\,,$$

(ez csoport-izomorfizmusként értendő, ha R tetszőleges gyűrű, és R-izomorfizmusként, ha R kommutatív). Általánosítsunk véges sok tényezős direkt szorzatra. Igaz marad-e az állítás végtelen sok tényezős direkt szorzatra, illetve direkt összegre?

Az eddigieket összekombinálva

$$\mathrm{Hom}_R({}_RR^m, {}_RR^n) = {}_RR^{mn}\,,$$

ami az imént vektorterekre kimondott állítást általánosítja. A véges Abel-csoportok alaptétele miatt a 7.7.11. Feladat és a 7.7.9. Gyakorlat lehetővé teszi, hogy bármely két véges Abel-csoport Hom-csoportját kiszámítsuk.

7.7.12. Kérdés. Melyik ismert csoporttal izomorf a $\mathrm{Hom}(\mathbb{Q}^+, \mathbb{Z}^+)$ Abel-csoport?

Most az elemrendek vizsgálata nem segít, egy új ötletre van szükségünk. Tegyük föl, hogy $\varphi \in \mathrm{Hom}(\mathbb{Q}^+, \mathbb{Z}^+)$ és $\varphi(1) = b \in \mathbb{Z}$. Mi lesz az $1/n$ tört képe φ-nél? Nyilván

$$b = \varphi(1) = \varphi\big(n(1/n)\big) = n\varphi(1/n)\,,$$

ahonnan $\varphi(1/n) = b/n$. Mivel $\varphi(1/n) \in \mathbb{Z}$, ez azt jelenti, hogy b minden nem nulla egész számmal osztható, és így csakis nulla lehet. Ugyanez a gondolatmenet nemcsak az 1 képére mondható el, hanem $\mathbb{Q}$ mindegyik elemének a képére is. Ezért $\varphi = 0$, és így $\mathrm{Hom}(\mathbb{Q}^+, \mathbb{Z}^+) = 0$.

7.7.13. Definíció. Azt mondjuk, hogy az A Abel-csoport egy a eleme osztható az n egész számmal, ha van olyan $b \in A$, melyre $a = nb$. Az A *osztható csoport*, ha minden eleme minden nem nulla egész számmal osztható (vagyis ha $nA = A$ minden $n \neq 0$ egészre).

7.7.14. Gyakorlat. Mutassuk meg, hogy ha A osztható csoport, és a B csoportnak nincs a $\{0\}$ részcsoporton kívül osztható részcsoportja, akkor $\mathrm{Hom}(A, B) = 0$.

7.7.15. Gyakorlat. Mutassuk meg, hogy ha egy tetszőleges csoportban az a elem rendje $n < \infty$, akkor a osztható minden n-hez relatív prím számmal.

7.7.16. Definíció. Legyen p prímszám. A p-hatványadik komplex egységgyökök csoportját a szorzásra *kváziciklikus csoportnak* nevezzük, és $\mathbb{Z}_{p^\infty}$-nel jelöljük.

Az elnevezést a következő gyakorlat magyarázza meg.

7.7.17. Gyakorlat. Igazoljuk, hogy a $\mathbb{Z}_{p^\infty}$ csoport minden valódi részcsoportja p-hatvány rendű ciklikus csoport, minden n-re pontosan egy p^n rendű részcsoport van, és bármely két részcsoport közül az egyik tartalmazza a másikat (vagyis a részcsoportok láncot alkotnak).

7.7.18. Gyakorlat. Mutassuk meg, hogy a kváziciklikus csoportok oszthatók.

7.7.19. Feladat. Mutassuk meg, hogy véges Abel-csoport nem lehet osztható, kivéve ha csak a nullából áll.

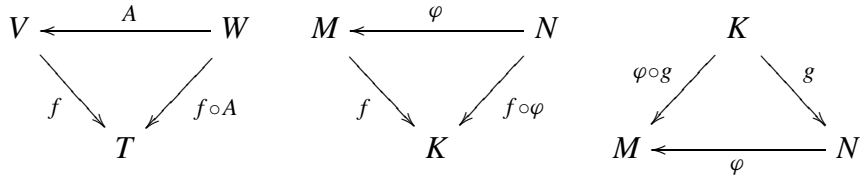
Nevezetes tétel a következő, amelyet bizonyítás nélkül közlünk.

7.7.20. Tétel. *Egy Abel-csoport akkor és csak akkor osztható, ha a $\mathbb{Q}^+$ és a $\mathbb{Z}_{p^\infty}$ csoportok példányainak direkt összegével izomorf (mindegyik fajta tényezőből akár végtelen sokat, akár nulla darabot is vehetünk).*

Lineáris algebrában vizsgáltuk egy T test fölötti V vektortér úgynevezett duális terét, ez a $V^* = \mathrm{Hom}(V, T)$ vektortér, amelyről meg lehet mutatni, hogy véges dimenziós V esetén V-vel izomorf. Ha $A : W \to V$ egy lineáris leképezés, akkor legyen $A^* : V^* \to W^*$ az a leképezés, amely tetszőleges $f \in V^*$-hoz azt az $A^*(f) \in W^*$ leképezést rendeli, amelyre

$$\big(A^*(f)\big)(w) = f\big(A(w)\big)\,.$$

tetszőleges $w \in V$ esetén. Mászóval $A^*(f) = f \circ A$.



7.7.21. Feladat. Mutassuk meg, hogy az A^* mátrixa az A mátrixának transzponáltja alkalmas bázispárban.

Az előző feladat az A^* leképezés fontosságát támasztja alá. Az eddigieket általánosíthatjuk: egyrészt a T alaptest helyett tetszőleges vektorteret vehetünk, másrészt vektorterek helyett modulusokról beszélhetünk. Ennek alapján, ha $\varphi : N \to M$ egy R-homomorfizmus, és K tetszőleges modulus, akkor definiálhatjuk a $\chi : \mathrm{Hom}_R(M, K) \to \mathrm{Hom}_R(N, K)$ leképezést a fentihez hasonlóan a

$$\big(\chi(f)\big)(w) = f\big(\varphi(w)\big)$$

képlettel, ahol $f \in \mathrm{Hom}_R(M, K)$ és $w \in N$ (tehát $\chi(f) = f \circ \varphi$). Hasonlóképpen definiálhatjuk a $\chi : \mathrm{Hom}_R(K, N) \to \mathrm{Hom}_R(K, M)$ leképezést is a

$$\big(\chi(g)\big)(u) = \varphi\big(g(u)\big)$$

képlettel, ahol $g \in \mathrm{Hom}_R(K, N)$ és $u \in K$ (tehát most $\chi(g) = \varphi \circ g$). Valójában mindez speciális esete a következő definíciónak.

7.7.22. Definíció. Legyenek M, N, K, L modulusok az R fölött, $\varphi \in \mathrm{Hom}_R(N, M)$ és $\psi \in \mathrm{Hom}_R(K, L)$. Ekkor $\mathrm{Hom}(\varphi, \psi)$ az a leképezés $\mathrm{Hom}_R(M, K)$-ból $\mathrm{Hom}_R(N, L)$-be, amelyre tetszőleges $f \in \mathrm{Hom}_R(M, K)$ esetén $\mathrm{Hom}(\varphi, \psi)(f) = \psi \circ f \circ \varphi$.

$$\begin{array}{ccc} M & \xrightarrow{f} & K \\ {\scriptstyle\varphi}\uparrow & & \downarrow{\scriptstyle\psi} \\ N & \xrightarrow{\psi\circ f\circ\varphi} & L \end{array}$$

7.7.23. Gyakorlat. Mutassuk meg, hogy a most definiált $\mathrm{Hom}(\varphi, \psi)$ leképezés csoporthomomorfizmus, és kommutatív R esetén R-homomorfizmus is.

Speciálisan ha $\varphi \in \mathrm{Hom}_R(N, M)$, akkor

$$\mathrm{Hom}(\varphi, id_K) : \mathrm{Hom}_R(M, K) \to \mathrm{Hom}_R(N, K)$$

és

$$\mathrm{Hom}(id_K, \varphi) : \mathrm{Hom}_R(K, N) \to \mathrm{Hom}_R(K, M)$$

az előző bekezdésben tárgyalt homomorfizmusok. Még speciálisabban a fenti A^* lineáris leképezés valójában $\mathrm{Hom}(A, id_T)$.

7.7.24. Gyakorlat. Mutassuk meg, hogy a fenti leképezések tartják a kompozíció műveletét, vagyis ha $\varphi : N \to M$ és $\psi : M \to L$ modulus-homomorfizmusok, akkor

$$\mathrm{Hom}(\psi \circ \varphi, id_K) = \mathrm{Hom}(\varphi, id_K) \circ \mathrm{Hom}(\psi, id_K)$$

és

$$\mathrm{Hom}(id_K, \psi \circ \varphi) = \mathrm{Hom}(id_K, \psi) \circ \mathrm{Hom}(id_K, \varphi)\,.$$

Felhívjuk a figyelmet arra, hogy a $\varphi \mapsto \mathrm{Hom}(\varphi, id_K)$ leképezés „megfordítja a nyilak irányát”, vagyis egy $N \to M$ leképezésből egy $\mathrm{Hom}_R(M, K) \to \mathrm{Hom}_R(N, K)$ leképezést csinál (az M és N betűk megcserélődtek). Emiatt a kompozíció (azaz a φ és a ψ) sorrendje is „megfordul” az előző gyakorlat első egyenlőségében. Erről a jelenségről a kategóriákról szóló szakaszban, az úgynevezett kontravariáns funktorok tárgyalásakor lesz részletesebben szó (lásd 8.8.9. Definíció).

A most definiált $\mathrm{Hom}(\varphi, \psi)$ leképezések elsődleges haszna az, hogy információt nyújtanak a $\mathrm{Hom}_R(M, K)$ és $\mathrm{Hom}_R(N, L)$ csoportokról, mindez a homlógiaelmélet egyik alappillére. Ennek részleteiről itt nem beszélünk (megelégszünk azzal, hogy néhány konkrét $\mathrm{Hom}(\varphi, \psi)$ homomorfizmust kiszámítunk a 7.7.27. Feladatban). Az Olvasónak érdemes

fellapoznia a [**13**] könyv 9. Fejezetét, különösen az egzakt sorozatokról és a modulusbővítésekről szóló részeket, ha minderről több információt akar kapni.

Gyakorlatok, feladatok

7.7.25. Gyakorlat. Melyik ismert Abel-csoporttal izomorfak az alábbi csoportok?

(1) $\mathrm{Hom}(\mathbb{Z}_n^+, \mathbb{Z}^+)$.
(2) $\mathrm{Hom}(\mathbb{Q}^+, \mathbb{Z}_n^+)$.
(3) $\mathrm{Hom}(\mathbb{Q}^+, \mathbb{Q}^+)$.
(4) $\mathrm{Hom}(\mathbb{Z}_{p^\infty}, \mathbb{Z}_n^+)$.

7.7.26. Gyakorlat. Legyen B Abel-csoport. Mutassuk meg, hogy $\mathrm{Hom}(\mathbb{Z}_m^+, B) \cong B[m]$, ahol $B[n] = \{b \in B \,:\, mb = 0\}$ (vö. 7.3.12. Definíció).

7.7.27. Feladat. Legyen A rendre $\mathbb{Z}^+$, $\mathbb{Z}_m^+$, $\mathbb{Z}_{p^\infty}$, $\mathbb{Q}^+$, és φ az alábbi négyféle leképezés:

(1) $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ az a homomorfizmus, ami minden elemhez az n-szeresét rendeli.
(2) $\varphi : \mathbb{Z}_m \to \mathbb{Z}_{nm}$, az n-nel szorzás.
(3) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ a mod n vett maradék képzése.
(4) φ a $\mathbb{Z} \to \mathbb{Q}$ beágyazás.

Számítsuk ki a $\mathrm{Hom}(id_A, \varphi)$ és $\mathrm{Hom}(\varphi, id_A)$ homomorfizmusokat. Vizsgáljuk meg, hogyan függ össze φ és az eredmény injektivitása, illetve szürjektivitása.

7.7.28. Gyakorlat. Legyen A Abel-csoport. Ebben a gyakorlatban áttekintjük azokat a gyűrűket, amelyek fölött az A csoport R-modulussá tehető. Legyen S az A endomorfizmusainak (vagyis az $A \to A$ homomorfizmusoknak) a gyűrűje a pontonkénti összeadásra és a kompozícióra.

(1) Mutassuk meg, hogy S tényleg gyűrű, és a $\varphi a = \varphi(a)$ definíció az A-t bal oldali (unitér) S-modulussá teszi.
(2) Tegyük föl, hogy A egy (unitér) R-modulus. Tetszőleges $r \in R$ esetén jelöljük $\Theta(r)$-rel azt az $A \to A$ leképezést, amely az $a \in A$-hoz az ra-t rendeli. Mutassuk meg, hogy $\Theta(r) \in S$, és $\Theta : R \to S$ egy gyűrűhomomorfizmus, amely az egységelemet az egységelembe viszi.
(3) Tegyük föl, hogy R egy gyűrű, és $\Theta : R \to S$ egy gyűrűhomomorfizmus, amely az egységelemet az egységelembe viszi. Mutassuk meg, hogy akkor az A csoportból (unitér) R-modulus lesz, ha a szorzást az $ra = \Theta(r)(a)$ képlettel definiáljuk.

7.8. A tenzorszorzat

Legyenek M és N bal oldali R-modulusok. Az M-ből N-be képező R-homomorfizmusok $\mathrm{Hom}_R(M, N)$ halmazáról láttuk, hogy csoport az összeadásra, sőt kommutatív R esetén R-modulus. Lineáris algebrában fontos szerepe volt a bilineáris leképezéseknek is. Ezeket modulusok esetében *bihomomorfizmusoknak* hívják. Most megmutatjuk, hogyan lehet

a bihomomorfizmusok vizsgálatát közönséges R-homomorfizmusok vizsgálatára visszavezetni. Itt is megváltozik a fogalmak viselkedése, ha az R gyűrű nem kommutatív. Ezért ***ebben a szakaszban minden gyűrűről feltesszük, hogy kommutatív.***

7.8.1. Definíció. Legyenek M, N és K bal oldali R-modulusok. Azt mondjuk, hogy az

$$f : M \times N \to K$$

leképezés *bihomomorfizmus*, ha mindkét változójában R-homomorfizmus (miközben a másik változó fixen marad). Vagyis tetszőleges $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ és $r \in R$ esetén

(1) $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$.
(2) $f(rm, n) = rf(m, n)$.
(3) $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$.
(4) $f(m, rn) = rf(m, n)$.

Nyilván $f(0, n) = 0 = f(m, 0)$ és $f(-m, n) = -f(m, n) = f(m, -n)$ teljesül minden f bihomomorfizmusra, hiszen minden homomorfizmus nullát nullába visz, és az ellentettképzést is tartja. Most két fontos példát mutatunk bihomomorfizmusra. A másodikat már ismerjük lineáris algebrából. Az első példa szerint a *szorzás* tipikus bihomomorfizmus.

7.8.2. Gyakorlat. Legyen R (kommutatív) gyűrű. Mutassuk meg, hogy az $f(x, y) = xy$ leképezés bihomomorfizmus ${}_R R \times {}_R R$-ből ${}_R R$-be.

Ha R nem kommutatív, akkor a szorzás, vagyis az $(x, y) \to xy$ leképezés nem lesz bihomomorfizmus a fenti értelemben, mert ahhoz $r(xy) = x(ry)$-nak kellene teljesülnie. De a gyengébb $(xr)y = x(ry)$ összefüggés teljesül. Ezért nemkommutatív gyűrűk fölött a bihomomorfizmus definíciójában csak egy ennek megfelelő, gyengébb feltételt követelnek meg.

7.8.3. Gyakorlat. Legyen T test, $M = T^k$ és $N = T^\ell$, ezeket most T-modulusnak (vagyis vektortérnek) tekintjük. Ekkor tetszőleges $f : M \times N \mapsto {}_T T$ bihomomorfizmus a következő képlettel adható meg: ha

$$u = \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} \qquad \text{és} \qquad v = \begin{bmatrix} y_1 \\ \vdots \\ y_\ell \end{bmatrix},$$

akkor

$$f(u, v) = \sum_{i=1}^{k} \sum_{j=1}^{\ell} t_{ij} x_i y_j \,,$$

ahol $t_{ij} \in T$ alkalmas elemek (amelyek az f-et meghatározzák).

Az itt szereplő t_{ij} elemeket egy mátrixba tettük, és ezt a mátrixot hívtuk az f bilineáris *függvény* mátrixának (a bilineáris függvények azok a bilineáris leképezések, amelyek a T alaptestbe képeznek). Ez a második példa úgy is felfogható, hogy f az $x_i y_j$ képlettel

megadott bihomomorfizmusok (vagyis szorzások) egy lineáris kombinációja. Ahhoz, hogy ez a mondat értelmes legyen, az kell, hogy a bihomomorfizmusok is modulust alkossanak.

7.8.4. Gyakorlat. Mutassuk meg, hogy az $M \times N$-ből K-ba vezető bihomomorfizmusok a pontonkénti műveletekre nézve R-modulust alkotnak.

Át szeretnénk tekinteni, adott M és N esetén az összes $M \times N$-en értelmezett bihomomorfizmust. Ezek persze nem függetlenek egymástól, ha egyet ismerünk, akkor egy homomorfizmus utánafűzésével másmilyeneket is tudunk gyártani.

7.8.5. Gyakorlat. Tegyük föl, hogy $f : M \times N \to K$ bihomomorfizmus, és $\varphi : K \to K'$ egy R-homomorfizmus. Mutassuk meg, hogy az

$$(m, n) \mapsto \varphi f(m, n)$$

képlettel definiált $\varphi f : M \times N \to K'$ függvény is bihomomorfizmus.

Az általános eset vizsgálata előtt néhány konkrét példát számolunk ki. Az Olvasót arra biztatjuk, hogy ismételje át a 7.7.25. Gyakorlat és a 7.7.10. Feladat megoldását, mielőtt az alábbiakat elolvasná.

7.8.6. Példa. Legyen $M = N = \mathbb{Z}^+$ (mint Abel-csoport, vagyis $\mathbb{Z}$-modulus).

Mivel $\mathbb{Z}$ gyűrű is, egy bihomomorfizmust biztosan ismerünk, mégpedig a szorzást, vagyis az $f_0(m, n) = mn$ leképezést $\mathbb{Z}$-be. Ha tehát $\varphi : \mathbb{Z}^+ \to K$ egy csoporthomomorfizmus egy K csoportba, akkor az $f(m, n) = \varphi(mn)$ bihomomorfizmus lesz $\mathbb{Z}^+ \times \mathbb{Z}^+$-ból K-ba. Tudunk-e még más példát is mondani?

A válasz az, hogy nem. Tegyük föl ugyanis, hogy $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to K$ egy bihomomorfizmus, és jelölje az $f(1, 1)$ elemet g. Ekkor

$$f(m, n) = f(m \cdot 1, n \cdot 1) = mnf(1, 1) = mng\,.$$

Legyen $\varphi : \mathbb{Z}^+ \to K$ az a homomorfizmus, melyre $\varphi(n) = ng$. Ekkor nyilván

$$f(m, n) = \varphi(mn)\,,$$

mert mindkettő mng.

7.8.7. Gyakorlat. Legyen $M = N = \mathbb{Z}_3^+$ mint Abel-csoport. Módosítsuk az iménti gondolatmenetet annak megmutatására, hogy minden $f : \mathbb{Z}_3^+ \times \mathbb{Z}_3^+ \to K$ bihomomorfizmus $f(m, n) = \varphi(mn)$ alakú alkalmas $\varphi : \mathbb{Z}_3^+ \to K$ homomorfizmusra.

7.8.8. Példa. Legyen $M = \mathbb{Z}_2^+$ és $N = \mathbb{Z}_3^+$ mint Abel-csoport.

Ez könnyebb, mint az eddigiek. Ha ugyanis $f : \mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \to K$ bihomomorfizmus, és $g = f(1, 1)$, akkor $2g = f(2 \cdot 1, 1) = f(0, 1) = 0$ és $3g = f(1, 3 \cdot 1) = f(1, 0) = 0$. Innen $g = 0$. De akkor f is azonosan nulla.

De akkor, miként az előző két példában, most is van egy olyan „kitüntetett” bihomomorfizmus, hogy az összes többi ebből egy homomorfizmus utánafűzésével kapható! Ez a kitüntetett bihomomorfizmus most a nulla (amely a nulla csoportba megy).

7.8.9. Példa. Legyen M és N a sík, mint $\mathbb{R}$ fölötti vektortér.

Most nem tippeljük meg előre a „kitüntetett" bihomomorfizmust, mint eddig, hanem megpróbálunk rájönni, mi is lehet ez. Legyen tehát $f : M \times N \to K$ bihomomorfizmus, ahol most K egy $\mathbb{R}$ fölötti vektortér. Legyen b_1, b_2 a sík egy bázisa. Az alábbi átalakítás ismerős lineáris algebrából:

$$f(x_1b_1 + x_2b_2, y_1b_1 + y_2b_2) = \\ = x_1y_1f(b_1, b_1) + x_1y_2f(b_1, b_2) + x_2y_1f(b_2, b_1) + x_2y_2f(b_2, b_2)\,.$$

Ha tehát a $g_{ij} = f(b_i, b_j) \in K$ elemeket valaki megmondja, akkor már f-et ki tudjuk számítani. Mivel a lehető legáltalánosabb bihomomorfizmust keressük, az ehhez tartozó K_0-t úgy választjuk, hogy ez a négy elem lineárisan független legyen.

Legyen tehát K_0 egy rögzített négydimenziós vektortér, amelyben a b_{11}, b_{12}, b_{21}, b_{22} elemek bázist alkotnak, és definiáljunk egy f_0 bilineáris függvényt a

$$f_0(x_1b_1 + x_2b_2, y_1b_1 + y_2b_2) = x_1y_1b_{11} + x_1y_2b_{12} + x_2y_1b_{21} + x_2y_2b_{22}$$

képlettel. Ekkor egy tetszőleges $f : M \times N \to K$ megkapható f_0-ból egy homomorfizmus utánafűzésével. Valóban, ezt a $\varphi : K_0 \to K$ homomorfizmust úgy definiálhatjuk, hogy

$$\varphi(b_{ij}) = f(b_i, b_j)$$

legyen. Ilyen φ az előírhatósági tétel miatt egyértelműen létezik, és nyilván $f = \varphi f_0$.

7.8.10. Tétel. *Legyenek M és N bal oldali R-modulusok (ahol R egy kommutatív gyűrű). Ekkor van egy „legáltalánosabb" $M \times N$-en értelmezett bihomomorfizmus, abban az értelemben, hogy minden bihomomorfizmus ebből egy homomorfizmus utánafűzésével kapható. Pontosabban, létezik egy K_0 bal oldali R-modulus, és egy $f_0 : M \times N \to K_0$ bihomomorfizmus, hogy tetszőleges $f : M \times N \to K$ bihomomorfizmushoz egyértelműen található egy $\varphi : K_0 \to K$ modulus-homomorfizmus, melyre $f = \varphi f_0$ teljesül.*

Bizonyítás. Egy nagyon tanulságos, tipikusan algebrista módszerrel megkonstruálunk egy K_0 modulust, és hozzá egy f_0 bihomomorfizmust, amelyek teljesítik a feltételeket. Durván fogalmazva: ezeket olyan szabadra csináljuk, amennyire csak lehetséges. Az Olvasónak esetleg érdemes átismételnie a definiáló relációkról szóló csoportelméleti tételeket (4.9. Szakasz), mielőtt ezt a bizonyítást megismeri.

A legjobb az lenne, ha K_0-ban szabad generátorrendszert, más szóval bázist alkotnának az $f_0(m, n)$ elemek. Mert egy bázison előírhatjuk a homomorfizmusokat, és így találhatnánk olyan φ-t is, mely $f_0(m, n)$-et a kívánt helyre, vagyis $f(m, n)$-be képzi.

Ennyire szabadon azonban nem dolgozhatunk. Hiszen például $f_0(0, 0)$ a nullelem kell hogy legyen K_0-ban, és így nem lehet benne bázisban. De ez nem okoz bajt, mert $f(0, 0)$ is a nullelem lesz K-ban, és bármelyik $\varphi : K_0 \to K$ homomorfizmus a nullát nullába viszi, vagyis a $(0, 0)$ elempár automatikusan rendben lesz.

Vannak az $f_0(m, n)$ vektorok között további „kényszerű" összefüggések is. Például $f_0(m_1 + m_2, n)$ az $f_0(m_1, n)$ és az $f_0(m_2, n)$ összege kell, hogy legyen. De ez megint nem okoz majd bajt, mert ugyanezt az összefüggést f-nek is teljesítenie kell.

Tekintsük tehát azt az F szabad R-modulust (azaz ${}_RR$ alkalmas számú példányban vett direkt összegét), amelynek pont annyi báziseleme van, ahány $(m, n) \in M \times N$ pár. Ezeket a báziselemeket jelöljük $b(m, n)$-nel. Az $f_0(m, n) = b(m, n)$ leképezés persze nem lesz bihomomorfizmus. Ezért F-et lefaktorizáljuk úgy, hogy már az legyen.

Tekintsük F-nek a következő elemeit, midőn m_1, m_2, m befutja M-et, n_1, n_2, n befutja N-et, és r befutja R-et.

(1) $b(m_1 + m_2, n) - b(m_1, n) - b(m_2, n)$.
(2) $b(rm, n) - rb(m, n)$.
(3) $b(m, n_1 + n_2) - b(m, n_1) - b(m, n_2)$.
(4) $b(m, rn) - rb(m, n)$.

Jelölje E az összes ilyen elem által generált részmodulust, legyen $K_0 = F/E$, és definiáljuk az $f_0 : M \times N \to K_0$ függvényt az

$$f_0(m, n) = b(m, n) + E$$

képlettel. Megmutatjuk, hogy ezek kielégítik a feltételeket.

Az f_0 bihomomorfizmus lesz, mert a faktorizálást ennek megfelelően végeztük. Például az $f_0(rm, n) = rf_0(m, n)$ összefüggés bizonyítása: $b(rm, n) - rb(m, n) \in E$, és így

$$f_0(rm, n) = b(rm, n) + E = rb(m, n) + E = rf_0(m, n)$$

(az utolsó egyenlőség azért igaz, mert így definiáltuk faktormodulusban az r-rel való szorzást). Hasonlóan látható be a többi azonosság is, és így f_0 tényleg bihomomorfizmus.

Legyen most $f : M \times N \to K$ egy tetszőleges bihomomorfizmus. Meg akarjuk mutatni, hogy f megkapható f_0-ból egy alkalmas φ utánafűzésével, vagyis van olyan $\varphi : K_0 \to K$ modulus-homomorfizmus, melyre $f(m, n) = \varphi f_0(m, n)$ tetszőleges $(m, n) \in M \times N$ esetén. Ehhez tekintsük azt a $\varphi_0 : F \to K$ modulus-homomorfizmust, melynél tetszőleges $b(m, n)$ szabad generátor képe $f(m, n)$. Ilyen φ_0 létezik, hiszen F szabad. Legyen $u \in F$ esetén

$$\varphi(u + E) = \varphi_0(u)\,.$$

Meg kell mutatnunk, hogy az így definiált φ függvény jóldefiniált, azaz hogy $u+E = v+E$ esetén $\varphi_0(u) = \varphi_0(v)$. Valóban, ha $u - v \in E$, akkor $u - v$ fölírható E generátorainak R-beli együtthatós lineáris kombinációjaként:

$$u - v = \sum r_i w_i\,,$$

ahol mindegyik w_i a fenti (1) – (4) pontokban fölírt elemek valamelyike. Ahhoz, hogy $\varphi_0(u - v) = 0$ teljesüljön, elég tehát megmutatni, hogy $\varphi(w_i) = 0$ minden ilyen w_i-re (hiszen φ_0 modulus-homomorfizmus). Ezt csak az (1) típusú generátorokra tesszük meg, a másik három esetet az Olvasóra bízzuk. Ha tehát $w_i = b(m_1+m_2, n)-b(m_1, n)-b(m_2, n)$,

akkor

$$\begin{aligned}\varphi_0(w_i) &= \varphi_0(b(m_1+m_2,n)-b(m_1,n)-b(m_2,n)) = \\ &= \varphi_0(b(m_1+m_2,n)) - \varphi_0(b(m_1,n)) - \varphi_0(b(m_2,n)) = \\ &= f(m_1+m_2,n) - f(m_1,n) - f(m_2,n) = 0\,,\end{aligned}$$

hiszen f bihomomorfizmus. Ezzel tehát beláttuk, hogy φ jóldefiniált.

Azt könnyű kiszámolni, hogy φ művelettartó (lásd a 7.1.14. Gyakorlatot). Nyilvánvalóan teljesül az $f(m,n) = \varphi f_0(m,n)$ összefüggés is, hiszen

$$\varphi f_0(m,n) = \varphi(b(m,n)+E) = \varphi_0(b(m,n)) = f(m,n)\,.$$

Tehát φ a kívánt tulajdonságú.

Meg kell még mutatni, hogy φ egyértelmű. Ez abból következik, hogy a $b(m,n)$ elemek generálják F-et, tehát a K_0-t is generálják ezek képei, vagyis az $f_0(m,n)$ alakú elemek, ahol (m,n) befutja $M\times N$-et. De φ értéke az $f_0(m,n)$ elemen meg van adva (nevezetesen $f(m,n)$), és ezért az ilyen elemek lineáris kombinációin is ki tudjuk számítani az értékét. Tehát φ tényleg egyértelműen meghatározott. □

Ez a kitüntetett f_0 bilineáris leképezés annyira fontos, hogy külön nevet és jelet kapott: ez lesz a tenzorszorzat.

7.8.11. Definíció. Az előző tételben szereplő K_0 modulust az M és N *tenzorszorzatának* nevezzük, és $M\otimes N$-nel jelöljük. Az $f_0(m,n)$ helyett az $m\otimes n$ jelölést alkalmazzuk.

A tenzorszorzatot az előző tételben megadott tulajdonság egyértelműen meghatározza (lásd 7.8.22. Gyakorlat). Használatakor, kiszámításakor *ne a fenti faktormodulusos konstrukciót használjuk, hanem magát az előző tételt!* Ezt az új jelölés segítségével még egyszer megfogalmazzuk, és a használatára két példát is mutatunk.

7.8.12. Tétel. *Legyenek M és N modulusok az R kommutatív gyűrű fölött. Ekkor minden $f: M\times N\to K$ bihomomorfizmushoz egyértelműen létezik egy olyan $\varphi: M\otimes N\to K$ modulus-homomorfizmus, hogy tetszőleges $(m,n)\in M\times N$ esetén*

$$f(m,n) = \varphi(m\otimes n)\,.$$

Az $M\otimes N$ elemei a $\sum r_i(m_i\otimes n_i)$ lineáris kombinációk, ahol $r_i\in R$ és $(m_i,n_i)\in M\times N$.

Az előbbi példák szerint tehát $\mathbb{Z}^+\otimes\mathbb{Z}^+\cong\mathbb{Z}^+$ és $\mathbb{Z}_2^+\otimes\mathbb{Z}_3^+ = 0$. Most kidolgozunk egy példát a fenti tétel használatának illusztrálására.

7.8.13. Példa. $\mathbb{Q}^+\otimes\mathbb{Q}^+\cong\mathbb{Q}^+$, mint Abel-csoport, vagyis $\mathbb{Z}$-modulus.

A megoldásnak két lépése van. Az elsőben megmutatjuk, hogy $\mathbb{Q}^+\otimes\mathbb{Q}^+$ „nem nagyobb", mint $\mathbb{Q}^+$. E tenzorszorzat általános eleme

$$\sum r_i(p_i\otimes q_i)\,,$$

ahol r_i, p_i, $q_i \in \mathbb{Q}$. Ezt az összeget egyszerűbb alakra hozzuk. Ha a, b, c, d egészek, akkor

$$(a/b)\otimes(c/d) = (a/b)\otimes(cb/bd) = b((a/b)\otimes(c/bd)) = a\otimes(c/bd) = 1\otimes(ac/bd)\,.$$

Tehát beláttuk, hogy $p_i \otimes q_i = 1 \otimes p_i q_i$. Hasonló technikával az r_i együtthatókat is „bevihetjük" a második tényezőbe. Összevonás után tehát a fenti összeg az

$$1 \otimes \Big(\sum r_i\, p_i q_i\Big)$$

alakot ölti. Így beláttuk, hogy $\mathbb{Q}^+ \otimes \mathbb{Q}^+$ minden eleme $1 \otimes q$ alakú, ahol $q \in \mathbb{Q}$.

A második lépésben megmutatjuk, hogy $\mathbb{Q}^+ \otimes \mathbb{Q}^+$ „legalább akkora", mint $\mathbb{Q}^+$. Tekintsük az $f(p, q) = pq$ leképezést $\mathbb{Q} \times \mathbb{Q}$-ból $\mathbb{Q}$-ba. Ez bihomomorfizmus, és így keresztülvezethető a tenzorszorzaton, azaz létezik egy olyan $\varphi : \mathbb{Q}^+ \to \mathbb{Q}^+$ homomorfizmus, melyre

$$\varphi(p \otimes q) = pq\,.$$

Speciálisan $\varphi(1 \otimes q) = q$.

Most már látjuk, hogy $\mathbb{Q}^+ \otimes \mathbb{Q}^+ \cong \mathbb{Q}^+$, hiszen a $\varphi : (1 \otimes q) \mapsto q$ és a $\psi : q \mapsto (1 \otimes q)$ homomorfizmusok egymás inverzei, és pont a kívánt izomorfizmust létesítik.

7.8.14. Tétel. *Legyenek V és W vektorterek a T test fölött, $b_1, \ldots, b_k$ bázis V-ben, és $c_1, \ldots, c_\ell$ bázis W-ben. Ekkor $V \otimes W$ egy $k\ell$-dimenziós vektortér, amelyben bázist alkotnak a $b_i \otimes c_j$ vektorok.*

Bizonyítás. Most is a fenti mintamegoldásban bemutatott két lépést tesszük meg. Tudjuk, hogy $V \otimes W$ elemei a $\sum t_i(v_i \otimes w_i)$ alakú lineáris kombinációk. Ha az itt szereplő u_i és v_i vektorokat fölírjuk a megfelelő bázisokban, és a $\otimes$ bilinearitása szerint ezeket kibontjuk (ahhoz hasonlóan, ahogy a 7.8.9. Példa kiszámítása során eljártunk), majd összevonunk, akkor a végén a $b_i \otimes c_j$ vektorok egy T-beli együtthatós lineáris kombinációját kapjuk. Ezek tehát generálják a $V \otimes W$ tenzorszorzatot.

Meg kell még mutatnunk, hogy függetlenek is, ehhez egy ügyes bihomomorfizmust kell megadnunk. Legyen $[v]$ a $v \in V$-hez tartozó oszlopvektor a $c_1, \ldots, c_k$ bázisban, és definiáljuk a $[w]$ oszlopvektort analóg módon (ahol $w \in W$). Tekintsük az $f(v, w) = [v][w]^T$ leképezést (itt $[w]^T$ a $[w]$ transzponáltja, az egymás mellé írás pedig mátrix-szorzást jelöl). Ez az f átvezethető a tenzorszorzaton, vagyis létezik egy $\varphi : V \otimes W \to T^{k\times\ell}$ lineáris leképezés, melyre $\varphi(v \otimes w) = [v][w]^T$. Azonnal látjuk, hogy a $b_i \otimes c_j$ vektorok képei lineárisan független mátrixok lesznek, ezért maguk is függetlenek.

A most használt $[v][w]^T$ alakú mátrixokat a lineáris algebrában *diádoknak* nevezik. Ez a bizonyítás mutatja, hogy a tenzorszorzat és a diádok között szoros kapcsolat van. □

Zárásként röviden szót ejtünk leképezések tenzorszorzatáról, ez kicsit hasonlít ahhoz, ahogy a $\mathrm{Hom}(\varphi, \psi)$ leképezést definiáltuk az előző szakasz végén.

7.8.15. Definíció. Legyenek M, N, K, L modulusok az R fölött, $\psi \in \mathrm{Hom}_R(M, K)$ és $\chi \in \mathrm{Hom}_R(N, L)$. Tekintsük azt az $f : M \times N \to K \otimes L$ bihomomorfizmust, amelyre tetszőleges $m \in M$ és $n \in N$ esetén

$$f(m, n) = \psi(m) \otimes \chi(n) .$$

Azt az egyértelműen létező $\varphi : M \otimes N \to K \otimes L$ homomorfizmust, amelyre

$$\varphi(m \otimes n) = \psi(m) \otimes \chi(n) ,$$

a ψ és χ *leképezések tenzorszorzatának* nevezzük, és $\psi \otimes \chi$-vel jelöljük.

Speciálisan ha lineáris leképezésekről van szó, akkor a tenzorszorzatuk mátrixát a következőképpen lehet fölírni. Tegyük föl, hogy $A : V \to U$ lineáris leképezés két vektortér között, melynek mátrixa az $(\mathbf{a}, \mathbf{c})$ bázispárban a $k \times m$-es $M = ((m_{pi}))$ mátrix. Ugyanígy legyen a $B : W \to Z$ lineáris leképezés mátrixa a $(\mathbf{b}, \mathbf{d})$ bázispárban az $\ell \times n$-es $N = ((n_{qj}))$ mátrix. Ekkor az $A \otimes B : V \otimes W \to U \otimes Z$ lineáris leképezés az $a_i \otimes b_j$ bázisvektort $A(a_i) \otimes B(b_j)$-be viszi. A lineáris leképezés mátrixának definíciója miatt

$$A(a_i) = m_{1i}c_1 + \ldots + m_{ki}c_k \quad \text{és} \quad B(b_j) = n_{1j}d_1 + \ldots + n_{\ell j}d_\ell .$$

Ezért

$$(A \otimes B)(a_i \otimes b_j) = A(a_i) \otimes B(b_j) = \sum_{p,q} m_{pi}n_{qj}(c_p \otimes d_q) ,$$

ahol $1 \le p \le k$ és $1 \le q \le \ell$. Ez azt jelenti, hogy ha K jelöli az $A \otimes B$ mátrixát abban a bázispárban, amelynek első komponense az $a_i \otimes b_j$ vektorokból álló bázis, második komponense pedig a $c_p \otimes d_q$ vektorokból álló bázis, akkor ennek a mátrixnak $k\ell$ sora és mn oszlopa van, és az $a_i \otimes b_j$ vektorhoz tartozó oszlop és a $c_p \otimes d_q$ vektorhoz tartozó sor metszéspontjában az $m_{pi}n_{qk}$ skalár áll. A K mátrixot tehát a következőképpen kaphatjuk meg. Vegyük az N mátrixot, és ebben mindegyik n_{qj} elem helyébe írjuk be az $Mn_{qj} = ((m_{pi}n_{qj}))$ mátrixot.

7.8.16. Definíció. Az előző bekezdésben leírt K mátrixot az M és N mátrixok *tenzorszorzatának*, vagy *Kronecker-szorzatának* nevezzük, és $M \otimes N$-nel jelöljük.

Azt láttuk be tehát, hogy az A és B lineáris leképezések tenzorszorzatának mátrixa az A és B mátrixainak Kronecker-szorzata (alkalmas bázispárban).

Gyakorlatok, feladatok

7.8.17. Gyakorlat. Melyik Abel-csoporttal ($\mathbb{Z}$-modulussal) izomorfak az alábbi csoportok? Itt p prímszám, és $\mathbb{Z}_{p^\infty}$ a kváziciklikus csoport (7.7.16 Definíció).

(1) $\mathbb{Z}^+ \otimes \mathbb{Z}_n^+$.
(2) $\mathbb{Z}_m^+ \otimes \mathbb{Z}_n^+$.
(3) $\mathbb{Q}^+ \otimes \mathbb{Z}_n^+$.
(4) $\mathbb{Z}_{p^\infty} \otimes \mathbb{Z}_n^+$.
(5) $\mathbb{Z}_{p^\infty} \otimes \mathbb{Z}_{p^\infty}$.

7.8.18. Gyakorlat. Igazoljuk, hogy tetszőleges A Abel-csoportra $\mathbb{Z}^+ \otimes A \cong A$. Általánosítsuk az állítást $\mathbb{Z}$ helyett tetszőleges gyűrűre.

7.8.19. Gyakorlat. Igazoljuk, hogy tetszőleges B Abel-csoportra $\mathbb{Z}_m^+ \otimes B \cong B/mB$.

7.8.20. Gyakorlat. Igazoljuk, hogy osztható csoportnak torziócsoporttal vett tenzorszorzata nulla.

7.8.21. Gyakorlat. Adjunk példát olyan $A \leq B$ és C Abel-csoportokra, továbbá $a \in A$ és $c \in C$ elemekre, hogy $a \otimes c = 0$ ha azt a $B \otimes C$ csoportban értelmezzük, de nem nulla, ha azt az $A \otimes C$ csoportban értelmezzük, sőt $A \otimes C$ nem is izomorf $B \otimes C$ egy részcsoportjával. Igazoljuk, hogy ez nem fordulhat elő, ha A direkt összeadandója B-nek.

7.8.22. Gyakorlat. Mutassuk meg, hogy a tenzorszorzat egyértelmű a következő értelemben. Ha M és N adott R-modulusok, és K_0, f_0, illetve a K_1, f_1 egyaránt teljesítik a 7.8.10. Tételben kirótt kívánalmakat, akkor $K_0 \cong K_1$, sőt f_0 és f_1 is „ugyanúgy viselkedik", azaz olyan $\varphi : K_0 \to K_1$ izomorfizmus is létezik, melyre tetszőleges $(m, n) \in M \times N$ esetén $f_1(m, n) = \varphi f_0(m, n)$.

7.8.23. Feladat. Legyenek M, N, K tetszőleges bal oldali R-modulusok. Igazoljuk az alábbi izomorfizmusokat.

(1) $M \otimes N \cong N \otimes M$ (a tenzorszorzat kommutatív).
(2) $(M \otimes N) \otimes K \cong M \otimes (N \otimes K)$ (a tenzorszorzat asszociatív).
(3) $(M \times N) \otimes K \cong (M \otimes K) \times (N \otimes K)$. Igaz marad-e az állítás végtelen sok tényezős direkt szorzatra? És direkt összegre?
(4) $\mathrm{Hom}_R(M \otimes N, K) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, K))$.

7.8.24. Gyakorlat. Legyen $\varphi : x \mapsto 2x$ a $\mathbb{Z}_2^+ \to \mathbb{Z}_4^+$ beágyazás. Ekkor az $\varphi \otimes \varphi$ kifejezést kétféleképpen érthetjük. Az első értelmezés szerint ez két leképezés tenzorszorzata, a második szerint pedig a $\mathrm{Hom}(\mathbb{Z}_2^+, \mathbb{Z}_4^+)$ csoport önmagával vett tenzorszorzatának egy eleme. Mutassuk meg, hogy ez a két értelmezés nem lehet ugyanaz, mert $\varphi \otimes \varphi$ az egyik értelmezés szerint nulla, a másik szerint nem.

7.8.25. Feladat. Legyen A rendre $\mathbb{Z}^+$, $\mathbb{Z}_m^+$, $\mathbb{Z}_{p^\infty}$, $\mathbb{Q}^+$, és φ az alábbi négyféle leképezés:

(1) $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ az a homomorfizmus, ami minden elemhez az n-szeresét rendeli.
(2) $\varphi : \mathbb{Z}_m \to \mathbb{Z}_{nm}$, az n-nel szorzás.
(3) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ a mod n vett maradék képzése.
(4) φ a $\mathbb{Z} \to \mathbb{Q}$ beágyazás.

Számítsuk ki az $id_A \otimes \varphi$ homomorfizmusokat. Vizsgáljuk meg, hogyan függ össze φ és az eredmény injektivitása, illetve szürjektivitása.

7.8.26. Feladat. Legyen R főideálgyűrű, T ennek a hányadosteste, és M egy végesen generált R-modulus. Mutassuk meg, hogy az $T \otimes M$ modulus vektortérré tehető T fölött, amelynek a dimenziója ugyanannyi, mint az M ciklikus modulusok direkt összegére való felbontásában a nulla rendű összeadandók száma. Hogyan segít ez az észrevétel a felbontás egyértelműségének bizonyításában?

7.9. Összefoglaló

8. ALGEBRAI STRUKTÚRÁK, HÁLÓK

A filozófiának, egzakt elméletként, annyit kellene tennie a fizikáért, mint amennyit Newton tett érte. Úgy gondolom nagyon is lehetséges, hogy egy ilyen filozófiai elmélet ki fog fejlődni a következő száz évben, vagy még hamarább.

Kurt Gödel
(szóbeli idézet[1])

Általános algebrai struktúrán, röviden algebrán az eddig tanult konkrét struktúrák (vektorterek, csoportok, gyűrűk, modulusok) közös általánosítását értjük, vagyis egy műveletekkel ellátott halmazt. (Ne keverjük össze ezt a fogalmat a gyűrűelméletben tanult, test fölötti algebrákkal, itt csak a nevek egybeeséséről van szó.) Az általános algebrák elmélete egy absztrakciós szinttel a korábbi anyagrészek fölött van. Olyan fogalmakat és tételeket vizsgálunk, amelyek minden eddig tanult konkrét struktúrában (csoportban, gyűrűben, modulusban) ugyanúgy működnek, és a legkényelmesebben, legtermészetesebben az általános algebrák szintjén kezelhetők. Ilyenek például a homomorfizmus-tétel, az izomorfizmustételek, vagy a generált részstruktúra definíciója és elemeinek a leírása. Láttuk korábban, hogy ezek a gyűrűkben, a csoportokban és a modulusokban egy kaptafára mennek.

Ne gondoljuk azonban, hogy az általános algebrák elmélete csupán a hasonló triviális általánosításokra korlátozódik. Jó analógia a csoportelmélet példája. A csoport fogalmának bevezetését indokolandó, először csak bizonyos hasonlóságokat vettünk észre (például azt, hogy a rend fogalma ugyanúgy viselkedik komplex egységgyökökre, mint amikor egész számokkal modulo n számolunk). Ezeket még gond és erőfeszítés nélkül általánosíthattuk az újonnan bevezetett csoportokra. De azután új problémák, új tételek keletkeztek, egy új világ tárult föl a szemünk előtt, ami a valóság egy eddig ismeretlen szeletét írta le, és váratlan alkalmazásokkal szolgált. A korábbi konkrét helyzetekre, például a számelmélet kongruenciáira pedig magasabbról tudtunk ránézni, és ezért néhány régi problémában (de messze nem az összesben) messzebbre láttunk. Ez a matematika fejlődésének természetes menete.

Ugyanez a folyamat zajlott le az általános algebrák elméletének kifejlődésekor is: előtérbe kerültek új fogalmak, problémák (nem ritkán a matematikai logikából származó motivációval), és az ezekhez kapcsolódó, általában már nemtriviális tételek. Ez a tudományág

[1] Hao Wang: *A Logical Journey*. From Gödel to Philosophy, lásd [**18**].

igen fiatal, az említett mélyebb eredmények csak az 1960-as éveket követően kezdtek megszületni. Elsősorban Ralph McKenzie (és sok más matematikus) munkássága nyomán betekintést nyerhettünk az általános algebrák mélyebb szerkezetébe. Ez nemcsak erős apparátust ad a kezünkbe problémák megoldásához, hanem magyarázatot is szolgáltat arra, hogy korábban miért az eddig tanult „klasszikus" struktúrákat (csoportokat, modulusokat) vizsgálták (vagyis, hogy miért pont ezek jöttek elő a fontos alkalmazásokban). Tehát immáron a klasszikus struktúrákra tudunk magasabbról nézni (ami ismét nem jelenti azt, hogy minden ide tartozó problémát az általános algebrák eszközeivel lehetne a legkényelmesebben kezelni).

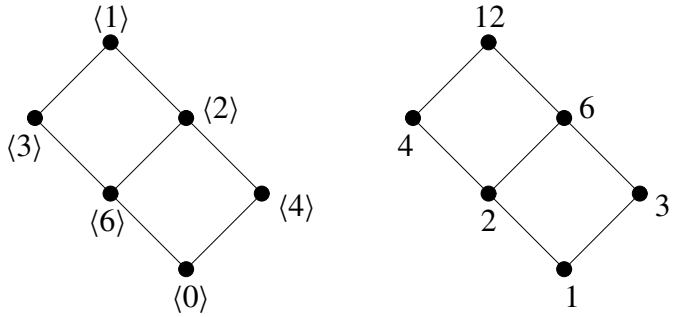
Természetesen ezekről a mélyebb eredményekről a gyűrűelmélethez hasonlóan mindössze egy kitekintés formájában emlékezünk meg. Csak arra van terünk, hogy az Olvasónak megmutassuk a korábbi anyagrészek magasabb szintű összefüggéseit egy-egy általános algebrai fogalmon, vagy tételen keresztül, és így lehetőséget adjunk arra, hogy a korábban tanultakat integrálja, azaz egy szinttel mélyebben megértse, mint eddig. Ezért az anyag fölépítése az eddig megszokottnál vázlatosabb lesz. A precíz részletek elolvashatók Fried Ervin [**13**] könyvében. Ha az Olvasó ennél jobban el akar mélyedni az általános algebrák elméletében, akkor a magyar nyelvre is lefordított [**3**] könyvet ajánljuk, amelynek angol [**4**] eredetije az interneten szabadon elérhető.

A fejezet másik célja az általános algebrák elméletével szoros szimbiózisban élő hálóelmélet alapjainak tárgyalása. A hálók olyan struktúrák, amelyek egy halmaz részhalmazait, vagy egy csoport részcsoportjait általánosítják, két kétváltozós műveletre koncentrálva: a metszetre és az egyesítésre. Az egyesítés műveletét részcsoportok között úgy értjük, mint a két részcsoportot tartalmazó legszűkebb részcsoportot (vagyis az általuk generált részcsoportot). A hálók szerkezetét is akkor érthetjük meg, ha mint önálló, absztrakt objektumokat vizsgáljuk őket. A fejezet végén a kategóriaelméletről is szót ejtünk, és röviden bemutatjuk a fogalom-analízis elméletének alapjait, amelyet a valós életből vett problémákra is sikerrel alkalmaznak.

8.1. Hálók

A fejezetet nem az általános algebrák bemutatásával, hanem a hálókéval kezdjük, mert ezek fontos, de a csoportoktól sokban eltérő példát szolgáltatnak, és így könnyebb lesz az általános algebrákra vonatkozó kiinduló fogalmakat megértenünk.

A 6.5. Szakaszban láttuk, hogy a D_4 csoport összes részcsoportjait (vagy az $x^4 - 2$ polinom felbontási testének résztesteit) sokkal könnyebb áttekinteni, ha lerajzoljuk őket a 6.1. Ábrán látható formában. Ez az ábra azért hasznos, mert a részcsoportok közötti rendezést is mutatja (vagyis azt, hogy melyik részcsoport mely részcsoportokat tartalmazza). Az ábra a feje tetejére volt állítva (vagyis a nagyobb részcsoporthoz tartozó pontot lejjebb rajzoltuk), hogy hasonlítson a közbülső testek hálójához. Készítsük el a hasonló rajzot a $\mathbb{Z}_{12}^+$ csoport esetében is, de most már a fejéről a talpára állítva (8.1. Ábra). Feltüntettük a részcsoportok rendjeit (azaz a 12 osztóit) is egy másik „ugyanolyan" rajzon.



8.1. Ábra. A $\mathbb{Z}_{12}^{+}$ részcsoporthálója és a 12 osztóhálója.

Az ilyesfajta rajzok tehát általában egy részben rendezett P halmazt ábrázolnak (vö. 5.8.1. Definíció). Ha $x < y$, akkor az x pontot lejjebb, az y pontot följebb rajzoljuk, és ha x és y között már nincs P-nek eleme, akkor egy vonallal összekötjük őket.

8.1.1. Definíció. Legyen P részben rendezett halmaz és $x, y \in P$. Azt mondjuk, hogy y *fedi* az x-et, ha $x < y$, és nincs olyan $z \in P$, melyre $x < z < y$. Jelölés: $x \prec y$ vagy $y \succ x$.

Vagyis a rajzon a fedő elemeket kötjük össze. A rendezést a rajzról leolvashatjuk: $x < y$ akkor és csak akkor, ha a vonalak mentén fölfelé haladva x-ből y-ig juthatunk.

A P részben rendezése a 8.1. Ábrán a részcsoportok esetében a tartalmazás, a számok esetében az oszthatóság. A két rajz azért ugyanolyan, mert a $\mathbb{Z}_{12}$ csoportban 12 minden d osztójához pontosan egy d rendű H_d részcsoport van, és $H_c \subseteq H_d$ akkor és csak akkor, ha $c \mid d$. Ezt általában is tudjuk a 4.3.21. Állítás miatt, és úgy fejezzük majd ki, hogy a $\mathbb{Z}_n^{+}$ ciklikus csoport részcsoporthálója az n szám osztóhálójával izomorf (8.5.6. Gyakorlat).

Képzeljük azt, hogy csak a 8.1. Ábrát kapjuk meg, de nem árulták el, hogy melyik „pont” melyik részcsoportnak (vagyis a $\mathbb{Z}_{12}$ melyik részhalmazának) felel meg. A rendezést le tudjuk olvasni, például látjuk, hogy $\langle 4 \rangle$ részcsoportja $\langle 1 \rangle$-nek, de $\langle 3 \rangle$-nak nem. De le lehet-e olvasni a $\langle 3 \rangle$ és a $\langle 2 \rangle$ részcsoportok M metszetét is? Tudjuk, hogy két részcsoport metszete is részcsoport, ezért az M metszetet az ábrán levő pontok között kell keresnünk. Az M része a $\langle 3 \rangle$-nak és $\langle 2 \rangle$-nek is, ezért csak a $\langle 0 \rangle$ és a $\langle 6 \rangle$ pontok jöhetnek szóba. Ezek közül az M a magasabban lévő lesz, vagyis a $\langle 6 \rangle$, a következő gyakorlat szerint.

8.1.2. Gyakorlat. Mutassuk meg, hogy egy G csoport H és K részcsoportjainak metszete a legbővebb azon M részcsoportok között, amelyek H-nak és K-nak is részhalmazai.

Egy csoportban a H és K részcsoportok uniója általában nem részcsoport. Ugyanakkor a H-t és a K-t tartalmazó részcsoportok között van legszűkebb, ez a $H \cup K$ által generált részcsoport. Az ábráról leolvasható, hogy a $\langle 6 \rangle$ és a $\langle 4 \rangle$ által generált részcsoport a $\langle 2 \rangle$.

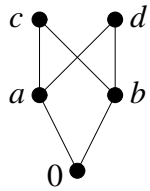
A 4.4.23. Definícióban már szó esett egy halmazrendszer legszűkebb és legbővebb, valamint minimális és maximális elemeiről is. Az eddig elhangzottakat a következőképpen általánosíthatjuk részben rendezett halmazokra.

8.1.3. Definíció. Legyen P részben rendezett halmaz a $\leq$ rendezésre és $X \subseteq P$.

(1) Azt mondjuk, hogy $m \in P$ *alsó korlátja* X-nek, ha minden $x \in X$ esetén $m \leq X$. Az m *felső korlátja* X-nek, ha minden $x \in X$-re $m \geq x$.
(2) Az m *legnagyobb eleme* X-nek, ha felső korlátja, és $m \in X$. Az m *legkisebb eleme* X-nek, ha alsó korlátja, és $m \in X$.
(3) Az m *maximális eleme* X-nek, ha $m \in X$, és X-ben nincs m-nél nagyobb elem. Analóg módon értelmezzük a *minimális elem* fogalmát.
(4) Az m az X-nek *legnagyobb alsó korlátja*, ha az X alsó korlátaiból álló halmaznak legnagyobb eleme. Másképp fogalmazva: m az X-nek alsó korlátja, és ha m' is alsó korlátja X-nek, akkor $m' \leq m$. Szintén analóg módon definiáljuk az X *legkisebb felső korlátjának* a fogalmát: ez X felső korlátai között a legkisebb.

Speciálisan a P legkisebb elemét (ha létezik, akkor) *nullelemnek*, a legnagyobb elemét pedig *egységelemnek* nevezzük. A 0 és 1 szimbólumok mindig ilyen elemeket fognak jelölni. Ezek helyett néha 0_P-t és 1_P-t írunk.

A legnagyobb alsó és a legkisebb felső korlát nem mindig létezik. Például a 8.2. Ábrán szereplő részben rendezett halmazban az a és b elemeknek két közös felső korlátja is van, a c és a d, de ezek között nincs legkisebb. Hasonlóképpen a c és d elemeknek nincs legnagyobb alsó korlátja, és egyetlen közös felső korlátjuk sincs. Legkisebb elem van (a 0), legnagyobb elem azonban nem létezik.



8.2. Ábra. A c és d elemeknek nincs legnagyobb alsó korlátja.

Így tehát egy csoport részcsoportjainak részben rendezett halmazában két részcsoport metszete a legnagyobb alsó korlátjuk, az általuk generált részcsoport pedig a legkisebb felső korlátjuk.

8.1.4. Gyakorlat. Legyen P részben rendezett halmaz és $X \subseteq P$. Mutassuk meg a következő állításokat.

(1) Az X legnagyobb (legkisebb eleme), ha létezik, akkor egyértelműen meghatározott.
(2) Az X legnagyobb alsó (legkisebb felső) korlátja, ha létezik, akkor szintén egyértelműen meghatározott.
(3) Ha X-nek van legkisebb (legnagyobb) eleme, akkor ez egyúttal az X-nek a legnagyobb alsó (legkisebb felső) korlátja.

Speciálisan P legkisebb és legnagyobb eleme, ha létezik, akkor szintén egyértelműen meg van határozva.

A (legkisebb) felső korlát fogalmát a (legnagyobb) alsó korlát fogalmából úgy is megkaphattuk volna, ha a rendezést a „feje tetejére állítjuk”, vagyis a $\leq$ helyett a $\geq$ rendezést tekintjük.

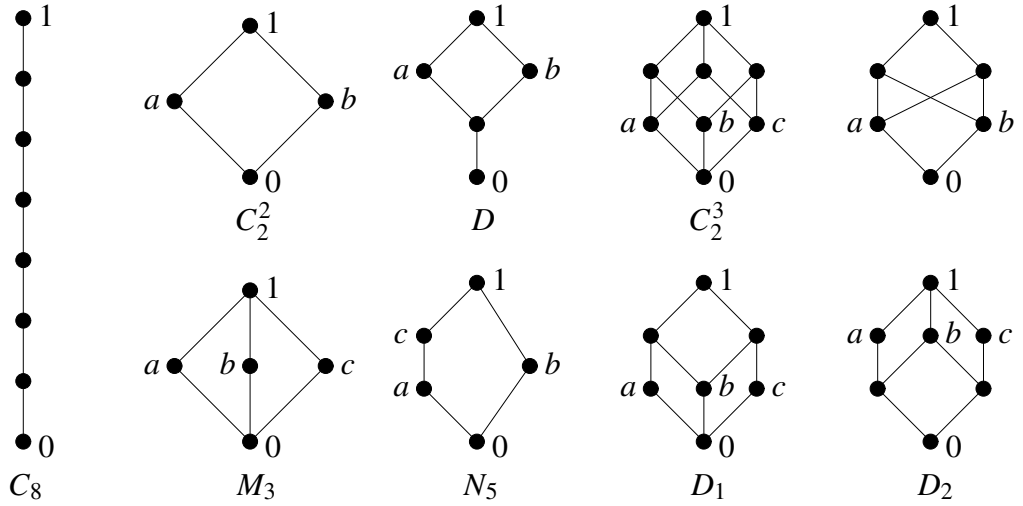
8.1.5. Definíció. Egy P részben rendezett halmaz *duálisának* nevezzük azt a részben rendezett halmazt, amely a rendezés megfordításából adódik a fenti értelemben.

8.1.6. Gyakorlat. Igazoljuk, hogy egy P részben rendezett halmaz duálisa is részben rendezett halmaz, és az $X \subseteq P$ elemek legnagyobb alsó korlátja akkor és csak akkor m a $\leq$ rendezésre, ha m az X legkisebb felső korlátja a megfordított $\geq$ rendezésre.

Ez azt jelenti, hogy ha egy állítást bebizonyítottunk a legnagyobb alsó korlátról, akkor ugyanezt az állítást megkapjuk a legkisebb felső korlátra is, ha a rendezést megfordítjuk. Ez a *dualitás elve*.

8.1.7. Definíció. Egy részben rendezett halmazt *hálónak* nevezünk, ha bármely két elemének van legnagyobb alsó és legkisebb felső korlátja. A h és k elemek legnagyobb alsó korlátját $h \wedge k$, legkisebb felső korlátját $h \vee k$ jelöli. A $h \wedge k$ a h és a k *metszete*, a $h \vee k$ pedig az *egyesítése*.

Egy háló duálisa is nyilván háló, amelyben az egyesítés és a metszet művelete helyet cserél. Rendkívül fontos példa, hogy ha P a nemnegatív egészek halmaza, és $\leq$ az *osztatóság reláció* (vagyis nem a szokásos rendezés, hanem $m \leq n$-et úgy értjük, hogy $m \mid n$), akkor a legnagyobb alsó korlát a kitüntetett közös osztó, a legkisebb felső korlát pedig a kitüntetett közös többszörös, és így hálót kapunk (vö. 8.1. Ábra).



8.3. Ábra. Néhány példa részben rendezett halmazra.

8.1.8. Gyakorlat. Döntsük el a 8.3. Ábrán szereplő kilenc részben rendezett halmazról, hogy hálók-e. Melyek azok, amelyeknek a duálisa is szerepel az ábrán?

8.1.9. Definíció. Egy C részben rendezett halmaz h és k elemeit *összehasonlíthatónak* nevezzük, ha $h \leq k$ vagy $k \leq h$. A C *lánc*, ha bármely két eleme összehasonlítható (vagyis ha a rendezés elrendezés az 5.8.1. Definíció értelmében). Az n elemű láncot C_n fogja jelölni.

8.1.10. Gyakorlat. Igazoljuk, hogy mindegyik lánc háló, és adjunk példát olyan láncra, amelyben egyetlen fedés sincsen.

8.1.11. Definíció. Egy háló legkisebb elemének a fedőit *atomoknak* nevezzük. A duális fogalom a *koatom* (ezek tehát azok az elemek, amelyeket a legnagyobb elem fed).

8.1.12. Gyakorlat. A 8.3. Ábrán szereplő hálók közül melyek azok, ahol minden nem nulla elem atomok egyesítése, és melyek azok, ahol minden 1-től különböző elem koatomok metszete?

8.1.13. Gyakorlat. Igazoljuk, hogy ha x, y, u, v elemei egy hálónak, akkor $x \leq u$ és $y \leq v$ esetén $x \vee y \leq u \vee v$ és $x \wedge y \leq u \wedge v$ (vagyis a hálóműveletek *monotonok*).

Megadhatjuk a hálókat műveletekkel is. A metszet és az egyesítés alapvető tulajdonságait foglalja össze a következő gyakorlat.

8.1.14. Gyakorlat. Legyen L háló. Mutassuk meg, hogy (tetszőleges $x, y \in L$ esetén) a következők teljesülnek.

(1) A $\wedge$ és $\vee$ műveletek asszociatívak.
(2) A $\wedge$ és $\vee$ műveletek kommutatívak.
(3) A $\wedge$ és $\vee$ műveletek *idempotensek*, azaz $x \wedge x = x$ és $x \vee x = x$.
(4) Érvényes az *elnyelési tulajdonság*, vagyis $x \vee (x \wedge y) = x$ és $x \wedge (x \vee y) = x$.

A metszet és az egyesítés műveletéből visszanyerhető a rendezés a következőképpen.

8.1.15. Gyakorlat. Mutassuk meg, hogy ha h, k elemei egy P részben rendezett halmaznak, akkor $h \leq k$ akkor és csak akkor, ha h és k legnagyobb alsó korlátja h, akkor és csak akkor, ha h és k legkisebb felső korlátja k.

A következő tétel azt mutatja, hogy a hálókat a metszet és az egyesítés műveletével is definiálni lehetne. Az egyszerű bizonyítást az Olvasóra hagyjuk.

8.1.16. Tétel. *Ha adott egy L nem üres halmazon a metszet $\wedge$ és az egyesítés $\vee$ művelete a 8.1.14. Gyakorlatban felsorolt tulajdonságokkal, akkor az előző gyakorlatban megadott rendezésre L háló, amelyben a legnagyobb alsó korlátot $\wedge$, a legkisebb felső korlátot $\vee$ adja meg.* □

8.1.17. Feladat. Bizonyítsuk be, hogy a 8.1.14. Gyakorlatban szereplő (3) tulajdonság következik a (4)-ből (vagyis az elnyelési tulajdonságnak következménye az idempotencia).

A részcsoportok hálójában nem csak kettő, hanem akárhány részcsoport metszete is részcsoport, most ezt a jelenséget általánosítjuk.

8.1.18. Definíció. Az L részben rendezett halmazt *teljes hálónak* nevezzük, ha minden részhalmazának van legnagyobb alsó és legkisebb felső korlátja. Az X legnagyobb alsó korlátját $\bigwedge X$, legkisebb felső korlátját $\bigvee X$ jelöli. Ezeket is metszetnek illetve egyesítésnek nevezzük.

Ha L teljes háló, akkor van legkisebb (0_L-lel jelölt) eleme (az összes elem metszete), és legnagyobb (1_L-lel jelölt) eleme is (az összes elem egyesítése).

8.1.19. Gyakorlat. Mutassuk meg, hogy ha L teljes háló, akkor az üres halmaz legnagyobb alsó korlátja 1_L, legkisebb felső korlátja pedig 0_L.

A részcsoporthálók esetében a H és K egyesítése a $H \cup K$ generálta részcsoport, amit úgy definiáltunk, mint a $H \cup K$ halmazt tartalmazó részcsoportok metszetét. Ez azt sugallja, hogy ha egy hálóban végtelen metszetről is beszélhetünk, akkor ezzel az egyesítést is megadtuk.

8.1.20. Tétel. *Legyen L részben rendezett halmaz, amelyben minden részhalmaznak van legnagyobb alsó korlátja. Ekkor L teljes háló.*

Bizonyítás. Legyen $X \subseteq L$, és jelölje Y az X felső korlátainak a halmazát. Megmutatjuk, hogy $m = \bigwedge Y$ az X elemeinek legkisebb felső korlátja. Valóban, ha $x \in X$, akkor x alsó korlátja Y elemeinek, és így m definíciója miatt $x \leq m$. Ezért m felső korlátja X elemeinek. Azt, hogy a felső korlátok között legkisebb, az biztosítja, hogy $m = \bigwedge Y$. □

Így egy csoport részcsoportjai, normálosztói, egy gyűrű balideáljai teljes hálót alkotnak, hiszen tetszőleges metszetük is részcsoport, normálosztó, illetve balideál. Természetesen minden véges háló is teljes. Teljes hálóra ezen kívül nagyon fontos példa a valós számok halmaza a szokásos rendezéssel, ha hozzávesszük a $-\infty$ és $+\infty$ szimbólumokat, ahogy analízisben szokásos (ez a háló egy lánc). Itt az X részhalmaz egyesítése $\sup X$, metszete pedig $\inf X$.

Most már talán érthető, hogy az 5.8. Szakaszban miért nem hívtuk teljesnek a trichotóm rendezéseket. Például a racionális számok halmazának szokásos rendezése elrendezés, de az $X = \{q \in \mathbb{Q} : q^2 < 2\}$ halmaznak nincs legkisebb felső korlátja (hiszen minden $\sqrt{2}$-nél nagyobb racionális szám felső korlát, és ezek között nincs legkisebb). Létezik olyan hálóelméleti eljárás, amellyel hálókat teljessé lehet tenni, és ez egy lehetséges módot ad arra, hogy a valós számokat a racionális számokból megkaphassuk.

Utolsó példánk teljes hálóra az úgynevezett partícióháló. Legyen U nem üres halmaz, és tekintsük az U-n értelmezett összes partíciót. Ha θ egy partíció az U halmazon, akkor azt, hogy $x, y \in U$ egy osztályban van a θ-nál, a következő módokon fogjuk írni:

$$x \; \theta \; y \quad \text{vagy} \quad x \equiv y \; (\theta) \quad \text{vagy} \quad x \overset{\theta}{\text{———}} y \; .$$

A 4.4.6. Tételben láttuk, hogy az így kapott $\equiv$ egy ekvivalencia-reláció (és ez a megfeleltetés kölcsönösen egyértelmű a partíciók és az ekvivalencia-relációk között).

A θ-hoz tartozó ekvivalencia-relációt azon (x, y) párok halmazának fogjuk tekinteni, melyekre $x \equiv y\ (\theta)$ (lásd a 4.4.5. Definíció előtti megjegyzést, vagy a 8.2.28. Definíciót). Így a halmazelméleti tartalmazás részben rendezést definiál az ekvivalencia-relációk között. Érdemes ezt lefordítani a partíciók nyelvére.

8.1.21. Definíció. Azt mondjuk, hogy a θ_1 partíció *finomabb* a θ_2 partíciónál, ha θ_1 minden osztálya része θ_2 valamelyik osztályának, képletben $\theta_1 \leq \theta_2$. Ilyenkor azt is mondjuk, hogy θ_2 *durvább*, mint θ_1.

8.1.22. Gyakorlat. Igazoljuk, hogy a θ_1 partíció akkor és csak akkor finomabb a θ_2 partíciónál, ha a θ_1-hez tartozó $\equiv_1$ ekvivalencia-reláció részhalmaza a θ_2-höz tartalmazó $\equiv_2$ ekvivalencia-relációnak.

Tehát egy partíciót úgy lehet finomítani, hogy az osztályait kisebb osztályokra bontjuk, és úgy lehet durvítani, ha osztályokat összevonunk.

Könnyen látható, hogy tetszőleges számú ekvivalencia-reláció metszete is ekvivalencia-reláció. Ezért partíciók tetszőleges X halmazának létezik legnagyobb alsó korlátja: ennél az $x, y \in U$ elemek akkor és csak akkor vannak egy osztályban, ha mindegyik X-be tartozó partíciónál egy osztályban vannak. Például az $\{\{1, 2\}, \{3, 4, 5\}\}$ és az $\{\{1, 3, 4\}, \{2, 5\}\}$ partíciók legnagyobb alsó korlátja az $\{\{1\}, \{2\}, \{3, 4\}, \{5\}\}$ partíció, hiszen a 3 és a 4 az egyetlen olyan elempár, amely mindkét partíciónál egy osztályba tartozik. A 8.1.20. Tétel szerint tehát a partíciók teljes hálót alkotnak.

8.1.23. Definíció. Az U nem üres halmaz összes partícióinak teljes hálóját az U *partícióhálójának* nevezzük. A 0_U ennek a legkisebb eleme (ahol U minden eleme külön osztályban van), az 1_U pedig a legnagyobb eleme (ahol az U összes eleme egyetlen osztályt alkot). Ezek az U *triviális partíciói*.

Rajzoljuk le egy négyelemű halmaz partícióhálóját. Az egyelemű osztályokat nem mindig írjuk ki, és a zárójeleket is elhagyjuk, például a 23 az $\{\{1\}, \{2, 3\}, \{4\}\}$ partíciót rövidíti. A vesszők helyett vonalat húzunk, tehát $\{\{1, 3\}, \{2, 4\}\}$-et a 8.4. Ábrán 13|24 jelöli.

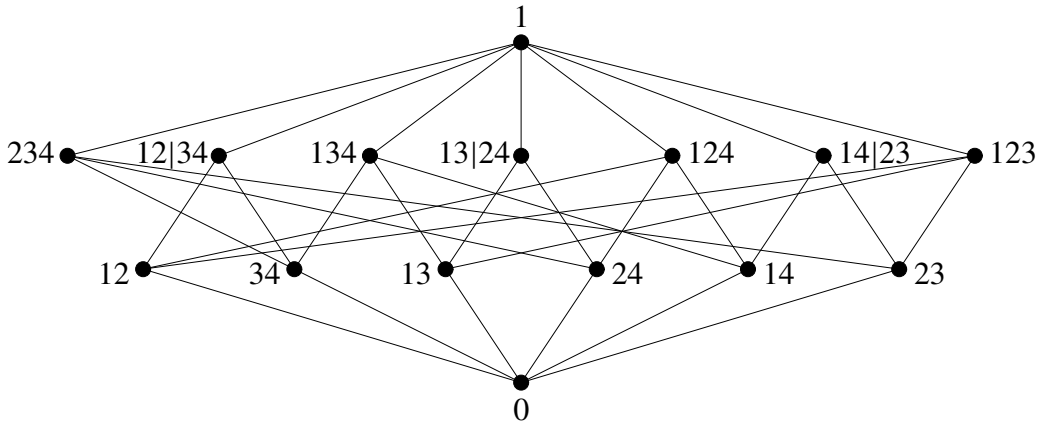
8.1.24. Gyakorlat. Számítsuk ki az $\{1, 2, \ldots, 9\}$ halmazon a 23|45|67|89 és 19|58 partíciók egyesítését.

8.1.25. Feladat. Igazoljuk, hogy ha θ és ρ partíciók az U halmazon, akkor az $x, y \in U$ elemek akkor és csak akkor vannak egy osztályban a $\theta \vee \rho$ partíciónál, ha x és y között van U-ban egy alkalmas hosszúságú

$$x = z_0 \overset{\theta}{\text{——}} z_1 \overset{\rho}{\text{——}} z_2 \overset{\theta}{\text{——}} z_3 \overset{\rho}{\text{——}} z_4 \quad \ldots \quad z_{n-1} \overset{\rho}{\text{——}} z_n = y$$

sorozat. Miért tehetjük föl, hogy a sorozat θ-val kezdődik és ρ-val végződik?

A gráfelmélet alapjaihoz értő Olvasó számára az előző feladat a következőképpen is fogalmazható. Készítsünk egy gráfot az U halmazon úgy, hogy az x és y közé élet rajzolunk, ha x és y egy osztályban vannak θ vagy ρ szerint. Ha a kapott gráfnak elkészítjük az (összefüggőségre vonatkozó) komponenseit, akkor ezek pontosan a $\theta \vee \rho$ osztályai lesznek.



8.4. Ábra. A négyelemű halmaz partícióhálója.

A továbbiakban egyre inkább el fogjuk mosni a partíció és az ekvivalencia-reláció közötti különbséget, beszélünk például egy ekvivalencia-reláció osztályairól, vagy a θ partícióhoz tartozó ekvivalencia-relációt is ugyanúgy θ-val jelöljük.

Végül egy olyan fogalommal ismerkedünk meg, amelyre például a direkt szorzat jellemzésénél lesz szükségünk. Halmazok között nemcsak a metszet és az egyesítés, hanem a komplementum-képzés is alapvető művelet. Ha Y részhalmaza X-nek, akkor Y komplementuma az $X - Y$ halmaz (amelynek elemei azok az X-beli elemek, amelyek Y-ban nincsenek benne). Az Y komplementumát Y'-vel jelöljük. Az Y' komplementumot egyértelműen meghatározza, hogy $Y \cup Y' = X$ és $Y \cap Y' = \emptyset$. Ez lehetővé teszi a következő általánosítást:

8.1.26. Definíció. Legyen L nulla és egységelemes háló. Azt mondjuk, hogy az $x, y \in L$ elemek egymás *komplementumai*, ha metszetük 0 és egyesítésük 1. Az L háló *komplementumos*, ha minden elemének van komplementuma.

Gyakorlatok, feladatok

8.1.27. Gyakorlat. Rajzoljuk le egy kételemű, illetve egy háromelemű halmaz összes részhalmazainak hálóját, valamint e halmazok partícióhálóját.

8.1.28. Gyakorlat. Melyek komplementumosak a 8.3. Ábra hálói közül?

8.1.29. Gyakorlat. Igazoljuk, hogy minden halmaz partícióhálója komplementumos.

8.1.30. Gyakorlat. Rajzoljuk le az S_3, A_4 és Q csoportok részcsoporthálóját (Q a nyolcelemű kvaterniócsoportot jelöli), valamint a D_4 diédercsoport normálosztóhálóját.

8.2. Algebrai struktúrák

Általános algebrai struktúrán egy műveletekkel ellátott halmazt értünk. Szó lesz a három legalapvetőbb fogalomról: a részalgebráról, a homomorfizmusról és a direkt szorzatról. A homomorfizmusok magjai a kongruenciák. Mind a részalgebrák, mind a kongruenciák teljes hálót alkotnak.

8.2.1. Definíció. Legyen A nem üres halmaz. Az A-n értelmezett, n-változós *műveletnek* egy A-n értelmezett, A-ba képző n-változós függvényt nevezünk, vagyis egy tetszőleges

$$f : A^n = A \times A \times \ldots \times A \to A$$

leképezést (ahol $n \geq 1$ egész). Az n szám az f művelet *aritása*.

Beszélnek néha nulla változós műveletről is. Ha belegondolunk a pontos halmazelméleti definíciókba, akkor A^0 egy egyelemű halmaz (egyetlen eleme az üres függvény), és így egy nulla változós művelet az A egy elemét jelöli ki. Ennek van értelme, például egy gyűrűben egy nullváltozós művelettel néha ki szokás jelölni az egységelemet, azt biztosítandó, hogy csak azok számítsanak részgyűrűnek, amelyek az egységelemet tartalmazzák (2.2.35. Gyakorlat, 2.4.24. Feladat). Mi nullváltozós műveletekkel nem foglalkozunk, mert ugyanennek a célnak megfelel egy konstans egyváltozós művelet is.

Az aritás szó onnan származik, hogy az egyváltozós műveleteket *unáris*, a kétváltozósakat *bináris*, a háromváltozósakat *ternáris* műveleteknek is hívják. Unáris műveletre nagyon fontos példa az inverzképzés, vagy vektortérben, modulusban a skalárral való szorzás (lásd 368. oldal).

8.2.2. Definíció. Algebrai struktúrának (röviden *algebrának*) egy nem üres A halmazt nevezünk, amelyen értelmezve van néhány (akár végtelen sok) művelet.

Ha nagyon precízek akarnánk lenni, akkor meg kellene különböztetnünk az algebrát az alaphalmazától, hiszen a kettő nyilván nem ugyanaz, és már korábban is találkoztunk olyan jelenséggel, hogy ugyanazon a halmazon többféle struktúrát is értelmeztünk. Például a $\mathbb{C}$ halmaz néha testet, néha meg $\mathbb{R}$ fölötti vektorteret jelentett. Ezért szokás az algebrai struktúrát úgy definiálni, mint egy $\mathbf{A} = (A, F)$ párt, ahol A az alaphalmaz, F pedig a műveletek halmaza. Mivel könyvünk hangsúlyozottan bevezető jellegű, ilyen finomságokkal nem foglalkozunk, hanem az algebrákat továbbra is (pongyolán) az alaphalmazukkal jelöljük. Ez nem fog félreértést okozni, viszont egyszerűsíti a jelöléseket, és így a lényeg megértését.

8.2.3. Definíció. Az A algebrának a $B \subseteq A$ nem üres részhalmaz *részalgebrája*, ha B zárt az A műveleteire, vagyis A tetszőleges f műveletére és tetszőleges $b_1, \ldots, b_n \in B$ elemekre $f(b_1, \ldots, b_n) \in B$ (itt n az f aritását jelöli). Jele $B \leq A$.

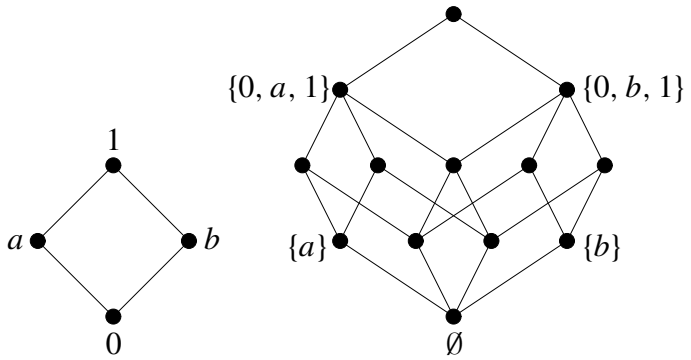
Ez a definíció is elvileg pontosításra szorul, mert ha f egy művelete A-nak, akkor az egy $f : A^n \to A$ függvény. Ha B zárt f-re, attól még f maga nem lesz B-nek művelete, hanem f helyett az f *megszorítását* kell venni a B^n halmazra. Ennek az értelmezési tartománya B^n, és minden elem n-eshez ugyanazt rendeli, mint f. Így kapjuk a B rész*algebrát*.

8.2.4. Gyakorlat. Mutassuk meg, hogy a csoportok között a részcsoport fogalma megegyezik a fenti általános részalgebra fogalmával, ha az inverzképzést egyváltozós műveletnek bevesszük, de ha csak a szorzást vesszük be műveletnek, akkor nem. Be kell-e venni az egységelemet is konstans egyváltozós (vagy nullváltozós) műveletnek?

Csoportokban, gyűrűkben részalgebrák metszete is részalgebra (részcsoport, részgyűrű) volt, és ezért a részalgebrák teljes hálót alkottak. Ez lényegében általában is teljesül, hiszen azt triviális belátni, hogy ha az A algebra bizonyos részhalmazai zártak A műveleteire, akkor e részhalmazok metszete is zárt ugyanezekre a műveletekre. Ezért a 8.1.20. Tétel miatt a részalgebrák teljes hálót alkotnak.

8.2.5. Definíció. Az A algebra részalgebráinak hálóját az A *részalgebrahálójának* nevezzük, és $\mathrm{Sub}(A)$-val jelöljük.

Problémát jelent, hogy részalgebrák metszete az üres halmaz is lehet, amit nem tekintünk részalgebrának. Például egy tetszőleges hálóban minden egyelemű részhalmaz részháló (hiszen $x \vee x = x \wedge x = x$ minden x-re). De már két ilyen részhalmaz metszete is az üres halmaz. Ilyesmi csoportokban nem fordulhat elő, mert az egységelem mindegyik részcsoportban benne van. A problémát úgy kerüljük meg, hogy noha az üres halmazt nem tekintjük részalgebrának, mégis bevesszük a részalgebrahálóba, ha szükséges (vagyis ha a részalgebrák metszete az üres halmaz). Példa erre a 8.5. Ábrán látható négyelemű háló részháló-hálója. Ez a jelenség problémát okoz az üres halmaz által generált részalgebrával is, amely „normális esetben” az algebra legkisebb részalgebrája lenne.



8.5. Ábra. Egy négyelemű háló, és a részháló-hálója.

8.2.6. Gyakorlat. Hálót alkotnak-e a 8.3. Ábrán látható D hálóban a $0, a, b, 1$ elemek a háló rendezésére? Részhálót alkotnak-e?

8.2.7. Gyakorlat. Mely hálókban lesz minden nem üres részhalmaz részháló?

8.2.8. Definíció. Legyen A algebra és $X \subseteq A$. Ekkor az X által *generált részalgebra* az A legszűkebb olyan részalgebrája, amely az X-et tartalmazza. Jele $\langle X \rangle$.

Az X által generált részalgebra nyilván létezik, mint az X-et tartalmazó részalgebrák metszete. A generált részalgebra elemeinek általános leírásáról később lesz szó.

Következő témánk a homomorfizmus fogalma lenne, ezzel azonban probléma van. Képzeljük el, hogy adott két gyűrű, az első az R halmazon értelmezett f és g műveletekkel, a másik az S halmazon értelmezett h és k műveletekkel. Az f és g tehát kétváltozós függvények az R halmazon, az egyik az összeadás, a másik a szorzás. Ugyanígy h és k is kétváltozós függvények S-en. Hogyan definiáljuk a $\varphi : R \to S$ művelettartó leképezést? A

$$\varphi f(x, y) = h\big(\varphi(x), \varphi(y)\big) \quad \text{vagy a} \quad \varphi f(x, y) = k\big(\varphi(x), \varphi(y)\big)$$

a jó képlet?

A válasz az, hogy egy gyűrűben a műveleteket nemcsak függvényként adjuk meg, hanem *megmondjuk*, hogy melyik művelet az összeadás és melyik a szorzás! Hiszen másképp még a gyűrűaxiómákat sem tudnánk ellenőrizni. Ez azt jelenti, hogy az általános algebrának a 8.2.2. Definícióban megadott fogalma nem kielégítő, mert a valóságban a műveletek nemcsak konkrét függvények, hanem *nevük* is van, mint összeadás, szorzás, metszet, egyesítés. Ezért a korábban definiált fogalmat *nem indexelt algebrának* fogjuk hívni, és bevezetjük a következőt.

8.2.9. Definíció. Tegyük föl, hogy adott műveleti szimbólumok egy Ω halmaza, és mindegyik eleméről megadjuk azt is, hogy az hány változós (ami egy τ függvény Ω-ból a pozitív egészek halmazába). Ekkor egy τ *típust* adtunk meg.

Például a gyűrűket tekinthetjük úgy, hogy típusuk $\Omega = \{+, -, \cdot, 0\}$, ahol $\tau(+) = 2$, $\tau(-) = 1$, $\tau(\cdot) = 2$ és $\tau(0) = 1$. Itt $-$ az ellentettképzés, amit egyváltozós műveletnek tekintünk (a kivonás, mint tudjuk, ebből az $x - y = x + (-y)$ képlettel kapható). A 0 azt az egyváltozós konstans műveletet jelenti, amely minden helyen a gyűrű nullelemét veszi föl.

Ha formálisak akarunk lenni, akkor a típust definiálhatjuk úgy, mint az τ függvényt, hiszen az meghatározza az Ω halmazt, mint az értelmezési tartományát. A típust néha *hasonlósági típusnak*, az azonos típusú algebrákat pedig ilyenkor *hasonló* algebráknak hívják.

8.2.10. Definíció. Legyen τ egy típus a műveleti jelek Ω halmazával. Ekkor az A halmaz egy τ *típusú (indexelt) algebra*, ha minden $f \in \Omega$ műveleti jelhez meg van adva A-nak egy $\tau(f)$ változós f^A művelete.

Ez magyarul azt jelenti, hogy egy R gyűrűben az összeadás műveletét $+^R$ jelöli, ahol $+$ az általános összeadási szimbólum (amely közös az összes gyűrűben). Persze nem leszünk ilyen pedánsak, és a kitevőből az R-et általában lehagyjuk. De nem érdemes lehagyni akkor, amikor a gyűrű-homomorfizmus fogalmát akarjuk általánosítani. Ez ugyanis egy olyan $\varphi : R \to S$ leképezés, amelyre

$$\varphi(r_1 +^R r_2) = \varphi(r_1) +^S \varphi(r_2) \quad \text{és} \quad \varphi(r_1 \cdot^R r_2) = \varphi(r_1) \cdot^S \varphi(r_2)$$

tetszőleges $r_1, r_2 \in R$ esetén. Most már pontosítani tudjuk a 2.2.32. definíciót is. A művelettartás azt fejezi ki, hogy mindegy, hogy előbb a műveletet és azután a homomorfizmust, vagy pedig először a homomorfizmust és utána a műveletet végezzük-e el.

8.2.11. Definíció. Legyenek A és B azonos típusú algebrák. A $\varphi : A \to B$ leképezés *homomorfizmus*, ha A és B típusának minden f műveleti jelére és tetszőleges $a_1, \dots, a_n \in A$ elemekre

$$\varphi\big(f^A(a_1, \dots, a_n)\big) = f^B\big(\varphi(a_1), \dots, \varphi(a_n)\big)\,,$$

ahol n az f aritása.

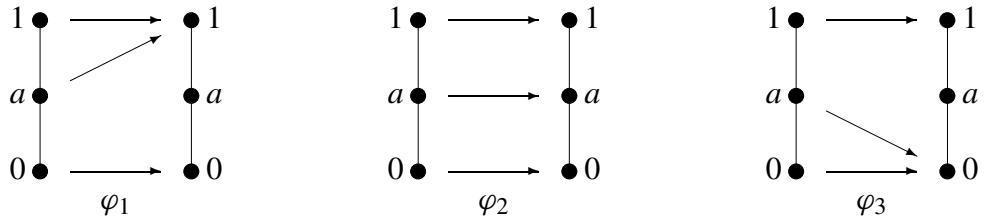
Egy $\varphi : A \to B$ homomorfizmust *izomorfizmusnak* nevezünk, ha kölcsönösen egyértelmű. Az $A \to A$ homomorfizmusok neve *endomorfizmus*, az $A \to A$ izomorfizmusok neve *automorfizmus*.

Ez a definíció vektortérben, modulusban tényleg a megszokott homomorfizmus-fogalmat adja (lásd a 7.1.6. Definíció utáni megjegyzéseket). Az, hogy homomorfizmust csak azonos típusú algebrák között értelmeztünk, modulusok esetében azt jelenti, hogy csak ugyanazon gyűrű fölötti modulusok között beszélhetünk homomorfizmusról. Ha a gyűrűk definíciójában az egységelemet is bevesszük konstans egyváltozós műveletnek, akkor a homomorfizmusok az egységelemet mindig az egységelembe fogják vinni (csoportok esetében ez az egységelem kijelölése nélkül is automatikusan teljesül a 2.2.41. Feladat miatt, gyűrűkben viszont nem feltétlenül, lásd 5.1.19. Gyakorlat). Az unitér modulusokat definiáló azonosságok fölírásához is szükségünk van az alapgyűrű egységelemére, mint műveletre.

Hálók között a homomorfizmus fogalmát szintén a műveletek, és nem a rendezés segítségével definiáljuk: a $\varphi : L \to K$ akkor háló-homomorfizmus, ha tetszőleges $a, b \in L$ esetén $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$ és $\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$.

8.2.12. Definíció. Legyenek P és Q részben rendezett halmazok, és $\varphi : P \to Q$ egy leképezés. Azt mondjuk, hogy φ *rendezéstartó*, ha tetszőleges $a, b \in P$ esetén $a \leq b$-ből $\varphi(a) \leq \varphi(b)$ következik. A rendezéstartó függvényeket néha *monotonnak* is hívják. A φ *rendezésfordító*, ha tetszőleges $a, b \in P$ esetén $a \leq b$-ből $\varphi(a) \geq \varphi(b)$ következik.

Rendezésfordító leképezésre a Galois-elmélet főtételében láttunk példát, de egy halmaz részhalmazai között a komplementumképzés is rendezésfordító.



8.6. Ábra. Három háló-homomorfizmus.

8.2.13. Gyakorlat. Igazoljuk, hogy minden háló-homomorfizmus rendezéstartó.

Ha L háló, P részben rendezett halmaz, és $\varphi : L \to P$ olyan rendezéstartó bijekció, melynek az inverze is rendezéstartó, akkor P is háló, és φ háló-izomorfizmus (hiszen a két részben rendezett halmaz teljesen egyforma, és a háló-műveleteket a rendezés segítségével definiáltuk). A 8.2.14. Gyakorlat azt mutatja, hogy ezen a feltételen nem lehet gyengíteni.

8.2.14. Gyakorlat. Adjunk meg egy rendezéstartó bijekciót két háló között, amely nem háló-homomorfizmus.

Egy φ csoporthomomorfizmus magján az egységelem teljes inverz képét értjük, amely meghatározza az összes többi elem teljes inverz képét is (ezek a $\mathrm{Ker}(\varphi)$ mag szerinti mellékosztályok). Általában a helyzet nem ennyire rózsás, amint a 8.6. Ábrán lerajzolt három háló-homomorfizmus példáján láthatjuk. Már eleve az sem világos, hogy a 0 vagy az 1 teljes inverz képét érdemes-e nézni. De akármelyiket nézzük is, az nem határozza meg a homomorfizmust, hiszen például a 0 teljes inverz képe φ_1-nél és φ_2-nél is $\{0\}$, és ez mégis két különböző homomorfizmus.

A megoldás az, hogy egy homomorfizmus magjaként nemcsak egy elem teljes inverz képét, hanem az összes elem teljes inverz képét meg kell adnunk. Ez azt jelenti, hogy a mag egy partíció lesz. A fenti példában tehát

$$\mathrm{Ker}(\varphi_1) = \{\{0\}, \{a, 1\}\}, \quad \mathrm{Ker}(\varphi_2) = \{\{0\}, \{a\}, \{1\}\}, \quad \mathrm{Ker}(\varphi_3) = \{\{0, a\}, \{1\}\}.$$

8.2.15. Definíció. Legyen $\varphi : A \to B$ egy homomorfizmus. Ekkor a φ homomorfizmus *képe* az $\mathrm{Im}(\varphi) = \{\varphi(a) : a \in A\} \leq B$ részalgebra (vagyis φ értékkészlete). A φ *magja* az A-nak az a partíciója, amelynél a_1 és a_2 akkor és csak akkor van egy osztályban, ha $\varphi(a_1) = \varphi(a_2)$. A mag jele $\mathrm{Ker}(\varphi)$.

Ebben a definícióban igazából nem a $\mathrm{Ker}(\varphi)$ partíciót, hanem a hozzá tartozó ekvivalencia-relációt adtuk meg. Az Olvasó azonban könnyen ellenőrizheti, hogy a $\mathrm{Ker}(\varphi)$ osztályai tényleg a $\varphi^{-1}(b) = \{a \in A : \varphi(a) = b\}$ teljes inverz képek, ahol b befutja az $\mathrm{Im}(\varphi)$ részalgebrát.

Ha tehát általános algebrai szemmel nézünk egy csoportot (vagy gyűrűt), akkor egy homomorfizmus magja nem egy normálosztó (vagy ideál), hanem egy normálosztó (ideál) szerinti mellékosztályok által alkotott partíció lesz.

Csoportoknál, gyűrűknél a mag részstruktúra is volt az eredeti algebrában. Általános algebrák esetén egy $\varphi : A \to B$ homomorfizmusnál a $b \in \mathrm{Im}(\varphi)$ teljes inverz képe pontosan akkor lesz részalgebra A-ban, ha $\{b\}$ egyelemű részalgebrája B-nek. Így csoportoknál az egységelem teljes inverz képe részcsoport, hálók esetében pedig (ahol minden egyelemű részhalmaz részalgebra), minden kongruenciaosztály részalgebra lesz. Tetszőleges A és B esetén azonban előfordulhat, hogy egyik elem teljes inverz képe sem lesz részalgebra. Ugyanakkor meg fogjuk látni, hogy a maghoz, mint partícióhoz tartozó ekvivalencia-reláció, mint párok halmaza, részalgebrája lesz az $A \times A$ direkt szorzatnak (8.2.27. Definíció, 8.3.10. Gyakorlat).

Csoportok esetében a normálosztókat, gyűrűknél az ideálokat jellemeztük egyfajta „zártsági" tulajdonsággal, a homomorfizmus fogalmára nem utalva (csoportoknál a konjugáltságra, gyűrűknél a külső elemekkel való szorzásra kellett a zártságot megkövetelnünk). Most ezt megtesszük általában is. Ez semmi újdonságot nem fog jelenteni, mert gyűrűknél már bevezettük a „kongruenciákat" általában is, azaz ha I ideál, akkor az

$$r_1 \equiv r_2 \ (I)$$

jelölést arra, hogy r_1 és r_2 egy mellékosztályban van I szerint (vagyis $r_1 - r_2 \in I$). Az 5.2.3. Gyakorlatban beláttuk, hogy ezek a kongruenciák összeadhatók és összeszorozhatók.

8.2.16. Definíció. Az A algebra egy θ partícióját (ekvivalencia-relációját) *kongruenciának* nevezzük, ha *kompatibilis* A műveleteivel, vagyis tetszőleges f műveletre, ha

$$a_1 \equiv b_1 \ (\theta)\,, \ \ldots\,, \ a_n \equiv b_n \ (\theta)\,,$$

akkor

$$f(a_1, \ldots, a_n) \equiv f(b_1, \ldots, b_n) \ (\theta)\,,$$

ahol n az f művelet aritása. (Általános kompatibilis relációkról a 8.3.12. és a 8.3.13. Definíciókban lesz szó.) A θ kongruencia *triviális*, ha mint partíció az, vagyis ha 0_A-val, vagy 1_A-val egyezik meg.

8.2.17. Tétel. *Az A algebra egy θ partíciója akkor és csak akkor magja egy alkalmas A-n értelmezett homomorfizmusnak, ha kongruencia.*

Bizonyítás. Ha $\theta = \mathrm{Ker}(\varphi)$ és $a_i \equiv b_i \ (\theta)$, akkor a mag definíciója szerint $\varphi(a_i) = \varphi(b_i)$ minden i-re. Mivel φ homomorfizmus,

$$\varphi\big(f(a_1, \ldots, a_n)\big) = f\big(\varphi(a_1), \ldots, \varphi(a_n)\big) = f\big(\varphi(b_1), \ldots, \varphi(b_n)\big) = \varphi\big(f(b_1, \ldots, b_n)\big)\,.$$

Ezért $f(a_1, \ldots, a_n) \equiv f(b_1, \ldots, b_n) \ (\theta)$.

Tegyük most föl, hogy θ kongruencia, konstruálnunk kell egy homomorfizmust, amelynek a magja θ. Ez csoportokban, gyűrűkben a faktor fogalmának bevezetésével történt, most is így járunk el. Készítsük el a C algebrát, melynek elemei a θ kongruencia osztályai. A műveleteket reprezentánsok segítségével definiáljuk. Legyen f egy n-változós műveleti szimbólum, és $X_1, \ldots, X_n$ a θ osztályai. Válasszunk tetszőlegesen $a_i \in X_i$ reprezentánsokat, és legyen $f^C(X_1, \ldots, X_n)$ a θ-nak az az osztálya, amelyik az $f^A(a_1, \ldots, a_n)$ elemet tartalmazza.

A jóldefiniáltságot most is ellenőrizni kell, de ez pont a kongruencia definíciójában megadott feltétel. Valóban, ha ugyanezen osztályokból az a_i helyett a b_i reprezentánsokat választjuk, akkor $a_i \equiv b_i \ (\theta)$, és mivel θ kongruencia, az $f(b_1, \ldots, b_n)$ ugyanabban az osztályban lesz, mint $f(a_1, \ldots, a_n)$. Végül legyen $\varphi : A \to C$ az a leképezés, amely minden $a \in A$ elemhez az őt tartalmazó θ-osztályt rendeli. Ez homomorfizmus a C-beli műveletek definíciója miatt, és magja θ. □

8.2.18. Definíció. Az előző bizonyításban konstruált C algebrát az A algebrának a θ kongruenciája szerinti *faktoralgebrájának* nevezzük, és A/θ-val jelöljük. Ha $a \in A$, akkor a θ partíciónak az a elemet tartalmazó osztályát a/θ jelöli. A $\varphi : a \mapsto a/\theta$ leképezés neve *természetes homomorfizmus*.

8.2.19. Tétel [Homomorfizmus-tétel]. *Ha A és B azonos típusú algebrák, és $\varphi : A \to B$ homomorfizmus, akkor* $\mathrm{Im}(\varphi) \cong A/\,\mathrm{Ker}(\varphi)$.

Bizonyítás. Legyen $\theta = \mathrm{Ker}(\varphi)$. Az $a/\theta \mapsto \varphi(a)$ leképezés nyilvánvalóan jóldefiniált és izomorfizmus (mert a/θ pont a $\varphi(a)$ teljes inverz képe φ-nél). □

Most az izomorfizmus-tételeket általánosítjuk. Ezek kimondásához olyan jelöléseket kell bevezetni, amiket nem használunk a későbbiekben. A 8.2.20. Feladat útmutatójában megtalálhatók ezek a jelölések, az állítások pedig elolvashatók a megoldásban. Azt tanácsoljuk, hogy az Olvasó próbálja meg maga kimondani a tételeket, és megtalálni a megfelelő jelöléseket.

8.2.20. Feladat. Fogalmazzuk meg és bizonyítsuk be a faktoralgebra részalgebráit leíró tételt az 5.2.11. Tétel mintájára. Általánosítsuk a két izomorfizmus-tételt is.

Egy A algebra kongruenciái ekvivalencia-relációk, és így párok halmazai. A halmazelméleti tartalmazás tehát részben rendezést ad a kongruenciák között, ugyanúgy, ahogy az A partíciói között is (8.1.23. Definíció).

8.2.21. Gyakorlat. Mutassuk meg, hogy az A algebra tetszőleges kongruenciáinak az A partícióhálójában vett metszete is kongruencia.

Ez a metszet a kongruenciák között is legnagyobb alsó korlát (hiszen minden kongruencia partíció). A 8.1.20. Tétel miatt tehát az A algebra kongruenciái teljes hálót alkotnak.

8.2.22. Definíció. Az A algebra kongruenciáinak teljes hálóját az *A kongruencia-hálójának* nevezzük, és $\mathrm{Con}(A)$-val jelöljük. Ennek legkisebb elemét 0_A, legnagyobb elemét 1_A jelöli (ugyanúgy, mint a 8.1.23. Definícióban). Az A algebra *egyszerű*, ha pontosan két kongruenciája van, a 0_A és az 1_A, vagyis ha A kongruencia-hálója a kételemű háló.

A részalgebrákat nem úgy kell egyesíteni, mint a részhalmazokat, hiszen például két részcsoport uniója általában nem részcsoport, és így az egyesítésük az uniójuknál nagyobb. Így a G csoport részcsoporthálója nem részhálója a G részhalmazaiból álló hálónak. Némileg meglepő, de fontos észrevétel, hogy kongruenciák esetében jobb a helyzet.

8.2.23. Tétel. *Az A algebra kongruencia-hálója teljes részhálója az A halmaz partícióhálójának, azaz kongruenciák tetszőleges halmazának, mint partícióknak az egyesítése (és a metszete is) ugyanaz, mint a partícióként való egyesítésük.*

Bizonyítás. A fentiekhez hasonlóan elegendő azt megmutatni, hogy kongruenciáknak a partícióhálóban vett egyesítése is kongruencia. Két partíció egyesítését a 8.1.25. Feladatban írtuk le. Csak erre az esetre és csak kétváltozós műveletre bizonyítunk, az általános eset meggondolását az Olvasóra hagyjuk (vö. 8.3.19. Gyakorlat). Legyenek tehát θ és ρ kongruenciák az A algebrán, és $*$ egy kétváltozós művelet. Azt kell megmutatni, hogy ha $a \equiv b\ (\theta \vee \rho)$ és $c \equiv d\ (\theta \vee \rho)$, akkor $a * c \equiv b * d\ (\theta \vee \rho)$.

Elég belátni, hogy $a * c \equiv b * c\ (\theta \vee \rho)$ és $b * c \equiv b * d\ (\theta \vee \rho)$, mert akkor $\theta \vee \rho$ tranzitivitása miatt készen vagyunk. Mivel $a \equiv b\ (\theta \vee \rho)$, a 8.1.25. Feladat szerint létezik egy

$$a = z_0 \overset{\theta}{\text{——}} z_1 \overset{\rho}{\text{——}} z_2 \overset{\theta}{\text{——}} z_3 \overset{\rho}{\text{——}} z_4 \quad \dots \quad z_{n-1} \overset{\rho}{\text{——}} z_n = b$$

sorozat. Tudjuk, hogy $c \equiv c\ (\theta)$ és $c \equiv c\ (\rho)$, és ezért $z_i * c \equiv z_{i+1} * c\ (\theta)$ ha i páros, és $z_i * c \equiv z_{i+1} * c\ (\rho)$ ha i páratlan (hiszen kongruenciákat szabad összeszorozni). Vagyis a $z_i * c$ elemek egy olyan sorozatot alkotnak, amely az $a * c \equiv b * c\ (\theta \vee \rho)$ összefüggést bizonyítja. A $b * c \equiv b * d\ (\theta \vee \rho)$ bizonyítása hasonló. □

A csoporthatások újabb fontos példát szolgáltatnak a most bevezetett fogalmakra. A vektorterekhez és a modulusokhoz hasonlóan most is annyi unáris műveletet vezetünk be, amennyi az alapcsoport elemszáma.

8.2.24. Definíció. Ha a G csoport hat az X halmazon (4.6.17. Definíció), akkor g minden eleméhez vegyünk föl egy unáris f_g műveletet, amelyre $f_g(x) = g * x$ teljesül minden $x \in X$ esetén. Így az X halmaz algebrává válik, amelynek minden művelete unáris.

Az így kapott algebrát az angol nyelvű szakirodalomban G-set elnevezéssel illetik (a „set" magyarul halmazt jelent). Az alábbi két állítás triviálisan adódik a definíciókból.

8.2.25. Állítás. *Egy G csoport hatása az X_1 és X_2 halmazokon akkor és csak akkor ekvivalens (4.6.23. Definíció), ha az X_1 és X_2 algebrák izomorfak. Ha G hat X-en, akkor ennek a hatásnak a kongruenciái (a csoportelméleti értelemben, lásd 4.11.13. Definíció) ugyanazok, mint az X kongruenciái az általános algebrai értelemben.*

8.2.26. Állítás. *Legyen G csoport, H részcsoportja G-nek, és hasson G balszorzással a H szerinti bal mellékosztályok X halmazán (4.6.25. Definíció). A 4.11.17. Gyakorlat szerint az X kongruenciái kölcsönösen egyértelmű megfeleltetésben állnak a G csoport H-t tartalmazó részcsoportjaival. Ez a megfeleltetés mindkét irányban rendezéstartó, és így háló-izomorfizmus. Ezért X kongruencia-hálója izomorf a G csoport H-t tartalmazó részcsoportjainak a hálójával.*

Végül a direkt szorzat fogalmát általánosítjuk. Legyenek A_i azonos típusú algebrák (ahol $i \in I$), és

$$A = \prod_{i \in I} A_i$$

az A_i alaphalmazok Descartes-szorzata. Ennek elemei az olyan $\mathbf{a} = (\ldots, a_i, \ldots)$ sorozatok, amelyekre $a_i \in A_i$ mindegyik i-re. Ha f egy n-változós műveleti jel, és $\mathbf{a}^1, \ldots, \mathbf{a}^n$ az A halmaz n darab eleme, akkor ezeken az f-et komponensenként értelmezzük. Ez azt jelenti, hogy ha az $\mathbf{a}^j$ vektor i-edik komponensét a_i^j jelöli, akkor az $f^A(\mathbf{a}^1, \ldots, \mathbf{a}^n)$ elem i-edik komponense $f^{A_i}(a_i^1, \ldots, a_i^n)$. Fontos észrevennünk, hogy az a π_i leképezés, amely a direkt szorzat $\mathbf{a} = (\ldots, a_i, \ldots)$ eleméhez az a_i-t rendeli, egy A-ból A_i-re képző homomorfizmus.

8.2.27. Definíció. Az imént definiált A algebrát az A_i algebrák *direkt szorzatának* nevezzük. A π_i homomorfizmust az i-edik *projekciónak* hívjuk. Véges sok tényező esetén az $A = A_1 \times \ldots \times A_k$ jelölést is alkalmazzuk. Ha mindegyik A_i ugyanaz a B algebra, akkor *direkt hatványról* beszélünk, jele B^I vagy B^k.

Csoportoknál (gyűrűknél) a direkt szorzatot normálosztók (illetve ideálok) segítségével jellemeztük (4.8.12. Tétel), ezek a projekciók magjaiként keletkeztek. Ezért az általános esetben a direkt szorzatot nem részstruktúrák, hanem kongruenciák segítségével célszerű jellemezni. Megjegyezzük, hogy az $A_1 \times A_2$ direkt szorzatnak sokszor nincs is az A_1-gyel vagy az A_2-vel izomorf részalgebrája.

Legyen tehát $A = A_1 \times A_2$ egy direkt szorzat. Tekintsük a π_1 és π_2 projekciókat (tehát $\pi_1(a_1, a_2) = a_1$, illetve $\pi_2(a_1, a_2) = a_2$), és jelölje η_i a π_i homomorfizmus magját. Ez azt jelenti, hogy

$$(a_1, a_2) \equiv (b_1, b_2)\ (\eta_1) \iff a_1 = b_1\,,$$

és hasonló állítás igaz η_2-re is. Innen azonnal látszik, hogy ha (a_1, a_2) és (b_1, b_2) az η_1-nél és η_2-nél is kongruens, akkor $(a_1, a_2) = (b_1, b_2)$. Ez tehát azt jelenti, hogy $\eta_1 \wedge \eta_2 = 0_A$ (ami az $A^* \cap B^* = \{1_G\}$ összefüggésnek felel meg a 4.8.11. Állításban).

A csoportokra a 4.8.11. Állításban bizonyított $A^*B^* = G$ összefüggést úgy is fogalmazhatjuk, hogy az A^* és a B^* normálosztók generálják a G direkt szorzatot. Azt gondolhatnánk, hogy ennek most $\eta_1 \vee \eta_2 = 1_A$ felel meg. Ennél azonban több is igaz. Az $\eta_1 \vee \eta_2 = 1_A$ azt jelenti, hogy A bármely két eleme között létezik a 8.1.25. Feladatban leírt sorozat. Valójában azonban mindig van olyan sorozat is, amely csak egyetlen közbülső elemet tartalmaz (azaz olyan rövid, amilyen rövid csak lehet).

Ha (a_1, a_2) és (b_1, b_2) az A algebra tetszőleges elemei, akkor

$$(a_1, a_2) \overset{\eta_1}{\text{———}} (a_1, b_2) \overset{\eta_2}{\text{———}} (b_1, b_2) \quad \text{és} \quad (a_1, a_2) \overset{\eta_2}{\text{———}} (b_1, a_2) \overset{\eta_1}{\text{———}} (b_1, b_2)\ .$$

Ez a fajta speciális egyesítés annyira fontos, hogy nevet is adunk neki.

8.2.28. Definíció. Legyen A egy halmaz. Egy A-n értelmezett *kétváltozós reláció* az $A \times A$ tetszőleges részhalmaza, vagyis A-beli párok egy halmaza. (Általában az A^n részhalmazait n-változós relációknak nevezzük.) Ha θ és ρ kétváltozós relációk az A halmazon, akkor ezek *kompozíciója*

$$\theta \circ \rho = \{(a, c)\ :\ \text{létezik } b \in A, \text{melyre } a \overset{\theta}{\text{———}} b \overset{\rho}{\text{———}} c\ \}\,.$$

Relációk kompozícióját nem véletlenül hívjuk és jelöljük ugyanúgy, mint a függvényekét. A halmazelmélet precíz felépítésében ugyanis egy $f : A \to A$ függvényt úgy szokás értelmezni, mint az $(x, f(x))$ párok halmazát, vagyis egy speciális kétváltozós relációt. Könnyű látni, hogy a függvények kompozíciója a fenti reláció-kompozícióval azonos. Persze $f : A \to B$ függvények is vannak. Ennek megfelelően a kétváltozós relációt kicsit általánosabban is definiálhattuk volna, az $A \times B$ részhalmazainak, ahol A és B két tetszőleges halmaz. Erre az általánosabb reláció-fogalomra azonban nem lesz szükségünk.

A kompozíció nyilván asszociatív művelet az általános kétváltozós relációk körében is. Alkalmas arra is, hogy a tranzitivitást kifejezzük vele: egy θ reláció akkor és csak akkor tranzitív, ha $\theta \circ \theta \subseteq \theta$. Speciálisan ha θ ekvivalencia-reláció, akkor $\theta \circ \theta = \theta$.

8.2.29. Definíció. Legyenek θ és ρ az U halmaz ekvivalencia-relációi. Azt mondjuk, hogy ezek *felcserélhetők*, ha $\theta \circ \rho = \rho \circ \theta$.

8.2.30. Gyakorlat. Mutassuk meg, hogy ha θ és ρ felcserélhető ekvivalencia-relációk, akkor a partícióhálóban vett egyesítésük, $\theta \vee \rho = \theta \circ \rho$.

Az imént tehát azt láttuk be, hogy az $A = A_1 \times A_2$ direkt szorzatban vizsgált két kongruenciára $\eta_1 \circ \eta_2 = 1_A = \eta_2 \circ \eta_1$.

8.2.31. Állítás. *Tegyük föl, hogy $A = A_1 \times A_2$, jelölje η_i a projekciók magjait. Ekkor*

(1) $\eta_1 \wedge \eta_2 = 0_A$;
(2) $\eta_1 \circ \eta_2 = 1_A = \eta_2 \circ \eta_1$;
(3) $A_i \cong A/\eta_i$ *(ha* $i = 1, 2$*).*

Speciálisan a két projekció magja egymásnak komplementuma. Megfordítva, ha az A algebrán adottak az η_1 és η_2 kongruenciák az (1) *és* (2) *feltételekkel, akkor*

$$A \cong A/\eta_1 \times A/\eta_2 .$$

Bizonyítás. Az (1) és (2) állításokat már beláttuk, a (3) a homomorfizmus-tételből adódik, ha azt a π_i projekcióra alkalmazzuk.

Megfordítva, tegyük föl, hogy (1) és (2) teljesül az η_i kongruenciákra. Tekintsük a

$$\varphi : a \mapsto (a/\eta_1, a/\eta_2)$$

leképezést A-ból $A/\eta_1 \times A/\eta_2$-be, ahol az a/η_i az a elem osztályát jelöli η_i-nél (lásd 8.2.18. Definíció). Az nyilvánvaló, hogy φ művelettartó, megmutatjuk, hogy bijekció is. Ehhez azt kell ellenőrizni, hogy $\mathrm{Ker}(\varphi) = 0_A$ és $\mathrm{Im}(\varphi) = A/\eta_1 \times A/\eta_2$.

Ha $\varphi(a) = \varphi(b)$, akkor $a/\eta_1 = b/\eta_1$, vagyis $a \equiv b\ (\eta_1)$. Ugyanígy $a \equiv b\ (\eta_2)$, és ezért $a \equiv b\ (\eta_1 \wedge \eta_2)$. De $\eta_1 \wedge \eta_2 = 0_A$, vagyis $a = b$. Tehát $\mathrm{Ker}(\varphi) = 0_A$ és így φ injektív.

Annak igazolásához, hogy φ szürjektív, legyen a/η_1 és b/η_2 az A/η_1 és az A/η_2 egy-egy tetszőleges eleme. Ekkor $\eta_1 \circ \eta_2 = 1_A$ miatt van olyan $c \in A$, hogy $a \equiv c\ (\eta_1)$ és $c \equiv b\ (\eta_2)$. Ez azt jelenti, hogy $\varphi(c) = (c/\eta_1, c/\eta_2) = (a/\eta_1, b/\eta_2)$. □

A véges sok tényezős direkt szorzat jellemzését (vagyis a 4.8.13. Gyakorlat általánosítását) az alábbi állítás fogalmazza meg. A bizonyítást az Olvasóra hagyjuk.

8.2.32. Állítás. *Tegyük föl, hogy A az $A_1, \ldots, A_n$ algebrák direkt szorzata. Jelölje π_i az i-edik projekciót, vagyis azt az $A \to A_i$ homomorfizmust, amely $(a_1, \ldots, a_n)$-hez a_i-t rendel. Legyen $\eta_i = \mathrm{Ker}(\pi_i)$ és*

$$\eta_i' = \eta_1 \wedge \eta_2 \wedge \ldots \wedge \eta_{i-1} \wedge \eta_{i+1} \wedge \ldots \wedge \eta_n .$$

Ekkor $1 \le i \le n$ esetén

(1) $\eta_1 \wedge \eta_2 \wedge \ldots \wedge \eta_n = 0_A$, *és így* $\eta_i \wedge \eta_i' = 0_A$;
(2) $\eta_i = \eta_1' \circ \eta_2' \circ \ldots \circ \eta_{i-1}' \circ \eta_{i+1}' \circ \ldots \circ \eta_n'$;
(3) $\eta_i \circ \eta_i' = 1_A = \eta_i' \circ \eta_i$;
(4) $\eta_1' \circ \eta_2' \circ \ldots \circ \eta_n' = 1_A$.

Speciálisan η_i és η_i' egymás komplementumai. Megfordítva, ha $\eta_1, \ldots, \eta_n$ egy A algebra kongruenciái, és a belőlük a fenti módon származtatott η_i' kongruenciákra teljesül az (1) *és a* (3) *állítás, akkor*

$$A \cong A/\eta_1 \times \ldots \times A/\eta_n .$$

Gyakorlatok, feladatok

8.2.33. Gyakorlat. Hány kétváltozós művelet van egy négyelemű halmazon?

8.2.34. Gyakorlat. A csoportoknál tanult Cayley-táblázathoz hasonló módon írjuk fel az alábbi struktúrák műveleti tábláit, és osztályozzuk a kapott struktúrákat izomorfia szerint.

(1) Az $\{1, i, -1, -i\}$ számok a szorzásra.
(2) A $\{0, 2, 4, 6\}$ halmaz a modulo 8 összeadásra.
(3) A $\{0, 2, 4, 6\}$ halmaz a modulo 8 szorzásra.
(4) A $\{0, 4, 8, 12\}$ halmaz a modulo 16 szorzásra.
(5) A $\{3, 9, 27, 81\}$ halmaz a modulo 81 szorzásra.
(6) Egy négyelemű halmaz összes önmagába menő *konstans* leképezése a kompozíció műveletére.
(7) Egy kételemű halmaz összes önmagába menő leképezése a kompozícióra.
(8) A $\mathbb{Z}_2$ fölötti összes polinomfüggvények a szorzásra.
(9) Egy kételemű halmaz összes részhalmaza az unióra.
(10) Egy kételemű halmaz összes részhalmaza a metszetre.
(11) a $\{0, 1, 2, 3\}$ halmaz a min műveletre.
(12) Az $\{1, 2\} \times \{1, 2\}$ halmaz az $(a, b) * (c, d) = (a, d)$ műveletre.

Melyek lesznek egyszerűek a felsorolt struktúrák közül, melyek generálhatók egy elemmel, és melyek bonthatók fel nemtriviális módon direkt szorzatra?

8.2.35. Gyakorlat. Bizonyítsuk be, hogy egy $\equiv$ ekvivalencia-reláció pontosan akkor háló-kongruencia, ha minden a, b, c-re $a \equiv b$-ből $a \vee c \equiv b \vee c$ és $a \wedge c \equiv b \wedge c$ következik (hasonló állítást alkalmaztunk a 8.2.23. Tétel bizonyításában is).

8.2.36. Gyakorlat. Egy L háló egy C részhalmaza *konvex*, ha tetszőleges $h \leq a \leq k$ esetén, ha $h, k \in C$, akkor $a \in C$. Mutassuk meg, hogy egy háló-kongruencia minden osztálya konvex részháló.

8.2.37. Gyakorlat. Tekintsük a 8.3. Ábrán látható hálókat. Rajzoljuk le M_3, N_5, D_1 és D_2 kongruencia-hálóját, és a nemtriviális kongruenciáik szerinti faktorhálókat is. Melyek egyszerűek az ábrán szereplő hálók közül? Keressünk mindegyik hálóban minimális elemszámú generátorrendszert. Melyek bonthatók nemtriviális módon direkt szorzatra?

8.2.38. Gyakorlat. Adjuk meg izomorfia erejéig az összes legfeljebb ötelemű hálót.

8.2.39. Feladat. Van-e olyan kétváltozós művelet egy négyelemű halmazon, hogy a kapott struktúrának csak egy részalgebrája és két kongruenciája legyen (a triviálisak)?

8.2.40. Feladat. Igazoljuk, hogy ha egy nullelemes véges félcsoportban minden elem alkalmas hatványa nulla, akkor minden elég hosszú szorzat nulla. (Egy félcsoport *nulleleme* egy olyan 0 elem, hogy mindegyik s elemre $s * 0 = 0 * s = 0$).

8.2.41. Feladat. Bizonyítsuk be, hogy minden véges halmaz partícióhálója egyszerű.

8.3. Kifejezések, polinomok, szabad algebrák

A (formális) kifejezések és a polinomok úgy keletkeznek, hogy egy algebra műveleteit egymásba helyettesítgetjük. Ezek vizsgálata lehetővé teszi a generált rész és a szabad algebrák elemeinek a leírását is. A szabad algebra a szabad csoport fogalmát általánosítja.

A komplex együtthatós polinom fogalmát úgy definiáltuk, hogy ezek a határozatlanokból és komplex számokból az összeadás, kivonás, szorzás segítségével fölépített kifejezések. Vagyis egy gyűrű alapműveleteit kell egymásba helyettesítgetnünk az összes lehetséges módon.

Ettől teljesen eltérő jellegű példa a következő. Képzeljük el, hogy integrált áramkörökből számítógépet akarunk építeni. Mindegyik alkatrésznek vannak „bemenetei" és egy „kimenete". A bemenetekre többféle jelet vezethetünk, és ekkor a kimeneten is megjelenik egy jel. Ezeket az alkatrészeket egymáshoz csatlakoztathatjuk, azaz kimeneteket hozzáforraszthatunk bemenetekhez (egy kimenetet több bemenethez is, de egy bemenethez legfeljebb egy kimenet csatlakozhat). Az így kapott gép összetett számításokat tud végezni: a szabadon maradó bemenetekre jeleket vezetünk, és megnézzük egy szabadon maradó kimeneten kapott jeleket. Az ilyen „gépeket" *logikai hálózatoknak* nevezik.

Hogyan modellezhetjük mindezt algebrailag? Egy-egy integrált áramkör függvényként viselkedik, ami az összes lehetséges jelek A halmazán van értelmezve, annyi változós, ahány bemenet van, a függvény értéke pedig a kimeneten kapott jel. Az egymáshoz való forrasztások azt jelentik, hogy ezeket a függvényeket korlátlanul szabad egymásba helyettesíteni.

8.3.1. Definíció. Legyen f egy n-változós, $g_1, \dots, g_n$ pedig n darab k-változós függvény egy A halmazon. Ekkor a k-változós $f \circ (g_1, \dots, g_n)$ függvényt az

$$\big(f \circ (g_1, \dots, g_n)\big)(x_1, \dots, x_k) = f\big(g_1(x_1, \dots, x_k), \dots, g_n(x_1, \dots, x_k)\big)$$

képlettel definiáljuk, és az $f, g_1, \dots, g_n$ függvények *kompozíciójának* nevezzük.

Természetesen ez a fogalom a korábban tanult szokásos függvény-kompozíció általánosítása (azt az $n = k = 1$ speciális esetben kapjuk). A $\circ$ jelet sokszor elhagyjuk, és csak az $f(g_1, \dots, g_n)$ *összetett függvényről* beszélünk.

Az Olvasó joggal kérdezheti, hogy mi lesz az olyasfajta helyettesítésekkel, mint például $f(g_1(y, y), g_2(z), g_3(z, x))$. Ezeket is kompozíciónak érezzük, ugyanakkor a fenti definícióból kimaradtak. A megoldás nem az, hogy a fenti definíciót elbonyolítjuk, hanem hogy az ilyesfajta függvényeket egynél több lépésben, több kompozíció eredményeként állítjuk elő. Ebben az úgynevezett *projekciók* segítenek (ezek ugyanazok a függvények, mint amiket a direkt szorzatnál már megismertünk, csak most az A algebra véges változós függvényeinek tekintjük őket). Az eljárást csak egy gyakorlatban mutatjuk be.

8.3.2. Definíció. Az A halmazon értelmezett n-változós

$$\pi_i^n : (a_1, \dots, a_n) \mapsto a_i$$

függvényt (az n-változós, i-edik) *projekciónak* nevezzük.

8.3.3. Gyakorlat. Igazoljuk, hogy az $f\big(g_1(x_2, x_2), g_2(x_3), g_3(x_3, x_1)\big)$ összetett függvény megkapható az f, g_1, g_2, g_3 függvényekből és alkalmas projekciókból a 8.3.1. Definícióbeli értelemben vett kompozíció többszöri alkalmazásával. Mutassuk meg, hogy a projekciókkal való kompozíció segítségével egy függvény változói cserélgethetők, azonosíthatók, és olyan extra változók is bevezethetők, amelyektől a függvény nem is függ.

A fenti számítógépes példában arra van szükség, hogy az összes olyan kompozíciót áttekintsük, amely a megadott függvények segítségével felírható. Az így kapott függvények halmazát klónnak nevezzük. Az eredetileg megadott függvényeket pedig egy A algebra alapműveleteinek tekinthetjük.

8.3.4. Definíció. Az A halmazon értelmezett véges változós függvények egy halmazát *klónnak* nevezzük, ha zárt a kompozícióra, és tartalmazza az összes π_i^n projekciót.

8.3.5. Definíció. Legyen A algebra. Azokat a véges változós függvényeket, amelyek az A alapműveleteiből és a projekciókból a kompozíció segítségével (több lépésben) megkaphatók, az A algebra *kifejezésfüggvényeinek* nevezzük, halmazukat $\mathrm{Clo}(A)$-val jelöljük (ez az A algebra klónja). Az n-változós kifejezésfüggvények halmazát $\mathrm{Clo}_n(A)$ jelöli.

Most végre kiderül, miért is olyan fontosak a lineáris kombinációk a lineáris algebrai vizsgálatokban.

8.3.6. Gyakorlat. Mutassuk meg, hogy egy V vektortér kifejezésfüggvényei pontosan az

$$f(x_1, \ldots, x_n) = \lambda_1 x_1 + \ldots + \lambda_n x_n$$

alakú függvények, ahol $\lambda_1, \ldots, \lambda_n$ rögzített skalárok. Hogyan általánosítható ez az eredmény modulusokra?

Csoportok esetében a szorzás és az inverzképzés műveleteit kell egymásba helyettesítgetni. Az asszociativitás miatt ekkor pontosan az olyasféle függvényeket kapjuk, mint

$$f(x, y) = x^{-2}y^6xy^2x^{-1}y^2xy^{-3}\,.$$

Az ilyen „szavakkal” két helyen is találkoztunk a csoportelméletben: a generált részcsoport leírásakor, és a szabad csoport elemeinek vizsgálatakor.

8.3.7. Tétel. *Legyen A algebra és $a_1, \ldots, a_n \in A$. Ekkor*

$$\langle a_1, \ldots, a_n\rangle = \{t(a_1, \ldots, a_n) \,:\, t \in \mathrm{Clo}_n(A)\}\,.$$

Vagyis a generált részalgebra elemeit úgy kapjuk, hogy a generátorokra az összes lehetséges módon a kifejezésfüggvényeket alkalmazzuk.

Bizonyítás. Jelölje C a tételben szereplő halmazt. A $C \subseteq \langle a_1, \ldots, a_n\rangle$ tartalmazáshoz a következő állítást kell megmutatni, és a $B = \langle a_1, \ldots, a_n\rangle$ részalgebrára alkalmazni.

8.3.8. Lemma. *Tegyük föl, hogy B részalgebrája az A algebrának. Ekkor B zárt az A kifejezésfüggvényeire, vagyis ha $t \in \mathrm{Clo}_n(A)$ és $b_1, \ldots, b_n \in B$, akkor $t(b_1, \ldots, b_n) \in B$.*

Bizonyítás. A t kifejezésfüggvény a kompozíció ismételt alkalmazásával keletkezik alapműveletekből és projekciókból. A felhasznált kompozíciók száma (vagyis *t komplexitása*) szerinti indukcióval bizonyítunk. A B részalgebra nyilván zárt az A alapműveleteire és a projekciókra is. Tegyük föl, hogy B zárt minden t-nél kevésbé komplex kifejezésfüggvényre. Mivel t kifejezésfüggvény, $t = f \circ (g_1, \dots, g_k)$, ahol f és g_i a t-nél kevésbé komplex kifejezésfüggvények, és ezért B ezekre zárt. Így $c_i = g_i(b_1, \dots, b_n) \in B$ minden i-re. De akkor $t(b_1, \dots, b_n) = f(c_1, \dots, c_k) \in B$. □

Az $\langle a_1, \dots, a_n \rangle \subseteq C$ tartalmazáshoz azt kell megmutatni, hogy C egy olyan részalgebra, amely az a_i elemeket tartalmazza (hiszen akkor a legszűkebb ilyen részalgebra, vagyis $\langle a_1, \dots, a_n \rangle$, része lesz C-nek). A π_i^n projekció kifejezésfüggvény, és $a_1, \dots, a_n$-re alkalmazva a_i-t ad eredményül, vagyis $a_i \in C$. Tegyük föl, hogy f alapművelete A-nak, amely k-változós, és $c_1, \dots, c_k \in C$. Ekkor

$$c_i = t_i(a_1, \dots, a_n)$$

alkalmas t_i kifejezésfüggvényekre. Legyen $t = f \circ (t_1, \dots, t_n)$, ez is kifejezésfüggvény, és így

$$f(c_1, \dots, c_k) = t(a_1, \dots, a_n) \in C\,.$$

Ezért C tényleg részalgebra. □

Az iménti bizonyítás végén csak olyan kompozíciókat használtunk, ahol a külső függvény alapművelete az A algebrának. A következő gyakorlat állítása megmagyarázza, hogy ez miért történhetett így.

8.3.9. Gyakorlat. Amikor az A algebra klónját generáljuk, akkor az A alapműveleteiből és a projekciókból indulunk ki, majd az olyan $t \circ (g_1, \dots, g_k)$ kompozíciókat hajtjuk végre (sokszor egymás után), ahol t-t és a g_i-ket már korábban megkaptuk ilyen módon. Bizonyítsuk be, hogy ha csak olyan kompozíciókat engedünk meg, ahol t az algebra alapművelete, akkor is ugyanazokat a függvényeket (vagyis A összes kifejezésfüggvényét) kapjuk.

A 8.3.8. Lemma szerint A minden részalgebrája zárt A kifejezésfüggvényeire. Megmutatjuk, hogy a kifejezésfüggvények az A kompatibilis relációit (például kongruenciáit) is tartják. Ehhez definiálnunk kell, mit értünk általában kompatibilis reláció alatt. A 8.2.28. Definícióban láttuk, hogy egy kétváltozós reláció párok egy halmaza.

8.3.10. Gyakorlat. Igazoljuk, hogy az A algebra θ partíciója akkor és csak akkor kongruencia, ha az

$$\{(x, y) \in A \times A \,:\, x \equiv y \ (\theta)\}$$

halmaz részalgebrája az $A \times A$ direkt szorzatnak.

8.3.11. Gyakorlat. Mutassuk meg, hogy egy $\varphi : A \to B$ függvény akkor és csak akkor homomorfizmus, ha az

$$\big\{\big(x, \varphi(x)\big) \,:\, x \in A\big\}$$

halmaz (a *φ gráfja*) részalgebrája az $A \times B$ direkt szorzatnak.

Másik igen fontos példa kompatibilis relációra hálókban a rendezés. Ha L háló, akkor a $\leq$ relációt a következő halmaznak is tekinthetjük:

$$R = \{(a, b) \in L^2 \,:\, a \leq b\}\,.$$

Nevezzük az $f : L^n \to L$ függvényt *rendezéstartónak*, vagy *monotonnak*, ha

$$x_1 \leq y_1\,,\ \ldots\,,\ x_n \leq y_n \implies f(x_1, \ldots, x_n) \leq f(y_1, \ldots, y_n)$$

(egyváltozós függvény esetében ez a fogalom már szerepelt a 8.2.12. Definícióban). Az előző két gyakorlat megoldása alapján láthatjuk, hogy a monotonitás annak az átfogalmazása, hogy R részalgebra $A \times A$-ban „az f-re nézve".

8.3.12. Definíció. Legyen f egy n-változós függvény az A halmazon és $R \subseteq A^k$. Jelölje (A, f) azt az algebrát az A halmazon, amelynek az egyetlen művelete az f. Azt mondjuk, hogy f *megőrzi* vagy *tartja* az R részhalmazt (relációt), vagy hogy R *kompatibilis* az f függvénnyel, ha R részalgebrája az $(A, f)^k$ direkt hatványnak (amelyen az f-et komponensenként értelmeztük).

Tehát f akkor és csak akkor monoton, ha a $\leq$ rendezés f-fel kompatibilis (vagyis ha f tartja a rendezést). Mivel az L háló két alapművelete (az egyesítés és a metszet) monoton függvények (8.1.13. Gyakorlat), az R részalgebrája az $L \times L$ direkt szorzatnak.

8.3.13. Definíció. Az A^n direkt hatvány részalgebráit az A algebra n-változós *kompatibilis relációinak* nevezzük.

8.3.14. Gyakorlat. Mutassuk meg, hogy ha R az A^n direkt hatvány egy részalgebrája, akkor R kompatibilis A kifejezésfüggvényeivel.

A klónok (8.3.4. Definíció) elmélete központi helyet foglal el az általános algebrák vizsgálatában. Általában ugyanis igen nehéz kérdés annak eldöntése, hogy egy megadott függvényt elő lehet-e állítani más megadott függvények kompozíciójaként. Az elmélet alapjait csak egy példán (és néhány feladatban) illusztráljuk.

Legyen $A = \{0, 1\}$ (képzelhetjük azt, hogy a 0 elem a „hamis", az 1 elem az "igaz" szót rövidíti, de azt is, hogy a 0 az alacsony-feszültségű, az 1 pedig a magas feszültségű jel). Háromféle alkatrészt (függvényt) definiálunk.

Az „és-kapu" kétváltozós, és akkor ad „igaz" eredményt, ha mindkét bemenete „igaz" (érdemes ezt összevetni az A.1. Függelék logikai részében a logikai műveletekről írottakkal). Vagyis $e(x, y) = 1$ akkor és csak akkor, ha $x = y = 1$. A kétváltozós „vagy-kapu" eredménye akkor „hamis", ha mindkét változó értéke „hamis". Tehát $v(x, y) = 0$ akkor és csak akkor, ha $x = y = 0$. Végül az egyváltozós „nem-kapu" igazból hamisat, hamisból igazat csinál, azaz $\neg(0) = 1$ és $\neg(1) = 0$.

8.3.15. Feladat. Mutassuk meg, hogy a $\{0, 1\}$ halmazon az e, v és $\neg$ függvényekkel minden véges változós függvény kifejezhető.

Az előző feladat azt jelenti, hogy minden, akármilyen bonyolult logikai állítást el tudunk mondani az „és", a „vagy" és a „nem" segítségével. Például a „ha x, akkor y" függvény a $v(\neg(x), y)$. A logikusok ezt úgy fejezik ki, hogy „az ítéletkalkulus teljes".

Ugyanakkor az e és a v függvények segítségével az n nem fejezhető ki. Ennek belátásához vegyük észre, hogy ha a $\{0, 1\}$ halmazt a $0 < 1$ rendezéssel hálónak képzeljük, akkor $e(x, y) = x \wedge y$ és $v(x, y) = x \vee y$. Az imént láttuk, hogy ennek a hálónak mindegyik kifejezésfüggvénye monoton. Mivel a $\neg$ függvény nem monoton, tényleg nem állítható elő a kívánt kompozícióként.

Ez a példa mutatja, hogy a klónok leírásában alapvető szerepet kell, hogy játsszanak a kompatibilis relációk. Ez így is van: az összes (nemcsak kétváltozós) kompatibilis relációk egyértelműen meghatározzák az összes lehetséges kompozíciók halmazát, vagyis a klón elemeit (8.7.11. Feladat).

Ha A kételemű (ez logikában a legfontosabb eset), akkor az összes lehetséges klónok halmaza viszonylag áttekinthető, Emil Post munkássága nyomán (ezek a klónok megszámlálható halmazt alkotnak, és a tartalmazásra vett hálójukat is jól le lehet rajzolni). Legalább háromelemű halmazon viszont már az olyan klónok halmaza is áttekinthetetlen, amelyek az összes konstansot tartalmazzák (a számuk annyi, mint a valós számoké).

8.3.16. Feladat. Mutassuk meg, hogy az $L = \{0, 1\}$ háló kifejezésfüggvényei pontosan a monoton függvények.

Azt gondolhatnánk, hogy a gyűrűk kifejezésfüggvényei a polinomokhoz kapcsolódnak, hiszen itt az összeadást, kivonást, szorzást kell egymásba helyettesítgetni. Azonban több okból is óvatosnak kell lennünk.

Először is, az $\mathbb{R}$ gyűrűnek $x \mapsto x + 1$ nem kifejezésfüggvénye. Az alapműveletek az $x + y$, a $-x$ és az xy. Akárhogyan is helyettesítjük ezeket egymásba, konstans tag nem keletkezik. Ez magyarázza, hogy az 5.1.2. Állításban, ahol leírtuk kommutatív, egységelemes gyűrűben a generált részgyűrű elemeit, csupa konstans tag nélküli polinom szerepel.

Ahhoz, hogy a konstans tagok megjelenjenek, az egységelemet is be kell venni, mint konstans egyváltozós (vagy nullváltozós) művelet eredményét. Ekkor azonban még mindig nem lesz kifejezésfüggvény például az $x \mapsto \sqrt{2}+\pi x+x^2$, hanem csak az egész együtthatós polinomokból származó polinomfüggvényeket kapjuk meg. Ahhoz, hogy az $\mathbb{R}[x_1, \ldots, x_n]$ elemeihez tartozó polinomfüggvények kijöjjenek, az $\mathbb{R}$ elemeit is föl kell használnunk.

8.3.17. Definíció. Legyen A algebra. Azokat a véges változós függvényeket, amelyek az A alapműveleteiből, a projekciókból és a konstans függvényekből a kompozíció segítségével megkaphatók, az A algebra *polinomfüggvényeinek* nevezzük, halmazukat $\mathrm{Pol}(A)$-val jelöljük. Az n-változós polinomfüggvények halmazát $\mathrm{Pol}_n(A)$ jelöli.

Ha tehát T test, akkor a T-nek az n-változós polinomfüggvényei (az előző definíció értelmében) pontosan azok, amiket régebben is polinomfüggvénynek neveztünk (vö. 2.6.9. Gyakorlat). Azt is könnyű megmutatni, hogy az A algebra polinomfüggvényei pontosan a

$$p(x_1, \ldots, x_n) = t(x_1, \ldots, x_n, a_1, \ldots, a_k)$$

alakú függvények, ahol t kifejezésfüggvénye A-nak, $a_1, \ldots, a_k$ pedig A rögzített elemei.

8.3.18. Gyakorlat. Mutassuk meg, hogy egy V vektortér polinomfüggvényei pontosan az

$$f(x_1, \ldots, x_n) = \lambda_1 x_1 + \ldots + \lambda_n x_n + v$$

alakú függvények, ahol $\lambda_1, \ldots, \lambda_n$ rögzített skalárok és $v \in V$ rögzített elem. Hogyan általánosítható ez az eredmény modulusokra?

Ahogy a kifejezésfüggvények a részalgebrákkal, úgy a polinomfüggvények a kongruenciákkal állnak szoros kapcsolatban.

8.3.19. Gyakorlat. Mutassuk meg, hogy az A algebra kongruenciáit (mint $A \times A$ részalgebráit, lásd 8.3.10. Gyakorlat) az A polinomfüggvényei is megőrzik. Megfordítva, igazoljuk, hogy ha θ ekvivalencia-reláció az A-n, amelyet az egyváltozós polinomfüggvények megőriznek, akkor θ kongruencia. Hogyan segít ez az észrevétel a 8.2.23. Tétel pontosabb bizonyításában?

A polinomok és a polinomfüggvények között igen fontos különbséget tettünk annak idején: a polinom maga nem függvény, hanem egy formális képlet. Hasonló kapcsolatban állnak az úgynevezett formális kifejezések is a kifejezésfüggvényekkel. Ezekre van szükségünk ahhoz, hogy például azonosságokról beszélhessünk. A formális kifejezéseket úgy kell elképzelni, hogy a műveleti jeleket egymásba helyettesítgetjük (természetesen ehhez előbb egy típust rögzítenünk kell). Például csoportok esetében az

$$(xy)z\,, \quad x(yz) \quad \text{és} \quad [(xy)^{-1}(x^{-1})](xz)$$

képletek formális kifejezéseket adnak meg. Tehát semmiféle átalakítást, csoportelméleti azonosságot nem használhatunk föl e kifejezések egyszerűsítésére, ezek nemcsak csoportokban, hanem minden olyan algebrában működni fognak, amelyben van egy kétváltozós és egy egyváltozós művelet. Sőt azt, hogy egy ilyen algebra csoport, pontosan formális kifejezések közötti azonosságokkal írhatjuk le (ilyen például az asszociativitás).

A formális kifejezések konstrukcióját csak igen vázlatosan ismertetjük. A lényeg az, hogy a fenti kifejezéseket minden kombinációban elkészítsük. A 8.3.9. Gyakorlat szellemében „kívülre” mindig alapműveletet fogunk írni. Azt képzeljük tehát, hogy jeleket írunk egy papírra, a következő szabályok szerint. Adott egy τ típus és egy X halmaz, ennek elemeit *változóknak* (vagy határozatlanoknak) nevezzük. Ezután indukcióval építkezünk. Legyen $F_0 = X$. Ha az F_k már megvan, akkor elkészítjük az összes olyan

$$f(g_1, \ldots, g_n)$$

formális jelsorozatot, ahol f egy műveleti jel a τ típusban, n ennek a változószáma, és $g_1, \ldots, g_n$ az F_k elemei. Álljon F_{k+1} az F_k elemeiből és az összes így képzett kifejezésből. Végül legyen $F^\tau(X)$ az összes így kapott kifejezések összessége, vagyis

$$F^\tau(X) = \bigcup_{k=0}^{\infty} F_k\,.$$

Felhívjuk a figyelmet arra, hogy F_{k+1}-be bevettük az F_k elemeit is, vagyis a most definiált halmaz a növő $F_0 \subseteq F_1 \subseteq \ldots$ lánc uniója. Ezért az $F^\tau(X)$ halmaz valójában egy τ típusú algebra lesz. Ehhez azt kell megmutatni, hogy ha f egy n-változós műveleti jel és $g_1, \ldots, g_n \in F^\tau(X)$, akkor az $f(g_1, \ldots, g_n)$ jelsorozatot is bevettük $F^\tau(X)$-be. Mivel mindegyik g_i eleme valamelyik F_{k_i}-nek, ezért ha k a k_i számok legnagyobbika, akkor $f(g_1, \ldots, g_n) \in F_{k+1}$. Érdemes azt is észrevenni, hogy az X halmaz generálja az $F^\tau(X)$ algebrát.

8.3.20. Definíció. Az $F^\tau(X)$ algebra elemeit τ típusú, X változójú *(formális) kifejezéseknek* nevezzük.

A magyar nyelvben a „kifejezés” szónak köznapi, az általános algebrák elméletétől független jelentése is van, amit a matematikában (sőt nyelvtani értelemben is) gyakran használunk. Ezért amikor a fenti értelemben vett kifejezésekről beszélünk, igyekszünk majd minél többször használni a „formális” jelzőt. Angolul ez nem okoz problémát: a fenti fogalom megfelelője a *term* szó, a kifejezésfüggvények neve term function. A köznapi értelemben vett kifejezés szónak inkább az „expression” a megfelelője. Éppen ezért az általános algebrák elméletében magyar nyelven is sokszor használják a „term” és a „term-függvény” kifejezéseket.

A formális kifejezések legfontosabb tulajdonsága, hogy tetszőleges τ típusú A algebra elemeit be lehet helyettesíteni. Egyszerűen azt kell csinálni, hogy mindegyik változó helyébe beírjuk az A egy elemét, és a műveletek eredményét kiszámoljuk. Az eljárást bemutatjuk egy fokkal pontosabban is. A jobb érthetőség kedvéért legyen $X = \{x_1, \ldots, x_n\}$, és a t kifejezésnek kiírjuk a változóit is, vagyis t helyett $t(x_1, \ldots, x_n)$-et írunk. Rendeljük hozzá mindegyik x_i-hez az A algebra egy a_i elemét. Ekkor tetszőleges $t(x_1, \ldots, x_n)$ kifejezéshez is hozzárendelhetjük az A algebrának egy $t^A(a_1, \ldots, a_n)$ elemét a t komplexitása szerinti indukcióval, a következőképpen. Ha már a $g_i(x_1, \ldots, x_n)$ kifejezésekbe sikeresen behelyettesítettünk, azaz megkaptuk a $g_i^A(a_1, \ldots, a_n)$ elemeket, akkor $t = f(g_1, \ldots, g_n)$ esetén legyen

$$t^A(a_1, \ldots, a_n) = f^A\big(g_1^A(a_1, \ldots, a_n), \ldots, g_n^A(a_1, \ldots, a_n)\big)\,.$$

Ez a képlet azt is mutatja, hogy *a behelyettesítés homomorfizmus* $F^\tau(x_1, \ldots, x_n)$-ből A-ba (hiszen azt fejezi ki, hogy ha először behelyettesítünk, majd az eredményre alkalmazzuk az f^A műveletet, az ugyanaz, mint ha először az f^F műveletet alkalmazzuk, majd a kapott formális kifejezésbe helyettesítünk be). Általános X esetén tehát a következőt kapjuk.

8.3.21. Állítás. *Legyen X változók egy halmaza, A egy τ típusú algebra, és X minden x eleméhez rendeljünk hozzá egy $\varphi(x) \in A$ elemet. Ekkor egyértelműen létezik egy*

$$\varphi^* : F^\tau(X) \to A$$

homomorfizmus, amely φ-nek kiterjesztése (vagyis $\varphi^*(x) = \varphi(x)$ teljesül minden $x \in X$ esetén). □

8.3.22. Definíció. Ha $X = \{x_1, x_2, \ldots\}$ változók egy halmaza, A egy τ típusú algebra, $a_1, a_2, \ldots$ az A elemei és $t = t(x_1, x_2, \ldots)$ egy kifejezés, akkor

$$t^A(a_1, a_2, \ldots) \in A$$

jelöli azt az értéket, amelyet az $x_i \mapsto a_i$ helyettesítéssel t-ből kapunk (vagyis az előző állításban megadott $\varphi^*(t) \in A$ elemet).

Így ha $t(x_1, \ldots, x_n)$ egy formális kifejezés, akkor t^A egy n-változós függvény az A halmazon (amely az $a_1, \ldots, a_n$ elemekhez az imént definiált $t^A(a_1, \ldots, a_n) \in A$ elemet rendeli). A 8.3.9. Gyakorlatból világos, hogy az n-változós kifejezésekhez a most leírt módon rendelt függvények pontosan az A algebra n-változós kifejezésfüggvényei lesznek.

8.3.23. Gyakorlat. Mutassuk meg, hogy az $A \times B$ direkt szorzat kifejezésfüggvényeit úgy kaphatjuk meg, hogy veszünk egy tetszőleges $t(x_1, \ldots, x_n)$ kifejezést, és az első komponensben a t^A, a második komponensben a t^B függvényként operálunk. Igazoljuk azt is, hogy ha $\varphi : A \to B$ homomorfizmus, akkor tetszőleges $t(x_1, \ldots, x_n)$ kifejezésre és $a_1, \ldots, a_n \in A$ elemekre

$$\varphi\big(t^A(a_1, \ldots, a_n)\big) = t^B\big(\varphi(a_1), \ldots, \varphi(a_n)\big)\,,$$

vagyis a homomorfizmusok a kifejezésfüggvényeket is tartják.

Lehetetlen nem észrevenni a 8.3.21. Állítás hasonlóságát azzal, ahogy a szabad csoportot definiáltuk (4.9.1. Definíció).

8.3.24. Definíció. Legyen F egy τ típusú algebra, és X generátorrendszere F-nek. Azt mondjuk, hogy az X *szabadon generálja* F-et τ típusú algebrák egy $\mathcal{K}$ osztálya fölött (más szóval X *szabad* generátorrendszer), ha bárhogyan is veszünk egy $A \in \mathcal{K}$ algebrát és egy $\varphi : X \to A$ tetszőleges függvényt, ez kiterjeszthető egy $\varphi^* : F \to A$ homomorfizmussá. Az F algebra *szabad* a $\mathcal{K}$ fölött, ha van szabad generátorrendszere.

Ezek szerint tehát a szabad csoportok szabadok az összes csoportból álló osztály fölött, a 8.3.21. Állítás pedig azt fejezi ki, hogy a τ típusú kifejezések algebrája szabad az összes τ típusú algebrák osztálya fölött. Vektortérben, modulusban a szabad generátorrendszerek pontosan a bázisok (7.2.15. Tétel).

8.3.25. Gyakorlat. Tegyük föl, hogy F és G is az X által szabadon generált algebrák a $\mathcal{K}$ osztály fölött, és $F, G \in \mathcal{K}$. Mutassuk meg, hogy ekkor F és G izomorfak (vagyis a szabad algebra egyértelműen meghatározott).

Kérdés, hogy vannak-e szabad gyűrűk, szabad hálók, és így tovább. Természetesen a hálók osztálya fölött szabad a hálók típusának megfelelő $F^\tau(X)$ algebra, de ez nem lesz háló. Olyan $\mathcal{K}$ fölött szabad algebrákat keresünk, amelyek maguk is a $\mathcal{K}$ osztály elemei. Birkhoff tétele egészen általános feltételek mellett lehetővé teszi, hogy ilyen szabad algebrát találjunk.

8.3.26. Tétel [Birkhoff tétele a szabad algebrákról]. *Tegyük föl, hogy $\mathcal{K}$ azonos típusú algebrák egy osztálya, amely tartalmaz egy legalább kételemű algebrát. Ekkor minden X halmazhoz létezik egy olyan X által generált, $\mathcal{K}$ fölött szabad algebra, amely izomorf egy $\mathcal{K}$ elemeiből készített direkt szorzat egy részalgebrájával.*

A tételben $\mathcal{K}$ algebrák egy *osztályáról* van szó. Olyasmire kell gondolni, mint az összes Abel-csoportok, vagy testek osztálya. Az A.1. Függelékben vázoltuk, hogy (halmazelméleti jellegű nehézségek miatt) miért nem a halmaz szót használjuk.

Az Olvasó a most következő bizonyításban nyugodtan úgy képzelheti, hogy algebrák egy $\mathcal{K}$ halmazáról van szó. A bizonyítás így nem lesz precíz, de halmazelméleti problémákkal nem akarunk foglalkozni. Aki ismeri a halmazelmélet alapjait, és az osztály pontos fogalmát, az könnyen precízzé teheti halmazelméleti értelemben is a bizonyítást. Csak azt kell észrevennie, hogy egy X halmazzal generálható τ típusú algebrák izomorfia erejéig csak „halmaznyi sokan" lehetnek.

Bizonyítás. A könnyebb áttekinthetőség végett képzeljük először azt, hogy $\mathcal{K}$ véges sok véges algebrából áll, és X is véges halmaz. Tekintsük az összes olyan $\varphi : X \to A$ függvényt, ahol $A \in \mathcal{K}$. Ez csak véges sok lehetséges függvény, számozzuk be őket 1-től n-ig. Ugyanígy számozzuk be a $\mathcal{K}$ elemeit is: ha a $\varphi_i : X \to A$, akkor ezt az A algebrát A_i-vel jelöljük. Tehát ugyanaz az $A \in \mathcal{K}$ algebra sokféle számot kap: $A_i = A$ minden olyan esetben, amikor φ_i az A-ba képez. Legyen

$$B = A_1 \times \ldots \times A_n\,.$$

Ebben kijelölünk minden $x \in X$ esetén egy $\psi(x)$ elemet: $\psi(x) = \big(\varphi_1(x), \ldots, \varphi_n(x)\big)$.

A $\psi(x)$ elemek páronként különbözők. Valóban, a feltevésünk szerint a $\mathcal{K}$ osztályban van egy legalább kételemű A algebra. Ha $x \neq y \in X$, akkor van egy olyan $\varphi : X \to A$ függvény, amelyre $\varphi(x) \neq \varphi(y)$. Ha ezt a φ függvényt éppen i-ediknek számoztuk, vagyis $\varphi = \varphi_i$ és ennek megfelelően $A_i = A$, akkor a $\psi(x)$ elem i-edik komponense $\varphi_i(x)$, a $\psi(y)$ elem i-edik komponense pedig $\varphi_i(y)$. Ezek különbözők, tehát $\psi(x) \neq \psi(y)$.

Legyen $X' \subseteq B$ a $\psi(x)$ alakú elemek halmaza, ahol $x \in X$. Az imént igazoltak szerint ψ bijekció X és X' között. Jelölje F az X' által generált részalgebrát B-ben. Megmutatjuk, hogy F-nek X' szabad generátorrendszere $\mathcal{K}$ fölött.

Valóban, tegyük föl, hogy adott egy tetszőleges $\varphi' : X' \to A$ függvény, ahol $A \in \mathcal{K}$. Legyen $\varphi = \varphi' \circ \psi$, ekkor φ egy $X \to A$ függvény, amelyre $\varphi(x) = \varphi'\big(\psi(x)\big)$ minden $x \in X$-re. Jelölje i azt az indexet, amelyre $\varphi = \varphi_i$, és legyen π_i a B direkt szorzat i-edik projekciója (amely B minden eleméhez annak az i-edik komponensét rendeli). Megmutatjuk, hogy π_i (pontosabban az F-re vett megszorítása) megfelelő lesz, vagyis egy olyan $F \to A = A_i$ homomorfizmus, amely φ'-nek kiterjesztése. Az, hogy homomorfizmusról van szó, nyilvánvaló. Ha $\psi(x) \in X'$, akkor $\varphi'\big(\psi(x)\big) = \varphi(x) = \varphi_i(x)$. Másfelől $\psi(x) = \big(\varphi_1(x), \ldots, \varphi_n(x)\big)$, és ehhez az i-edik projekció szintén $\varphi_i(x)$-et rendeli. Ezzel beláttuk, hogy X' tényleg szabadon generálja az F-et $\mathcal{K}$ fölött.

A bizonyítást azzal fejezhetjük be, hogy X-et sorra kicseréljük ψ mentén az X' elemeivel (ugyanazon a módon ahogy a 6.4.3. Tételt követő megjegyzésben is eljártunk). Így egy

F-fel izomorf algebrát kapunk, amit már maga az X (és nem a vele bijekcióban álló X' halmaz) generál. Ennek részleteivel nem fárasztjuk az Olvasót.

Ha X és $\mathcal{K}$ végtelen is lehet, a bizonyítás ugyanaz, mint fent, még egyszerűbb is (bár talán nehezebben követhető és jelölhető), mert elmarad a $\varphi : X \to A$ homomorfizmusok „beszámozása". Egyszerűen ezeknek a homomorfizmusoknak a halmazát vesszük indexhalmaznak, és így készítünk el egy nagy B direkt szorzatot. A $\psi : X \to B$ leképezésnél a $\psi(x)$ elem φ-hez tartozó komponense $\varphi(x)$ lesz. Ismét a projekciók biztosítják, hogy a $\psi(X) = X' \to A \in \mathcal{K}$ leképezések kiterjeszthetők legyenek az $\psi(X)$ által generált F algebrára, amely ezért szabad. A részletek kidolgozását az Olvasóra hagyjuk. □

8.3.27. Következmény. *Ha X véges halmaz, és $\mathcal{K}$ véges sok véges algebrából álló osztály, akkor az előző tételből kapott, $\mathcal{K}$ fölött X által generált szabad algebra is véges.*

Gyakorlatok, feladatok

8.3.28. Gyakorlat. Legyen az A algebra alaphalmaza $\{0, 1\}$, az egyetlen művelete pedig a háromváltozós $x +_2 y +_2 z$. Határozzuk meg az n-változós kifejezésfüggvények, illetve polinomfüggvények számát.

8.3.29. Feladat. Hány eleme van az egy, illetve a két elemmel generált szabad hálónak?

8.3.30. Feladat. Határozzuk meg a kommutatív gyűrűk osztályában a szabad algebrákat (vö. 5.1.2. Állítás, 5.1.25. Gyakorlat). Tegyük meg ugyanezt az egységelemes kommutatív gyűrűk osztályában is (ahol az egységelemet művelettel jelöljük ki).

8.3.31. Feladat. Tetszőleges véges halmazon adjunk meg egy kétváltozós műveletet úgy, hogy a kapott algebrában minden n-változós függvény kifejezésfüggvény legyen (minden $n \geq 1$ esetén).

Az előző feladatból láthatjuk, hogy egy véges halmazon minden véges változós függvény felírható kétváltozós függvények kompozíciójaként (ez *Sierpiński* tétele.)

Számos további, klónokkal, kifejezésfüggvényekkel és polinomfüggvényekkel kapcsolatos gyakorlat és feladat szerepel a Czédli–Szendrei–Szendrei-féle [**6**] feladatgyűjtemény X. Fejezetének első szakaszában. Felhívjuk a figyelmet arra, hogy a szerzők a polinomfüggvényt algebrai függvénynek nevezik.

8.4. Varietások

A varietás algebrák egy olyan osztálya, amely azonosságokkal definiálható (mint például a csoportok, vagy a kommutatív gyűrűk). Ezek Birkhoff tétele szerint pontosan a részalgebra, faktoralgebra és direkt szorzat képzésére zárt osztályok. Ezután Birkhoff harmadik tételét bizonyítjuk, amely lehetővé teszi, hogy egy tetszőleges algebrát nála „egyszerűbb" algebrákból fölépíthessünk direkt szorzat részalgebrájaként.

Az asszociativitást kifejező $(xy)z = x(yz)$ azonosságban valójában két formális kifejezés szerepel, amelyeket a csoportoknak megfelelő típusban írtunk föl. Emlékeztetjük az Olvasót, hogy ha $a_1, \ldots, a_n$ elemek egy A algebrában, akkor ezeket minden $t(x_1, \ldots, x_n)$ kifejezésbe behelyettesíthetjük, és így egy $t^A(a_1, \ldots, a_n) \in A$ elemet kapunk (lásd a 8.3.22. Definíciót, és az azt megelőző megjegyzéseket).

8.4.1. Definíció. Legyen $t_1, t_2 \in F^\tau(x_1, \ldots, x_n)$ két τ típusú kifejezés, ahol n alkalmas egész szám. Azt mondjuk, hogy az n-változós $t_1 \approx t_2$ *azonosság* teljesül a τ típusú A algebrában, ha tetszőleges $a_1, \ldots, a_n \in A$ elemekre

$$t_1^A(a_1, \ldots, a_n) = t_2^A(a_1, \ldots, a_n)\,.$$

Ezt $A \models t_1 \approx t_2$ (vagy egyszerűen $A \models t_1 = t_2$) jelöli.

Az előző definícióban nem mondtuk meg, mi a $t_1 \approx t_2$ azonosság, hanem csak azt, hogy mikor teljesül. Ez hasonlít a komplex számok nem precíz bevezetéséhez, amikor az $a+bi$ számot nem definiáltuk, csak megmondtuk, hogyan kell vele számolni. Ahogy az 1.6. Szakaszban az $a + bi$ komplex számot az (a, b) rendezett párként definiáltuk, úgy most is megtehetjük, hogy a $t_1 \approx t_2$ azonosságot a (t_1, t_2) rendezett párnak tekintjük.

Az azonosság fogalmát véges sok változó segítségével definiáltuk. Ez azért nem jelent megszorítást, mert bármilyen halmaz is az X, az $F^\tau(X)$ mindegyik elemében az X-nek nyilván csak véges sok eleme szerepelhet.

A gyakorlatban a $\approx$ jel helyett sokszor egyszerűen csak egyenlőséget írnak (az asszociativitást például mi sem $(xy)z \approx x(yz)$ alakban írtuk föl eddig). Ez persze elvileg helytelen, mert a $t_1 = t_2$, ha pontosak akarunk lenni, azt jelenti, hogy t_1 és t_2 ugyanaz a formális kifejezés. Például $(xy)z \neq x(yz)$, hiszen ez a két képlet, mint *formális kifejezés*, nem ugyanaz. Ugyanakkor a jelölés egyszerűbbé válik, és ha a $t_1 = t_2$ egyenlőséget azonosságnak értjük, azt úgyis mindig megmondjuk.

8.4.2. Definíció. Azonos típusú algebrák egy $\mathcal{V}$ osztályát *varietásnak* nevezzük, ha azonosságokkal definiálható, vagyis ha van azonosságok egy olyan I halmaza, hogy $A \in \mathcal{V}$ akkor és csak akkor, ha $A \models t_1 = t_2$ teljesül minden I-beli $t_1 = t_2$ azonosságra.

8.4.3. Gyakorlat. Mutassuk meg, hogy ha egy algebra teljesít egy azonosságot, akkor azt az azonosságot az algebra részalgebrái és homomorf képei is teljesítik. Igazoljuk, hogy ha A az A_i algebrák direkt szorzata, és mindegyik A_i teljesíti a $t_1 = t_2$ azonosságot, akkor A is teljesíti ezt az azonosságot.

8.4.4. Gyakorlat. Definiálható-e a test fogalma azonosságokkal? És a nullosztómentes gyűrűé? Varietást alkotnak-e a csoportok, ha csak a szorzást tekintjük műveletnek?

8.4.5. Tétel [Birkhoff tétele a varietásokról]. *Azonos típusú algebrák egy osztálya akkor és csak akkor varietás, ha zárt a részalgebra, a homomorf kép és a direkt szorzat képzésére.*

Az, hogy minden varietás zárt a részalgebra, a homomorf kép és a direkt szorzat képzésére, a 8.4.3. Gyakorlat állítása. A megfordítás bizonyítása Birkhoff szabad algebrákról szóló tételére támaszkodik, és mivel egy technikai elemet is tartalmaz (8.4.24. Feladat), ezért a 8.4.25. Feladat megoldásában olvasható. A kulcs a következő észrevétel.

8.4.6. Gyakorlat. Legyen $\mathcal{V}$ egy varietás, és F az $X = \{x_1, \ldots, x_n\}$ által generált szabad algebra $\mathcal{V}$-ben (vö. 8.3.26. Tétel). Mutassuk meg, hogy a $t_1(x_1, \ldots, x_n) \approx t_2(x_1, \ldots, x_n)$ azonosság akkor és csak akkor teljesül a $\mathcal{V}$ minden algebrájában, ha az F algebrában a szabad generátorokra teljesül, vagyis ha $t_1^F(x_1, \ldots, x_n) = t_2^F(x_1, \ldots, x_n)$. Röviden: az azonosságokat elegendő a szabad algebrák szabad generátorain ellenőrizni.

8.4.7. Definíció. Legyen $\mathcal{K}$ azonos típusú algebrák egy osztálya. Ekkor

(1) $\mathsf{H}(\mathcal{K})$ a $\mathcal{K}$-beli algebrák összes homomorf képeiből álló osztály;
(2) $\mathsf{S}(\mathcal{K})$ a $\mathcal{K}$-beli algebrák összes részalgebráiból álló osztály;
(3) $\mathsf{P}(\mathcal{K})$ a $\mathcal{K}$-beli algebrák összes direkt szorzataiból álló osztály.

Az A algebra homomorf képei alatt az olyan B algebrákat értjük, amelyekre létezik $\varphi : A \to B$ *szürjektív* homomorfizmus. Ezért $\mathsf{H}(\mathcal{K})$ valójában az $\mathcal{K}$-beli algebrák faktoralgebráival izomorf algebrákból áll.

8.4.8. Gyakorlat. Legyen $\mathcal{K}$ azonos típusú algebrák tetszőleges osztálya. Igazoljuk az alábbi tartalmazásokat.

(1) $\mathsf{S}\,\mathsf{H}(\mathcal{K}) \subseteq \mathsf{H}\,\mathsf{S}(\mathcal{K})$.
(2) $\mathsf{P}\,\mathsf{H}(\mathcal{K}) \subseteq \mathsf{H}\,\mathsf{P}(\mathcal{K})$.
(3) $\mathsf{P}\,\mathsf{S}(\mathcal{K}) \subseteq \mathsf{S}\,\mathsf{P}(\mathcal{K})$.
(4) $\mathsf{H}\,\mathsf{H}(\mathcal{K}) \subseteq \mathsf{H}(\mathcal{K})$.
(5) $\mathsf{S}\,\mathsf{S}(\mathcal{K}) \subseteq \mathsf{S}(\mathcal{K})$.
(6) $\mathsf{P}\,\mathsf{P}(\mathcal{K}) \subseteq \mathsf{P}(\mathcal{K})$.

Vezessük le ebből, hogy $\mathsf{H}\,\mathsf{S}\,\mathsf{P}(\mathcal{K})$ zárt a részalgebra, a homomorf kép és a direkt szorzat képzésére, vagyis a $\mathcal{K}$ osztályt tartalmazó legszűkebb varietás.

8.4.9. Definíció. Legyen $\mathcal{K}$ azonos típusú algebrák egy osztálya. Ekkor a $\mathsf{H}\,\mathsf{S}\,\mathsf{P}(\mathcal{K})$ varietást a $\mathcal{K}$ által *generált varietásnak* nevezzük, és $\mathsf{V}(\mathcal{K})$-val jelöljük.

8.4.10. Gyakorlat. Mutassuk meg, hogy ha X szabadon generálja az F algebrát a $\mathcal{K}$ osztály fölött, akkor szabadon generálja a $\mathsf{H}\,\mathsf{S}\,\mathsf{P}(\mathcal{K})$ osztály fölött is.

8.4.11. Feladat. Igazoljuk, hogy ha $\mathcal{K}$ véges sok véges algebrából áll, akkor a $\mathsf{V}(\mathcal{K})$ varietásban minden végesen generált algebra véges.

Az algebrista egyik legfontosabb dolga, hogy minél pontosabban leírja általános feltételekkel megadott struktúrák szerkezetét. Eddig már több példát láttunk struktúratételre, például a véges Abel-csoportok (vagy általánosabban a végesen generált, főideálgyűrű fölötti modulusok) alaptételét, vagy a Wedderburn–Artin-tételt. Ezekben az a közös, hogy a vizsgált struktúrát nála egyszerűbb, lehetőleg ismert szerkezetű struktúrákból építjük föl, egy olyan konstrukció segítségével, amelynek a tulajdonságait már ismerjük (és így könnyű benne számolni). Például a véges Abel-csoportok alaptételében az építőkövek a prímhatványrendű ciklikus csoportok, a konstrukció pedig a direkt szorzat.

Kézenfekvő ötlet tehát, ha egy tetszőleges algebrát megpróbálunk felbontani direkt szorzatra, ameddig csak lehet, majd megvizsgáljuk a tovább már nem bontható, úgynevezett *direkt*

felbonthatatlan algebrák szerkezetét. Ez az út azonban általában nem járható. Ennek oka egyrészt, hogy már a látszólag egyszerű esetekben, például a véges feloldható csoportok között is áttekinthetetlenül sok és bonyolult szerkezetű direkt felbonthatatlan van. De azt sem lehet megcsinálni, hogy egy algebrát „addig bontunk direkt szorzatra, amíg lehet". Például van olyan (végtelen) Abel-csoport, amelyet egyáltalán nem lehet felbontani direkt felbonthatatlanok direkt szorzatára.

Ilyen körülmények között kész csoda, hogy létezik egy egészen általános felbontási tétel, amely szintén Birkhoff-tól származik. Amire bontunk, az nem direkt szorzat, hanem a direkt szorzatnak részalgebrája. Ha B részalgebrája az A_i algebrák direkt szorzatának, és abban reménykedünk, hogy a B szerkezetét az A_i algebrák szerkezetére vezetjük majd vissza, akkor már az első lépésben érdemes kidobálni az A_i „fölösleges" elemeit, azokat, amelyeknek B-hez „nincs köze". Például

$$K = \{(0,0), (0,2), (2,0), (2,2)\} \leq \mathbb{Z}_4^+ \times \mathbb{Z}_4^+ ,$$

de a K-nak ebben a felbontásában a $\mathbb{Z}_4^+$ csoport 1 és 3 elemei fölöslegesek, mert K része a $H \times H$-nak is, ahol $H = \{0, 2\} \leq \mathbb{Z}_4$. Ez a $H = \{0, 2\}$ részcsoport úgy adódott, hogy K-nak a képét vettük a direkt szorzat két projekciójánál. Ez indokolja az alábbi definíciót.

8.4.12. Definíció. Azt mondjuk, hogy a

$$B \leq A = \prod_{i \in I} A_i$$

szubdirekt részalgebrája ennek a direkt szorzatnak (vagy hogy B az A_i algebrák egy szubdirekt szorzata), ha tetszőleges $i \in I$ esetén $\pi_i(B) = A_i$ (ahol π_i jelöli a direkt szorzat i-edik projekcióját).

A feltétel tehát azt jelenti, hogy minden $i \in I$ esetén minden $a \in A_i$-hez van B-nek egy olyan eleme, amelynek az i-edik komponense a.

Az $A = B \times C$ direkt szorzatot triviálisnak nevezhetjük, ha B és C egyike az egyelemű algebra. Ekkor a másik tényező A-val izomorf. Egy szubdirekt szorzat azonban lehet triviális másféleképpen is. Például legyen A tetszőleges, nem egyelemű algebra, és

$$A \cong B = \{(a, a) \,:\, a \in A\} \leq A \times A \,.$$

Ekkor B szubdirekt részalgebra, és az $A \times A$ direkt szorzatban egyik tényező sem egyelemű. Ez a szubdirekt felbontás mégis triviális, hiszen $B \cong A$ szerkezetéről ez a felbontás semmi információt nem ad, szó sincs arról, hogy a B algebrát nála „kisebb", „egyszerűbb" algebrákkal állítottuk volna elő. A bajt az okozza, hogy például az első projekció, vagyis a $\pi_1 : (a, a) \to a$ leképezés izomorfizmus B és A között.

8.4.13. Definíció. Ha B szubdirekt részalgebrája az A_i algebrák direkt szorzatának, akkor ezt a szubdirekt felbontást *triviálisnak* nevezzük, ha van olyan i index, amelyre a π_i projekció izomorfizmust létesít B és A_i között. A legalább kételemű B algebra *szubdirekt irreducibilis*, ha minden szubdirekt felbontása triviális.

8.4.14. Lemma. *Az S algebra akkor és csak akkor szubdirekt irreducibilis, ha a nem nulla kongruenciái között van legkisebb, vagyis ha létezik olyan $0 \neq \mu \in \mathrm{Con}(S)$, hogy tetszőleges $0 \neq \theta \in \mathrm{Con}(S)$ esetén $\mu \leq \theta$.*

Ezt a legkisebb nem nulla kongruenciát szokás (a csoportelméletből származó terminológiával) *S monolitjának* nevezni.

Bizonyítás. Ha

$$B \leq A = \prod_{i \in I} A_i$$

szubdirekt részalgebra, akkor jelölje $\eta_i \in \mathrm{Con}(B)$ azt a kongruenciát, amelynél két elem akkor kongruens, ha az i-edik komponensük megegyezik. Természetesen az η_i kongruenciák metszete nulla, mert ha két elem minden komponense megegyezik, akkor egyenlőek. Mindezt már láttuk a direkt szorzat kongruenciákkal történő jellemzésénél.

Az η_i kongruencia a π_i projekció (B-re vett megszorításának a) magja. Mivel B szubdirekt, $\pi_i(B) = A_i$, és ezért a homomorfizmus-tétel miatt $A_i \cong B/\eta_i$. A fenti szubdirekt felbontás akkor és csak akkor triviális, hogy valamelyik π_i izomorfizmus, és mivel mindegyik szürjektív, ez azzal ekvivalens, hogy a megfelelő $\eta_i = 0$.

Tegyük föl, hogy B nem nulla kongruenciái között van egy μ legkisebb. Meg kell mutatnunk, hogy a fenti szubdirekt felbontás triviális, vagyis valamelyik η_i kongruencia nulla. Ha ez nem lenne igaz, akkor mindegyik η_i nagyobb vagy egyenlő lenne μ-nél. Ezért az η_i kongruenciáknak a metszete is tartalmazná μ-t, vagyis nem lenne nulla. Ez ellentmondás, tehát B minden szubdirekt felbontása tényleg triviális.

Most megfordítjuk az eddig bizonyított állításokat. Tegyük föl, hogy adottak η_i ($i \in I$) kongruenciák, melyek metszete nulla. Legyen $A_i = B/\eta_i$. Tekintsük a B-n értelmezett

$$\varphi : b \mapsto (\ldots, b/\eta_i, \ldots) \in \prod_{i \in I} A_i$$

leképezést (itt b/η_i a b elem η_i-osztálya, ez lesz tehát a $\varphi(b)$ elem i-edik komponense). A φ függvény nyilvánvalóan művelettartó, megmutatjuk, hogy injektív. Ha $b, c \in B$ és $\varphi(c) = \varphi(b)$, akkor $b/\eta_i = c/\eta_i$ mindegyik i-re. Ezért $b \equiv c\ (\eta_i)$, azaz b és c kongruens az η_i kongruenciák metszeténél is, ami nulla. Ezért $b = c$, vagyis φ tényleg injektív.

Ez azt jelenti, hogy $B \cong \mathrm{Im}(\varphi)$, tehát a B algebrának (pontosabban egy vele izomorf algebrának) egy szubdirekt felbontását kaptuk (az nyilvánvaló, hogy a projekciók szürjektívek, hiszen $A_i = B/\eta_i$, és a természetes homomorfizmus szürjektív). Ez a felbontás nyilván akkor triviális, ha valamelyik η_i egyenlő nullával.

Tegyük most föl, hogy a B algebra nem nulla kongruenciái között nincs legkisebb. Tekintsük ezeknek a nem nulla kongruenciáknak a μ metszetét. Ez csak nulla lehet, mert

különben μ legkisebb nem nulla kongruencia lenne. Ezért B nem nulla kongruenciái egy olyan kongruenciarendszert adnak, amelyből egy nemtriviális szubdirekt felbontás készíthető a fenti módon. □

Az előző bizonyításban arra is fény derült, hogy egy algebrának hogyan lehet megkonstruálni a szubdirekt felbontásait, mert valójában az alábbi állítást láttuk be.

8.4.15. Következmény. *Egy A algebra szubdirekt felbontásainak az A olyan kongruenciáinak rendszere felel meg, amelyek metszete nulla. Egy ilyen felbontás pontosan akkor triviális, ha a kongruenciák között a nulla is szerepel.*

Birkhoff tétele azt mondja ki, hogy minden algebra felbontható szubdirekt irreducibilisek szubdirekt szorzatára. A most következő lemma ennek bizonyítását készíti elő. Kérjük az Olvasót, hogy a most következő gondolatmenetet vesse össze Krull tételének bizonyításával (5.3.13. Tétel, a bizonyítás a 260. oldalon kezdődik).

8.4.16. Lemma. *Legyenek a és b különböző elemei a B algebrának. Ekkor van olyan ρ kongruencia, hogy B/ρ szubdirekt irreducibilis, és $a \not\equiv b\ (\rho)$.*

Bizonyítás. A Zorn-lemmát alkalmazzuk (A.1.2. Tétel). Tekintsük B kongruenciáit párok halmazainak, tehát $B \times B$ részalgebráinak (vö. 8.3.10. Gyakorlat). Legyen $\mathcal{X}$ a B azon kongruenciáinak a halmaza, melyek az (a, b) párt nem tartalmazzák. Az $\mathcal{X}$ nem üres, mert $a \neq b$ miatt $0_B \in \mathcal{X}$. Megmutatjuk, hogy a Zorn-lemma feltétele teljesül, vagyis bárhogyan választjuk ki $\mathcal{X}$ egy olyan $\mathcal{L}$ részrendszerét, amelyik lánc, az $\mathcal{L}$ elemeinek σ uniója (a halmazelméleti uniója, nem az egyesítése) is eleme az $\mathcal{X}$ halmazrendszernek.

Azt, hogy σ maga is kongruencia, vagyis hogy részalgebrája $B \times B$-nek és ekvivalenciareláció, az 5.4.4. Lemmához hasonlóan bizonyíthatjuk, ezt az Olvasóra hagyjuk. Az nyilvánvaló, hogy az (a, b) pár nincs benne σ-ban, hiszen az unió egyik tagjában sincs benne. Vagyis $\mathcal{X}$ teljesíti a Zorn-lemma feltételét.

A Zorn-lemma szerint tehát $\mathcal{X}$-nek van egy maximális ρ eleme. Ez azt jelenti, hogy ha $\eta > \rho$ is egy kongruencia, akkor η már nem lehet eleme $\mathcal{X}$-nek, vagyis $(a, b) \in \eta$. A B/ρ faktoralgebra nem egyelemű, mert $(a, b) \notin \rho$. Be kell látnunk, hogy szubdirekt irreducibilis, vagyis hogy nullánál nagyobb kongruenciáinak a metszete nem lehet nulla.

A B/ρ kongruenciái a B algebra ρ-t tartalmazó kongruenciáinak felelnek meg kölcsönösen egyértelmű és rendezéstartó módon (8.2.20. Feladat), a nulla kongruencia ρ-nak felel meg. Ezért azt kell megmutatnunk, hogy ha η_i olyan kongruenciái B-nek, amelyekre $\eta_i > \rho$, akkor az η metszetük szintén nagyobb ρ-nál. Az nyilvánvaló, hogy $\eta \geq \rho$. A ρ maximalitása és $\eta_i > \rho$ miatt $a \equiv b\ (\eta_i)$. Ezért a és b kongruensek az η_i kongruenciák η metszeténél is. De akkor $\eta \neq \rho$, hiszen $(a, b) \notin \rho$. Tehát B/ρ tényleg szubdirekt irreducibilis. □

8.4.17. Tétel [Birkhoff tétele a szubdirekt felbontásról]. *Minden algebra előáll szubdirekt irreducibilis algebrák szubdirekt szorzataként (és a tényezők az eredeti algebra homomorf képei).*

Bizonyítás. Legyen B algebra, és minden $a \neq b$ elempárjához vegyünk egy olyan $\rho_{a,b}$ kongruenciát, amelyre $B/\rho_{a,b}$ szubdirekt irreducibilis és $a \not\equiv b\ (\rho_{a,b})$. Ilyen az előző lemma miatt létezik. Az összes ilyen $\rho_{a,b}$ kongruenciák metszete nulla, hiszen minden (a, b) pár kimarad valamelyikből (nevezetesen a $\rho_{a,b}$-ből). Ezért a 8.4.15. Következmény szerint ezek a kongruenciák egy szubdirekt felbontást adnak, amelynek a tényezői a $B/\rho_{a,b}$ szubdirekt irreducibilis algebrák. □

Birkhoff tételének fontos alkalmazását látjuk majd a következő fejezetben, amikor a disztributív hálókra és a Boole-algebrákra bizonyítjuk segítségével Stone reprezentációs tételét.

Gyakorlatok, feladatok

8.4.18. Gyakorlat. Döntsük el, hogy a 8.3. Ábrán látható M_3, N_5, D_1 és D_2 hálók szubdirekt irreducibilisek-e. (A kongruencia-hálójukat már kiszámoltuk a 8.2.37. Gyakorlatban).

8.4.19. Gyakorlat. A $\mathbb{C}[x]$ gyűrűt, illetve a páratlan nevezőjű törtek gyűrűjét bontsuk föl szubdirekt irreducibilisek szubdirekt szorzatára.

8.4.20. Feladat. Határozzuk meg a szubdirekt irreducibilis Abel-csoportokat.

8.4.21. Feladat. Mi lesz a $\mathbb{Z}^+$ csoport illetve a $\mathbb{Z}$ gyűrű által generált varietás?

8.4.22. Feladat. Bizonyítsuk be, hogy a Q illetve a D_4 csoportok ugyanazt a varietást generálják.

8.4.23. Feladat. Határozzuk meg az S_3 csoport által generált csoportvarietás szubdirekt irreducibilis elemeit, és adjuk meg ezt a varietást véges sok azonossággal.

8.4.24. Feladat. Legyen A algebra, és $\mathcal{K}$ az A végesen generált részalgebráinak a halmaza. Mutassuk meg, hogy $A \in \mathsf{HSP}(\mathcal{K})$.

8.4.25. Feladat. Tegyük föl, hogy a $\mathcal{K}$ osztály zárt a részalgebra, a homomorf kép és a direkt szorzat képzésére, $X = \{x_1, x_2, \ldots, x_n\}$, és F az X által generált szabad algebra $\mathcal{K}$-ban (8.3.26. Tétel). Tekintsük azokat $t_1(x_1, \ldots, x_n) \approx t_2(x_1, \ldots, x_n)$ azonosságokat, melyekre $t_1^F(x_1, \ldots, x_n) = t_2^F(x_1, \ldots, x_n)$ teljesül. Mutassuk meg, hogy ha n befutja a pozitív egészeket, akkor ezek az azonosságok pontosan a $\mathcal{K}$ osztályt definiálják.

8.5. Disztributív hálók és Boole-algebrák

A gyűrűknél megismert disztributív azonosságnak fontos szerep jut a hálók elméletében is, ha azt az összeadás és a szorzás helyett a két hálóműveletre alkalmazzuk. Így kapjuk a disztributív háló fogalmát, amelyre a legfontosabb példát egy halmaz összes részhalmazai adják az unió és a metszet műveletére, továbbá ezeknek a hálóknak a részhálói. Izomorfia erejéig nincs is másmilyen példa Stone reprezentációs tétele szerint, amit bebizonyítunk.

Nevezetes tény, hogy minden háló kongruencia-hálója disztributív. A szakaszban szó lesz még a Boole-algebrákról. Ezek a komplementumos disztributív hálók, és a logikában játszanak fontos szerepet.

8.5.1. Gyakorlat. Mutassuk meg, hogy ha L tetszőleges háló, akkor az

$$(x \wedge y) \vee z \approx (x \vee z) \wedge (y \vee z)$$

és az

$$(x \vee y) \wedge z \approx (x \wedge z) \vee (y \wedge z)$$

azonosságok ekvivalensek (vagyis ha az egyik igaz L-ben, akkor a másik is).

8.5.2. Definíció. Azt mondjuk, hogy az L háló *disztributív*, ha érvényes benne az előző gyakorlatban megadott két disztributív azonosság bármelyike (és így mindkettő).

8.5.3. Gyakorlat. Igazoljuk, hogy a 8.3. Ábrán látható M_3 és N_5 hálók nem disztributívak.

Az M_3 és N_5 hálók azért fontosak, mert egy háló akkor és csak akkor disztributív, ha ezek egyikével sincs izomorf részhálója (8.6.16. Tétel).

A disztributív azonosságok ellenőrzésekor érdemes észrevenni, hogy a két oldal egyike minden hálóban kisebb vagy egyenlő a másiknál. Például az első azonosság esetében

$$(x \wedge y) \vee z \leq (x \vee z) \wedge (y \vee z)$$

minden háló minden x, y, z elemére igaz. Ennek magyarázatát a következő elv szolgáltatja: *a legkisebb óriás is nagyobb, mint a legnagyobb törpe.* Valóban, az azonosság bal oldalán szereplő $x \wedge y$ és z tagok törpék, hiszen mindegyikük kisebb vagy egyenlő, mint a jobb oldalon szereplő $x \vee z$ és $y \vee z$ tagok, amelyek tehát óriások. Mivel minden törpe alsó korlátja az óriások halmazának, ezért az óriások metszetének is. Ez felső korlátja mindegyik törpének, tehát a törpék egyesítésének is. Ezért a fenti egyenlőtlenség igaz.

A két disztributív azonosság természetesen egymás duálisa, és így ha egy disztributív háló duálisát vesszük, az szintén disztributív háló lesz. Ugyancsak világos, hogy egy X halmaz összes részhalmazainak $\mathcal{P}(X)$ hálója az $\cup$ és $\cap$ műveletekre disztributív, sőt ennek minden részhálója is disztributív, mert a disztributív azonosság részhálókra öröklődik.

8.5.4. Gyakorlat. Legyen $C_2 = \{0, 1\}$ a kételemű háló (a $0 < 1$ rendezéssel). Mutassuk meg, hogy a C_2^X direkt hatvány izomorf a $\mathcal{P}(X)$ hálóval.

8.5.5. Gyakorlat. Igazoljuk, hogy minden lánc disztributív háló.

8.5.6. Gyakorlat. Igazoljuk, hogy a nemnegatív egészek disztributív hálót alkotnak az oszthatósággal megadott rendezésre. Vezessük le ebből, hogy minden ciklikus csoport részcsoporthálója disztributív.

Most leírjuk a disztributív hálók kongruenciáit. A gyűrűkhöz hasonlóan ezek is „ideálokhoz" kapcsolódnak.

8.5.7. Definíció. Egy P részben rendezett halmaz egy X részhalmaza *leszálló*, ha minden $x \in X$ elemével együtt az x-nél kisebb P-beli elemeket is tartalmazza. A fogalom duálisa a *felszálló* részhalmaz. Ha L háló, akkor a nem üres $I \subseteq L$ részhalmaz *ideál*, ha leszálló, és zárt az egyesítésre. Ha $b \in L$, akkor a b-nél kisebb vagy egyenlő elemekből álló ideált a b által generált *főideálnak* nevezzük, és $(b]$-vel jelöljük. Az ideál duálisa a *filter*, más szóval *szűrő*, a főideálé a *főfilter*, jele $[b)$.

Könnyű ellenőrizni, hogy minden főideál tényleg ideál. A $(b]$ jelölés az analízisből ismert félig zárt intervallum fogalmához kapcsolódik (ott $(a, b]$ azon x számok halmaza, melyekre $a < x \leq b$). Az intervallum hálóelméleti fogalmáról a 8.6.17. Definícióban lesz szó.

Az ideál elnevezést a felszínes hasonlóság is indokolja, hiszen az ideál zárt az egyik műveletre (az egyesítésre), és a külső elemmel való „bemetszésre" is (ez jelenti azt, hogy leszálló). A Boole-algebrák kapcsán majd megértjük, hogy az ideál elnevezés ennél többet takar (lásd a 8.5.23. Feladat utáni megjegyzéseket).

8.5.8. Feladat. Tegyük föl, hogy I ideálja, F pedig filtere az L disztributív hálónak. Legyen $a \equiv b \ (\theta_I)$ akkor és csak akkor, ha van olyan $x \in I$, melyre $a \vee x = b \vee x$, és ρ_F a duális módon F-hez rendelt reláció.

(1) Bizonyítsuk be, hogy θ_I kongruencia, amelynek I osztálya.
(2) Igazoljuk, hogy ha az I ideál és az F filter olyan, hogy tetszőleges $c \in I$ és $f \in F$ esetén mindig $c \leq f$, akkor $\theta_I \wedge \rho_F = 0_L$.
(3) Mutassuk meg, hogy az egyetlen szubdirekt irreducibilis disztributív háló a kételemű háló.

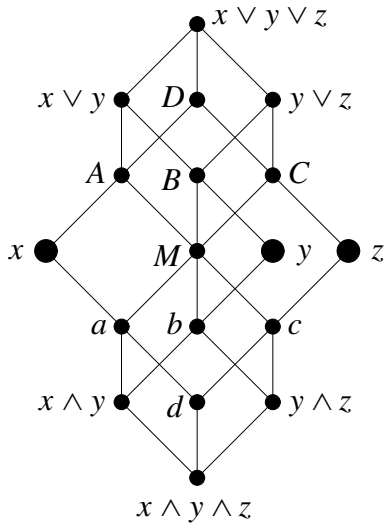
8.5.9. Tétel [Stone reprezentációs tétele]. *Minden disztributív háló izomorf egy alkalmas halmaz összes részhalmazaiból álló háló egy részhálójával.*

Bizonyítás. Birkhoff tétele (8.4.17. Tétel) szerint minden L disztributív háló előáll szubdirekt irreducibilis algebrák szubdirekt szorzataként, amelyek az eredeti háló faktorai, és így szintén disztributív hálók. A 8.5.8. Gyakorlat miatt az egyetlen szubdirekt irreducibilis disztributív háló a kételemű $C_2 = \{0, 1\}$ háló. Ezért L részalgebrája egy alkalmas C_2^X direkt hatványnak. A 8.5.4. Gyakorlat szerint viszont C_2^X izomorf az X összes részhalmazaiból álló hálóval. □

Stone tétele nem dönt el minden állítást automatikusan disztributív hálókról, még a végesen generált szabad disztributív hálók elemszámát sem könnyű kiszámítani (ezek mind végesek, lásd 8.5.25. Gyakorlat).

8.5.10. Tétel. *A három elemmel generált szabad disztributív háló elemszáma* 18, *rajza a 8.7. Ábrán látható.*

A tétel bizonyítása egyszerű számolás, amit elhagyunk (azt, hogy ezt a számolást hogyan kell végezni, az Olvasó megtudhatja a 8.6.11. Tétel hasonló bizonyításából). Az ábrán szerepel az elemek legegyszerűbb felírása is a generátorok segítségével. Az M kifejezésnek van egy igen fontos tulajdonsága.



$$D = x \vee z$$
$$A = x \vee (y \wedge z)$$
$$B = y \vee (x \wedge z)$$
$$C = z \vee (x \wedge y)$$
$$M = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$$
$$a = x \wedge (y \vee z)$$
$$b = y \wedge (x \vee z)$$
$$c = z \wedge (x \vee y)$$
$$d = x \wedge z$$

8.7. Ábra. Az x, y és z által generált szabad disztributív háló.

8.5.11. Definíció. Azt mondjuk, hogy $t(x, y, z)$ az A algebra *többségi kifejezése*, ha A-ban érvényesek a

$$t(x, x, y) \approx t(x, y, x) \approx t(y, x, x) \approx x$$

azonosságok (vagyis ha t két változója megegyezik, akkor az értéke is ez a változó lesz).

8.5.12. Gyakorlat. Mutassuk meg, hogy ha L tetszőleges (nem feltétlenül disztributív) háló, akkor mind az

$$M(x, y, z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)\,,$$

mind az

$$m(x, y, z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$$

kifejezés többségi kifejezés, és $m(x, y, z) \leq M(x, y, z)$ tetszőleges $x, y, z \in L$ esetén. Igazoljuk, hogy ha L disztributív, akkor $M \approx m$ azonosság L-ben.

Az M-et felső, az m-et alsó *mediánsnak* nevezzük. Nem nehéz belátni, hogy ha egy hálóban teljesül az $m \approx M$ azonosság, akkor az disztributív. A többségi kifejezések jelentőségét a következő tétel világítja meg.

8.5.13. Tétel. *Ha az A algebrának van többségi kifejezése, akkor A kongruencia-hálója disztributív.*

Bizonyítás. Elegendő igazolni, hogy az A algebra tetszőleges α, β, γ kongruenciáira

$$\alpha \wedge (\beta \vee \gamma) \leq (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)\,,$$

hiszen a másik irányú tartalmazás (az óriás-törpe elv miatt) teljesül. Legyenek az $a, b \in A$ elemek kongruensek a bal oldali kongruenciára nézve. Meg kell mutatni, hogy a jobb oldalon lévő kongruenciára nézve is azok.

Tudjuk tehát, hogy $a \equiv b\ (\alpha)$ és $a \equiv b\ (\beta \vee \gamma)$. A 8.2.23. Tétel miatt kongruenciák egyesítése ugyanaz, mint a megfelelő partíciók egyesítése, amit a 8.1.25. Feladatban írtunk le. Eszerint létezik egy

$$a = z_0 \overset{\beta}{\text{---}} z_1 \overset{\gamma}{\text{---}} z_2 \overset{\beta}{\text{---}} z_3 \overset{\gamma}{\text{---}} z_4 \quad \dots \quad z_{n-1} \overset{\gamma}{\text{---}} z_n = b$$

sorozat. Legyen t többségi kifejezése A-nak és

$$u_i = t^A(a, z_i, b)\,.$$

Ekkor $u_0 = t^A(a, z_0, b) = t^A(a, a, b) = a$, hiszen t többségi, és hasonlóan $u_n = b$. Továbbá tudjuk, hogy a polinomfüggvények megőrzik a kongruenciákat (8.3.19. Gyakorlat). Mivel $z_i \equiv z_{i+1}$ a β vagy a γ szerint (attól függően, hogy i páros-e, vagy páratlan), azt kapjuk, hogy

$$u_i = t^A(a, z_i, b) \equiv t^A(a, z_{i+1}, b) = u_{i+1}$$

a β vagy a γ szerint. Ezért a következő sorozat keletkezik:

$$a = u_0 \overset{\beta}{\text{---}} u_1 \overset{\gamma}{\text{---}} u_2 \overset{\beta}{\text{---}} u_3 \overset{\gamma}{\text{---}} u_4 \quad \dots \quad u_{n-1} \overset{\gamma}{\text{---}} u_n = b\ .$$

Ez a sorozat tehát legalább ugyanazt tudja, mint a fenti z_i sorozat. Azonban $a \equiv b\ (\alpha)$ miatt tetszőleges i-re

$$u_i = t^A(a, z_i, b) \equiv t^A(a, z_i, a) = a\ (\alpha)\,,$$

hiszen t többségi kifejezés. Vagyis mindegyik u_i elem benne van az a elem α-osztályában, és ezért $z_i \equiv z_{i+1}\ (\alpha)$ mindegyik i-re. Így valójában

$$a = u_0 \overset{\alpha\wedge\beta}{\text{---}} u_1 \overset{\alpha\wedge\gamma}{\text{---}} u_2 \overset{\alpha\wedge\beta}{\text{---}} u_3 \overset{\alpha\wedge\gamma}{\text{---}} u_4 \quad \dots \quad u_{n-1} \overset{\alpha\wedge\gamma}{\text{---}} u_n = b$$

teljesül, és így $a \equiv b$ modulo $(\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$. □

Mivel minden hálónak van többségi kifejezése (bármelyik mediáns az a 8.5.12. Gyakorlat szerint), a következőt kapjuk.

8.5.14. Következmény. *Minden háló kongruencia-hálója disztributív.*

A most bizonyított tétel jelentősége a következő. Birkhoff tételét a szubdirekt felbontásról akkor lehet hatékonyan alkalmazni, ha ismerjük a szubdirekt irreducibilis algebrákat (mint a Stone-tétel bizonyításában). Ha az algebráink kongruencia-hálója disztributív, akkor Jónsson alábbi tétele lehetővé teszi a szubdirekt irreducibilisek megtalálását. A tételt csak a véges algebrákra vonatkozó gyengébb (de érthetőbb) formájában ismertetjük, és nem bizonyítjuk.

8.5.15. Tétel [Jónsson-lemma]. *Tegyük föl, hogy $A_1, \dots, A_k$ véges algebrák, és hogy a $\mathcal{V} = \mathsf{V}(A_1, \dots, A_k)$ varietás minden algebrájának a kongruencia-hálója disztributív. Ekkor $\mathcal{V}$ minden szubdirekt irreducibilis algebrája valamelyik A_i algebra egyik részalgebrájának homomorf képe.*

A tételt tehát alkalmazhatjuk, ha az A_i algebráknak van közös többségi kifejezése, például ha mindannyian hálók.

8.5.16. Gyakorlat. Határozzuk meg a 8.3. Ábrán látható M_3 és N_5 hálók által generált varietásban a szubdirekt irreducibilis hálókat. Igazoljuk (a Jónsson-lemma felhasználásával), hogy mindkét háló teljesít olyan háló-azonosságot, ami a másikban nem igaz.

A szakasz hátralévő részében a Boole-algebrák fogalmával ismerkedünk meg: ezek a komplementumos disztributív hálók (8.1.26. Definíció). A definíciót óvatosabban fogalmazzuk, mert fontos, hogy a komplementumot (és a 0, 1 elemeket is) művelettel jelöljük ki. Ezt a következő gyakorlat állítása teszi lehetővé.

8.5.17. Gyakorlat. Igazoljuk, hogy disztributív hálóban minden elemnek legfeljebb egy komplementuma lehet.

8.5.18. Definíció. *Boole-algebrának* nevezünk egy olyan B algebrát, melynek a műveletei az $\vee$ (egyesítés), a $\wedge$ (metszet), a $'$ (komplementum), a 0 és az 1 (konstansok), a következő tulajdonságokkal.

(1) B az egyesítésre és metszetre disztributív háló.
(2) A 0 a B legkisebb, az 1 a B legnagyobb eleme.
(3) B-ben érvényesek az $x \wedge x' \approx 0$ és $x \vee x' \approx 1$ azonosságok.

A nulla- és egységelemes, komplementumos disztributív hálókat szokás *Boole-hálónak* nevezni. (Ezek nem Boole-algebrák a szó szigorú értelmében, mert kevesebb műveletük van.)

Az X halmaz összes részhalmazaiból álló $\mathcal{P}(X)$ disztributív hálót Boole-algebrának is tekintjük, ahol 0 az üres halmaz, 1 az X halmaz, és a komplementum a szokásos. A két- és háromelemű halmaz esetében a kapott Boole-háló rajza a 8.3. Ábrán látható C_2^2 és C_2^3.

8.5.19. Gyakorlat. Legyen $K = \{0, 1\}$ a kételemű Boole-algebra. Mutassuk meg, hogy az K^X direkt hatvány izomorf a $\mathcal{P}(X)$ Boole-algebrával.

8.5.20. Gyakorlat. Mutassuk meg, hogy minden Boole-algebrában igaz az $x'' \approx x$ azonosság, továbbá teljesülnek az $(x \vee y)' \approx x' \wedge y'$ és $(x \wedge y)' \approx x' \vee y'$ azonosságok is (ezek az úgynevezett *De Morgan azonosságok*). Ezért Boole-algebrában a komplementumképzés rendezésfordító leképezés.

A Boole-algebrák vizsgálatának másik motivációja a logika. Korábban már láttuk, hogy ha a 0 a „hamis” és az 1 az „igaz” igazságértékeket jelenti, akkor a kapott kételemű hálóban az „és” művelet a metszetnek, a „vagy” művelet pedig az egyesítésnek felel meg (lásd a megjegyzéseket a 436. oldalon). Vegyük észre, hogy a komplementumképzés pontosan a tagadásnak (a „nem”-kapuknak) megfelelő művelet. Így a kételemű Boole-algebrát felfoghatjuk úgy is, mint az igazságértékek algebráját. A 8.3.15. Feladat a kételemű Boole-algebráról szól.

Tekintsük az olyasfajta kijelentéseket, hogy „esik az eső”, vagy „Melinda ötöst kapott matekból”. Ezeket ítéleteknek nevezzük (mert vagy igazak, vagy nem). Az „és”, a „vagy” és a „nem” logikai műveletekkel ezeket összekapcsolhatjuk, és így Boole-algebrát kapunk, amit az ítéletek Boole-algebrájának nevezünk. Megjegyezzük, hogy nemcsak az ilyesfajta ítéleteket,

hanem a „minden ember halandó” típusúakat (tehát a kvantort tartalmazókat) is vizsgálhatjuk alkalmas műveletek segítségével. Így az algebrai eszközöket a logikában felhasználhatjuk. Ezt a tárgykört *algebrai logikának* nevezzük.

8.5.21. Gyakorlat. Mutassuk meg, hogy ha B egy Boole-algebra, akkor a 8.5.8. Gyakorlatban definiált kongruenciákat a Boole-műveletek is tartják, és így az egyetlen szubdirekt irreducibilis Boole-algebra a kételemű.

Így Birkhoff szubdirekt felbontásról szóló tételéből a 8.5.9. Tétel mintájára adódik a következő eredmény.

8.5.22. Tétel [Stone reprezentációs tétele]. *Minden Boole-algebra izomorf egy alkalmas halmaz összes részhalmazaiból álló Boole-algebra egy részalgebrájával.*

A véges Boole-algebrák szerkezete teljesen leírható: ezek egy véges halmaz *összes* részhalmazaiból állnak (8.5.26. Feladat). A végtelen Boole-algebrák szerkezete viszont roppant bonyolult lehet (lásd a 8.5.29. Feladatot, és az azt követő megjegyzést). A végesen generált szabad Boole-algebrákat a 8.5.27. Feladat írja le.

A Boole-algebrák ideáljai a 8.5.21. Gyakorlat szerint kongruenciákat adnak. Megfordítva, minden kongruencia egy ideálhoz tartozik, és ez a megfeleltetés kölcsönösen egyértelmű. Ezt könnyű lenne „kézzel” is kiszámolni, de ehelyett megmutatjuk, hogy a Boole-algebrák valójában gyűrűknek is felfoghatók. Emlékeztetjük az Olvasót, hogy két halmaz szimmetrikus differenciáján azoknak az elemeknek a halmazát értjük, amelyek a két halmaz közül pontosan egyben vannak benne.

8.5.23. Feladat. Legyen B Boole-algebra, és definiáljuk a következő műveleteket. Az x és y szorzata legyen $xy = x \wedge y$. Az x és y összege legyen

$$x + y = (x \wedge y') \vee (x' \wedge y)$$

(vagyis az x és y szimmetrikus differenciája). Mutassuk meg, hogy ekkor B alaphalmazán egy R kommutatív, egységelemes gyűrűt kaptunk, amelyben $x^2 = x$ és $2x = 0$ teljesül minden elemre. Megfordítva, mutassuk meg, hogy ha az R egységelemes gyűrűben érvényes az $x^2 \approx x$ azonosság, akkor kommutatív, karakterisztikája kettő, és az

$$x \vee y = x + y - xy\,, \quad x \wedge y = xy\,, \quad x' = 1 - x$$

műveletekre Boole-algebrát kapunk. Igazoljuk, hogy egy részhalmaz akkor és csak akkor ideál a gyűrűelméleti értelemben, ha a hálóelméleti értelemben az.

Az előző feladat miatt az $x^2 \approx x$ azonosságnak eleget tevő egységelemes gyűrűket *Boole-gyűrűknek* nevezzük. Mivel a Boole-algebra műveletek és a gyűrűműveletek egymással kifejezhetők, egy Boole-algebrának és a hozzá tartozó Boole-gyűrűnek *ugyanazok a kifejezésfüggvényei*. De a kifejezésfüggvények meghatározzák a kompatibilis relációkat, és így a kongruenciákat is. Mivel a gyűrűkben a kongruenciák ideálokkal adhatók meg, ezért a Boole-algebrák kongruenciái is kölcsönösen egyértelmű megfeleltetésben állnak az ideálokkal: minden ideálhoz pontosan egy kongruencia tartozik a 8.5.8. Gyakorlatban leírt

módon, és minden kongruencia megkapható ezen a módon. Mindez megmagyarázza azt is, miért használtuk hálók esetében az „ideál” elnevezést.

Gyakorlatok, feladatok

8.5.24. Gyakorlat. Melyek disztributívak a 8.3. Ábrán lerajzolt hálók közül? Melyek lesznek Boole-hálók?

8.5.25. Gyakorlat. Bizonyítsuk be, hogy minden végesen generált disztributív háló, illetve Boole-algebra véges.

8.5.26. Feladat. Mutassuk meg, hogy ha B egy véges Boole-algebra, akkor izomorf a kételemű Boole-algebra egy direkt hatványával, vagyis egy véges halmaz összes részhalmazainak Boole-algebrájával.

8.5.27. Feladat. Legyenek $X_1, \ldots, X_n$ az X halmaz részhalmazai. Bizonyítsuk be, hogy ezek akkor és csak akkor alkotnak szabad generátorrendszert az általuk generált F Boole-algebrában, ha *általános helyzetűek* a következő értelemben. Bárhogyan is választunk ki az X_i halmazok közül néhányat, van olyan $x \in X$, ami ezekben benne van, a többi X_j halmazban viszont nincs benne. Vezessük le ebből, hogy az n elemmel generált *szabad Boole-algebra* elemszáma 2^{2^n}.

8.5.28. Feladat. Mutassuk meg, hogy az előző feladatban szereplő általános helyzetű halmazok által generált részháló az n elemmel generált *szabad disztributív háló*. Adjunk alsó és felső becslést ennek elemszámára.

8.5.29. Feladat. Mutassuk meg, hogy van olyan Boole-algebra, amely *atommentes*, vagyis a 0 elemnek egyetlen fedője sincs.

Egy atommentes Boole-algebra természetesen nem lehet izomorf egyetlen halmaz összes részhalmazainak Boole-algebrájával sem. A véges Boole-algebrák szerkezete olyan egyszerű, hogy az ember azt hinne, a végteleneké is az. Erről szó sincsen, S. Shelah híres eredménye, hogy minden úgynevezett reguláris κ számosságra (ilyenekből nagyon sok van) létezik 2^κ darab páronként nem izomorf κ elemű Boole-algebra.

8.5.30. Feladat. Egy $I \neq L$ ideál *prímideál* az L hálóban, ha $x \wedge y \in I$-ből $x \in I$ vagy $y \in I$ következik; a duális fogalom az *ultrafilter*. Mutassuk meg, hogy tetszőleges L disztributív hálóban teljesülnek a következők.

(1) Egy I ideál akkor és csak akkor prímideál, ha a komplementere (vagyis az $L - I$ halmaz) filter.
(2) Ha I prímideál, akkor az $\{I, L - I\}$ partíció kongruencia.
(3) Az L maximális kongruenciái (amelyeknek az 1_L kongruencia fedője) pontosan a (2)-ben leírt kongruenciák.
(4) Legyen F filter, ami nem az egész L. Ha I maximális az L azon ideáljai között, amelyek F-től diszjunktak, akkor I prímideál.
(5) Minden valódi ideál része egy alkalmas prímideálnak.

8.6. Moduláris hálók

A modularitás a disztributivitáshoz hasonlóan egy háló-azonosság, amely azért került előtérbe, mert a legfontosabb klasszikus algebrai struktúrák (csoportok, gyűrűk, modulusok) kongruencia-hálója moduláris. Először ennek pontos okát tárjuk föl, utána megismerkedünk a moduláris hálók fontosabb tulajdonságaival, mint az intervallum-izomorfizmus, a Jordan–Hölder-tételt általánosító Jordan–Dedekind-tétel, a dimenziófüggvény létezése, és a Noether–Lasker-tételt általánosító Kuros–Ore-tétel.

8.6.1. Gyakorlat. Legyenek H és K részcsoportok egy G csoportban, és jelölje θ, illetve ρ a hozzájuk tartozó bal oldali mellékosztályok alkotta partíciót. Bizonyítsuk be, hogy $HK = KH$ akkor és csak akkor, ha a θ és ρ partíciók felcserélhetők, azaz ha $\theta \circ \rho = \rho \circ \theta$ (8.2.29. Definíció).

Mivel bármely két normálosztó felcserélhető, ezért az előző gyakorlat azt mutatja, hogy a csoportok bármely két kongruenciája felcserélhető.

8.6.2. Definíció. A $\mathcal{V}$ varietást *Malcev-varietásnak* nevezzük, ha minden algebrájának bármely két kongruenciája felcserélhető.

Ez a fogalom azért kapta A. I. Malcevről a nevét, mert neki jutott először eszébe, hogy a kongruenciák felcserélhetősége formális kifejezések segítségével jellemezhető. A csoportok varietása azért ilyen, mert a $d(x, y, z) = xy^{-1}z$ kifejezés a következő tulajdonsággal rendelkezik.

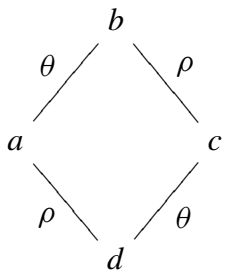
8.6.3. Definíció. Azt mondjuk, hogy $d(x, y, z)$ az A algebra *Malcev-kifejezése*, ha A-ban érvényesek a

$$d(x, x, z) \approx d(z, x, x) \approx z$$

azonosságok. Egy varietás Malcev-kifejezése egy olyan formális kifejezés, amely a varietás minden algebrájának Malcev-kifejezése.

8.6.4. Tétel [Malcev tétele]. *Egy $\mathcal{V}$ varietás akkor és csak akkor Malcev-varietás, ha van Malcev-kifejezése.*

Bizonyítás. Először megmutatjuk, hogy ha d Malcev-kifejezése $\mathcal{V}$-nek, $A \in \mathcal{V}$, és θ, ρ az A kongruenciái, akkor $\theta \circ \rho \subseteq \rho \circ \theta$. Tegyük föl, hogy $(a, c) \in \theta \circ \rho$, vagyis létezik olyan $b \in A$, hogy $a \equiv b\ (\theta)$ és $b \equiv c\ (\rho)$. Legyen $d = d^A(a, b, c)$, belátjuk, hogy $a \equiv d\ (\rho)$ és $d \equiv c\ (\theta)$:



(és így $(a, c) \in \rho \circ \theta$). Valóban, mivel a polinomfüggvények megőrzik a kongruenciákat,

$$d = d^A(a, b, c) \equiv d(a, c, c) = a \ (\rho) \,,$$

és hasonlóan $d \equiv c \ (\theta)$. Így igazoltuk, hogy $\theta \circ \rho \subseteq \rho \circ \theta$. A θ és a ρ szerepét felcserélve a fordított irányú tartalmazást kapjuk, és ezért θ és ρ tényleg felcserélhetők.

Megfordítva, tegyük föl, hogy a $\mathcal{V}$ varietás algebráinak kongruenciái felcserélhetők. Legyen F az $X = \{x, y, z\}$ által generált szabad algebra ebben a varietásban (8.3.26. Tétel). Mivel F szabad, az az $X \to F$ függvény, amelyre

$$x \mapsto x \,, \quad y \mapsto x \,, \quad z \mapsto z$$

kiterjeszthető egy $\varphi : F \to F$ homomorfizmussá. Legyen θ ennek a magja. Hasonlóképpen, legyen $\rho = \mathrm{Ker}(\psi)$, ahol $\psi(x) = x$, $\psi(y) = z$ és $\psi(z) = z$.

Mivel $\varphi(x) = \varphi(y)$, ezért $x \equiv y \ (\theta)$, és hasonlóan $y \equiv z \ (\rho)$. Ezért $(x, z) \in \theta \circ \rho$. Mivel θ és ρ felcserélhetők, $(x, z) \in \rho \circ \theta$, vagyis van olyan $d \in F$, hogy $x \equiv d \ (\rho)$ és $d \equiv z \ (\theta)$. Az x, y, z elemek generálják F-et, és ezért $d = d^F(x, y, z)$ alkalmas d formális kifejezésre (a 8.3.7. Tétel miatt). Megmutatjuk, hogy d Malcev-kifejezése a $\mathcal{V}$ varietásnak.

A $d(x, x, z) \approx z$ azonosságot elegendő az F szabad algebra x, y, z elemein ellenőrizni (8.4.6. Gyakorlat), vagyis azt megmutatni, hogy $d^F(x, x, z) = z$. Tudjuk, hogy $d \equiv z \ (\theta)$, vagyis $\varphi(d) = \varphi(z) = z$. Másrészt a φ homomorfizmus tartja a kifejezésfüggvényeket (8.3.23. Gyakorlat), ezért

$$z = \varphi(z) = \varphi(d) = \varphi\big(d^F(x, y, z)\big) = d^F\big(\varphi(x), \varphi(y), \varphi(z)\big) = d^F(x, x, z) \,.$$

Ugyanígy bizonyítható a $d^F(x, z, z) = z$ összefüggés, és ezzel a $d(x, z, z) \approx x$ azonosság is, tehát d tényleg Malcev-kifejezés. □

A most bizonyított tétel első jelentősége az, hogy nemcsak a csoportok kongruenciái felcserélhetők, hanem minden olyan algebráé, amelyet a csoportokból újabb műveletek hozzávételével kapunk. Ilyenek a gyűrűk, a vektorterek, a modulusok.

8.6.5. Állítás. *A Boole-algebrák varietása kongruencia-felcserélhető.*

Bizonyítás. A 8.5.23. Gyakorlat miatt van olyan kifejezés, ami a Boole-algebrák osztályán csoport-összeadást, illetve inverzképzést ad, ezekből pedig egy Malcev-kifejezés összerakható, hiszen a csoportok varietása kongruencia-felcserélhető. (Konkrétan kiszámítva

$$x + y + z = (x \wedge y' \wedge z') \vee (y \wedge x' \wedge z') \vee (z \wedge x' \wedge y') \vee (x \wedge y \wedge z)$$

Malcev-kifejezés lesz.) □

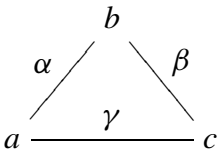
Ennél fontosabb, hogy a Malcev-kifejezés segítségével számolni is lehet (lásd például a 8.6.35. és a 8.6.36. Feladatok megoldását), ami lehetővé teszi Malcev-varietásokra mély tételek bizonyítását. Erről később röviden mesélni fogunk.

8.6.6. Állítás. *Tegyük föl, hogy az A algebra kongruenciái felcserélhetők, és legyenek α, β, γ kongruenciái A-nak. Ekkor*

$$\alpha \leq \gamma \implies (\alpha \vee \beta) \wedge \gamma = \alpha \vee (\beta \wedge \gamma)\,.$$

A fenti egyenlőség megjegyzésében, és a bizonyítás követésében segíthet a 8.8. Ábra, amely azt a tipikus helyzetet ábrázolja, amikor az egyenlőség nem teljesül.

Bizonyítás. Az óriás-törpe elv miatt $(\alpha \vee \beta) \wedge \gamma \geq \alpha \wedge (\beta \vee \gamma)$. A fordított egyenlőtlenség igazolásához tegyük föl, hogy $(a, c) \in (\alpha \vee \beta) \wedge \gamma$. Ekkor $a \equiv c\ (\gamma)$. Mivel A kongruenciái felcserélhetők, $\alpha \vee \beta = \alpha \circ \beta$ (8.2.30. Gyakorlat), vagyis van olyan $b \in A$, hogy

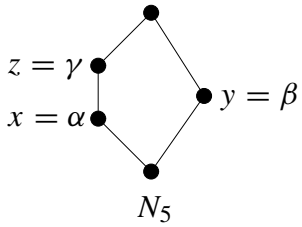


Mivel $\alpha \leq \gamma$, ezért $a \equiv b\ (\gamma)$, így γ tranzitivitása miatt $b \equiv c\ (\gamma)$. Ezért $b \equiv c\ (\beta \wedge \gamma)$, vagyis a b elem azt mutatja, hogy $(a, c) \in \alpha \circ (\beta \wedge \gamma)$. □

8.6.7. Definíció. Az L háló *moduláris*, ha tetszőleges $x, y, z \in L$ esetén

$$x \leq z \implies (x \vee y) \wedge z = x \vee (y \wedge z)\,.$$

Így minden csoport kongruencia-hálója moduláris (amit a 4.5.29. Gyakorlatban már közvetlenül beláttunk). Megjegyezzük, hogy a modularitás valójában hálóazonosság. Ezt az azonosságot úgy kaphatjuk meg, ha a fenti egyenlőségben z helyére $x \vee u$-t írunk (mert akkor az $x \leq z = x \vee u$ feltétel fölöslegessé válik). Ezért moduláris hálók részhálója, direkt szorzata és homomorf képe is moduláris.



8.8. Ábra. A tipikus helyzet, amikor a modularitás nem teljesül.

8.6.8. Gyakorlat. Igazoljuk az alábbi állításokat.

(1) Minden disztributív háló moduláris.
(2) A modularitás definíciójában elég az $(x \vee y) \wedge z \leq x \vee (y \wedge z)$ egyenlőtlenséget megkövetelni.
(3) Ha a (2)-beli egyenlőtlenséget nemcsak $x \leq z$-re, hanem minden x, y, z-re megköveteljük, akkor a disztributivitás fogalmát kapjuk.

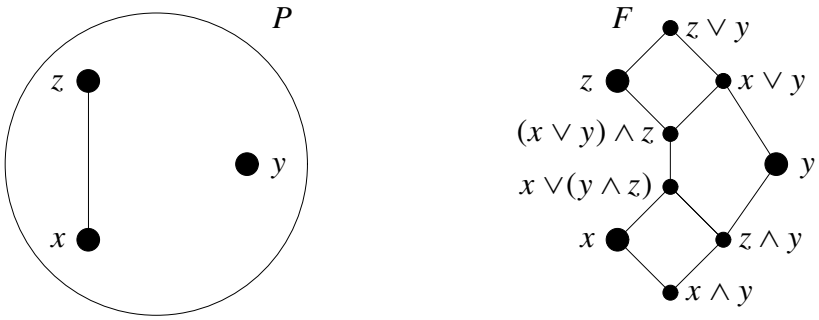
8.6.9. Gyakorlat. Mutassuk meg, hogy moduláris háló duálisa is moduláris.

A 8.8. Ábrán látható N_5 háló nemcsak a moduláris azonosság megjegyzéséhez nyújt segítséget: tényleg ez az egyetlen „tilos” konfiguráció, a következő tétel szerint.

8.6.10. Tétel [Dedekind tétele]. *Az L háló akkor és csak akkor moduláris, ha nincs az N_5 hálóval izomorf részhálója.*

A bizonyításhoz egy önmagában is fontos segédállításra lesz szükségünk.

8.6.11. Tétel. *A 8.9. Ábrán látható F hálóra igaz a következő. Ha $a \le c$ és b egy tetszőleges L háló elemei, akkor van olyan $\varphi : F \to L$ háló-homomorfizmus, amelyre $\varphi(x) = a$, $\varphi(y) = b$ és $\varphi(z) = c$.*



8.9. Ábra. Az $x \le z$ és y elemek által generált „legszabadabb” háló.

A tétel bizonyítása hasonló a három elemmel generált szabad disztributív hálót (8.7. Tétel), illetve a három elemmel generált szabad moduláris hálót (8.10. Tétel) leíró állítások bizonyításához. A három számolás közül a mostani a legegyszerűbb, ezért csak ezt mutatjuk be.

Bizonyítás. Elsőként azt gondoljuk végig, hogy a rajzon tényleg háló szerepel, amelyben a címkék azok, amiket az elemek mellé írtunk. Ehhez az összes elempárnak meg kell keresni az egyesítését és a metszetét, és belátni, hogy a címkék „stimmelnek”.

Azt, hogy hálóról van szó, úgy is beláthatjuk, hogy az $\{1, 2, 3, 4, 5, 6\}$ halmaz partícióhálójában kiszámítjuk az $x = 12$, $z = 12|3456$, $y = 13|24|56$ esetében az ábrán szereplő kilenc címkének megfelelő partíciót, és ellenőrizzük, hogy ezek F-fel izomorf részhálót alkotnak.

Most tegyük föl, hogy L tetszőleges háló, és $a, b, c \in L$, melyekre $a \le c$. Készítsük el a rajzon látható kilenc címkézett elemnek megfelelő

$$\begin{array}{ccccccccccc} x \wedge y, & & x, & & z \wedge y, & x \vee (y \wedge z), & y, & (x \vee y) \wedge z, & z, & x \vee y, & z \vee y \\ \downarrow & & \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ a \wedge b, & & a, & & c \wedge b, & a \vee (b \wedge c), & b, & (a \vee b) \wedge c, & c, & a \vee b, & c \vee b \end{array}$$

elemeket L-ben, és legyen φ a lefelé menő nyilakkal megadott megfeleltetés. A felsorolt elemek nem feltétlenül különbözők, például ha $a = b = c$, akkor mind a kilenc egybeesik.

Próbáljuk meg kiszámítani ezeknek az elemeknek a metszeteit és egyesítéseit pusztán a hálók definíciójában szereplő azonosságokra és az $a \leq c$ egyenlőtlenségre támaszkodva. Például az $a \vee (b \wedge c)$ és a b egyesítése $a \vee b$ lesz, hiszen az elnyelési tulajdonság miatt

$$[a \vee (b \wedge c)] \vee b = a \vee [(b \wedge c) \vee b] = a \vee b\,.$$

Másik példaként $a \leq (a \vee b) \wedge c$ nyilván következik $a \leq c$-ből, és így e két elem metszete biztosan a lesz. Ezek a számolások persze az F hálóban is érvényesek, az $x = a$, $y = b$, $z = c$ speciális esetben azt kapjuk, hogy például

$$[x \vee (y \wedge z)] \vee y = x \vee y\,.$$

Ez viszont azt jelenti, hogy

$$\varphi\big([x \vee (y \wedge z)] \vee y\big) = \varphi\big(x \vee (y \wedge z)\big) \vee \varphi(y)\,.$$

Tehát φ tartja ennek a két elemnek az egyesítését. A tétel állítása azon múlik, hogy ilyen módon bármely két elem egyesítése és metszete kiszámítható (csak $a \leq c$-re támaszkodva, és úgy, hogy az eredmény a felsorolt kilenc elem között legyen). Ennek ellenőrzését az Olvasóra hagyjuk. □

A tételben szereplő háló persze nem szabad a 8.3.24. Definíció értelmében már saját maga fölött sem, hiszen az $x \leq z$ elemeket csakis összehasonlítható elemekbe képezhetjük. A hálóelméletben azonban szokás egy P részben rendezett halmaz által „szabadon” generált F hálóról beszélni: azt követeljük meg, hogy P-nek minden L hálóba menő rendezéstartó leképezése kiterjeszthető legyen egy $F \to L$ homomorfizmussá. Ebben az értelemben az 8.9. Ábrán megadott P pontosan az F-et generálja szabadon.

Korábbi tanulmányainkhoz közelebb áll egy másik szemléletmód. Az F háló valójában az $x \wedge z = x$ feltételhez „képest” szabad. Ez a jelenség ismerős csoportelméletből: például az $f^3 = 1 = t^2$ és $ft = tf^{-1}$ feltételek mellett a „legszabadabb” f és t által generált csoport a D_3 diédercsoport (4.9.10. Állítás). A fenti tételt tehát úgy is felfoghatjuk, hogy az $x \wedge z = x$ definiáló relációval megadott szabad háló elemeit számoltuk ki. Az Olvasó különösebb erőfeszítés nélkül megadhatja a definiáló reláció fogalmát tetszőleges varietásban, és bebizonyíthatja a csoportelméletben tanult 4.9.13. Tételnek, valamint Dyck tételének (4.9.16. Következmény) az általánosítását.

8.6.12. Feladat. Mutassuk meg, hogy a három elemmel generált szabad hálónak végtelen sok eleme van.

Most már be tudjuk látni a 8.6.10. Tételt.

Bizonyítás. Az N_5 hálóban a 8.8. Ábrán x, y, z-vel jelölt elemekre $(x \vee y) \wedge z = z$ és $x \vee (y \wedge z) = x$, tehát N_5 nem moduláris. Ezért olyan háló nem lehet moduláris, amelynek N_5 részhálója (hiszen a moduláris hálók varietást alkotnak).

Megfordítva, tegyük föl, hogy L nem moduláris, vagyis van olyan $a, b, c \in L$, melyekre $a \leq c$, de $a \vee (b \wedge c) \neq (a \vee b) \wedge c$. Tekintsük a 8.6.11. Tételben szereplő „szabad” F hálót, és ennek a tételben megadott φ homomorfizmusát L-be. A feltétel szerint az

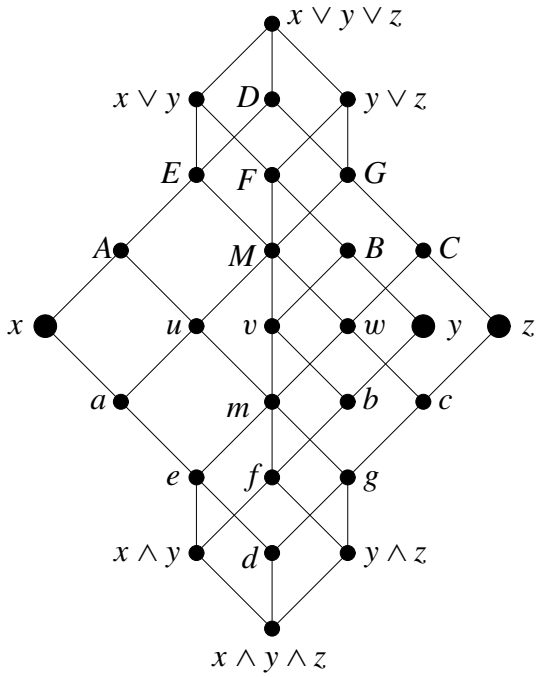
$u = x \vee (y \wedge z)$ és a $v = (x \vee y) \wedge z$ elemek képe φ-nél különböző, vagyis ez a két elem nem kongruens a $\theta = \mathrm{Ker}(\varphi)$ kongruenciánál.

Az F hálóban a $K = \{z \wedge y,\ u,\ y,\ v,\ x \vee y\}$ elemek egy N_5-tel izomorf részhálót alkotnak, jelölje ρ a θ kongruencia megszorítását a K részhálóra. A 8.4.18. Gyakorlat megoldásában láttuk, hogy a $K \cong N_5$ háló szubdirekt irreducibilis, és a legkisebb nem nulla kongruenciájánál u és v egy osztályban vannak. Ezért ha $\rho \neq 0_K$ lenne, akkor $u \equiv v\ (\rho)$, ami lehetetlen, hiszen u és v nem kongruensek θ-nál. Ezért $\rho = 0_K$, vagyis a φ homomorfizmus a K elemeit az L-nek csupa különböző elemeibe viszi. Ezek tehát L-ben egy N_5-tel izomorf részhálót alkotnak. □

A fenti bizonyítás az eddig tanult fogalmak szép összjátéka. Elmondható lenne ezek nélkül is, közvetlen számolással, de akkor kevesebbet látnánk a bizonyítás lényegéből, abból, hogy miért is igaz a tétel (például miért fontos az, hogy N_5 szubdirekt irreducibilis). Így a szükséges számolások két külön modulba lettek koncentrálva, amelyek később is felhasználhatók.

Dedekind 8.6.10. Tételéből szintén következik a 8.6.9. Gyakorlatban már belátott állítás, hogy moduláris háló duálisa is moduláris, hiszen az N_5 háló duálisa önmaga.

8.6.13. Tétel. *A három elemmel generált szabad moduláris háló elemszáma* 28*, rajza a 8.10. Ábrán látható.*



$D = x \vee z$
$E = (x \vee y) \wedge (x \vee z)$
$F = (y \vee x) \wedge (y \vee z)$
$G = (z \vee x) \wedge (z \vee y)$
$A = x \vee (y \wedge z)$
$B = y \vee (x \wedge z)$
$C = z \vee (x \wedge y)$
$M = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$
$u = [x \wedge (y \vee z)] \vee (y \wedge z)$
$v = [y \wedge (x \vee z)] \vee (x \wedge z)$
$w = [z \wedge (x \vee y)] \vee (x \wedge y)$
$m = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$
$a = x \wedge (y \vee z)$
$b = y \wedge (x \vee z)$
$c = z \wedge (x \vee y)$
$e = (x \wedge y) \vee (x \wedge z)$
$f = (y \wedge x) \vee (y \wedge z)$
$g = (z \wedge x) \vee (z \wedge y)$
$d = x \wedge z$

8.10. Ábra. Az x, y és z által generált szabad moduláris háló.

Ezt a tételt ugyanúgy kell bizonyítani, mint a 8.6.11. Tételt, vagyis bármely két felsorolt „címke” egyesítéséről és metszetéről meg kell mutatni, hogy szintén szerepel a „címkék”

között, és a számolásokban csak a moduláris szabályt használhatjuk. Míg a disztributivitást könnyű alkalmazni, mert középiskolában ezt a szabályt (valós számokra és polinomokra is) begyakoroltuk, addig a moduláris szabály alkalmazásában kevesebb a rutinunk. Ezért azt javasoljuk, hogy az Olvasó, ha nem is számolja ki az összes egyesítést és metszetet, oldja meg az alábbi gyakorlatot.

8.6.14. Gyakorlat. Mutassuk meg, hogy ha x, y, z elemei az L moduláris hálónak, akkor

$$[x \wedge (y \vee z)] \vee [z \wedge (x \vee y)] = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)\,.$$

A csoportoknál már meséltünk arról, hogy a szóprobléma eldönthetetlen, azaz megadhatunk úgy definiáló relációkat, hogy ne létezzen olyan algoritmus, amely eldöntené, hogy két adott szót egymásba alakíthatunk-e, vagy sem (lásd 208. oldal). Azt, hogy a moduláris azonossággal milyen nehéz számolni, mi sem bizonyítja jobban, mint hogy hasonló eredmény érvényes ebben az esetben is.

Tegyük föl, hogy adott egy $t_1(x_1, \ldots, x_n) \approx t_2(x_1, \ldots, x_n)$ háló-azonosság, és azt szeretnénk eldönteni, hogy érvényes-e minden moduláris hálóban, vagyis hogy következik-e a moduláris azonosságból. Ha csak három változó van, akkor egyszerű a dolog: mindkét oldalt kiszámoljuk az imént lerajzolt, három elemmel generált szabad moduláris hálóban úgy, hogy x_1, x_2, x_3 helyére az x, y, z generátorokat helyettesítjük. Ha a hálónak ugyanaz az eleme jön ki, akkor az azonosság következik a modularitásból, egyébként nem (8.4.6. Gyakorlat).

A négyváltozós esetben a helyzet gyökeresen megváltozik. A négy elemmel generált szabad moduláris háló nemcsak hogy végtelen (8.6.32. Gyakorlat), hanem algoritmus sincs, ami eldöntené, hogy a négyváltozós esetben t_1 és t_2 a moduláris szabályt felhasználva egymásba alakítható-e. Ne feledjük, hogy itt nem tetszőleges definiáló relációkról, hanem *csak* a moduláris szabályról van szó. Az eredményt a következő, nehéz tétel foglalja össze.

8.6.15. Tétel [Freese–Herrmann-tétel]. *A legalább négy elemmel generált szabad moduláris háló szóproblémája eldönthetetlen.*

A tételt természetesen nem bizonyítjuk. Belátjuk viszont a következő állítást, amely a disztributív hálókat jellemzi tiltott részhálók segítségével.

8.6.16. Tétel [Birkhoff]. *Egy háló akkor és csak akkor disztributív, ha nincs a 8.3. Ábrán látható M_3 és N_5 hálók egyikével sem izomorf részhálója.*

Bizonyítás. Az N_5 és M_3 hálók nem disztributívak (8.5.3. Gyakorlat), és így egyetlen disztributív hálónak sem lehetnek részhálói. Megfordítva, tegyük föl, hogy az L hálónak nem részhálója az M_3 és az N_5. A 8.6.10. Tétel miatt L moduláris. Tegyük föl, hogy L nem disztributív, vagyis van olyan $r, s, t \in L$, melyre

$$r \vee (s \wedge t) \neq (r \vee s) \wedge (r \vee t)\,.$$

Tekintsük a 8.6.13. Tételben szereplő F hálót. Mivel L moduláris és F szabad, van olyan $\varphi : F \to L$ homomorfizmus, melynél x, y, z képe rendre $r, s, t \in L$. A 8.10. Ábra jelöléseivel a fenti egyenlőtlenség azt jelenti, hogy $\varphi(A) \neq \varphi(E)$, vagyis A és E nem kongruens a $\theta = \mathrm{Ker}(\varphi)$ kongruenciánál. Emiatt $u \not\equiv M\ (\theta)$, mert ha $u \equiv M\ (\theta)$ lenne, akkor ezt a kongruenciát A-val egyesítve $A \equiv E\ (\theta)$ adódna.

Az F hálóban a $K = \{m, u, v, w, M\}$ elemek egy M_3-mal izomorf részhálót alkotnak, jelölje ρ a θ kongruencia megszorítását a K részhálóra. A 8.2.37. Gyakorlat megoldásában láttuk, hogy a $K \cong M_3$ háló egyszerű. Mivel $u \not\equiv M$ (ρ), a ρ csak a K nulla kongruenciája lehet. Így a φ homomorfizmus a K elemeit az L-nek csupa különböző elemeibe viszi. Ezek tehát L-ben egy M_3-mal izomorf részhálót alkotnak. □

A csoportelméleti első izomorfizmus-tétel analogonjának tekinthető a moduláris hálók intervallum-izomorfizmus tétele. Ennek segítségével lehetővé válik majd a 4.12.3. Jordan–Hölder-tétel hálóelméleti általánosítása. Ha G csoport, és A, B normálosztók G-ben, akkor az első izomorfizmus-tétel szerint $AB/B \cong A/(A \cap B)$. Természetesen A és B egyesítése AB a normálosztók hálójában. Ezért AB/A felfogható úgy, mint a G csoport „B és AB közötti darabja”, és hasonlóan $B/(A \cap B)$, mint a G-nek az „$A \cap B$ és A közötti darabja”.

8.6.17. Definíció. Ha L háló és $a, b \in L$, akkor $[a, b] = \{x \in L : a \leq x \leq b\}$ az $[a, b]$ *intervallum*.

Nyilván minden intervallum részháló.

8.6.18. Tétel [Intervallum-izomorfizmus tétel]. *Legyen L moduláris háló és $a, b \in L$. Ekkor $[b, a \vee b] \cong [a \wedge b, a]$ izomorf részhálói L-nek.*

Ezt a két intervallumot geometriai ihletéssel szokás *perspektívnek* is nevezni.

Bizonyítás. A $\varphi(x) = x \vee b$ leképezés az $[a \wedge b, a]$ intervallumot a $[b, a \vee b]$ intervallumba képezi rendezéstartó módon (hiszen $\varphi(a \wedge b) = b$ az elnyelési tulajdonság miatt). Ugyanígy, a $\psi(x) = x \wedge a$ leképezés a $[b, a \vee b]$ intervallumot képzi az $[a \wedge b, a]$ intervallumba. Elegendő belátni, hogy φ és ψ egymás inverzei, mert akkor mindkettő rendezéstartó bijekció, és így háló-izomorfizmus.

Ha $a \wedge b \leq x \leq a$, akkor

$$\psi\varphi(x) = (x \vee b) \wedge a = x \vee (b \wedge a) = x$$

a moduláris szabály miatt (az utolsó egyenlőség $x \geq (a \wedge b)$ miatt teljesül). Ezért $\psi \circ \varphi$ az identitás. A $\varphi \circ \psi = id$ összefüggés ennek duálisa, ha a-t és b-t megcseréljük. Mivel moduláris háló duálisa is moduláris (8.6.9. Gyakorlat), ez is teljesül. □

Most pontosítjuk a lemma előtti megjegyzést. Ha A és B normálosztók a G csoportban, akkor a lemma szerint a G-nek a B és AB közötti normálosztóinak hálója izomorf a G-nek az $A \cap B$ és A közötti normálosztóinak hálójával. Ha G Abel-féle, akkor persze mindkét háló izomorf az $AB/B \cong A/(A \cap B)$ normálosztóhálójával, de általában nem feltétlenül (hiszen az AB normálosztói nem feltétlenül normálosztói G-nek is).

Ez a jelenség gondot okoz a Jordan–Hölder-tétel általánosításában. A tétel ugyanis kompozícióláncokról szól, és ezeknél csak azt tesszük föl, hogy a lánc minden eleme a lánc eggyel nagyobb indexű elemében normálosztó. Tehát a lánc elemei általában nincsenek is benne a csoport normálosztóhálójában. Így az általánosítás során kompozícióláncok helyett normálosztók olyan láncaira kell gondolnunk, ahol csupa fedések szerepelnek (ezeket a csoportelméletben *főláncnak* nevezik).

8.6.19. Definíció. Legyen L háló és $a \leq b \in L$. Az

$$a = a_0 < a_1 < \ldots < a_n = b$$

sorozatot a és b közötti láncnak nevezzük, amelynek a *hossza* n. A fenti lánc *maximális*, ha $0 \leq i < n$ esetén $a_i \prec a_{i+1}$ (vagyis a_{i+1} fedi a_i-t). Az $[a, b]$ intervallum *hossza* az a és b közötti leghosszabb (maximális) lánc hossza (illetve ∞, ha nincs leghosszabb lánc). Az $[a, b]$ intervallum hosszát $\delta(a, b)$ jelöli.

Példaként érdemes megvizsgálni, hogy az A_4 alternáló csoport esetében mi a helyzet. A 4.12.1. Definíció után láttuk, hogy az A_4 egyik kompozíciólánca

$$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 .$$

Itt $\{id, (12)(34)\}$ nem normálosztója A_4-nek, tehát ez a lánc a normálosztóhálóban „nem is látszik". Ugyanakkor a normálosztóhálóban maximális lánc (azaz A_4 főlánca)

$$\{id\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 .$$

Ezt a példát érdemes szem előtt tartani, ha az alábbi tételt egy csoport normálosztóhálójára akarjuk alkalmazni. Ugyanilyen probléma Abel-csoportok, vagy általánosabban modulusok esetében persze nem lép föl.

8.6.20. Tétel [Jordan–Dedekind-tétel]. *Legyen L moduláris háló és $a \leq b \in L$. Ha létezik a és b között maximális lánc, melynek hossza n, akkor mindegyik a és b közötti lánc hossza legfeljebb n, és minden a és b közötti maximális lánc hossza pontosan n. Speciálisan minden lánc kibővíthető maximális lánccá.*

A bizonyítás ugyanaz a kombinatorikus jellegű indukció, mint a Jordan–Hölder-tétel bizonyításában (ahol az első izomorfizmus-tételt az intervallum-izomorfizmus tétel helyettesíti), és ezért azt az Olvasóra hagyjuk.

Ha a Jordan–Hölder-tételnek a 4.12. Szakaszban látott bizonyítását lefordítjuk a moduláris hálók nyelvére, akkor valójában csak annyi adódik, hogy a és b között minden maximális lánc hossza ugyanaz. Ettől elvileg előfordulhatna, hogy a és b között van egy ennél sokkal hosszabb lánc is, csak éppen az nem része egyetlen maximális láncnak sem. A 4.12.4. Lemma hálóelméleti változata segítségével azonban ezt a lehetőséget könnyen kizárhatjuk. Ennek meggondolását szintén az Olvasóra hagyjuk.

8.6.21. Gyakorlat. Mutassuk meg, hogy ha a G csoportnak van főlánca, akkor minden főlánca ezzel csoportelméleti értelemben is izomorf (4.12.2. Definíció).

8.6.22. Definíció. Legyen L nullelemes moduláris háló. Ekkor az $a \in L$ elem *magassága* a $[0, a]$ intervallum $d(a) = \delta(0, a)$ hossza. A d függvény neve L magasságfüggvénye, vagy *dimenziófüggvénye*.

Az elnevezést az indokolja, hogy egy vektortér altereinek (moduláris) hálójában egy altér magassága a dimenziójával egyezik meg. Így végtelen hálóban is lehet minden elem magassága véges.

8.6.23. Definíció. Egy nullelemes hálót *véges magasságúnak* nevezünk, ha van olyan n egész szám, hogy minden elem magassága legfeljebb n.

A Jordan–Dedekind-tétel miatt egy moduláris háló akkor és csak akkor véges magasságú, ha egységelemes, és az egységelem magassága véges. Az alterek összegének dimenziójára vonatkozó, lineáris algebrában tanult összefüggés moduláris hálókban is érvényes.

8.6.24. Állítás. *Legyen L nullelemes moduláris háló. Ha a és b véges magasságú elemek L-ben, akkor*

$$d(a \vee b) = d(a) + d(b) - d(a \wedge b)\,.$$

Ez a dimenzió-egyenlőség.

Bizonyítás. A Jordan–Dedekind-tétel miatt a $0 \leq a \wedge b \leq b$ lánc kiegészíthető maximális lánccá. Ennek a 0 és az $a \wedge b$, továbbá az $a \wedge b$ és b közötti darabja is maximális lánc, tehát $d(b) = d(a \wedge b) + \delta(a \wedge b, b)$. Ugyanígy $d(a) = d(a \wedge b) + \delta(a \wedge b, a)$, ezért

$$d(a) + d(b) - d(a \wedge b) = d(a \wedge b) + \delta(a \wedge b, a) + \delta(a \wedge b, b)\,.$$

Az intervallum-izomorfizmus tétel miatt $\delta(b, a \vee b) = \delta(a \wedge b, a)$, speciálisan $[b, a \vee b]$ is véges hosszúságú. Az előző 0-tól b-ig tartó lánccal kombinálva kapjuk, hogy $a \vee b$ magassága is véges, és $d(a \vee b) = d(b) + \delta(b, a \vee b)$. Így az előbbi egyenlőségekből az állítás adódik. □

Utolsó moduláris hálókról szóló tételünk az 5.11.6 Noether–Lasker-tételhez (valójában a számelmélet alaptételéhez) kapcsolódik. A Noether–Lasker-tétel azt vizsgálja, hogy egy gyűrű ideáljai milyen feltételek mellett bonthatók föl úgynevezett primér ideálok metszetére. Meg lehet mutatni, hogy ha egy ideál csak triviálisan bontható föl két ideál metszetére, akkor primér (pontosan ez a Noether–Lasker-tétel bizonyításának a lényege).

8.6.25. Definíció. Az L háló m eleme *metszet-irreducibilis*, ha $a \wedge b = m$-ből $a = m$ vagy $b = m$ következik minden $a, b \in L$ esetén. Az *egyesítés-irreducibilitás* a duális fogalom.

Teljes hálóban egy elemet *teljesen metszet-irreducibilisnek* nevezünk, ha végtelen metszetként is csak triviálisan állítható elő. Például egy algebra akkor és csak akkor szubdirekt irreducibilis, ha a 0 kongruenciája teljesen metszet-irreducibilis (8.4.14. Lemma).

8.6.26. Tétel [Kuros–Ore-tétel]. *Tegyük föl, hogy L tetszőleges háló.*

(1) *Ha L-ben igaz a maximum-feltétel, vagyis L elemeinek tetszőleges nem üres H halmazából kiválasztható egy m maximális elem (vö. 5.4.3. Tétel), akkor L minden eleme előáll véges sok metszet-irreducibilis elem metszeteként.*

(2) *Tegyük föl, hogy L moduláris háló, és a $b \in L$ elem kétféleképpen is felbontható metszet-irreducibilis elemek rövidíthetetlen metszetére. Ekkor a két felbontásban a tagok száma megegyezik. (A rövidíthetetlen metszet azt jelenti, hogy a felbontás egyik eleme se hagyható el úgy, hogy a metszet még mindig b maradjon.)*

Bizonyítás. Az (1) állítás bizonyítása szó szerint ugyanaz, mint amikor az 5.5.7. Tételben a főideálokra vonatkozó maximum-feltételből beláttuk, hogy minden elem felbomlik irreducibilisek szorzatára (csak most az elemek közé szorzásjel helyett metszet jelet kell írni). Ezért ezt a bizonyítást az Olvasóra hagyjuk. A (2) állítást az intervallum-izomorfizmus tételből lehet megkapni (lásd a következő feladat megoldását). □

8.6.27. Feladat. Bizonyítsuk be a 8.6.26. Kuros–Ore-tétel (2) állítását.

A moduláris hálókra nemcsak egy vektortér alterei adnak fontos példát, hanem a tér pontjaiból, egyeneseiből, síkjaiból és magából a térből álló részben rendezett halmaz is (lásd 8.6.32. Gyakorlat). Ehhez azonban projektív teret kell elképzelnünk (vagyis az úgynevezett „ideális" pontokat hozzá kell vennünk a térhez, mert ha két párhuzamos egyenes metszetét üresnek vennénk, akkor a kapott háló nem lenne moduláris). Mindezt általánosíthatjuk magasabb dimenziókra, és a valós helyett más testekre is. A kapott hálókról meg lehet mutatni, hogy nemcsak modulárisak, hanem egyszerűek is lesznek. Ennek a tételnek a megfordítását (megfelelő feltételek fennállása esetén) Neumann János bizonyította be.

Gyakorlatok, feladatok

8.6.28. Gyakorlat. Melyek modulárisak a 8.3. Ábrán lerajzolt hálók közül?

8.6.29. Gyakorlat. Mutassuk meg, hogy moduláris hálóban nem lehet egy elemnek két különböző, összehasonlítható komplementuma.

8.6.30. Gyakorlat. Igazoljuk, hogy komplementumos moduláris háló minden intervalluma szintén komplementumos.

8.6.31. Gyakorlat. Mutassuk meg, hogy ha egy véges magasságú hálóban a magasságfüggvény teljesíti a dimenzió-egyenlőséget (8.6.24. Állítás), akkor a háló moduláris.

Így véges magasságú hálóban az intervallum-izomorfizmus tételből is következik a modularitás, hiszen a dimenzió-egyenlőség bizonyításához (sőt a Jordan-Dedekind tétel bizonyításához is) csak az intervallum-izomorfizmus tételt használtuk.

8.6.32. Gyakorlat. A valós projektív síkon tekintsük a pontok és az egyenesek halmazát. Mutassuk meg, hogy ezek az üres halmazzal és az egész síkkal kiegészítve egy moduláris L hálót alkotnak a tartalmazásra. Egyszerű-e az L? Négy általános helyzetű pont hány elemű részhálót generál? Mit mondhatunk ennek alapján a négy elemmel generált szabad moduláris háló elemszámáról?

8.6.33. Feladat. Bizonyítsuk be, hogy ha egy L véges magasságú moduláris hálóban az atomok egyesítése az L egységeleme, akkor L komplementumos, és L minden eleme atomok egyesítése.

Részmodulusokat akkor neveztünk függetlennek, ha összegük direkt összeg, vagyis mindegyik nullában metszi a többiek összegét (7.2.3. Gyakorlat, 8.6.34. Feladat). Hasonló elnevezés a Kuros–Ore-tétel bizonyítása kapcsán is fölmerült (lásd a 8.6.27. Feladat megoldása utáni megjegyzéseket). A következő feladatban ezeket a fogalmakat kapcsoljuk össze.

8.6.34. Feladat. Egy nullelemes L moduláris háló $a_1, \ldots, a_n$ elemeit *függetlennek* nevezzük, ha mindegyik nullában metszi a többiek egyesítését. Igazoljuk az alábbi állításokat.

(1) Ha $a_1, \ldots, a_n$ atomok, és egyesítésük rövidíthetetlen, akkor függetlenek.
(2) Ha $a_1, \ldots, a_n$ független, és az a elem nullában metszi az egyesítésüket, akkor $a_1, \ldots, a_n, a$ is független.
(3) Ha $a_1, \ldots, a_n$ függetlenek, akkor az általuk generált részháló disztributív, komplementumos (vagyis Boole-háló), elemszáma 2^n, és atomjai pontosan az a_i elemek.

Ezeknek az állításoknak a segítségével adjunk új megoldást a 8.6.33. Feladatra.

8.6.35. Feladat. Igazoljuk, hogy ha az A algebra eleme egy kongruencia-felcserélhető varietásnak, és $B \leq A \times A$ reflexív részalgebra (vagyis tartalmazza az (a, a) alakú párokat), akkor B kongruenciája A-nak.

8.6.36. Feladat. Igazoljuk, hogy ha A a B és C algebrák szubdirekt szorzata egy kongruencia-felcserélhető varietásban, akkor van olyan θ kongruencia B-n, olyan ρ kongruencia C-n, és egy $\varphi : B/\theta \to C/\rho$ izomorfizmus úgy, hogy $A = \{(b, c) \mid \varphi(b/\theta) = c/\rho\}$.

8.6.37. Feladat. Bizonyítsuk be, hogy ha egy kongruencia-felcserélhető varietásban az A algebra előáll véges sok egyszerű algebra szubdirekt szorzataként, akkor A izomorf a tényezők közül néhánynak a direkt szorzatával. Speciális esetként adjunk új bizonyítást arra az állításra, hogy minden véges Boole-algebra izomorf a kételemű Boole-algebra egy direkt hatványával (vö. 8.5.26. Feladat).

Ha $R_1, \ldots, R_n$ egyszerű gyűrűk (például teljes mátrixgyűrűk), akkor az előző feladat szerint minden szubdirekt szorzatuk izomorf néhány tényező direkt szorzatával. Ennek az észrevételnek fontos szerep jut a Wedderburn–Artin-tétel (5.12.4. Tétel) bizonyításában.

8.6.38. Feladat. Igazoljuk, hogy ha a G csoport direkt négyzetének részcsoporthálója moduláris, akkor G-ben minden részcsoport normálosztó.

Azokat a csoportokat, amelyeknek mindegyik részcsoportja normálosztó, *Hamilton-féle csoportoknak* nevezzük. Meg lehet mutatni, hogy egy véges csoport pontosan akkor ilyen, ha vagy kommutatív, vagy a nyolcelemű kvaterniócsoportnak, egy elemi Abel-féle 2-csoportnak és egy páratlan rendű Abel-csoportnak a direkt szorzata.

8.7. Galois-kapcsolat és fogalom-analízis

A Galois-kapcsolat rendezésfordító megfeleltetést biztosít két halmaz bizonyos, úgynevezett zárt részhalmazai között. Az algebrában sok helyen előfordul, legnevezetesebb példa rá a Galois-elmélet főtétele, ahol a közbülső testek és a Galois-csoport részcsoportjai között van ilyen kapcsolat. De Galois-kapcsolat áll fenn a $T^{n\times n}$ teljes mátrixgyűrű balideáljai és a T^n vektortér alterei között is, ami ezeknek a balideáloknak az áttekintését teszi lehetővé.

A Galois-kapcsolatok elméletét a Rudolf Wille vezette darmstadti iskola matematikusai oly módon fejlesztették tovább, hogy az alkalmasnak bizonyult az élet számos területén (az iparban, a zenében, a tudományban) felmerülő fogalmak formális matematikai elemzésére. A szakasz második felében ebből az alkalmazásból adunk ízelítőt.

8.7.1. Példa. Tekintsük az alábbi A és B halmazokon értelmezett páros gráfokat (lásd A.2.6. Definíció).

(1) Legyen $A = L$ egy test, K részteste L-nek, és $B = G(L/K)$ a $K \leq L$ bővítés Galois-csoportja. Az $a \in A$ testelemet akkor kötjük össze a $b \in B$ automorfizmussal, ha a fixpontja b-nek, vagyis ha $b(a) = a$.
(2) Legyen T test és $A = B = T^n$. Nevezzük a T^n vektortér a és b vektorait ortogonálisnak, képletben $a \perp b$, ha a szokásos skaláris szorzatuk nulla (vagyis $\lambda_1\mu_1 + \ldots + \lambda_n\mu_n = 0$, ahol a λ_i az a a μ_i a b vektor komponensei). Kössük össze A és B egy-egy elemét, ha ortogonálisak.
(3) Legyen A a T test fölötti $n \times n$-es mátrixok halmaza, B pedig a T^n oszlopvektorainak halmaza. Kössük össze az $a \in A$ mátrixot a $b \in B$ vektorral, ha a kettő szorzata, $ab = 0$.
(4) Legyen A a T test fölötti $T[x_1, \ldots, x_n]$ polinomgyűrű, B pedig T^n (amelynek elemeit pontoknak képzeljük). Kössük össze az a polinomot a b ponttal, ha b gyöke a-nak, vagyis ha $a(b) = 0$.
(5) Legyen A egy C halmazon értelmezett véges változós függvények halmaza, B pedig a C halmazon értelmezett véges változós relációk halmaza (ezek C véges direkt hatványainak részhalmazai). Kössük össze az $a \in A$ függvényt a $b \in B$ relációval, ha a megőrzi b-t (lásd 8.3.12. Definíció).

Az (1) példában ha $K \leq T \leq L$ közbülső test, akkor a hozzá tartozó részcsoport azoknak az automorfizmusoknak a halmaza, amelyek T minden elemét fixen hagyják (vagyis a fenti gráfban T minden elemével össze vannak kötve). Ugyanígy, ha H részcsoportja a Galois-csoportnak, akkor a hozzá tartozó közbülső test a H közös fixpontjainak a halmaza, vagyis azoknak az A-beli pontoknak a halmaza, amelyek H minden elemével össze vannak kötve.

8.7.2. Definíció. Legyen $G = (A, B, E)$ páros gráf. Ha $X \subseteq A$, akkor álljon $X^\sharp \subseteq B$ azokból az elemekből, amelyek az X valamennyi elemével össze vannak kötve. Ugyanígy $U \subseteq B$ esetén álljon $U^\flat \subseteq A$ azokból az elemekből, amelyek az U valamennyi elemével össze vannak kötve.

Ha az (1) példában $X \subseteq A$, akkor $X^\sharp$ nyilvánvalóan részcsoport (akkor is, ha X nem közbülső test), hiszen ha két automorfizmus fixen hagyja X elemeit, akkor a kompozíciójuk és az inverzeik is. Ugyanígy $U \subseteq B$ esetén $U^\flat$ mindenképpen közbülső test. Ez az észrevétel mutatja, hogy ha még nem ismernénk a „részcsoport” illetve a „közbülső test” fogalmát, akkor hogyan jöhetnénk ezekre rá a fenti gráfból. Az általános esetben az ilyen részhalmazokat zártaknak fogjuk nevezni.

8.7.3. Definíció. Tekintsük a $G = (A, B, E)$ páros gráfhoz tartozó $\sharp$ és $\flat$ leképezéseket. A $V \subseteq B$ halmazt *zártnak* nevezzük, ha előáll $V = X^\sharp$ alakban alkalmas $X \subseteq A$-ra. Ugyanígy $Y \subseteq A$ zárt, ha előáll $Y = U^\flat$ alakban alkalmas $U \subseteq B$-re.

A Galois-elmélet főtétele (6.6.7. Tétel) azt mondja ki, hogy a $T \mapsto T^\sharp$ és a $H \mapsto H^\flat$ leképezések a közbülső testek, illetve a részcsoportok halmazán egymás inverzei. A bizonyítás valójában a következőképpen halad. Először megmutatjuk, hogy minden közbülső test, illetve részcsoport tényleg zárt halmaz (ez a nehéz rész, ami a testek és a csoportok elméletét használja). Ha ezen túl vagyunk, akkor a bizonyítás befejezése már egyszerű kombinatorika. Ezt fejezi ki az alábbi tétel, amit később bebizonyítunk.

8.7.4. Tétel. *Legyen $G = (A, B, E)$ páros gráf. Ekkor az A és a B zárt részhalmazai egy-egy teljes hálót alkotnak, és az $A \supseteq Y \mapsto Y^\sharp$, illetve a $B \supseteq V \mapsto V^\flat$ leképezések kölcsönösen egyértelmű és rendezésfordító megfeleltetést létesítenek az A és a B zárt részhalmazai között (más szóval ez a két háló „duálisan" izomorf).*

A „rendezésfordító" jelző azt jelenti, hogy $X \subseteq Y \subseteq A$ esetén $X^\sharp \supseteq Y^\sharp$, és ugyanígy $U \subseteq V \subseteq B$ esetén $U^\flat \supseteq V^\flat$ (8.2.12. Definíció). Ez nyilván így van, hiszen ha A egy részhalmazát növeljük, akkor egyre kevesebb olyan elem lesz B-ben, amely ennek minden elemével össze van kötve ($Y^\sharp$ minden eleme össze van kötve X minden elemével is).

8.7.5. Definíció. A 8.7.4. Tételben leírt megfeleltetést *Galois-kapcsolatnak* nevezzük.

Az irodalomban nem egységes a „Galois-kapcsolat" elnevezés használata. Ebben a könyvben csak olyan Galois-kapcsolatokról lesz szó, amelyek egy páros gráfból származnak a fenti módon. Szokás azonban Galois-kapcsolatnak nevezni alkalmas $Y \mapsto Y^\sharp$ illetve $V \mapsto V^\flat$ megfeleltetéseket A illetve B bizonyos részhalmazai között abban az esetben is, ha ezek nem gráfból származnak, de eleget tesznek a 8.7.4. Tételben leírt tulajdonságoknak. Sőt, néha az A illetve B részhalmazai helyett általános részben rendezett halmazokból indulnak ki.

8.7.6. Lemma. *Legyen $G = (A, B, E)$ páros gráf, $X \subseteq A$ és $U \subseteq B$. Ekkor $X \subseteq X^{\sharp\flat}$ és $X^{\sharp\flat\sharp} = X^\sharp$. Hasonlóan $U \subseteq U^{\flat\sharp}$ és $U^{\flat\sharp\flat} = U^\flat$.*

Bizonyítás. Ha $a \in X$, akkor a össze van kötve $X^\sharp$ minden elemével, és ezért $a \in X^{\sharp\flat}$. Így tényleg $X \subseteq X^{\sharp\flat}$. Innen a rendezésfordítás miatt $X^\sharp \supseteq X^{\sharp\flat\sharp}$. Analóg módon kapjuk, hogy $U \subseteq U^{\flat\sharp}$ és $U^\flat \supseteq U^{\flat\sharp\flat}$. Speciálisan $U = X^\sharp$-ra az $U \subseteq U^{\flat\sharp}$ összefüggést alkalmazva $X^\sharp \subseteq X^{\sharp\flat\sharp}$ adódik. Ezért $X^{\sharp\flat\sharp} = X^\sharp$, és ugyanígy $U^{\flat\sharp\flat} = U^\flat$. □

8.7.7. Gyakorlat. Legyen $G = (A, B, E)$ páros gráf. Mutassuk meg az alábbi állításokat tetszőleges $X, Y \subseteq A$ esetén.

(1) Az X-et tartalmazó legszűkebb zárt halmaz $\overline{X} = X^{\sharp\flat}$, és ha $X \subseteq Y$, akkor $\overline{X} \subseteq \overline{Y}$.
(2) $\overline{\overline{X}} = \overline{X}$.
(3) Az X halmaz akkor és csak akkor zárt, ha $\overline{X} = X$.
(4) Zárt részhalmazok tetszőleges metszete zárt, és így $\overline{X}$ az X-et tartalmazó zárt halmazok metszete.

8.7.8. Definíció. Legyen $G = (A, B, E)$ páros gráf. A hozzá tartozó Galois-kapcsolatban az $X \subseteq A$ halmaz *lezártja* az $\overline{X} = X^{\sharp\flat} \subseteq A$ halmaz. Hasonlóan az $Y \subseteq B$ lezártja $\overline{Y} = Y^{\flat\sharp} \subseteq B$.

Most már be tudjuk látni a 8.7.4. Tételt.

Bizonyítás. Legyen $Y \subseteq A$ egy zárt részhalmaz, ekkor $Y^{\sharp\flat} = \overline{Y} = Y$, és hasonlóan ha $V \subseteq B$ zárt, akkor $V^{\flat\sharp} = \overline{V} = V$. Ezért a $\sharp$ és $\flat$ leképezések egymás inverzei az A, illetve a B zárt részhalmazain. A 8.7.7. Gyakorlat (4) pontja miatt A és B zárt részhalmazai is egy-egy teljes hálót alkotnak. □

A most bizonyítottak szerint tehát egy Galois-kapcsolatban az első dolgunk mindig annak kiderítése, hogy mik a zárt halmazok, mert ezzel egy hasznos megfeleltetést nyerünk. Most ezt a módszert illusztráljuk.

8.7.9. Gyakorlat. Mutassuk meg, hogy a 8.7.1. Példa (2) pontjában megadott gráfhoz tartozó Galois-kapcsolatban mind A, mind B zárt részhalmazai pontosan az alterek. Igazoljuk azt is, hogy ha W altér, akkor $W^\flat = W^\sharp$ dimenziója $n - \dim W$. (A $W^\flat = W^\sharp$ alteret a lineáris algebrában $W^\perp$ szokta jelölni.)

8.7.10. Feladat. Igazoljuk, hogy a 8.7.1. Példa (3) pontjában megadott gráfhoz tartozó Galois-kapcsolatban $T^{n\times n}$ zárt részhalmazai pontosan a balideálok, T^n zárt részhalmazai pedig pontosan az alterek (és így ezek kölcsönösen egyértelmű, rendezésfordító megfeleltetésben állnak egymással). Megjegyezzük, hogy a balideálok és az alterek között rendezéstartó megfeleltetést is létesíthetünk (lásd 8.7.12. Feladat).

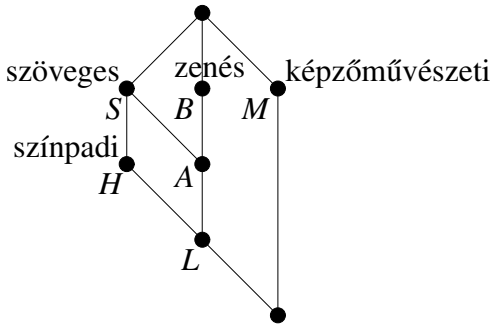
A 8.7.1. Példa (4) pontjában megadott példában a polinomok közötti zárt halmazokat algebrailag zárt test esetén Hilbert nullahelytétele írja le (5.11.1. Tétel), a pontok zárt halmazai pedig az algebrai halmazok (görbék, felületek).

8.7.11. Feladat. Bizonyítsuk be, hogy a 8.7.1. Példa (5) pontjában megadott Galois-kapcsolatban a függvények zárt halmazai pontosan a klónok.

A formális fogalom-analízis kiindulópontja a következő. Bizonyos *dolgok* bizonyos *tulajdonságait* vizsgáljuk. Például az alábbi táblázatban felsoroltunk műalkotásokat, és ezek néhány tulajdonságát.

	zenés	szöveges	színpadi	képzőművészeti
Abbey Road (Beatles)	×	×		
Bolero (Ravel)	×			
Hamlet (Shakespeare)		×	×	
Lohengrin (Wagner)	×	×	×	
Majális (Szinyei)				×
Solaris (Lem)		×		

A táblázatban az $\times$ jel azt jelenti, hogy a sorhoz tartozó dolognak megvan az oszlophoz tartozó tulajdonsága. Így egy páros gráfot kaptunk: egy műalkotás akkor van összekötve egy tulajdonsággal, ha a táblázat megfelelő helyén az $\times$ jel szerepel. Készítsük el a kapott Galois-kapcsolatban a zárt halmazokat. Ezek hálója a 8.11. Ábrán látható.



8.11. Ábra. Néhány művészeti fogalom hálója.

Az ábrán található címkék jelentése a következő. Az egyes műveket a kezdőbetűjükkel jelöljük (például a Bolero-t B-vel). Számítsuk ki a $\{H\}$ halmaz lezártját. A H-val összekötött fogalmak: szöveges és színpadi. Azok a művek, amelyek szövegesek is és színpadiak is, a H és az L. Tehát $\overline{\{H\}} = \{H, L\}$. (Ez azt fejezi ki, hogy a felsorolt tulajdonságok közül ami a Hamletre igaz, az igaz a Lohengrinre is). Ugyanígy láthatjuk, hogy $\overline{\{L\}} = \{L\}$. Az ábrán nagybetűkkel megjelölt pontok tehát a megfelelő egyelemű halmazok lezártjait jelentik. Így az ábráról is leolvasható, hogy $\overline{\{B\}} = \{A, B, L\}$, hiszen az ezekhez a betűkhöz tartozó pontok vannak *B alatt* az ábrán megadott részben rendezésben (és persze minden Galois-kapcsolatban $y \in \overline{\{x\}}$ akkor és csak akkor, ha $\overline{\{y\}} \subseteq \overline{\{x\}}$). Természetesen nem minden pontnak van nagybetűs címkéje, például a háló legnagyobb eleme egyetlen egyelemű műalkotás-halmaznak sem lesz a lezártja.

Ugyanezen az ábrán adtuk meg a tulajdonságok zárt halmazait is, és ismét az egyelemű halmazok lezártjait címkéztük föl. Az előbbihez hasonlóan kiszámolható, hogy

$$\overline{\{\text{színpadi}\}} = \{\text{színpadi, szöveges}\}\,.$$

Ez az ábráról úgy olvasható le, hogy a „színpadi” címkéjű pont *fölötti* címkék a „színpadi” és a „szöveges” (hiszen itt a rendezés megfordul). Az ábrán az is látszik, hogy például a zenés alkotások az A, B és L, mert ezek vannak a „zenés” címkéjű pont alatt. Ugyanígy az Abbey Road tulajdonságai „szöveges” és „zenés”, mert ezek vannak az A pont fölött.

Az ábrán szereplő pontok azok a ***fogalmak***, amelyek a fenti kontextusban megjelennek. Például a zenés és színpadi alkotásokat operának (vagy inkább dalműnek) nevezhetjük. Ez a fenti hálóban a „zenés” és „színpadi” pontok metszete, amit L-el címkéztünk (annak megfelelően, hogy a felsoroltak közül a Lohengrin az egyetlen opera). Így egy fogalmat kétféleképpen is jellemezhetünk: megadhatjuk azoknak a dolgoknak a listáját, amelyekre

a fogalom érvényes (az „opera” esetében ez csak az L), vagy pedig megadhatjuk a definícióját úgy, hogy felsoroljuk a rá jellemző tulajdonságokat (az „opera” esetében zenés, szöveges, színpadi mű).

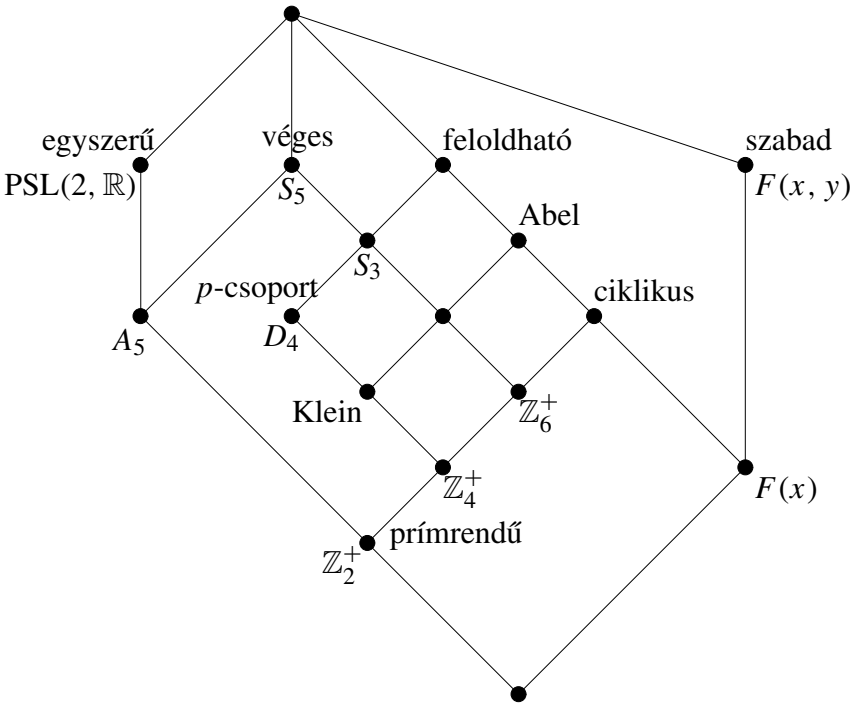
A most talált ábra tehát arra alkalmas, hogy a táblázatban szereplő adatokból kapott *fogalmakat rendszerezze, áttekinthető alakban ábrázolja,* ez a formális fogalom-analízis lényege. A fogalmak össze is hasonlíthatók, az ábráról „tételeket” is leolvashatunk. Például a „képzőművészeti” és a „zenés” fogalmak metszete a legalsó pont, ami az üres műalkotáshalmaznak felel meg. Ez azt fejezi ki, hogy nincs zenés képzőművészeti alkotás a felsoroltak között.

Természetesen a valódi alkalmazásokban arra kell törekednünk, hogy lehetőleg az összes dolgot és tulajdonságot számba vegyük. Például a fenti ábrából azt a következtetést is le lehetne vonni, hogy minden színpadi mű szöveges. Ez általában nem igaz, úgy lehet korrigálni, hogy a műalkotások listájához hozzáveszünk egy balettet is.

A fenti, műalkotásokkal kapcsolatos példa természetesen nagyon egyszerű, a valódi alkalmazásokban a szoftverek adatbázisokból veszik az adatokat. Egy fokkal kevésbé triviális példaként néhány csoportelméleti fogalom hálóját láthatjuk a 8.12. Ábrán (473. oldal).

	prímrendű	p-csoport	véges	ciklikus	Abel	fo.	egysz.	szabad
$\mathbb{Z}_2^+$	×	×	×	×	×	×	×	
$\mathbb{Z}_4^+$		×	×	×	×	×		
Klein		×	×		×	×		
$\mathbb{Z}_6^+$			×	×	×	×		
S_3			×			×		
D_4		×	×			×		
A_5			×				×	
S_5			×					
$F(x)$				×	×	×		×
$F(x, y)$								×
$\mathrm{PSL}(2, \mathbb{R})$							×	

A táblázatban fo. = feloldható, egysz. = egyszerű. A szereplő csoportok: $\mathbb{Z}_n^+$ az n elemű ciklikus csoport, D_4 a nyolcelemű diédercsoport, S_n, illetve A_n az n-edfokú szimmetrikus, illetve alternáló csoport, $F(x)$ és $F(x, y)$ az $\{x\}$, illetve $\{x, y\}$ által generált szabad csoport, végül $\mathrm{PSL}(2, \mathbb{R})$ a valós test fölötti kétdimenziós projektív speciális lineáris csoport (lásd 4.13.3. Definíció). Erről az ábráról is leolvashatunk tételeket, például hogy minden feloldható egyszerű csoport prímrendű, és így p-csoport.



8.12. Ábra. Néhány csoportelméleti fogalom hálója.

Az Olvasó talán úgy érezheti, hogy a fogalom-analízis nem „igazi” matematikai alkalmazás, hiszen a felhasznált matematikai apparátus (a Galois-kapcsolatok fent elmondott elmélete) matematikailag triviális. De persze ez más alkalmazásokról is elmondható: számos fizikai feladat megoldásához is csak az alapműveleteket, vagy egyszerű függvények deriválását használjuk föl a matematikából.

A fogalom-analízist számos területen használják, a meteorológiától a zeneelméletig és a pszichológiától a nyelvészetig. Ezek az alkalmazások felvetettek olyan matematikai problémákat is, amelyek már egyáltalán nem triviálisak. Például olyan algoritmusokat fejlesztettek ki, amelyek segítségével nagyon sok adat esetén is áttekinthető fogalom-háló rajzolható. Az Olvasó a

`http://www.upriss.org.uk/fca/fca.html`

internetes címen találhat fogalom-analízissel kapcsolatos hivatkozásokat. Itt alkalmazások leírásai éppúgy szerepelnek, mint elméleti cikkek, vagy az említett algoritmusokat megvalósító szoftverek.

Gyakorlatok, feladatok

8.7.12. Feladat. Legyen T test, $A = T^{n\times n}$ (mint gyűrű) és $B = T^n$ (mint vektortér). Ha U altér B-ben, akkor álljon $b(U)$ azokból a mátrixokból, amelyek sorvektorai U-ban vannak. Igazoljuk, hogy $b(U)$ balideál B-ben, és ez a megfeleltetés kölcsönösen egyértelmű és rendezéstartó a V alterei és a B balideáljai között.

8.8. Kategóriák és funktorok

Tapasztalhattuk, hogy a leképezések, a homomorfizmusok igen fontos szerepet játszanak az algebrai struktúrák elméletében. Több olyan fogalom és tétel van, amelyet ezen a nyelven lehet kényelmesen, precízen kifejezni. Ez indokolttá teszi annak az absztrakciós szintnek a vizsgálatát, amelyben csakis a leképezésekkel, és ezek kompozíciójával megfogalmazható tulajdonságokkal foglalkozunk. Ezt a szintet hívják kategóriaelméletnek.

A kategóriaelmélettel terjedelmi okoknál fogva csak néhány példán keresztül ismerkedhetünk meg. Fontos azonban leszögeznünk, hogy ez is egy mély eredményekkel rendelkező, hatalmas elmélet. Még arra is alkalmas, hogy a teljes matematikát (a halmazelmélet helyett) a kategóriaelméleten belül építsük föl. Az úgynevezett Abel-kategóriák és Grothendieck-kategóriák szerepe a már említett homomlógiaelméletben (és ezáltal az algebrai geometriában is) nélkülözhetetlen, ezek a modulusok egyfajta általánosításának tekinthetők. Kategóriákról az alábbiaknál kicsit több és precízebb információt találhat az Olvasó Fried Ervin [**13**] könyvének 15. Fejezetében. A következő lépcsőfok S. MacLane [**16**] (angol nyelvű) könyve, amely a kategóriaelmélet alapjait mutatja be a „többi" (tehát a nem kategóriaelméletre szakosodott) matematikusnak.

Kiinduló példaként azt vizsgáljuk meg, hogy a direkt szorzat fogalmát hogyan lehet megfogalmazni úgy, hogy csakis homomorfizmusokról essen benne szó, a szereplő algebrák elemeiről ne. Tudjuk, hogy ha A az A_i algebrák direkt szorzata (ahol i az I indexhalmazt futja be), akkor a $\pi_i : A \to A_i$ projekció az $\mathbf{a} = (\ldots, a_i, \ldots)$ elemhez ennek az i-edik komponensét, vagyis az $a_i \in A_i$ elemet rendeli. Természetesen az A-n kívül sok más olyan B algebrai struktúra is lehetséges, amelynek mindegyik A_i-be van egy φ_i homomorfizmusa. Ekkor azonban tekinthetjük a

$$\psi : b \mapsto (\ldots, \varphi_i(b), \ldots)$$

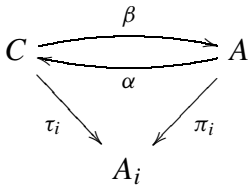
leképezést, amely B-ből az A direkt szorzatba képez (és nyilván művelettartó). A ψ leképezés fenti képletét úgy is fogalmazhatjuk, hogy minden i-re $\pi_i\psi(b) = \varphi_i(b)$ teljesül, azaz hogy $\pi_i \circ \psi = \varphi_i$ (ezek az egyenlőségek tehát egyértelműen meghatározzák ψ homomorfizmust). Fogalmazzuk meg a kapott tulajdonságot egy állítás formájában.

8.8.1. Állítás. *Legyen A az A_i algebrák direkt szorzata ($i \in I$), és jelölje π_i az i-edik projekciót. Ekkor minden B algebrához és $\varphi_i : B \to A_i$ homomorfizmusokhoz egyértelműen létezik egy $\psi : B \to A$ homomorfizmus, hogy $\pi_i \circ \psi = \varphi_i$ minden i-re teljesül.*

Most megmutatjuk, hogy ez a tulajdonság jellemzi is a direkt szorzatot.

8.8.2. Tétel. *Tegyük föl, hogy $\tau_i : C \to A_i$ homomorfizmusok ($i \in I$), melyekre igaz az előző állításban megfogalmazott tulajdonság (azaz tetszőleges B algebrára és $\varphi_i : B \to A_i$ homomorfizmusokra egyértelműen létezik egy olyan $\psi : B \to C$ homomorfizmus, hogy $\tau_i \circ \psi = \varphi_i$ minden i-re teljesül). Ekkor C izomorf az A_i algebrák direkt szorzatával.*

Bizonyítás. Jelölje A az A_i algebrák direkt szorzatát és π_i a projekciókat. A tételbeli feltételt alkalmazhatjuk $B = A$-ra, és $\tau_i = \pi_i$-re. Ekkor létezik egy $\alpha : A \to C$ homomorfizmus, melyre $\tau_i \circ \alpha = \pi_i$ minden i-re teljesül. A 8.8.1. Állítás miatt van egy $\beta : C \to A$ homomorfizmus is, hogy $\pi_i \circ \beta = \tau_i$ minden i-re. Megmutatjuk, hogy α és β egymás inverzei, és így izomorfizmust létesítenek A és C között. A most kapott homomorfizmusokat az alábbi diagrammon szemléltethetjük.



A $\gamma = \alpha \circ \beta : C \to C$ leképezésre

$$\tau_i \circ \gamma = \tau_i \circ \alpha \circ \beta = \pi_i \circ \beta = \tau_i \,.$$

De $\tau_i \circ id_C = \tau_i$ is teljesül minden i-re. A tételben szereplő feltételt tehát $B = C$ esetén a γ és az id_C leképezések is kielégítik. Az egyértelműség miatt ezért $id_C = \gamma = \alpha \circ \beta$. Ugyanígy

$$\pi_i \circ (\beta \circ \alpha) = \pi_i = \pi_i \circ id_A \,,$$

és így a 8.8.1. Állítás egyértelműségi része miatt $\beta \circ \alpha = id_A$. □

Az előző bizonyításban szereplő ábrához hasonlót már láttunk a hányadostest egyértelműsége kapcsán (270. oldal). Ezeket *kommutatív diagrammoknak* hívjuk. A „kommutatív" jelző arra utal, hogy a nyilak mentén bármilyen úton is haladunk két pont között, a megfelelő leképezések kompozíciója ugyanaz lesz. Ez a fenti ábra esetében a $\pi_i \circ \beta = \tau_i$ és a $\tau_i \circ \alpha = \pi_i$ egyenlőségeket jelenti.

Ha $\alpha, \beta : A \to A$ leképezések, akkor $\alpha \circ \beta = \beta \circ \alpha$ pontosan akkor teljesül, ha a

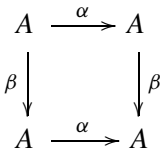


diagramm kommutatív. Ez egy magyarázat a „kommutatív diagramm" elnevezésre.

A következő feladatban két további példát mutatunk arra, hogy egy köznapi, elemekkel definiált tulajdonságot hogyan lehet elmondani a leképezések nyelvén. Meglátjuk, hogy a halmazok között a szürjektív leképezések azok, amelyekkel jobbról, az injektívek pedig azok, amelyekkel balról lehet egyszerűsíteni.

8.8.3. Feladat. Legyenek A és B halmazok és $\varphi : A \to B$ egy függvény. Mutassuk meg a következő állításokat.

(1) A φ pontosan akkor szürjektív, ha minden C halmazra és minden $\alpha, \beta : B \to C$ függvényre $\alpha \circ \varphi = \beta \circ \varphi$-ből $\alpha = \beta$ következik.
(2) A φ pontosan akkor injektív, ha minden C halmazra és minden $\alpha, \beta : C \to A$ függvényre $\varphi \circ \alpha = \varphi \circ \beta$-ból $\alpha = \beta$ következik.

Érvényesek-e hasonló állítások tetszőleges varietás algebrái közötti homomorfizmusokra?

Egy kategóriát úgy képzelhetünk el, hogy vannak bizonyos „objektumok" (például halmazok, algebrai struktúrák), amelyekről semmit sem tudunk, fekete doboz módjára viselkednek, és közöttük „morfizmusok" (a fenti példában függvények, illetve homomorfizmusok), amelyekről szintén csak annyit tudunk, hogy a kompozíció művelete elvégezhető és asszociatív. Minden objektumhoz odavesszük az „identikus leképezését", amelyről csak annyit teszünk föl, hogy kétoldali egységelem a kompozícióra.

8.8.4. Definíció. Azt mondjuk, hogy $\mathcal{C}$ egy *kategória*, ha

(1) vannak *objektumai*;
(2) bármely két objektum között lehetnek *morfizmusai* (az A és B objektumok közötti morfizmusok halmazát $\mathrm{Hom}(A, B)$ jelöli);
(3) értelmezve van a kompozíció művelete: ha A, B, C objektumok, $\alpha \in \mathrm{Hom}(B, C)$ és $\beta \in \mathrm{Hom}(A, B)$, akkor $\alpha \circ \beta \in \mathrm{Hom}(A, C)$;
(4) a kompozíció asszociatív, azaz $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$ tetszőleges olyan morfizmusokra, ahol a szereplő kompozíciók értelmezve vannak (vagyis ha $\alpha \in \mathrm{Hom}(C, D)$, $\beta \in \mathrm{Hom}(B, C)$, $\gamma \in \mathrm{Hom}(A, B)$);
(5) minden A objektumhoz van egy $id_A \in \mathrm{Hom}(A, A)$ morfizmus, melyre $\alpha \circ id_A = \alpha$ tetszőleges $\alpha \in \mathrm{Hom}(A, B)$-re, és $id_A \circ \alpha = \alpha$ tetszőleges $\alpha \in \mathrm{Hom}(B, A)$-ra.

A halmazelméletben különbséget tesznek „halmaz" és „osztály" között (lásd A.1. Függelék). Egy kategória objektumairól csak annyit teszünk föl, hogy osztályt alkotnak (hiszen például az összes csoportokat a csoport-homomorfizmusokkal kategóriának szeretnénk tekinteni, de a csoportok nem alkotnak halmazt). Ugyanakkor a $\mathrm{Hom}(A, B)$-ről föltesszük hogy halmaz, bármely A és B objektumok esetén.

Az imént tárgyalt példa alapján egy kategóriában akkor mondjuk, hogy az A objektum a $\pi_i \in \mathrm{Hom}(A, A_i)$ morfizmusokkal együtt az A_i objektumok direkt szorzata, ha tetszőleges B objektumhoz és $\varphi_i \in \mathrm{Hom}(B, A_i)$ morfizmusokhoz egyértelműen létezik egy $\psi \in \mathrm{Hom}(B, A)$ morfizmus, hogy $\pi_i \circ \psi = \varphi_i$ minden i-re teljesül.

Kategóriákat természetesen teljesen szabadon rajzolhatunk a fenti feltételekkel, és egy ilyen kategóriában egyáltalán nem biztos, hogy tetszőleges objektumoknak van direkt szorzata. Például az összes véges csoportok is kategóriát alkotnak a szokásos homomorfizmusokkal, és ebben végtelen sok objektumnak általában nem létezik a direkt szorzata.

8.8.5. Gyakorlat. Fogalmazzuk meg pontosan, és bizonyítsuk be tetszőleges kategóriában, hogy ha bizonyos objektumoknak létezik direkt szorzata, akkor az „izomorfia erejéig" egyértelműen meghatározott.

Ahogy hálók esetében a rendezés megfordítása a duális hálót eredményezte, úgy a kategóriák esetében is megtehetjük, hogy minden morfizmust „megfordítunk” (formálisan ez azt jelenti, hogy a $\mathrm{Hom}(A, B)$ halmazt kicseréljük a $\mathrm{Hom}(B, A)$ halmazzal, és a kompozíció sorrendjét is megváltoztatjuk). Könnyű belátni, hogy ekkor szintén kategóriát kapunk, amelyet az eredeti kategória *duálisának* nevezünk (néha *oppozit kategóriának* is hívják). Rendkívül fontos példa, hogy az injektív, illetve szürjektív leképezéseknek a 8.8.3. Állításban megadott „kategóriaelméleti” jellemzései ilyenkor helyet cserélnek. Ezt úgy is kifejezhetjük, hogy az injektivitás és a szürjektivitás (és hasonlóan egy homomorfizmus magja és képe is) duális fogalmak. Hasonlóan dualizálhatjuk a direkt szorzat fogalmát is.

8.8.6. Definíció. Egy $\mathcal{C}$ kategória egy A objektumát az A_i objektumok *szabad szorzatának* nevezzük a $\pi_i \in \mathrm{Hom}(A_i, A)$ morfizmusokkal, ha $\mathcal{C}$ tetszőleges B objektumához és tetszőleges $\varphi_i \in \mathrm{Hom}(A_i, B)$ morfizmusokhoz egyértelműen létezik egy $\psi \in \mathrm{Hom}(A, B)$ morfizmus, hogy $\psi \circ \pi_i = \varphi_i$ minden i-re teljesül.

Azt, hogy ez a dualizálás mennyire nem formális játék, hanem ismert fogalmak mélyebb megértéséhez vezet, a következő feladat világítja meg.

8.8.7. Feladat. Mutassuk meg, hogy

(1) a halmazok kategóriájában az X_i páronként diszjunkt halmazok szabad szorzata az uniójuk;
(2) az Abel-csoportok (vagy általában az R-modulusok) kategóriájában az M_i modulusok szabad szorzata a direkt összegük (más néven diszkrét direkt szorzatuk, ez a teljes direkt szorzatuknak azon elemeiből áll, amelyeknek véges sok kivétellel mindegyik komponense nulla, lásd 7.2.1. Definíció);
(3) Ha V egy varietás (például a csoportok varietása), akkor a páronként diszjunkt X_i halmazok által generált $F(X_i)$ szabad algebrák szabad szorzata az X_i halmazok X uniója által generált $F(X)$ szabad algebra.

A szabad szorzat elnevezést az előző feladat (3) állítása motiválja. A (2) és (3) állítás magyarázza meg annak az okát, hogy az R gyűrű feletti szabad modulusokat az ${}_R R$ modulus diszkrét direkt hatványaiként kapjuk meg (7.2.15. Tétel).

A szabad szorzatot néha általános kategóriákban is *direkt összegnek* hívják, ez azonban nem szerencsés, mert a direkt összeg kifejezés már eddig is többféle értelemben szerepelt, és az irodalomban sem egységes a használata. Most tisztázzuk a pontos jelentését.

(1) ***Alterek, ideálok összege.*** A direkt összeg kifejezéssel először vektortereknél találkozik az ember, az U és V alterek $U + V$ összege direkt összeg, ha $U \cap V = \{0\}$. Ilyenkor az $U + V$ altér elemei egyértelműen állnak elő $u + v$ alakban, ahol $u \in U$ és $v \in V$. Emiatt az $U \oplus V$ direkt összeg izomorf az U és V vektorterek $U \times V$ direkt szorzatával. A direkt *összeg* kifejezés tehát eredetileg onnan származik, hogy vektortérben a kétváltozós művelet neve az összeadás.
(2) ***A direkt szorzat belső jellemzése.*** A fenti $U \oplus V \cong U \times V$ izomorfizmust úgy neveztük, hogy a direkt szorzat belső jellemzése. Ezt véges sok tényezőre is kiterjesztettük (lásd 7.2.2. Gyakorlat). Abel-csoportok, vektorterek, általában modulusok esetén itt is bizonyos

részstruktúrák összege szerepel, ezért ezt is hívhatjuk direkt összegnek. Gyűrűk esetében ez a jellemzés ideálokkal történik (5.1.17. Állítás), így ideálok összegéről is lehet beszélni. Csoportoknál a jellemzésben normálosztók szorzata szerepel (4.8.11. Állítás), itt már az összeg szót nem használhatjuk. Általános algebrák esetében ez végképp értelmét veszti, nemcsak azért mert itt nem feltétlenül van összeadás nevű művelet, hanem azért sem, mert a direkt szorzat belső jellemzésekor már nem is részstruktúrákat, hanem kongruenciákat kell használnunk (8.2.31. Állítás).

(3) ***A végtelen sok tényező esete.*** Ha M_i végtelen sok modulus, akkor az M direkt szorzatukat nem is jellemeztük belsőleg. Álljon M_i^* az M-nek azon elemeiből, amelyek i-edik komponense tetszőleges, a többi viszont nulla. Ekkor az M_i^* részmodulusok összege azokból az elemekből áll, amelyeknek véges sok nem nulla komponense van, és ez magyarázza, hogy ezt a részmodulust miért neveztük direkt összegnek. Hasonló jelenség gyűrűk és csoportok esetében is fellép (a csoportoknál persze szorozni kell a megfelelő normálosztókat). Itt inkább a diszkrét direkt szorzat elnevezés használatos.

(4) ***Direkt összeg és szabad szorzat.*** Modulusok, például Abel-csoportok esetében összeesik a kategóriaelméleti szabad szorzat, és a korábban definiált direkt összeg fogalma a 8.8.7. Feladat (2) pontja szerint. Ez csoportokra már két tényező esetében sem igaz. Például a $\mathbb{Z}_2^+$ csoportnak az önmagával vett direkt szorzata a Klein-csoport (mind a kommutatív, mind a nemkommutatív csoportok kategóriájában). A szabad szorzatuk azonban függ attól, hogy melyik kategóriában tekintjük őket: Abel-csoportok között ez szintén a Klein-csoport lesz, a csoportok kategóriájában azonban egy végtelen csoport az eredmény (az $x^2 = y^2 = 1$ definiáló relációkkal megadott úgynevezett végtelen diédercsoport).

Összefoglalva: jobb, ha a kategóriaelméleti fogalmat nem hívjuk direkt összegnek (hanem szabad szorzatnak), mert ez modulusokban rendben van, de például gyűrűkben ütközik a néha más értelemben használt direkt összeg fogalmával.

Sokszor előfordul, hogy egy kategória objektumaihoz egy másik kategória objektumait rendeljük. Íme néhány példa.

(1) A T test fölötti V vektortérhez a $V^* = \mathrm{Hom}(V, T)$ duális teret.
(2) Az A Abel-csoporthoz a $\mathrm{Hom}(A, \mathbb{Z}^+)$ vagy a $\mathrm{Hom}(\mathbb{Q}^+, A)$ vagy az $A \otimes \mathbb{Q}^+$ Abel-csoportot.
(3) Az X halmazhoz az X által generált szabad csoportot.
(4) A G csoporthoz a G alaphalmazát.
(5) A B Boole-algebrához a neki a Stone-tételnél (8.5.22. Tétel) megfelelő, vele izomorf részalgebrát.

Ezekben a hozzárendelésekben az a közös, hogy nemcsak az objektumokhoz rendelünk objektumokat, hanem a morfizmusokhoz is morfizmusokat. Például legyen R kommutatív gyűrű, K egy rögzített R-modulus, és tekintsük az

$$F(X) = \mathrm{Hom}_R(X, K) \quad \text{és} \quad G(X) = \mathrm{Hom}_R(K, X)$$

leképezéseket, mindkettő az R-modulusok kategóriáját képzi önmagába. Ha $\varphi : N \to M$ egy R-homomorfizmus, akkor a 7.7.22. Definícióban megadtuk a

$$\mathrm{Hom}(\varphi, id_K) : F(M) = \mathrm{Hom}_R(M, K) \to F(N) = \mathrm{Hom}_R(N, K)$$

és

$$\mathrm{Hom}(id_K, \varphi) : G(N) = \mathrm{Hom}_R(K, N) \to G(M) = \mathrm{Hom}_R(K, M)$$

homomorfizmusokat. Legyen

$$F(\varphi) = \mathrm{Hom}_R(\varphi, id_K) \quad \text{és} \quad G(\varphi) = \mathrm{Hom}_R(id_K, \varphi)\,,$$

a 7.7.24. Gyakorlat szerint ezek a leképezések tartják a kompozíció műveletét. Az F leképezés „megfordítja a nyilakat”, a G nem. Ennek megfelelő az alábbi két definíció.

8.8.8. Definíció. Legyenek $\mathcal{C}$ és $\mathcal{D}$ kategóriák. Azt mondjuk, hogy a $G : \mathcal{C} \to \mathcal{D}$ egy *kovariáns funktor*, ha G a $\mathcal{C}$ minden A objektumához a $\mathcal{D}$ egy $G(A)$ objektumát rendeli, továbbá a $\mathcal{C}$ minden $\varphi \in \mathrm{Hom}(A, B)$ morfizmusához egy $G(\varphi) \in \mathrm{Hom}\big(G(A), G(B)\big)$ morfizmust rendel úgy, hogy a kompozíció műveletét tartja, vagyis

$$G(\psi \circ \varphi) = G(\psi) \circ G(\varphi)$$

tetszőleges $\varphi \in \mathrm{Hom}(A, B)$ és $\psi \in \mathrm{Hom}(B, C)$ morfizmusokra, végül $G(id_A) = id_{G(A)}$ tetszőleges A objektumra.

8.8.9. Definíció. Legyenek $\mathcal{C}$ és $\mathcal{D}$ kategóriák. Azt mondjuk, hogy az $F : \mathcal{C} \to \mathcal{D}$ egy *kontravariáns funktor*, ha F a $\mathcal{C}$ minden A objektumához a $\mathcal{D}$ egy $F(A)$ objektumát rendeli, továbbá a $\mathcal{C}$ minden $\varphi \in \mathrm{Hom}(A, B)$ morfizmusához egy $F(\varphi) \in \mathrm{Hom}\big(F(B), F(A)\big)$ morfizmust rendel úgy, hogy a kompozíció műveletét tartja, vagyis

$$F(\psi \circ \varphi) = F(\varphi) \circ F(\psi)$$

tetszőleges $\varphi \in \mathrm{Hom}(A, B)$ és $\psi \in \mathrm{Hom}(B, C)$ morfizmusokra, végül $F(id_A) = id_{F(A)}$ tetszőleges A objektumra.

A kontravariáns funktort tehát definiálhattuk volna olyan kovariáns funktorként, amely a $\mathcal{C}$ kategória duálisából képez a $\mathcal{D}$ kategóriába. Az előző példában a Hom_R leképezésből kaptunk két funktort úgy, hogy egy-egy változót rögzítettünk.

Az a tény, hogy a Hom funktor az első változójában kontravariáns, a másodikban pedig kovariáns, megmagyarázza a 7.7.11. Feladatban bizonyított

$$\mathrm{Hom}_R\Big(\bigoplus_i M_i, K\Big) \cong \prod_i \mathrm{Hom}_R(M_i, K) \;\text{ és }\; \mathrm{Hom}_R\Big(M, \prod_i K_i\Big) \cong \prod_i \mathrm{Hom}_R(M, K_i)\,.$$

összefüggéseket. Az első változóbeli direkt összegből azért lesz direkt szorzat, mert a két fogalom egymás duálisa, és Hom „megfordítja a nyilakat”.

Szokás definiálni a kétváltozós, úgynevezett *bifunktorokat* is, amire a fő példákat szintén a $\mathrm{Hom}_R(\varphi, \psi)$, valamint a tenzorszorzat szolgáltatja. Ezek kétváltozós „leképezések", amelyek mindkét változójukban funktorok, ha a másik változó rögzített. Bifunktorokkal ebben a könyvben nem foglalkozunk.

A kategóriákról szóló bevezetőnket két olyan példával zárjuk, amelyek fontos, funktorokkal megfogalmazható tulajdonságokat érzékeltetnek. A 7.8.23. Feladat (4) pontjában beláttuk, hogy

$$\mathrm{Hom}_R\left(M \otimes N,\, K\right) \cong \mathrm{Hom}_R\left(M,\, \mathrm{Hom}_R(N,\, K)\right)$$

tetszőleges kommutatív R gyűrű fölötti M, N, K modulusokra. Legyen $F(X) = X \otimes N$ és $G(X) = \mathrm{Hom}(N, X)$. Ekkor a fenti összefüggés a

$$\mathrm{Hom}_R\left(F(M),\, K\right) \cong \mathrm{Hom}_R\left(M,\, G(K)\right)$$

alakban írható. A következő gyakorlat egy hasonló tulajdonságú funktor-párra ad példát.

8.8.10. Gyakorlat. Legyen $\mathcal{S}$ a halmazok kategóriája (ahol a morfizmusok a tetszőleges leképezések), és $\mathcal{G}$ a csoportok kategóriája (ahol a morfizmusok a homomorfizmusok). Jelölje $F : \mathcal{S} \to \mathcal{G}$ azt a funktort, amely minden halmazhoz az általa generált szabad csoportot, $G : \mathcal{G} \to \mathcal{S}$ pedig azt a funktort, amely minden csoporthoz az alaphalmazát rendeli. Mutassuk meg, hogy F-et és G-t a morfizmusokon megadhatjuk úgy, hogy kovariáns funktorokat kapjunk, továbbá tetszőleges M halmazra és K csoportra

$$\mathrm{Hom}\left(F(M),\, K\right) \cong \mathrm{Hom}\left(M,\, G(K)\right).$$

Az $\cong$ jel itt azt jelenti, hogy a két halmaz között van kölcsönösen egyértelmű leképezés.

A most kapott képlet emlékeztet a lineáris algebrában tanult $\langle Au, v\rangle = \langle u, A^*v\rangle$ képletre, amely az adjungált lineáris transzformációt írja le. Ezért a fenti típusú F és G funktorokat is szokás *adjungált funktoroknak* nevezni. A pontos definíció elolvasható Fried Ervin [**13**] könyvének 15.2. Szakaszában.

A másik jelenség, amire föl szeretnénk hívni a figyelmet, a következő. Már több példát láttunk arra, hogy bizonyos matematikai objektumokat úgy lehet megérteni, hogy „másképp nézünk rájuk", a másik oldalukról vizsgáljuk őket. Ha adottak bizonyos struktúrák, akkor kölcsönösen egyértelmű módon hozzájuk rendelhetünk egy másik struktúrát, amelyekkel a matematika egy másik területe foglalkozik (és így az ottani tételeket alkalmazhatjuk). Erre példa volt a Galois-elmélet főtétele, vagy a Boole-algebrák és a Boole-gyűrűk közötti kapcsolat (8.5.23. Gyakorlat).

Az ilyesfajta megfeleltetéseknél gyakori, hogy azt funktorok létesítik. Példaként tekintsük a Stone-féle reprezentációs tételt (8.5.22. Tétel). Az alábbiakat minden Olvasónak érdemes végigfutnia, mert a lényeg remélhetőleg érthető lesz, de a formális megértéshez szükséges ismerni a topologikus tér fogalmát.

Ha adott egy B Boole-algebra, akkor ezt úgy ágyaztuk be egy X halmaz összes részhalmazainak Boole-algebrájába, hogy tekintettük a szubdirekt irreducibilis faktorait. Mivel ezek kételeműek, valójában a B homomorfizmusait tekintettük a kételemű K Boole-algebrába. Ezért az X indexhalmazt úgy is föl lehet fogni, mint

$$F(B) = X = \mathrm{Hom}(B, K)\,.$$

Ez a halmaz még nem határozza meg a B Boole-algebrát, azt is meg kell mondani, hogy X mely részhalmazait kell bevenni. Ennek a felsorolás helyett egy másik lehetséges módja, hogy egy *topológiát* értelmezünk az X halmazon (a nyílt halmazok pontosan a B elemeinek megfelelő részhalmazok uniói lesznek). Az X tehát egy speciális topologikus térré, úgynevezett *Boole-térré* válik. Meg lehet mutatni, hogy a fenti $F : B \to \mathrm{Hom}(B, K)$ leképezés funktorrá tehető, amely egy Boole-algebrák közötti homomorfizmushoz a megfelelő topologikus terek közötti *folytonos* függvényt rendel. Megfordítva, ha X Boole-tér, akkor a neki megfelelő Boole-algebra megkapható

$$G(X) = B = \mathrm{Hom}(X, T)$$

alakban, ahol T a kételemű diszkrét topologikus tér, és a $\mathrm{Hom}(X, T)$ folytonos leképezéseket jelent.

Vegyük észre, hogy F és G csak „majdnem" lesznek egymás inverzei, az nem igaz, hogy $G\big(F(B)\big) = B$ minden B Boole-algebrára, hanem csak az, hogy ez a két Boole-algebra izomorf, és ez az izomorfizmus „uniform" (valamennyi Boole-algebrára „ugyanúgy" működik). Mindezt precízen ki lehet fejezni a kategóriaelmélet segítségével, így kapjuk az *ekvivalens kategóriák* és a *természetes homomorfizmus* pontosan definiálható fogalmát. Tehát a Boole-algebrák és a Boole-féle topologikus terek kategóriája ekvivalens.

Hasonló ekvivalenciára igen fontos példa a *Pontrjagin-dualitás*, amely azt mondja ki, hogy az Abel-csoportok kategóriája ekvivalens a kompakt Abel-féle topologikus csoportok kategóriájával. Az ekvivalenciát itt is a fenti módon kapjuk, alkalmas Hom-csoportokat tekintve, azonban nem a kételemű csoportba, hanem a komplex egységkörbe (mint multiplikatív csoportba) menő homomorfizmusokat kell tekinteni. Ez az ekvivalencia több nehéz probléma megoldását tette lehetővé, és kapcsolatban áll a csoport-reprezentációk elméletével is.

Az Olvasó kategóriaelméleti gyakorlatokat és feladatokat a Czédli–Szendrei–Szendrei-féle [**6**] feladatgyűjtemény XII. Fejezetében találhat.

8.9. Kitekintés

Ebben a szakaszban röviden szót ejtünk néhány mélyebb vagy nehezebb általános algebrai témakörről. Természetesen az általános algebrák elméletének és a hálóelméletnek is sok kutatási iránya van, amelyekről itt nem beszélhetünk, a válogatás tehát szükségképpen szubjektív. Kitérünk néhány magyar vonatkozásra is. Egy alkalmazást bemutattunk a 8.7. Szakaszban.

Kiindulásként egy klasszikus problémát vizsgálunk. Természetes kérdés, hogy egy algebra részalgebrahálójáról, vagy kongruencia-hálójáról milyen tételeket lehet általában bebizonyítani. Az könnyen látható, hogy nem minden teljes háló kapható meg így. Ennek oka a következő.

Egy algebra minden részalgebrája előáll a végesen generált részalgebráinak egyesítéseként. A végesen generált részalgebrákat azonban pusztán a részalgebrahálóból is föl lehet ismerni. Valóban, egy $C \leq A$ részalgebra akkor és csak akkor végesen generált, ha igaz rá a következő: bárhogy is veszünk $B_i \leq A$ részalgebrákat, ha C része a B_i részalgebrák egyesítésének, akkor már véges sok B_i egyesítésének is része (elég C minden generátoreleméhez egy olyan B_i részalgebrát venni, amely ezt a generátorelemet tartalmazza). Egy teljes háló ilyen tulajdonságú elemeit *kompaktnak* nevezzük (hiszen a topológiában a kompakt halmazok azok, amelyek minden nyílt fedéséből kiválasztható véges fedés). Egy teljes háló *algebrai háló*, ha minden eleme előáll kompakt elemek egyesítéseként. Egy algebra részalgebrahálója tehát algebrai háló, és könnyen láthatóan a kongruencia-hálója is az. Nem nehéz megmutatni, hogy minden algebrai háló előáll egy alkalmas algebra részalgebrahálójaként. Az alábbi már lényegesen nehezebb tétel.

8.9.1. Tétel [Grätzer–Schmidt-tétel]. *Minden algebrai háló előáll úgy, mint egy alkalmas algebra kongruencia-hálója.*

Ezek szerint a kongruencia-hálók nagyon csúnyák is lehetnek. Minden véges háló nyilvánvalóan algebrai, és ezért ezek is kongruencia-hálók. A kapott algebra azonban általában végtelen. A következő probléma a mai napig megoldatlan.

8.9.2. Probléma. Igaz-e, hogy minden véges háló egy véges algebra kongruencia-hálója?

Ha ez igaz, akkor minden véges hálót meg lehet adni, mint egy véges halmaz partícióhálójának részhálóját (hiszen beláttuk a 8.2.23. Tételben, hogy a kongruencia-háló a partícióhálóban részháló). Ezt a következményt sikerült is bebizonyítani.

8.9.3. Tétel [Pudlak–Tuma-tétel]. *Minden háló izomorf egy alkalmas U halmaz partícióhálójának egy részhálójával. Ha a háló véges, akkor az U halmaz is választható végesnek.*

Ez valójában kombinatorikai tétel, és a véges U halmazra vonatkozó bizonyítás rendkívül nehéz, nagyon bonyolult konstrukciót kell kontrollálni. A későbbi vizsgálatok során kiderült, hogy az előbbi probléma nem azért nehéz, mert rendkívül komplikált véges általános algebrák vannak, hanem azért, mert a véges csoportok részcsoporthálói nagyon bonyolultak lehetnek.

8.9.4. Tétel [Pálfy–Pudlak-tétel]. *A következő két állítás ekvivalens.*

(1) *A 8.9.2. Problémára igenlő a válasz, vagyis minden véges háló előáll egy alkalmas véges algebra kongruencia-hálójaként.*
(2) *Minden véges háló előáll egy alkalmas véges csoport részcsoporthálójának egy intervallumaként.*

Megjegyezzük, hogy az itt szereplő Pálfy Péter Pál, és az előző tétel szerzői, Grätzer György és Schmidt Tamás is magyar matematikusok.

Az Olvasó joggal csodálkozhat, hogy hogyan kerülnek ide részcsoporthálók, amikor kongruencia-hálókról van szó. A magyarázat az, hogy ha H részcsoportja G-nek, és a H szerinti bal oldali mellékosztályokon tekintjük G hatását balszorzással, akkor ezeket a balszorzásokat egyváltozós műveletnek tekintve a kapott algebrának a kongruencia-hálója izomorf a G részcsoporthálójában a H és G közötti intervallummal (8.2.26. Állítás). Az is érdekes, hogy a csoportelmélet mély eredményei, például a klasszifikáció, sem képesek megbirkózni a fenti kérdéssel.

A fenti tétel komoly vizsgálatokat indított el. A bizonyítása ugyanis (szintén Pálfy Péter Pál érdemeként) megmutatta, hogy minden véges algebrában találhatók olyan kis részhalmazok, amelyek feltérképezik az egész A algebrát, és a szerkezetük teljesen osztályozható, a következő öt típus lép föl.

(1) Egy permutációcsoport (a fenti leírt módon unáris algebrának tekintve).
(2) Egy véges vektortér egy véges test fölött.
(3) A kételemű Boole-algebra.
(4) A kételemű háló.
(5) A kételemű félháló (ebben a $\{0, 1\}$ halmazon csak a metszet műveletet tartjuk meg).

Az, hogy a legáltalánosabb algebrákban is a fenti klasszikus struktúrák jelennek meg, egyrészt egyfajta magyarázatot ad arra, hogy miért a szokásos klasszikus struktúrák az algebristák érdeklődésének célpontjai, másrészt azonban igen hasznos dolog, hiszen a klasszikus struktúrákról sok mély tételt ismerünk, és ezért viszonylag jól lehet számolni bennük. A most leírt ötleteket Ralph McKenzie fejlesztette tovább a *kongruencia-szelídítés* nevű elméletté. Az elmélet alapjait kifejtő [**15**] monográfia az internetről ingyenesen letölthető.

Az elmélet hatékonyságára egy másik indok a következő. Ha egy csoportot vizsgálunk, akkor abban általában a részcsoportokat nézzük. Néha előfordul, hogy gyűrűelméleti eredményeket is alkalmazhatunk. Ha azonban általános algebrákat is tudunk tekinteni (mert vannak róluk nemtriviális eredmények), akkor érdemes lehet egy tetszőleges részhalmazból algebrai struktúrát csinálni, mondjuk egy csoportban is, mert az esetleg ugyan nem csoportszerű, hanem inkább olyan, mint egy háló, de akkor a hálókra vonatkozó tételek segítségével mégis hasznos információt nyerhetünk. Így például egy indukciós bizonyítás sokkal hatékonyabb lehet, mert több részhalmazról tehetjük föl, hogy az állítás rájuk már igaz. Az általános algebrák elmélete átjárást biztosít az egyes konkrét struktúrafajták elmélete között.

A kongruencia-szelídítésnek több mély alkalmazása is van, logikai (például eldönthetőségi kérdésekről), vagy egy véges algebra által generált varietásban a szubdirekt irreducibilis algebrák eloszlásáról. Ízelítőül egy Quackenbush-tól származó problémát említünk meg, amely nagyon egyszerűnek látszik, mégis nyitott.

8.9.5. Probléma. Van-e olyan véges algebra, amelynek véges sok alapművelete van, az általa generált varietásban van akármilyen nagy elemszámú véges szubdirekt irreducibilis algebra, de nincs benne végtelen szubdirekt irreducibilis algebra?

Érdemes még megemlíteni, hogy noha a kongruencia-szelídítés elmélete véges algebrákról szól, hozzá kapcsolódik az úgynevezett *kommutátor-elmélet*, amely végtelen algebrákra is alkalmazható, de csak olyanokra, amelyeknek a kongruencia-hálója moduláris. Ennek alapötlete is hasonló, mint a kongruencia-szelídítésé: meg lehet mutatni, hogy ha egy ilyen algebra kongruencia-hálója „valahol" nem disztributív, akkor „ott" megjelenik egy (asszociatív gyűrű fölötti) modulus az algebrában (amelyben ismét csak hatékonyan számolhatunk). A modulus-műveleteket (például az összeadást) a korábban tárgyalt Malcev-kifejezésekkel való számolással lehet megadni.

Újabban az általános algebrák elmélete kapcsolatba került az algoritmuselmélettel is. Ha ugyanis általános relációkat (például egy gráfot, vagy egy részben rendezést) vizsgálunk, akkor ennek tanulmányozásához hozzásegíthet az, hogy ezt részalgebrának képzeljük, és az ezt tartó műveleteket tekintjük (nemcsak az egyváltozósakat, például a gráf automorfizmusait, hanem a többváltozósakat is). Az így kapott algebrára használhatjuk az általános algebrák elméletének tételeit. Az ide vonatkozó eredményekre „constraint satisfaction problem" néven kereshet az Olvasó.

Az alábbi probléma is megoldatlan. Azt könnyű meggondolni, hogy ha ismerjük az A algebra által generált varietásban a három elemmel generált szabad algebrát, akkor el tudjuk dönteni, hogy van-e az algebrának Malcev-kifejezése. A három elemmel generált szabad algebra elemszáma azonban a legrosszabb esetben n^{n^3} is lehet, ahol n az A elemszáma. Ezt tehát nagyobb n értékek esetén reménytelen kiszámítani.

8.9.6. Probléma. Adott egy véges algebra. Van-e hatékony (nem exponenciális futásidejű) algoritmus annak eldöntésére, hogy ennek van-e Malcev-kifejezése?

Az összefoglalót egy magyar vonatkozású eredménnyel zárjuk. Gyakran vizsgált kérdés, hogy egy algebra kongruencia-hálói milyen hálóazonosságoknak tesznek eleget (például modulárisak, disztributívak-e). Meglepő, Freese-től és Jónssontól származó észrevétel, hogy ha egy varietásban minden algebra kongruencia-hálója moduláris (például a csoportok esetében), akkor a varietás algebráinak kongruencia-hálói egy erősebb azonosságnak is eleget tesznek, amely a projektív geometria híres Desargues-tételéből származik. Ezt a tételt Pálfy Péter Pál és Szabó Csaba fejlesztették tovább: találtak egy másik projektív geometriai tételt, és egy annak megfelelő azonosságot, amelyre a következő teljesül.

8.9.7. Tétel [Pálfy–Szabó-tétel]. *Van olyan hálóazonosság, amely teljesül minden Abel-csoport kongruencia-hálójában, de nem teljesül minden csoport kongruencia-hálójában.*

8.10. Összefoglaló

9. HIBAJAVÍTÓ KÓDOK

(Helyreigazító közlemény.) Lapunk keddi számában hírt adtunk arról, hogy a svéd tudományos akadémia díszdoktorrá avatott egy magyar tudóst, akit — őszinte sajnálatunkra — „dr. Pálpéter Péter Pál" néven említettünk. [...] A jeles magyar tudós neve helyesen: doktor Pálpéter Péter Pál.

Örkény István: *Makacs sajtóhiba (egyperces novella)*

A „kódolás" azt jelenti, hogy adatokat (például egy szöveget, vagy egy számsort) bizonyos szabályok szerint megváltoztatunk (úgy, hogy az eredeti szöveget vissza lehessen kapni alkalmas eljárással, ez a „dekódolás"). Kódolást több célból is alkalmazunk. Például a titkosírások során a szöveget azért kódoljuk, hogy illetéktelenek ne érthessék meg (ezt szeretnénk elérni, amikor banki adatainkat kell elküldenünk az interneten). Az ilyen célú kódolással a *kriptográfia* foglalkozik.

Szorozzunk össze két hatalmas prímszámot! A kapott szorzatból igen nehéz meghatározni az eredeti két tényezőt (semmilyen gyors eljárást nem ismerünk, bár matematikailag még nem sikerült belátni, hogy ilyen gyors eljárás nem is létezhet). Ezen az észrevételen alapszik a manapság rendkívül széles körben alkalmazott RSA titkosírási rendszer (a [**11**] könyv 5.8. Szakaszában részletesebben is olvashatunk erről).

Kódolást alkalmazunk akkor is, ha a cél az adatok tömörítése (például a tárolóterület jobb kihasználása, vagy az adatok gyorsabb továbbítása végett). Ez az úgynevezett *forráskódolás*. Ebben a fejezetben egy harmadik fajta kódolással foglalkozunk, amelynek a célja a *hibajelzés* és *hibajavítás*. A teljesség igénye nélkül felsorolunk néhány olyan helyzetet, amikor ilyen kódolásra van szükség.

- Amikor az adatokat tároljuk egy olyan adathordozón (mondjuk egy merevlemezen, vagy kompakt lemezen), amelynek egyes részei meghibásodhatnak.
- Amikor egy szonda rádión elküldi a tudományos mérések adatait (vagy képeket).
- Amikor televíziós adást sugárzunk (például műholdról).
- Amikor mobiltelefonnal akarunk kapcsolatot teremteni.

A felsorolt példákban az a közös, hogy amikor az adatokat elküldjük, akkor a „csatornában" (például a rádióadás során) „zaj" keletkezhet, vagyis az üzenet egy kicsit megváltozhat.

Ezért kódolást alkalmazunk, például az üzenetet kiegészítjük „ellenőrző bitekkel”. Ekkor a kicsit megváltozott (elromlott) üzenetből az eredeti tartalom visszanyerhető lehet (feltéve, hogy „túl sok” hiba nem történt), de legalábbis felismerhetjük, ha hiba történt. A kódolással az üzenet meghosszabbodik, és így egy adott sebességű csatorna kevesebb információt tud csak átvinni. A kódelmélet feladata az, hogy hatékony kódolási eljárásokat találjunk, abban az értelemben, hogy a lehető leggyorsabban és a lehető legbiztonságosabban lehessen adatokat küldeni. Ezen kívül figyelembe kell venni számos egyéb tényezőt is, mint például a kódoló és dekódoló eljárások sebessége, vagy a csatorna tipikus hibáinak jellege. Ezért a hibajavító kódolás elmélete hatalmas, és sok tekintetben gyakorlati irányultságú.

A témáról magyar nyelvű irodalom is rendelkezésre áll. Györfi László, Győri Sándor és Vajda István [**14**] műve haladó tankönyv, amelyben a kódolási eljárások hatékonyságának valószínűségszámítási elemzése ugyanúgy szerepel, mint a gyakorlatban fellépő feladatok megvalósításában használt konkrét eljárások bemutatása. Freud Róbert már sokszor idézett [**10**] lineáris algebra könyvének tizedik fejezete olyan stílusú bevezetést ad a hibajavító kódok elméletébe, amelyben könyvünk eddigi része íródott (részletes magyarázatokkal, példákkal, feladatokkal). Ezért *csak arra vállalkoztunk, hogy az eddigieknél kissé tömörebb stílusban ízelítőt adjunk egy olyan kódolási eljárásból, amely algebrai eredményeken: a polinomok és a véges testek tulajdonságain alapszik.* Alkalmazásként szó lesz a számítógépekben alkalmazott CRC-hibafelismerő eljárásról, és a kompakt hanglemezeken (az audio CD-ken) található információ rögzítésekor használt módszerről is, amely az úgynevezett Reed–Solomon-kódokon alapszik.

9.1. Alapfogalmak

Ebben a fejezetben a következő jelöléseket végig használni fogjuk. Adott egy q elemű Q halmaz, az úgynevezett *ábécé* (nagyon sokszor $Q = \{0, 1\}$). Az üzenet, amit küldeni akarunk, a Q elemeiből készített véges sorozat (például 010000100100). Az üzenetet k hosszú darabokra vágjuk, vagyis a Q^k elemeit akarjuk kódolni. A kódolás azt jelenti, hogy tekintünk egy $\varphi : Q^k \to Q^n$ injektív függvényt, és az $u \in Q^k$ helyett a $v = \varphi(u) \in Q^n$ sorozatot küldjük el. Legyen C a φ értékkészlete, ami egy $C \subseteq Q^n$ halmaz.

9.1.1. Definíció. A q^k elemű $C \subseteq Q^n$ halmazokat (n, k) paraméterű *kódnak* nevezzük. A Q^n elemeit szavaknak is hívjuk, a C elemei a *kódszavak*. Az n szám a kód *hossza*.

9.1.2. Példa. Legyen $Q = \{0, 1\}$, $k = 1$, $n = 3$ és

$$\varphi(0) = 000\,, \quad \varphi(1) = 111\,.$$

Ekkor $C = \{000, 111\} \subseteq Q^3$ egy 3 hosszú, $(3, 1)$ paraméterű kód.

A 010 üzenetet tehát 000 111 000 kódolja (minden bitet megháromszorozunk). Ha a vevőkészülékbe ez eltorzítva 001 101 100 formában érkezik, akkor képesek vagyunk az

eredeti üzenetre következtetni a következő dekódolási eljárással: az abc hármast 0-vá dekódoljuk, ha a, b és c között a nulla legalább kétszer szerepel, és 1-nek egyébként (vagyis ha legalább két egyes van).

Mikor sikeres ez a dekódolás? Ha tudjuk, hogy három egymás utáni jel közül csak legfeljebb egy hibás, akkor biztosan. Ha kettő hibás, például a 000 eltorzul 110-vá, akkor is észrevesszük, hogy hiba történt, mert amit kaptunk, az nem kódszó. A dekódolás azonban most már hibás eredményre vezet.

9.1.3. Definíció. Legyen $t \geq 1$ egész szám. Azt mondjuk, hogy a $C \subseteq Q^n$ kód *t-hibajelző*, ha egy kódszót legfeljebb t helyen megváltoztatva az eredmény nem lehet kódszó. A C kód *t-hibajavító*, ha bárhogy is veszünk két $u \neq w$ kódszót, ha u-t is és w-t is legfeljebb t helyen megváltoztatjuk (ezek a helyek mások lehetnek u, mint w esetében), akkor nem kaphatjuk Q^n-nek ugyanazt az elemét.

A 9.1.2. Példában szereplő kód tehát 2-hibajelző, és 1-hibajavító. Az előbbi definíciót kényelmesebben is megfogalmazhatjuk az alábbi két fogalom segítségével.

9.1.4. Definíció. Ha $u = u_1 \dots u_n$ és $v = v_1 \dots v_n$ a Q^n elemei, akkor e két szó *Hamming-távolsága* azoknak az $1 \leq i \leq n$ koordinátáknak a száma, ahol u és v eltér:

$$d(u, v) = |\{i \leq n \,:\, u_i \neq v_i\}| \,.$$

A $C \subseteq Q^n$ kód *minimális távolsága* a különböző kódszavak Hamming-távolságainak minimuma:

$$d(C) = \min\{d(u, v) \,:\, u, v \in C, u \neq v\} \,.$$

Tehát $d(000, 111) = 3$, hiszen ez a két kódszó mindhárom koordinátában eltér. Így a 9.1.2. Példában szereplő kód minimális távolsága 3.

9.1.5. Gyakorlat. Igazoljuk, hogy $u, v, w \in Q^n$ esetén

$$d(u, w) \leq d(u, v) + d(v, w)$$

(ez a háromszög-egyenlőtlenség), és így d *metrika* Q^n-en.

9.1.6. Gyakorlat. Mutassuk meg, hogy a C kód pontosan akkor t-hibajelző, ha $t < d(C)$, és pontosan akkor t-hibajavító, ha $2t < d(C)$.

A 9.1.2. Példában szereplő kódolással minden üzenet hossza megháromszorozódik. Általában az üzenetek hossza n/k-szorosára nő. Azt szeretnénk tehát, hogy

(1) n minél kisebb legyen a k-hoz képest (ekkor használjuk hatékonyan a csatornát),
(2) a kód minél több hibát jelezzen és javítson, vagyis a minimális távolsága minél nagyobb legyen.

A kódszavak száma $|C| = q^k$, ezért az (1) pontot úgy is fogalmazhatjuk, hogy C elemszáma legyen minél nagyobb q^n-hez képest (vagyis minél több szó legyen kódszó). Az (1) és (2) ellenkező irányba húzó kívánalmak, a korlátokat az alábbi két becslés mutatja.

9.1.7. Állítás [Hamming-korlát]. *Ha a $C \subseteq Q^n$ kód minimális távolsága d, és $2t < d$, akkor*

$$q^{n-k} = \frac{q^n}{|C|} \geq \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \,.$$

Bizonyítás. Legyen $u \in C$ egy kódszó, és tekintsük a Q^n azon v elemeit, amelyekre $d(u, v) \leq t$ (ezek az u körüli, t sugarú „gömböt" alkotják). Mivel $2t < d$, ezek a gömbök páronként diszjunktak. A számuk $|C|$, és így $|C| \cdot s \leq q^n$, ahol s jelöli egy gömb elemszámát. Az u körüli gömb egy elemét úgy kaphatjuk meg, hogy kiválasztunk i darab koordinátát (ahol $i \leq t$), és ezeken a helyeken u-t megváltoztatjuk. Ezt minden koordinátában $q-1$-féleképpen tehetjük, és így s a fenti egyenlőtlenségben a jobb oldalon álló összeg. □

Az előző becslés persze akkor is érvényes, ha C-ről nem tesszük föl, hogy elemszáma q^k. Ha egyenlőség áll, vagyis ha a bizonyításban megadott gömbök le is fedik Q^n-et, akkor a kódot perfektnek nevezzük.

9.1.8. Definíció. Egy t-hibajavító $C \subseteq Q^n$ kód *perfekt*, ha minden $u \in Q^n$ szóhoz van tőle legfeljebb t Hamming-távolságra eső kódszó.

A 9.1.2. Példában szereplő kód nyilván perfekt. A 9.4. Szakasz végén látunk majd kevésbé triviális perfekt kódokat is (az úgynevezett Golay-kódokat). Nagyon kevés perfekt kód van, de ez nem okoz problémát, mert a hatékonyságot nem rontja lényegesen, ha a kód csak „közel optimális", és egy ilyen kód más szempontokból lehet előnyösebb.

9.1.9. Állítás [Singleton-korlát]. *Ha a $C \subseteq Q^n$ kód minimális távolsága d, akkor*

$$q^{n-k} = \frac{q^n}{|C|} \geq q^{d-1} \,.$$

Bizonyítás. Különböző kódszavak első $n-d+1$ koordinátája is különböző, mert ha egyenlő lenne, akkor ez a két szó csak az utolsó $d-1$ helyen térhetne el. Ezért a kódszavak száma legfeljebb q^{n-d+1} (hiszen ennyi $n-d+1$ hosszú szó létezik). □

A 9.1.2. Példában szereplő kód esetében a Singleton-féle korlátban is egyenlőség áll. Ennél a kódnál akkor tudunk hatékonyabbat tervezni, ha sok adatot kell küldeni, mert ilyenkor k és n értékét is növelni lehet. Ez lesz a következő szakaszok témája.

Gyakorlatok, feladatok

9.1.10. Gyakorlat. Legyen $Q = \{0, 1\}$. Kódoljunk egy k hosszúságú u-sorozatot úgy, hogy $k+1$-edik bitként az u végére írjuk az elemeinek mod 2 vett összegét (az úgynevezett paritásbitet). Milyen t-re lesz ez t-hibajelző, illetve t-hibajavító?

9.1.11. Gyakorlat. Legyen $Q = \{0, 1, \ldots, 9\}$ és $k = 9$. Kódoljuk az $u_1, \ldots, u_9$ sorozatot úgy, hogy tizedik jegyként hozzáírjuk a

$$\sum_{i=1}^{9} i u_i$$

összeg 11-gyel való osztási maradékát (ha ez 10, akkor a római tízes X számjegyet). Mutassuk meg, hogy ez 1-hibajelző kód, amely a szomszédos számjegyek felcserélését is jelzi.

Az előző gyakorlatban szereplő kód nem tesz eleget a 9.1.1. Definíciónak, hiszen egy újfajta jelet is használunk (az X-et). Ezt a kódolást használják a könyvek ISBN-számában, és a (magyarországi) személyi számban is. Láthatjuk, hogy a „csatorna" tipikus hibái befolyásolják a kód megválasztását, hiszen az ember gépeléskor hajlamos szomszédos számjegyeket és betűket felcserélni.

9.2. Lineáris kódok

A $Q = \{0, 1\}$ halmazt úgy is felfoghatjuk, mint a kételemű testet. Ekkor a 9.1.2. Példában szereplő két kódszó alteret alkot a Q^3 vektortérben.

9.2.1. Definíció. Ha Q a GF(q) test, és $C \subseteq Q^n$ altere a GF(q) fölötti Q^n vektortérnek, akkor a C-t *lineáris kódnak* nevezzük.

Mostantól kezdve az egész fejezetben csak lineáris kódokkal foglalkozunk. Lineáris algebrában (a [**10**] könyvben) megszoktuk, hogy a Q^n jelölés nem n hosszú sorozatokat, hanem n magas oszlopvektorokat jelent. Ezért a kódolandó sorozatokat (vagyis Q^k elemeit), és magukat a kódszavakat is sokszor oszlopvektornak fogjuk képzelni.

Lineáris kód esetében a kódolás eljárását, mint leképezést is célszerű lineárisnak választani, a következőképpen. Vegyünk egy $b_1, \ldots, b_k$ bázist a C altérben (amelyről tudjuk, hogy k-dimenziós, ha C elemszáma q^k). Az $u_1 u_2 \ldots u_k$ sorozathoz rendeljük hozzá az $u_1 b_1 + u_2 b_2 + \ldots + u_k b_k$ vektor komponenseiből álló kódszót. Az így kapott A leképezés nyilván lineáris Q^k-ból Q^n-be, mely injektív, és képtere C.

A most leírt kódolási eljárást mátrix-szorzással is elvégezhetjük, a következőképpen. Legyen $e_1, \ldots, e_k$ a Q^k vektortér szokásos bázisa (az e_i vektor i-edik koordinátája 1, a többi 0), és tekintsük a szokásos bázist a Q^n vektortérben is. Ekkor $A(e_i) = b_i$ teljesül minden $1 \leq i \leq k$ esetén. Ezért ha G jelöli az A lineáris leképezés mátrixát (a szokásos bázispárban), akkor G oszlopai pontosan a $b_1, \ldots, b_k$ vektorok lesznek. Ha $u \in Q^k$, akkor nyilván $A(u) = Gu$, vagyis a kódolás a G mátrixszal való szorzás segítségével történhet.

9.2.2. Definíció. Azt mondjuk, hogy a $G \in Q^{n \times k}$ a $C \subseteq Q^n$ lineáris kód egyik *generátormátrixa*, ha C a Gu vektorok halmaza, midőn u befutja Q^k-t.

A kódszavakat azért írtuk oszlopvektorokba, mert lineáris algebrai tanulmányaink során ezt szoktuk meg. Ez a konvenció sokmindent meghatároz, például azt is, hogy hogyan kell felírni egy A lineáris leképezés mátrixát úgy, hogy $[A(u)] = [A][u]$ teljesüljön. A kódelméletben azonban a kódvektorokat sokszor sorvektornak írják. Ezért az Olvasó ne csodálkozzon, ha a fenti G helyett sokszor a transzponáltját nevezik generátormátrixnak a szakirodalomban, és a C kód az uG alakú sorvektorok halmaza, ahol u a k hosszú sorvektorokat futja be. Ezt a konvenciót onnan lehet felismerni, hogy a generátormátrixnak k sora és n oszlopa van.

Célszerű, ha az $u \mapsto Gu$ kódolás során a Gu kódszó első k komponense maga u, vagyis kódoláskor az u után írunk további „ellenőrző" betűket. Ez nyilván pontosan akkor igaz, ha a G mátrix első k sora a $k \times k$-as egységmátrix. Az ilyen kódolást *szisztematikusnak* nevezzük.

Például a 9.1.2. Példában szereplő „háromszorozó" kód generátormátrixa a csupa 1-esből álló, három magas, egy széles mátrix. A 9.1.10. Gyakorlatban szereplő „paritásbites" kódolás szintén szisztematikus, és a G mátrixát úgy kapjuk, hogy a $k \times k$-as egységmátrix alá még egy csupa 1-esekből álló sort írunk (ami a paritásbitet számítja ki).

Lineáris kód esetén az u és v kódszavak Hamming-távolsága nyilván az $u - v$ vektor nem nulla komponenseinek a száma.

9.2.3. Definíció. Ha $v \in Q^n$, akkor a v *súlya* a nem nulla komponenseinek a száma, azaz

$$|\{i \leq n \,:\, v_i \neq 0\}|\,.$$

Egy lineáris kód minimális távolsága tehát a nem nulla kódszavak súlyának minimuma.

9.2.4. Gyakorlat. Legyen $C \leq Q^n$ egy k-dimenziós altér. Mutassuk meg, hogy a koordináták alkalmas permutálásával C-ből készíthetünk egy olyan $D \subseteq Q^n$ alteret, amelynek alkalmas generátormátrixában az első k sor a $k \times k$-as egységmátrix, és a D kód minimális távolsága ugyanaz, mint a C kódé.

Az előző gyakorlat szerint minden lineáris kód szisztematikusnak tekinthető. A következő fogalom a kód minimális távolságának kiszámításához és a dekódoláshoz is hasznos.

9.2.5. Definíció. Legyen $C \subseteq Q^n$ egy k-dimenziós lineáris kód. Az olyan $P \in Q^{(n-k)\times n}$ mátrixokat, melyre v akkor és csak akkor kódszó, ha $Pv = 0$, a kód *ellenőrző mátrixának* nevezzük.

A 9.2.2. Definíció utáni megjegyzéshez hasonlóan, ha a kódszavakat nem oszlopvektorokba, hanem sorvektorokba írjuk, akkor az ellenőrző mátrix is transzponálódni fog, és a kód szavai azok a vektorok lesznek, melyekre $vP = 0$. Egyes könyvekben előfordul azonban, hogy ehelyett a $vP^T = 0$ egyenlőséget követelik meg, vagyis az ellenőrző mátrixot „visszatranszponálják". Biztosat most is csak úgy tudhatunk, ha megnézzük a sorok és oszlopok számát.

9.2.6. Gyakorlat. Legyen C a G generátormátrixszal megadott lineáris kód. Igazoljuk, hogy létezik ellenőrző mátrixa, és pontosan azok a $P \in Q^{(n-k)\times n}$ mátrixok megfelelők, melyek rangja $n-k$ és melyekre $PG = 0$. Speciálisan ha C szisztematikus, és

$$G = \begin{bmatrix} E_k \\ M \end{bmatrix}, \quad \text{akkor} \quad P = \begin{bmatrix} -M & E_{n-k} \end{bmatrix}$$

ellenőrző mátrix lesz (itt E_m jelöli az $m \times m$-es egységmátrixot).

Természetesen az előző gyakorlatban szereplő P mátrix rangja legfeljebb $n-k$ lehet, hiszen $n-k$ sora van. Ezért P akkor lesz paritásellenőrző mátrix, ha $PG = 0$ mellett P-nek van $n-k$ független oszlopa (vagy ha P sorai függetlenek).

9.2.7. Állítás. *Legyen $C \subseteq Q^n$ egy k-dimenziós lineáris kód, melynek minimális távolsága d, és P a kód (egyik) ellenőrző mátrixa. Ekkor d a legkisebb olyan egész, amelyre P-nek van d darab lineárisan összefüggő oszlopa.*

Bizonyítás. A P oszlopainak a $\lambda_1, \ldots, \lambda_n$ együtthatókkal vett lineáris kombinációja akkor és csak akkor nulla, ha $Pv = 0$, ahol v a $\lambda_1, \ldots, \lambda_n$ komponensekből álló (oszlop)vektor, vagyis ha v kódszó. A v vektor súlya azt adja meg, hogy a λ_i elemek között hány nem nulla. Ha tehát néhány oszlop lineárisan összefügg, akkor van ennél nem nagyobb súlyú $v \neq 0$ kódszó. Megfordítva, mivel van d súlyú, nem nulla kódszó, ezért a megfelelő d oszlop biztosan lineárisan összefügg. □

Ennek az állításnak a felhasználásával könnyen gyárthatunk 1-hibajavító lineáris kódot (amely perfekt is lesz). Legyen $m \geq 2$, és P egy olyan mátrix, amelynek az oszlopaiban azok a $0 \neq w \in Q^m$ vektorok szerepelnek (pontosan egyszer), melyeknek az első nem nulla komponense 1.

Valójában csak az a fontos, hogy a P mátrix oszlopaiban Q^n minden nem nulla w vektorához pontosan egy w-vel párhuzamos vektor legyen (lásd a következő gyakorlat megoldását).

9.2.8. Gyakorlat. Mutassuk meg, hogy a most definiált P mátrix oszlopainak száma

$$n = \frac{q^m - 1}{q - 1} = q^{m-1} + q^{m-2} + \ldots + q + 1\,.$$

9.2.9. Definíció. Az imént megadott P mátrixszal, mint ellenőrző mátrixszal megadott kódot, vagyis a $C = \{v \in Q^n \,:\, Pv = 0\}$ kódot *Hamming-kódnak* nevezzük.

Annak igazolásához, hogy P tényleg ellenőrző mátrixa ennek a kódnak, meg kell mutatni, hogy a rangja ugyanaz, mint a sorainak az m száma (vö. 9.2.6. Gyakorlat). Ez igaz, mert az egységmátrix oszlopvektorait is megtalálhatjuk P oszlopai között. Ezért a Hamming kód $n-m$-dimenziós (ahol n a 9.2.8. Gyakorlatban megadott szám). Nyilván P bármely két oszlopa független, így a 9.2.7. Állítás miatt a Hamming-kód minimális távolsága legalább 3. Ezért ez a kód 1-hibajavító (9.1.6. Gyakorlat).

9.2.10. Gyakorlat. Igazoljuk, hogy a Hamming-kód perfekt 1-hibajavító kód.

Végül a dekódolásról ejtünk pár szót. Legyen $C \subseteq Q^n$ egy k-dimenziós kód, melynek generátormátrixa G, ellenőrző mátrixa P, és minimális távolsága d. Láttuk, hogy a kódolás az $u \mapsto v = Gu$ leképezéssel történhet. Ha a vevőkészülékbe ez a v szó hibátlanul érkezett, akkor mivel a G mátrixot ismerjük, az u egy lineáris egyenletrendszer megoldásával kapható. Ha a kód szisztematikus, akkor u egyszerűen a v első k koordinátája lesz.

Ha az átvitel során hiba keletkezett, akkor a Gu helyett egy $v = Gu + h$ vektort kapunk. Meg kell határoznunk a Gu vektort (feltéve, hogy a hibák száma nem túl nagy, vagyis a h hibavektornak kevés komponense különbözik nullától). Nyilván $Pv = PGu + Ph = Ph$, ezt a v vektor *szindrómájának* nevezzük. Ha a h komponensei $\lambda_1, \ldots, \lambda_n$, akkor Ph a P oszlopainak a λ_i együtthatókkal vett lineáris kombinációja. Ha a λ_i elemek közül csak t nem nulla van, ahol $2t < d$, akkor a Ph lineáris kombináció egyértelműen meghatározza a h hibavektort (a 9.2.7. Állítás miatt). Speciálisan Ph pontosan akkor nulla, ha v kódszó.

Az, hogy Ph-ból h milyen (lehetőleg gyors) algoritmussal kapható vissza, a kód megadásától függ. Például a Hamming-kód esetében ha $Ph \neq 0$, és feltesszük, hogy csak egy hiba történt, vagyis hogy a h vektor egyetlen nem nulla komponense a λ_i, akkor $Ph = \lambda_i p_i$, ahol p_i a P mátrix i-edik oszlopa. A λ_i leolvasható, mint a Ph első nem nulla komponense. Ezért ismerjük a p_i vektort, tehát az i számot is. Ezáltal sikerült h-t kiszámítani, ahonnan $Gu = v - h$.

Gyakorlatok, feladatok

9.2.11. Gyakorlat. Készítsünk egy olyan Hamming-kódot a háromelemű test fölött, melynek hossza 13 és dimenziója 10. Mutassuk meg ennek segítségével, hogy a TOTÓ-n elegendő $3^{10} = 59049$ hasábot (ügyesen) megjátszani ahhoz, hogy biztosan legyen legalább 12 találatunk.

9.3. Polinomkódok

Ha a lineáris kódokat polinomok segítségével adjuk meg, akkor ez segíthet a minimális távolság megtervezésében és a dekódolásban is. Ezért most az $u = u_1 u_2 \ldots u_{k-1} u_k$ szó helyett nem a megfelelő oszlopvektort, hanem az

$$u_1 x^{k-1} + u_2 x^{k-2} + \ldots + u_{k-1} x + u_k$$

polinomot tekintjük, ezek is Q^k-val izomorf vektorteret alkotnak Q fölött. Az alábbiak megértéséhez mindenképpen érdemes átismételni a véges testekről a 6.7. Szakaszban tanultakat, a konkrét példákat is beleértve.

9.3.1. Definíció. Legyen $g(x)$ egy $n - k$-adfokú polinom $Q = \mathrm{GF}(q)$ fölött, és C az $u(x)g(x)$ alakú polinomok halmaza, ahol u befutja a k-nál kisebb fokú $Q[x]$-beli polinomokat (ide értve a nullapolinomot is). A kapott C kódot *polinomkódnak* nevezzük, melynek *generátorpolinomja* g.

Természetesen C egy k-dimenziós altér a legfeljebb n-edfokú polinomok között, hiszen az $u \mapsto ug$ leképezés injektív és lineáris.

9.3.2. Gyakorlat. Írjuk föl a $g(x) = a_0 + a_1x + \ldots + a_{n-k}x^{n-k}$ polinomhoz tartozó polinomkód egyik generátormátrixát.

A minimális távolság becslésének alapvető eszköze a következő állítás.

9.3.3. Állítás. *Tekintsük az előző definícióban szereplő polinomkódot. Tegyük föl, hogy $\alpha \neq 0$ egy olyan eleme a Q test egy bővítésének, melynek rendje a szorzásra legalább n. Ha a g polinomot úgy választjuk, hogy $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ gyöke legyen valamely $d \leq n$ egészre, akkor a kód minimális távolsága legalább d.*

Bizonyítás. Azt kell belátni, hogy minden nem nulla kódszónak, vagyis minden $v = ug$ alakú nem nulla polinomnak legalább d darab nem nulla együtthatója van. Tegyük föl, hogy egy ilyen polinom a $v(x) = v_1x^{n_1} + \ldots + v_mx^{n_m}$, ahol $m < d$. Ennek gyöke $\alpha, \alpha^2, \ldots, \alpha^{d-1}$, és ezért

$$\begin{bmatrix} \alpha^{n_1} & \ldots & \alpha^{n_m} \\ \alpha^{2n_1} & \ldots & \alpha^{2n_m} \\ \vdots & & \vdots \\ \alpha^{mn_1} & \ldots & \alpha^{mn_m} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{bmatrix} = \begin{bmatrix} v(\alpha) \\ v(\alpha^2) \\ \vdots \\ v(\alpha^m) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Ez egy homogén lineáris egyenletrendszernek is felfogható a $v_1, \ldots, v_m$ ismeretlenekre, amelynek a determinánsa

$$\alpha^{n_1+\ldots+n_m} \prod_{i>j} (\alpha^{n_i} - \alpha^{n_j}),$$

hiszen az oszlopokból α^{n_i}-t kiemelve Vandermonde-determinánst kapunk (A.5.2. Tétel). Mivel a v polinom kódszóhoz tartozik, a foka kisebb, mint n, és így mindegyik n_i kitevő is n-nél kisebb. De α rendje legalább n, és így az α^{n_i} elemek páronként különbözők. Mivel $\alpha \neq 0$, a fenti determináns értéke sem nulla. De akkor a homogén lineáris egyenletrendszernek csak triviális megoldása van, vagyis mindegyik v_i nulla. Tehát $v = 0$. □

9.3.4. Gyakorlat. Bizonyítsuk be, hogy az előző 9.3.3. Állítás akkor is érvényben marad, ha $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ helyett α tetszőleges $d-1$ darab egymás utáni hatványát, vagyis az $\alpha^s, \alpha^{s+1}, \ldots, \alpha^{s+d-2}$ elemeket vesszük valamilyen s egészre.

Láttuk, hogy a kód hatékonyságát az $n-k$ szám, vagyis a g polinom foka méri. Ezért a g polinomot úgy célszerű választani, hogy a foka minél kisebb legyen. Ha viszont az előző állításban szereplő $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ gyöke g-nek, akkor ez g fokszámára alsó korlátot szab.

9.3.5. Definíció. Tegyük föl, hogy az előző 9.3.3. Állításban szereplő α magának a Q testnek (és nem egy bővítésének) az eleme, továbbá $g(x) = (x-\alpha)\ldots(x-\alpha^{d-1})$. A g generálta n hosszú kódot *Reed–Solomon-kódnak* nevezzük.

Mivel azt továbbra is feltesszük, hogy α rendje legalább n, a Reed–Solomon-kód minimális távolsága legalább d. Másfelől a $g(x)\cdot 1$ kódszónak legfeljebb d nem nulla együtthatója lehet, hiszen ez egy $d-1$ fokú polinom, tehát a minimális távolság pontosan d. Tudjuk, hogy $n-k$ éppen a g foka, vagyis $d-1$, és így a Singleton-féle korlátban (9.1.9. Állítás) egyenlőség áll (vagyis a Reed–Solomon-kód közel optimális).

Ugyanakkor ahhoz, hogy $d \le n$ elég nagy legyen, az α elem rendje, és így a Q test elemszáma, vagyis az ábécé jeleinek a száma sem lehet túl kicsi. Ha csak kevés jelet akarunk, például ha Q a kételemű test, akkor α egy valódi bővítésnek kell, hogy az eleme legyen. Ekkor minimális fokú generátorpolinomot a következőképpen választhatunk.

9.3.6. Definíció. Legyen $\alpha \neq 0$ a Q test egy bővítésének legalább n rendű eleme, és g az $\alpha, \alpha^2, \dots, \alpha^{d-1}$ elemek Q fölötti minimálpolinomjainak legkisebb közös többszöröse. A g generálta n hosszú kódot *BCH-kódnak* nevezzük, ahol a $d \le n$ szám a kód *tervezett távolsága*.

A BCH-kódok tehát a Reed–Solomon-kódok általánosításai. Az elnevezés a felfedezők nevéből (Bose és Ray-Chaudhuri, valamint Hocquenghem) származik.

A Reed–Solomon és a BCH kódok pontos definíciója távolról sem egységes a szakirodalomban. Van, ahol a definíció a 9.3.4. Gyakorlatnak megfelelő általánosságúvá módosul. Megfordítva, sokszor speciális feltételeket szabnak a fenti definíciókhoz képest. Gyakori feltevés például, hogy az α elem rendje pontosan n (és ne csak legalább n) legyen. Ez azt jelenti, hogy olyan hosszú kódszavakat használunk, amilyeneket csak α (rendje) megenged. Ilyenkor a fenti definícióban szereplő kódot *rövidített* kódnak nevezik. A Reed–Solomon-kód esetében néha feltételezik, hogy $n = q-1$ teljesül, vagyis hogy α generálja a Q test multiplikatív csoportját, más néven *primitív* elem. Végül természetes feltevés, hogy $d = 2t+1$, vagyis páratlan szám legyen (ha t-hibajavító kódot keresünk).

Először két kirívóan egyszerű, összetartozó példát adunk, amely azonban alkalmas az alapfogalmak bemutatására.

9.3.7. Példa. Legyen α a négyelemű test multiplikatív csoportjának egy generátoreleme, $n = 3$ (az α rendje), és $d = 3$.

Ha Reed–Solomon-kódot akarunk készíteni, akkor Q a négyelemű test, vagyis négy jelünk van. A 6.7.6. Tétel szerint a négyelemű test elemei az $x^4 - x$ polinom gyökei, amik között a nulla, és $\alpha^3 = 1$ is szerepel. Ezért

$$g(x) = (x-\alpha)(x-\alpha^2) = \frac{x^4-1}{x(x-1)} = x^2+x+1\,.$$

Az együtthatók tehát Q prímtestéből valók (ami egy általános Reed–Solomon-kód esetében nem feltétlenül teljesül). Mivel g foka $n-k=2$, ezért $n=3$ miatt a kód $k=1$-dimenziós. Jelölje β az α^2 elemet, akkor tehát a kód elemei a konstans polinomok g-szeresei, vagyis

$$\left\{0\,,\ \ x^2+x+1\,,\ \ \alpha x^2+\alpha x+\alpha\,,\ \ \beta x^2+\beta x+\beta\right\},\quad \text{azaz}\quad \{000\,,\ \ 111\,,\ \ \alpha\alpha\alpha\,,\ \ \beta\beta\beta\}\,.$$

Láthatjuk, hogy ez a 9.1.2. Példából jól ismert „háromszorozó” kódolás, csak éppen egy négyelemű ábécével. Természetesen a csatornán nem az α és β jeleket küldjük, hanem ezek bináris változatát a következő táblázat szerint:

$$0 \leftrightarrow 00\,, \quad 1 \leftrightarrow 01\,, \quad \alpha \leftrightarrow 10\,, \quad \beta = \alpha^2 \leftrightarrow 11\,.$$

Ez a megfeleltetés tehát $a\alpha + b \leftrightarrow ab$ (ahol a, b a GF(4) prímtestének elemei), vagyis az egyszerű bővítés elemeinek szokásos felírása (6.1.13. Tétel). Összefoglalva: ez a Reed–Solomon-kód a küldendő üzenetet két bit hosszú darabokra vágja föl, és minden ilyen bitpárt megháromszorozva küld. Egy hibát javít, kettőt jelez, és egy N bites üzenetet $3N$ hosszúra növel.

Most próbáljunk ugyanezen α felhasználásával egy BCH-kódot készíteni. Legyen Q a kételemű test. Az α és $\alpha^2 \in \mathrm{GF}(4)$ elemek közös minimálpolinomja Q fölött $x^2 + x + 1$, mint azt az imént beláttuk. Ha most is $n = d = 3$, akkor $k = 1$, és így a kapott BCH-kód a fenti, azzal a különbséggel, hogy most az ábécé csak két betűből áll, tehát pontosan a 9.1.2. Példában szereplő kódot kapjuk.

A következő példa azért érdekes, mert itt a Reed–Solomon-kódban és a BCH-kódban szereplő generátorpolinom már más lesz, és így a két kód dimenziója sem egyenlő.

9.3.8. Példa. Legyen α a nyolcelemű test multiplikatív csoportjának egy generátoreleme, $n = 7$ (az α rendje), és $d = 3$.

Ekkor a Reed–Solomon-kód esetében $g(x) = (x - \alpha)(x - \alpha^2)$ másodfokú polinom továbbra is, és így a kód dimenziója $k = 7 - 2 = 5$. Ha a kételemű test fölötti BCH-kódot akarunk készíteni, akkor az α minimálpolinomját kell kiszámítani, ami harmadfokú, hiszen a $2^3 = 8$ elemű test a kételemű testnek harmadfokú bővítése. Ez a polinom a kételemű test fölötti harmadfokú irreducibilis polinomok bármelyike lehet, akár $x^3 + x + 1$, akár $x^3 + x^2 + 1$ (ez az α választásától függ). Mindkét esetben tudjuk, hogy ennek a polinomnak α^2 is gyöke, mert a négyzetre emelés a $\mathrm{GF}(2) \leq \mathrm{GF}(8)$ bővítésnek relatív automorfizmusa (lásd a 6.7.9. Tétel után részletesen kidolgozott példát). Ezért g ebben az esetben harmadfokú lesz, és így a kód dimenziója $7 - 3 = 4$. Mindkét kód továbbra is egy hibát javít, kettőt jelez.

Számítsuk ki, hogyan változik az üzenetek hossza a kódolás során. A Reed–Solomon-kódnál az üzenetet most három bites darabokra vágjuk, mert az ábécé $2^3 = 8$ elemű. Ilyen három bites darabokból összesen ötöt veszünk, mert a kód ötdimenziós. Ehelyett küldünk $n = 7$ jelet, vagyis $7 \cdot 3 = 21$ bitet. Vagyis ha a kódolandó üzenet N bitből áll, akkor a kódolt üzenet hossza $21N/15 = (7/5)N$ bit. A BCH-kódnál négy a dimenzió, és így az N bites üzenetet helyett $(7/4)N$ bitet küldünk.

Ez a számítás azt a látszatot keltheti, hogy a BCH-kód a kevésbé hatékony, hiszen ugyanazt az üzenetet hosszabbra kódolja, miközben a hibajavító képessége ugyanaz. Ez azonban nem ilyen egyszerű! Képzeljük azt, hogy a csatorna 7 bitenként átlagosan 1-et hibázik. Megérkezik a vevőbe 21 bit, amiben 3 hiba is lehet. A Reed-Solomon-kód esetében ez egyetlen kódszó, amely 7 betűből áll, és három betű is elromolhatott, ezért a kód esetleg

nem is jelzi a hibát. A BCH-kód esetében viszont ez a 21 bit három egymás utáni kódszó, és ha a három hiba három különböző szóban van, akkor a kód mindhármat ki tudja javítani. Ha viszont a három hiba hajlamos egymás mellett lenni, akkor a Reed–Solomon-kódban esetleg csak egy betű romlott el, amit a kód ki tud javítani, miközben a BCH-kód esetleg nem is jelzi a hibát. Ez a példa jól mutatja, hogy a csatorna tipikus hibáinak a jellegét figyelembe kell venni a kódolás megválasztásakor.

A most következő példa két okból fontos. Egyrészt látni fogjuk, hogy az α elem rendje hogyan függ össze a minimálpolinomjának a választásával. Másrészt meg tudjuk vizsgálni a segítségével a dekódolás kérdését is.

9.3.9. Példa. Legyen α a tizenhat elemű L test multiplikatív csoportjának egy generátoreleme, $n = 15$ (az α rendje), és $d = 5$.

Adjuk meg az L testet GF(2)$[x]/(m)$ alakban, ahol $m(x) = x^4 + x^3 + 1$, és legyen $\alpha = x + (m)$ (be fogjuk látni, hogy ez tényleg generátorelem). Először az L testtel ismerkedünk meg, ezért az elemeit kétféle alakban is fölírjuk. Az egyik a GF(2) fölötti $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$, amit a kódelmélet szellemében az $a_3a_2a_1a_0 \in \{0, 1\}^4$ sorozattal rövidítünk. A másik alak az α hatványaként való felírás (a nulla ekkor kimarad). Az α^i-hez tartozó sorozatot úgy kapjuk, hogy az x^i polinomot maradékosan elosztjuk x^4+x^3+1-gyel. Azt tapasztaljuk, hogy α-nak tényleg 15 különböző hatványa van, a következő „logaritmustábla” szerint.

0	0000	α	0010	α^2	0100	α^3	1000
α^4	1001	α^5	1011	α^6	1111	α^7	0111
α^8	1110	α^9	0101	α^{10}	1010	α^{11}	1101
α^{12}	0011	α^{13}	0110	α^{14}	1100	α^{15}	0001

Az $m(x)$ polinom gyökei α, α^2, α^4, α^8, hiszen a négyzetre emelés relatív automorfizmus. Ezért m gyökei mind generátorelemek (a szorzásra), hiszen ezek a kitevők a 15-höz relatív prímek. Tehát m egy primitív polinom (6.7.10. Definíció). Mivel $\varphi(15) = 8$, e test multiplikatív csoportjának még négy generátoreleme van, ezek szintén az α-nak a 15-höz relatív prím kitevőjű hatványai, vagyis α^7, α^{14}, $(\alpha^{14})^2 = \alpha^{13}$ és $(\alpha^{13})^2 = \alpha^{11}$. Mivel ezek pont az α, α^2, α^4, α^8 reciprokai, a közös minimálpolinomjuk (a reciprok polinomokról tanultak alapján) $x^4 + x + 1$, ami tehát a másik primitív negyedfokú polinom. Az alaptest elemei 0 és $\alpha^{15} = 1$, ezek minimálpolinomja elsőfokú. A másodfokú elemek egy négyelemű testben vannak, és így multiplikatív rendjük csak három lehet. Ezek tehát α^5 és α^{10}, közös minimálpolinomjuk $x^2 + x + 1$ (ami szintén primitív). A kimaradó négy elem, vagyis α^3, α^6, α^{12} és $(\alpha^{12})^2 = \alpha^9$ tehát csakis a fennmaradó harmadik negyedfokú irreducibilis polinomnak, vagyis az $m_3(x) = x^4 + x^3 + x^2 + x + 1$-nek lehetnek a gyökei (3.3.17. Gyakorlat). Ezek pont a multiplikatív csoport ötödrendű elemei, és így ez a polinom nem primitív.

A BCH-kódhoz tartozó g generátorpolinom az α, α^2, α^3, α^4 minimálpolinomjainak legkisebb közös többszöröse, vagyis az előzőek szerint

$$g(x) = m(x)m_3(x) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^4 + x^2 + x + 1\,.$$

Ez nyolcadfokú, és így a kód dimenziója $k = 15 - 8 = 7$. Ez azt jelenti, hogy egy N bites üzenetet $(15/7)N$ bitessé kódolunk, azonban ez a kódolás már 2-hibajavító, hiszen $d = 5$.

Most vizsgáljuk meg a dekódolás kérdését. A vevőbe érkezett $v_1 v_2 \ldots v_{15}$ szóhoz tartozó v polinom akkor és csak akkor van benne a kódban, ha osztható g-vel. Ezt nemcsak polinomosztással ellenőrizhetjük, hanem az α és α^3 behelyettesítésével is (hiszen g többszörösei pontosan azok a polinomok, amelyeknek α és α^3 gyöke). Ezt felírhatjuk egy mátrixos egyenlet formájában is:

$$\begin{bmatrix} \alpha^{14} & \alpha^{13} & \ldots & \alpha & 1 \\ \alpha^{42} & \alpha^{39} & \ldots & \alpha^3 & 1 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_{15} \end{bmatrix} = \begin{bmatrix} v(\alpha) \\ v(\alpha^3) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Azt gondolhatnánk, hogy a baloldali mátrix ennek a kódnak (az egyik) ellenőrző mátrixa. Ez azonban nem egészen van így, mert e mátrix elemei nem a Q alaptestben, hanem az L bővítésben vannak. Ezen úgy segíthetünk, hogy a $v_1\alpha^{14} + v_2\alpha^{13} + \ldots + v_{15} = 0$ egyenletbe beírjuk mindegyik α^i-nek az $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$ alakú kifejezését a fenti logaritmustábla alapján. Így egy helyett négy egyenletet kapunk: rendre az α^3, α^2, α, 1 együtthatóját kell nullává tenni. Ezt mátrixosan úgy írhatjuk le, hogy a fenti 2×15-ös mátrixban mindegyik α^i elem helyére beírjuk a neki megfelelő Q^4-beli elemet, oszlopvektor formájában. A kapott mátrix a következő lesz:

$$P = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Ez már ellenőrző mátrix, hiszen $n - k = 8$ sora van. Általában is szokás a BCH-kódot úgy definiálni, hogy a

$$P = \begin{bmatrix} \alpha^{n-1} & \ldots & \alpha^2 & \alpha & 1 \\ \alpha^{2(n-1)} & \ldots & \alpha^4 & \alpha^2 & 1 \\ \vdots & & \vdots & \vdots & \vdots \\ \alpha^{(d-1)(n-1)} & \ldots & \alpha^{2(d-1)} & \alpha^{d-1} & 1 \end{bmatrix}$$

mátrixot adjuk meg (ahol mindegyik α^i helyére a neki megfelelő, alaptest feletti oszlopvektort írjuk), és azokat a v vektorokat tekintjük, amelyekre $Pv = 0$. Ebben az általános esetben is azok lesznek a kódpolinomok, amelyeknek $\alpha, \dots, \alpha^{d-1}$ gyöke, vagyis tényleg a 9.3.6. Definícióban szereplő g polinom többszörösei. A P akkor lesz az ellenőrző mátrix, ha sorainak száma megegyezik $n-k$-val (általában ennél több sora van).

Lássuk most, hogy az előbbi példában hogyan lehet két hibát is kijavítani. Tegyük föl, hogy a $v = 000000010001111$ szó érkezett, vagyis a $v(x) = x^7+x^3+x^2+x+1$ polinom. Ekkor a fenti logaritmustábla alapján számolva

$$v(\alpha) = \alpha^7 + \alpha^3 + \alpha^2 + \alpha + 1 = (\alpha^2 + \alpha + 1) + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^3\,,$$

és hasonlóan $v(\alpha^3) = \alpha^{21}+\alpha^9+\alpha^6+\alpha^3+1 = \alpha^3+\alpha^2$ (hiszen $\alpha^{21} = \alpha^6$ és $\alpha^9 = \alpha^2+1$ a táblázat szerint). Mivel nem mindkét kapott eredmény nulla, hiba történt. Tegyük föl, hogy a hibák száma legfeljebb kettő (hiszen 2-hibajavító kódról van szó). Ez azt jelenti, hogy az eredetileg küldött polinom $v(x)+x^i$, vagy $v(x)+x^i+x^j$ volt, aminek α és α^3 is gyöke. Legyen $r = \alpha^i$, és $s = \alpha^j$ (illetve ha csak egy hiba volt, akkor $s = 0$). A fenti számítás alapján (felhasználva, hogy 2 karakterisztikában $1 = -1$),

$$r + s = v(\alpha) = \alpha^3 \quad \text{és} \quad r^3 + s^3 = v(\alpha^3) = \alpha^3 + \alpha^2\,.$$

Ezt az egyenletrendszert kell megoldani L-ben. Az $r^3 + s^3 = (r+s)\big((r+s)^2 - 3rs\big)$ azonosságból $rs = \alpha^{14} + \alpha^6 + 1 = \alpha$, és így r és s az $x^2 + \alpha^3 x + \alpha = 0$ másodfokú egyenlet gyökei (a gyökök és együtthatók összefüggése miatt).

Kettő karakterisztikájú gyűrűben nem működik a másodfokú egyenlet megoldóképlete (lásd 5.7.12. Gyakorlat). A fenti testben mégis meg tudjuk oldani a másodfokú egyenleteket, ha az ismeretlent $x = a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$ alakban keressük. Ugyanis ezt a kifejezést is tagonként lehet négyzetre emelni, és $a_i^2 = a_i$, mert $a_i \in \{0, 1\}$. Így pedig a behelyettesítés után lineáris egyenletrendszert kapunk az a_i ismeretlenekre.

A most kapott $x^2 + \alpha^3 x + \alpha = 0$ másodfokú egyenletről ránézésre is látszik, hogy $x = \alpha^2$ gyöke, mert $\alpha^4 + \alpha^5 + \alpha = \alpha(\alpha^4 + \alpha^3 + 1) = \alpha m(\alpha) = 0$. Innen a másik gyök $(r+s) - \alpha^2 = \alpha^3 + \alpha^2$, ami a táblázatból visszakeresve α^{14}. A hiba tehát a jobbról számított $2+1 = 3$ és $14+1 = 15$ sorszámú koordinátában történt, vagyis az eredetileg küldött szó az 100000010001011 volt. A $g(x)$ polinommal osztva ebből dekódolás után 1000101 lesz.

Ez az algoritmus persze nem optimális (és mellesleg ilyen kis méretű kódok esetében a visszakeresés még táblázatosan is lehetséges). Híres algoritmusok (például Berlekamp–Massey, Chien, Forney algoritmusai) teszik lehetővé a dekódolás hatékony elvégzését.

Az ebben a szakaszban szereplő $v \mapsto vg$ kódolás általában nem szisztematikus. A következő szakaszban kiderül, kicsit általánosabb köntösben, hogy ezen a problémán hogyan lehet úrrá lenni.

Gyakorlatok, feladatok

9.3.10. Gyakorlat. Tekintsük a 9.3.6. definícióban megadott BCH-kódot, ahol Q a kételemű test. Tegyük föl, hogy az α elem rendje pontosan $n = 2^r - 1$, és $d = 2t + 1$. Mutassuk meg, hogy a kód dimenziója legalább $n - rt$. Igazoljuk azt is, hogy $t = 1$ esetén Hamming-kódot kapunk.

9.4. Ciklikus kódok

A BCH-kódoknak van egy hasznos tulajdonsága, amely egy általánosítást is lehetővé tesz, így kapjuk a ciklikus kódokat. Felírjuk ezek generátor- és ellenőrző mátrixát, és megemlítjük, hogy hogyan lehet a kódolást szisztematikussá tenni. Ezt az eljárást CRC-kód néven számtalan helyen alkalmazzák a számítástechnikában. Végül az úgynevezett kvadratikus maradék kódokról ejtünk szót, amelyek elvezetnek a Golay-féle perfekt kódokhoz.

9.4.1. Definíció. A C kódot *ciklikusnak* nevezzük, ha minden $v_1v_2v_3\dots v_n$ kódszó esetén $v_2v_3\dots v_nv_1$ is kódszó (vagyis kódszó minden ciklikus permutáltja is kódszó).

9.4.2. Állítás. *Tekintsük a 9.3.6. definícióban megadott BCH-kódot, és tegyük föl, hogy az α elem rendje pontosan n. Ekkor ez a kód ciklikus.*

Bizonyítás. Mivel $\alpha^n = 1$, ezért $(\alpha^i)^n - 1 = 0$ minden i-re. Ezért az α^i minimálpolinomja osztója $x^n - 1$-nek. Így ezeknek a legnagyobb közös osztója, azaz a g generátorpolinom is osztója $x^n - 1$-nek.

Ha $v_1v_2\dots v_n$ kódszó, akkor g osztója $v_1x^{n-1} + v_2x^{n-2} + \dots + v_n$-nek. A $v_2v_3\dots v_nv_1$ szóhoz tartozó polinom a

$$v_2x^{n-1} + v_3x^{n-2} + \dots + v_nx + v_1 = x(v_1x^{n-1} + v_2x^{n-2} + \dots + v_n) + v_1(1 - x^n)\,.$$

Ez tehát szintén osztható g-vel, és így a kódhoz tartozik. □

9.4.3. Feladat. Mutassuk meg, hogy ha C egy n hosszú ciklikus lineáris kód, akkor polinomkód is egyúttal, vagyis van olyan $g(x) \mid x^n - 1$ polinom, hogy C elemei pontosan a g-vel osztható polinomok.

A polinomkódok generátormátrixát már felírtuk a 9.3.2. Gyakorlatban. Ez a kódolást megadó $A\big(u(x)\big) = g(x)u(x)$ leképezés mátrixa volt a „szokásos” bázispárban, ahol az m-nél kisebb fokú polinomok vektorterének „szokásos” bázisán az $x^{m-1}, x^{m-2}, \dots, x, 1$ bázist értjük. Ennek a bázisnak az az előnye, hogy az $u_1u_2\dots u_m$ sorozathoz tartozó $u(x) = u_1x^{m-1} + u_2x^{m-2} + \dots + u_m$ polinom koordinátavektora ebben a bázisban éppen az az oszlopvektor, amelyben a koordináták felülről lefelé haladva $u_1, u_2, \dots, u_m$. Írjuk fel most a megfelelő ellenőrző mátrixot is, ciklikus polinomkód esetén.

Mivel ciklikus kódról van szó, a 9.4.3. Feladat miatt $x^n - 1 = g(x)p(x)$ alkalmas p polinomra. Tekintsük azt a B lineáris leképezést, amely egy n-nél kisebb fokú $v(x)$ polinomhoz a vp polinom $x^n - 1$-gyel való osztási maradékát rendeli. Ha v a kódban van,

akkor $v = ug$ alkalmas u-ra, és ekkor $vp = ugp$ osztható $x^n - 1$-gyel, tehát $B(v) = 0$. Megfordítva, ha $B(v) = 0$, akkor $g(x)p(x) = x^n - 1 \mid v(x)p(x)$, ahonnan $g \mid v$, tehát v a kódban van. Ez azt jelenti, hogy B magja pontosan a kódbeli polinomokból áll.

Írjuk fel most B mátrixát a szokásos bázispárban. A $[B(v)] = [B][v]$ egyenlőség miatt $[B][v]$ akkor és csak akkor nulla, ha v a kódban van. Ez fontos tulajdonsága a kód ellenőrző mátrixának is (lásd 9.2.5. Definíció), és így a p polinomot szokás e ciklikus kód *ellenőrző polinomjának* hívni. Ennek foka k, hiszen g foka $n - k$, és $g(x)p(x) = x^n - 1$.

A $[B]$ mátrix mégsem ellenőrző mátrixa a kódnak, hiszen B egy n-dimenziós vektortérből egy n-dimenziós vektortérbe képez, az ellenőrző mátrixnak pedig egy $(n - k) \times n$-es mátrixnak kell lennie. Megmutatjuk, hogy elég a B mátrixának csak az utolsó $n - k$ sorát megtartani. Ez a következőképpen néz ki:

$$P = \begin{bmatrix} b_0 & b_1 & b_2 & \dots & b_{k-1} & b_k & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_{k-2} & b_{k-1} & b_k & \dots & 0 \\ 0 & 0 & b_0 & \dots & b_{k-3} & b_{k-2} & b_{k-1} & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & b_{2k-n} & b_{2k-n+1} & b_{2k-n+2} & \dots & b_k \end{bmatrix},$$

ahol $p(x) = b_0 + b_1 x + \ldots + b_k x^k$. Tehát a P mátrix soraiba a p polinom együtthatóit írjuk a legalacsonyabb fokú tagnál kezdve, minden sorban eggyel jobbra ($n - k$ sor van, és n oszlop; az utolsó sorban szereplő együtthatókat úgy kell érteni, hogy $b_i = 0$ ha $i < 0$).

Miért lesz a P ellenőrző mátrix? Azt tudjuk, hogy B mátrixa minden kódszót nullába szoroz, és így a sorok elhagyásával kapott P mátrix is. Több szót azonban P nem szorozhat nullába, mert az utolsó $n-k$ oszlopa a mátrix alakjából láthatóan független ($b_k \neq 0$, hiszen p foka k), és így P rangja $n - k$, vagyis magtere k-dimenziós.

A 9.3.2. Gyakorlatban kapott generátormátrix nem szisztematikus. Ezen (ciklikus polinomkód esetén) a következő kódolási eljárással lehet segíteni.

9.4.4. Definíció. Legyen $g(x) \mid x^n - 1$, ahol g foka $n-k$, és kódoljunk a következőképpen. Ha $u(x) \in Q[x]$ a kódolandó polinom, akkor szorozzuk meg x^{n-k}-nal (vagyis írjunk a kódszó végére $n - k$ darab nullát). A kapott polinomot osszuk el maradékosan $g(x)$-szel, a maradékot jelölje $w(x)$. Az ennek megfelelő $n - k$ hosszú szó ellentettje lesz az ellenőrző rész, ezt küldjük az u kódszó után. Képletben: $u(x)$ kódolt alakja $v(x) = u(x)x^{n-k} - w(x)$.

9.4.5. Állítás. *Az előző 9.4.4. Definícióban szereplő megfeleltetés lineáris, injektív, és tetszőleges u-hoz egy g-vel osztható polinomot rendel, vagyis ez valóban a g generátorú polinomkódhoz tartozó (egyik szisztematikus) kódolási eljárás.*

Bizonyítás. A megfeleltetés nyilván lineáris, hiszen a maradék képzése az. Az injektivitás is nyilvánvaló, hiszen az első k helyen az eredeti kódszót küldjük el. Mivel $w(x)$ az $u(x)x^{n-k}$ maradéka $g(x)$-szel osztva, tudjuk, hogy $g(x) \mid u(x)x^{n-k} - w(x)$. De pontosan az ennek a polinomnak megfelelő szót rendeltük u-hoz hozzá, és így az általunk megadott megfeleltetés tényleg a kódba képez. □

Alkalmazásként szót ejtünk az úgynevezett CRC-kódról (az elnevezés az angol Cyclic Redundancy Check kifejezésből származik). Ennek a hibajelző kódnak többféle változata is van, és a segítségével ellenőrzik, hogy a számítógép merevlemezén, vagy hálózatokon való áthaladáskor sérültek-e az adatok. A CRC-kódolás pontosan a 9.4.4. Definícióban leírt eljárás, a g polinomot azonban speciálisan választják.

Legyen $m \geq 2$ és $g(x)$ egy m-edfokú primitív polinom GF(2) fölött, amelynek egy α gyöke tehát a GF(2^m) test multiplikatív csoportjának generátoreleme. Válasszuk n-et $2^m - 1$-nek, ami az α elem rendje. Persze α^2 is gyöke g-nek (hiszen a négyzetre emelés automorfizmus), és így g egy 1-hibajavító BCH-kódot határoz meg (ami a 9.3.10. Gyakorlat szerint igazából egy Hamming-kód). A kód hossza $n = 2^m - 1$, az ellenőrző bitek száma pedig m (hiszen g foka m).

A CRC-kódolásnál néha a g helyett az $f(x) = g(x)(x-1)$ polinomhoz tartozó (ciklikus) kódot használják. Ennek is gyöke α és α^2, tehát a kapott kód is 1-hibajavító. Valójában azonban a minimális távolsága már legalább 4 (a 9.3.4. Gyakorlat miatt), hiszen α^0, α^1, α^2 gyökei f-nek (és ez három egymást követő kitevő). Fontos szempont, hogy a polinommű-veleteket gyorsan lehessen végezni a mai számítógépeken, amelyek 8, 16, vagy 32 bites szavakat tudnak jól kezelni. A paramétereket ennek megfelelően választják. Ha például g foka $m = 15$, akkor az $f(x) = g(x)(x-1)$ polinomhoz tartozó ellenőrző szó 16 bites lesz, és a g polinom 16 együtthatója is elfér egy gépi szóban.

A CRC-CCITT szabvány az $f(x) = x^{16} + x^{12} + x^5 + 1$ polinomot használja, és $m = 15$. A kódszavak hossza tehát $2^{15} - 1 = 32767$ bit. Ez azt jelenti, hogy 32751 bit (vagyis durván négy kilobájt) adat mellé teszünk egy két bájtos ellenőrző jegyet (egy bájt 8 bittel egyenlő). Ez a CRC-kód megtalálható minden mai merevlemez kontrollerében. Nem hibajavításra, hanem csak hibajelzésre használják. A hálózati adatcsomagokban (az ethernet paketekben), az üvegszálas optikai kábelekben (FDDI) és a `pkzip` programban 32 bites CRC található, az itt használt g az

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

primitív polinom. Ezeknek a polinomoknak a megválasztása nagy gondosságot igényel, hogy érzékenyek legyenek a gyakorlatban ténylegesen előforduló, tipikus hibákra. Az Olvasó a CRC-kódolásról többet is megtudhat Ross Williams internetes bevezető cikkéből,

`http://www.repairfaq.org/filipg/LINK/F_crc_v3.html`

amelyben irodalomjegyzék is található.

Végezetül egészen röviden megemlítjük a ciklikus polinomkódok egy másik fajtáját is. Emlékeztetjük az Olvasót, hogy egy n-hez relatív prím szám akkor *kvadratikus maradék* mod n, ha egy alkalmas másik szám négyzetével kongruens mod n (vagyis a $\mathbb{Z}_n^\times$ csoport négyzetelemeiről van szó). Tegyük föl, hogy n páratlan prím. Ekkor a kvadratikus maradékok száma $(n-1)/2$, hiszen a négyzetre emelés csoporthomomorfizmus, melynek magja $\{1, -1\}$, vagyis kételemű. A kvadratikus maradékok tehát egy 2 indexű részcsoportot alkotnak. Tudjuk, hogy létezik primitív gyök modulo n, ennek pontosan a páros kitevőjű

hatványai lesznek kvadratikus maradékok. A hatvány rendjének képlete szerint tehát azok az r számok kvadratikus maradékok, melyekre $(n-1)/o_n(r)$ páros szám.

A BCH-kódok 9.3.6. Definíciójához hasonlóan indulunk el, vagyis választunk egy $n > 2$ egészet, egy GF(p) testet (ahol $p \neq n$ prímszám), és egy n rendű α elemet a GF(p) egy L bővítésében. Most azonban feltesszük, hogy az n kódhossz maga is prímszám, méghozzá olyan, amelyre nézve p kvadratikus maradék. A g polinom gyökeinek most nem az α első $d-1$ hatványát vesszük, mint a BCH-kódnál, hanem az α azon hatványait, amelyeknél a kitevő kvadratikus maradék modulo n. Ezeket a feltevéseket a következő állítás részben megmagyarázza.

9.4.6. Állítás. *A g polinom együtthatói a* GF(p) *alaptestben vannak.*

Bizonyítás. Mivel a p-edik hatványra emelés generálja a GF(p) $\leq L$ bővítés Galois-csoportját (6.7.9. Tétel), elegendő megmutatni, hogy ez permutálja g gyökeit, vagyis hogy ha r kvadratikus maradék mod n, akkor rp is az. Ez abból következik, hogy p kvadratikus maradék mod n. □

Így értelmes a következő definíció.

9.4.7. Definíció. A g által generált, n hosszú, $Q =$ GF(p) fölötti polinomkódot *kvadratikus maradék kódnak* nevezzük.

Ezek a BCH-kódoknál korábban keletkeztek Golay munkássága nyomán, és a Hamming-kódokon kívül az első nemtriviális példákat szolgáltatták perfekt kódokra (vagyis amelyeknél a 9.1.7. Hamming-korlátban egyenlőség áll). Például ha $p = 2$ és $n = 23$, akkor p rendje 11 lesz modulo 23, és így a 2 kvadratikus maradék. Ezek szerint $23 \mid 2^{11} - 1$, ami azt jelenti, hogy a $K =$ GF(2^{11}) testben már találhatunk egy 23 rendű α elemet. A g polinom foka a kvadratikus maradékok száma mod 23, ami szintén 11, és így a kapott polinomkód dimenziója $k = 23 - 11 = 12$. Meg lehet mutatni, hogy a minimális távolság 7, és így tényleg perfekt 3-hibajavító kódot kapunk, hiszen

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = \frac{2^{23}}{2^{12}} = 2^{11}\,.$$

Ezt a kódot *bináris Golay-kódnak* nevezzük. Hasonlóan kaphatunk egy perfekt 2-hibajavító Golay-kódot a háromelemű test fölött is, melynek hossza 11, dimenziója 6, ez a *ternáris Golay-kód*. A bináris Golay-kódot a műholdas tévéadásban alkalmazzák, a 3-hibajavító képessége miatt a legfontosabb adatokat védik vele.

9.5. A CD matematikája

Könyvünk utolsó szakaszához érkezvén egy kis ünneplést tartunk: vázlatosan ismertetjük, hogy milyen kódolással védik a kompakt lemezek tartalmát például karcolások vagy ujjnyomok ellen. A hanglemezek technikai specifikációját a Sony és a Philips cégek dolgozták ki, és az 1980-ban kiadott „piros könyv” (Red Book) tartalmazza. Ebben minden

technikai adat benne van, a korong átmérőjétől és a lézer-olvasó hullámhosszától kezdve a pontos adattérképig, aminek része a felhasznált hibajavító kódolás. A specifikáció lényegi részét az ECMA nemzetközi szervezet tette publikussá, az `ECMA-130.pdf` dokumentum letölthető a

`http://www.ecma-international.org/publications/`

internetes címről. Először pár szóval emlékeztetjük az Olvasót arra, hogy hogyan lesz a zenéből digitális forma, vagyis egy {0, 1}-sorozat.

A zenét felvevő mikrofon a levegő hangrezgéseit áramingadozásokká alakítja, amely az idő függvényének tekinthető. Ezt a függvényt föl lehet bontani „tisztán szinuszos" függvények összegére, egy úgynevezett Fourier-sorba. Minden összeadandónak jól meghatározott frekvenciája van. Ez ugyan egy végtelen sor, fülünk azonban nem hallja meg a húszezer Hz fölötti hangokat, és ezért az összegnek ezek a tagjai elhagyhatók. (A legmagasabb hangú hangszerek hangmagassága csak 4500 Hz körül van, de a hang karakterének a felismerésében, például hogy hegedű vagy orgona szól-e, az úgynevezett felhangok, vagyis a Fourier-sor magasabb frekvenciájú tagjai is szerepet játszanak, és így ezeket is reprodukálni kell.)

Ezt a függvényt egy A/D (analóg-digitális) konverter segítségével digitalizálják úgy, hogy nagyon sok helyen feljegyzik az értékét. Ez a (közelítő) érték egy 16 bites kettes számrendszerbeli szám, és mivel sztereó felvételről van szó, ezt a bal- és a jobb csatorna esetében is meg kell tenni. A mintavétel sűrűségét (vagyis, hogy másodpercenként hány mintát kell venni) a Nyquist-Shannon tétel szabályozza, mely szerint a mintavételezés frekvenciájának meg kell haladnia a sávszélesség kétszeresét. Esetünkben ez $2 \cdot 20000$ Hz, és így megállapodtak abban, hogy az audio CD-ken a mintavételezés frekvenciája 44,1 kHz (a DVD hangja esetében pedig 48 kHz). Ez durván 176 kilobájt átvitelét igényli másodpercenként (ennél a merevlemezek és az ethernet-hálózatok átviteli sebessége is sokkal nagyobb, a szokásos ADSL-hálózatoké 2004-ben azonban még nem, vagyis ezeken egyelőre nem lehet zenét CD-minőségben digitálisan közvetíteni). A kódolási eljárás során az információ durván a háromszorosára nő. Ahhoz, hogy a kompakt hanglemezt meghallgathassuk, a dekódolási eljárásnak legalább ennek megfelelő sebességűnek kell lennie.

A kódolás konkrét részletei elolvashatók a fent idézett dokumentumban. Mi csak a legfontosabb elveket és ötleteket mutatjuk be, viszont megadjuk a felhasznált Reed–Solomon-kódok pontos paramétereit. A dekódolás nincs sztenderdizálva, és így a jobb minőségű lejátszó pontosabb lehet: a hibáknál kisebb sercenést hallunk, és esetleg a nagyon karcos CD-t is le lehet vele játszani. A sercenést az okozza, hogy ha a hibajavítás nem sikerül, akkor a zene hibás részét a környező minták alapján interpolálják. Megjegyezzük azonban, hogy a Reed–Solomon-kódok nyújtotta összes hibajavítási lehetőséget még a modern dekóderek sem használják ki, a fent említett sebességi korlátok miatt.

A CD felületén egy karcolás sok „szomszédos" bitet tehet tönkre (ezt úgy mondjuk, hogy *csomós hiba*, angolul burst error). Ezért az eddig tanult hibajavító kódoláson kívül még arról is gondoskodni kell, hogy a biteket „alaposan összekeverjük" (ez a *kódátfűzés*, angolul interleaving). Ekkor ugyanis az üzenetben „lokálisan" mindig kevés hiba lesz, mert a karcolás által tönkretett, fizikailag közeli bitek a logikai sorrendben távol esnek egymástól. Mindezt egy egyszerű példával világítjuk meg.

Tegyük föl, hogy egy 10000 bit hosszú {0, 1}-sorozatot kell átvinnünk. Írjuk ezt sorfolytonosan be egy 100×100-as mátrixba, és ugyanezeket az adatokat küldjük oszlopfolytonosan. Ha ebben az új adatfolyamban 20 egymás utáni bit hibás lesz (ami egy hibajavító kód szempontjából kellemetlen lenne), akkor az eredeti folyamban a hibák között mindig 99 helyesen küldött bit van, és így a hibákat a kód könnyen ki tudja javítani.

Problémát okozhat az is, ha egy-egy jel a küldés során kimarad. Ha ugyanis a sorozat csak egy bittel is elcsúszik, akkor átlagban a bitek fele hibássá válhat. Ezen úgy segíthetünk, hogy a sorozatba könnyen felismerhető szinkronjeleket iktatunk. Természetesen jelezni kell azt is, hogy a CD hányadik track-jénél tartunk, és azon belül mennyi idő telt már el.

A CD-írás és -olvasás technikája fizikai szemmel nézve analóg (egy 1-nek vagy 0-nak szánt jel valójában bizonyos közelítő jelszinteket jelent). Ha egy kódsorozatban nagyon sűrűn váltakoznak a 0 és 1 jelek, akkor ez nagyobb hibázási lehetőséget jelent (mert az eszköznek nagyobb frekvenciájú jelet kell megbízhatóan átvinnie). Ezért a CD kódolásának egyik utolsó lépése az, hogy a 8 hosszú szavakat egy táblázat segítségével olyan 14 hosszú szavakká alakítják, amelyekben viszonylag kevés a $0 \leftrightarrow 1$ átmenet (ez mellesleg a kódszavak távolságát is megnöveli).

A CD-k kódolásában kétféle Reed–Solomon-kódot használnak, mindkétszer a kódátfűzés módszerével ötvözve. Legyen $L = \mathrm{GF}(2)[x]/(m)$, ahol $m(x) = x^8 + x^4 + x^3 + x^2 + 1$. Ez primitív polinom, az $\alpha = x + (m)$ elem generálja L multiplikatív csoportját. A Reed–Solomon-kódban a Q ábécé az L test, vagyis a kód minden „betűje” egy bájt. A kód 2-hibajavító, azaz d értékét 5-nek vesszük. Így $n - k$ értéke 4 lesz. Az n maximális lehetséges értéke $2^8 - 1 = 255$ lehetne, ennél azonban jóval redundánsabb a kódolás: az egyik esetben $n = 28$ (vagyis minden 24 bájthoz négy „ellenőrző bájtot” adunk), a másik kódolásnál pedig $n = 32$.

Végezetül néhány olyan internetes helyet adunk meg, ahol a fentiekről további információ olvasható, vagy hivatkozások (linkek) találhatók. Az irodalomjegyzékben is több kódelméleti mű szerepel.

`http://math.berkeley.edu/~berlek/alg.html`

`http://web.usna.navy.mil/~wdj/reed-sol.htm`

`http://www.videohelp.com/`

9.6. Összefoglaló

IV. rész

A gyakorlatok és feladatok megoldásai

10. ÚTMUTATÁSOK, ÖTLETEK A FELADATOKHOZ

... az ismeretlen jelenségek vizsgálatának klasszikus dilemmája. Ahhoz, hogy szabatosan elhatároljuk őket, ismerni kellene az oksági mechanizmust, ahhoz pedig, hogy megismerjük az oksági mechanizmust, jól körül kell határolni a jelenségeket.

Stanisław Lem: *Szénanátha*
(Murányi Beatrix fordítása)

10.1. Komplex számok

1.1.7. Használjuk fel, hogy ha x és y egészek, akkor $x = mp + \overline{x}$ és $y = mq + \overline{y}$ alkalmas p, q egészekre, és helyettesítsük ezt be a bizonyítani kívánt képletekbe.

1.1.16. Teljes négyzetté alakítással vezessük vissza a feladatot négyzetgyökvonásra modulo 101. A 20 helyett a 121-ből vonjunk négyzetgyököt.

1.1.18. Színezzünk a modulo m maradékokkal. Vagdossunk le a sakktábláról olyan darabokat, ahol mindegyik maradékból ugyanannyi van. Ha r a k szám m-mel való osztási maradéka, akkor a bal felső $r \times r$-es négyzetben hány $r - 1$ és hány 0 van?

1.1.19. Vizsgáljuk meg, hogy ezek a számok milyen maradékot adhatnak 3-mal osztva.

1.2.12. Mutassuk meg, hogy ha x nagy abszolút értékű szám, akkor $ax^3 + bx^2 + cx + d$ előjele ugyanaz, mint ax^3 előjele, mert az $|ax^3|$-höz képest a többi tag abszolút értékben még együttvéve is eltörpül.

1.3.13. Végezzük el a négyzetre emelést, és írjuk föl az eredmény valós, illetve képzetes részét. Így két egyenletet kapunk c-re és d-re.

1.4.11. A négyszöget a komplex számsíkra rajzolva képzeljük el, tehát a csúcsok komplex számok lesznek. Fejezzük ki a megfelelő négyzetek középpontjait a csúcsok segítségével. Használjuk fel, hogy két vektor akkor és csak akkor egyenlő hosszú és merőleges, ha az egyik a másiknak i-szerese.

1.4.12. A háromszög csúcsai segítségével fejezzük ki a szabályos háromszögek középpontjait. Használjuk fel, hogy egy háromszög akkor és csak akkor szabályos, ha az egyik oldalvektorát 60°-kal elforgatva egy másik oldalvektorát kapjuk. A $\cos 60^\circ + i \sin 60^\circ$ és a $\cos 120^\circ + i \sin 120^\circ$ számok közötti összefüggéseket ne az algebrai alakjukból, hanem a szabályos hatszög geometriai tulajdonságaiból vezessük le.

1.4.13. Mutassuk meg, hogy a $(z_3 - z_1)/(z_3 - z_2)$ szöge a $z_1z_2z_3$ háromszögnek a z_3-nál levő szöge. Használjuk a látókörről szóló geometriai tételt.

1.4.14. Használjuk föl az $(A - B)(C - D) + (A - D)(B - C) = (A - C)(B - D)$ azonosságot.

1.4.15. Az $\varepsilon = \cos(x/2) + i \sin(x/2)$ páros hatványait a mértani sor összegképletével adjuk össze. Az eredményt osszuk le ε egy olyan hatványával, hogy felhasználhassuk az $\varepsilon - (1/\varepsilon) = -2i \sin(x/2)$ és $\varepsilon^n - (1/\varepsilon)^n = -2i \sin(nx/2)$ összefüggéseket.

1.5.8. Melyik pontban lesz a bolha m lépés után? Hogyan írhatjuk fel oszthatóság segítségével, hogy ez a kiindulópont?

1.5.18. Keressük meg $-\varepsilon$ jó kitevőit.

1.5.22. Használjuk föl a binomiális tételt az $(1 + 1)^n$, $(1 - 1)^n$, $(1 + i)^n$ összegekre.

1.5.23. Hatványozzuk a $\cos x + i \sin x$ számot a Moivre-képlet alapján is, és a binomiális tétel segítségével is.

10.2. Polinomok

2.2.2. Először az $\big((a*b)*(c*d)\big)*e = a*\Big(\big((b*c)*d\big)*e\Big)$ speciális esetet mutassuk meg. Az általános esetben is arra törekedjünk, hogy minden szorzatot olyan alakra hozzunk, mint a fenti azonosság jobb oldala, ahol az összes nyitózárójel „annyira balra van, amennyire csak lehet”. Alkalmazzunk teljes indukciót a szorzat hosszára nézve.

2.2.5. Mutassuk meg, hogy ha egy könyvespolcra a könyvek összevissza vannak feltéve, akkor rendet tudunk csinálni úgy, hogy mindig csak két szomszédos könyvet cserélünk ki.

2.2.8. Ha volna kettő, akkor számítsuk ki kétféleképpen a szorzatukat.

2.2.10. Tegyük fel, hogy v balinverze, és w jobbinverze u-nak. Számítsuk ki kétféleképpen a $v * u * w$ szorzatot.

2.2.16. Legyen a H részcsoport neutrális eleme f, és jelölje f^{-1} az f elemnek a G csoportbeli inverzét. Számítsuk ki kétféleképpen az $f * f * f^{-1}$ szorzatot.

2.2.20. A disztributivitást alkalmazzuk a $(0 + 0)r$ és az $r\big(s + (-s)\big)$ kifejezésekre.

2.2.24. Alkalmazzuk a 2.2.16. Feladat állítását.

2.2.30. Legyenek $u_1, \ldots, u_k$ a $\mathbb{Z}_m$-nek az m-hez relatív prím elemei, és u ezek egyike. Mutassuk meg, hogy $u *_m u_1, \ldots, u *_m u_k$ páronként különbözők.

2.2.38. Tudjuk, hogy $(\sqrt{2}-1)(\sqrt{2}+1) = 1$, tehát ezek invertálhatók. Hogyan lehetne ebből az összefüggésből további invertálható elemeket gyártani?

2.2.39. Vizsgáljuk meg, hogy egy nem nulla elem „abszolút értéke" lehet-e nulla.

2.2.41. Egy csoportban mely g elemekre igaz, hogy $g^2 = g$?

2.2.42. Tegyük fel, hogy van ilyen. Mutassuk meg, hogy az 1 képe szükségképpen 1 lesz, majd vizsgáljuk meg, hogy milyen tulajdonságú elem lehet az i képe.

2.4.16. Legyen $f \in T[x]$. A 2.4.4. Gyakorlat miatt $f(x) = (x-b)q_0(x) + b_0$ alkalmas $q_0 \in T[x]$ polinomra és $b_0 \in T$ elemre. Alkalmazzuk ugyanezt a q_0 polinomra, majd a kapott q_1 polinomra, és így tovább. (Ez az eljárás hasonlít ahhoz, ahogy egy számot egy másik számrendszerbe alakítunk).

Az egyértelműség bizonyításához tegyük föl, hogy

$$f(x) = b_0 + b_1(x-b) + \ldots + b_n(x-b)^n = c_0 + c_1(x-b) + \ldots + c_n(x-b)^n$$

alkalmas $b_i, c_i \in T$ elemekre. A két polinomot kivonva

$$0 = (c_0 - b_0) + (c_1 - b_1)(x-b) + \ldots + (c_n - b_n)(x-b)^n .$$

Ezért azt kell megmutatni, hogy ha

$$d_0 + d_1(x-b) + \ldots + d_n(x-b)^n$$

a nullapolinom, akkor mindegyik $d_i = 0$. Helyettesítsünk x helyére b-t, és alkalmazzunk n szerinti indukciót.

2.4.17. Ha a nullosztó, akkor hány gyöke van legalább az ax polinomnak?

2.4.19. Használjuk föl az interpolációról tanultakat. Egy binomiális együtthatót képzelhetünk-e polinomnak?

2.4.20. Mivel $f(14) = 440$, az f-et kereshetjük $(x-14)g(x) + 440$ alakban, ahol g is egész együtthatós polinom.

2.4.21. Nem lehetséges. Legyenek az alappontok $a_1, \ldots, a_n$, és f egy olyan egész együtthatós polinom, amely ezeken a helyeken a kívánt értékeket veszi fel. Osszuk el f-et maradékosan $(x-a_1)\ldots(x-a_n)$-nel.

2.4.22. Legyen $r \neq 0$ eleme R-nek. Mivel az interpoláció korlátlanul elvégezhető, van olyan $f \in R[x]$ polinom, melyre $f(0) = 0$ és $f(r) = 1$.

2.4.24. Álljon S azokból a függvényekből, melyeknek a 2 szám gyöke. A másik kérdésre a válasz: nem fordulhat elő. Ennek igazolásához használjuk föl, hogy nullosztómentes gyűrűben nem nulla elemmel szabad egyszerűsíteni (2.2.26. Gyakorlat).

2.5.2. Vizsgáljuk az elsőfokú polinomokat.

2.5.13. Emeljük négyzetre az $(x_1 + \ldots + x_n)$ összeget a 2.1.4. Gyakorlat felhasználásával.

2.5.15. A (4) állításhoz: helyezzük el a sokszöget úgy, hogy a csúcsai az n-edik egységgyökök legyenek, húzzuk meg az 1 csúcsból induló átlókat, ezek hosszainak szorzatát írjuk fel abszolút érték segítségével, majd használjuk föl a feladat (2) állítását.

2.5.17. Először olyan polinomot próbáljunk készíteni, amelynek gyöke az illető test mindegyik eleme. Ezt módosítsuk olyan (nem konstans) polinommá, amelynek nincs gyöke az adott testben.

2.6.10. Igaz, alkalmazzunk indukciót a határozatlanok száma szerint.

2.6.11. Ha adott k darab különböző komplex szám n-es, akkor olyan n-határozatlanú polinomot keressünk, amelybe az első $k-1$ darab szám n-est helyettesítve nullát kapunk, de a k-adikat helyettesítve nem. Minden $i < k$-ra keressünk egy olyan koordinátát, amelyben a k-adik szám n-es különbözik az i-edik szám n-estől, és csak erre a koordinátára koncentráljunk.

2.7.17. Igazoljuk, hogy $\sigma_1^{k_1} \ldots \sigma_n^{k_n}$ homogén polinom, amely szükségképpen k-adfokú.

10.3. A polinomok számelmélete

3.1.28. Tegyük fel, hogy $p_1 \ldots p_k = q_1 \ldots q_\ell$ egy elem két felbontása irreducibilisek szorzatára. A p_1 prímtulajdonságát kihasználva keressük meg egy asszociáltját a q_j-k között, majd egyszerűsítsünk p_1-gyel.

3.1.31. Tudjuk, hogy $2 \mid 2 \cdot 2$. Osztója-e a 2 valamelyik tényezőnek a páros számok gyűrűjében is? Mutassuk meg, hogy $2 \cdot 18 = 6 \cdot 6$ a 36-nak két lényegesen különböző felbontása felbonthatatlanok szorzatára a páros számok gyűrűjében.

3.1.33. Használjuk fel, hogy $3 \cdot 3 = 9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$.

3.1.34. Az x^5y^2 és az x^2y^5 polinomoknak van-e kitüntetett közös osztójuk?

3.2.3. Ha $g = 0$, akkor nem oszthatunk vele maradékosan, hogyan végezzük ilyenkor az eljárást? Az is előfordulhat, hogy egyáltalán nincs nem nulla maradék az algoritmusban, mi ilyenkor a kitüntetett közös osztó?

3.2.7. Van I-ben legalacsonyabb fokú polinom?

3.2.11. Alkalmazzuk a 3.2.3, 3.1.26, 3.1.27, 3.1.28. Gyakorlatokat, illetve Feladatokat.

3.2.12. Tegyük fel, hogy van olyan nem konstans polinom, amely nem bontható föl irreducibilisek szorzatára. Legyen f a lehető legkisebb fokú ilyen polinom. Irreducibilis-e f?

3.2.23. Mutassuk meg, hogy minden ilyen I halmaz a legkisebb pozitív elemének a többszöröseiből áll. A 3.2.6. Tétel bizonyítását kövessük.

3.3.18. Használjuk föl a binomiális tételt. Illusztrációként érdemes elolvasni a 3.3.17. Gyakorlat megoldásának a középrészét is. A kis Fermat-tétel bizonyításához emeljük (tagonként) p-edik hatványra azt a b tagból álló $\mathbb{Z}_p$-beli összeget, amelynek mindegyik tagja 1.

3.3.20. Mutassuk meg a gyöktényezős alak beszorzásával, hogy x^4-10x^2+1 összes gyökei $\pm\sqrt{2}\pm\sqrt{3}$. A beszorzást végezzük el háromféleképpen is, mindig máshogy összepárosítva két-két gyöktényezőt. A $\mathbb{Q}$ fölötti irreducibilitás bizonyításához a 3.3.11. Példában leírt módszert használjuk. Vizsgáljuk meg, hogy a $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ gyökvonások melyike végezhető el $\mathbb{Z}_5$, $\mathbb{Z}_7$, illetve $\mathbb{Z}_{11}$ fölött.

3.5.6. Használjuk föl a következő összefüggést:

$$1+x+\ldots+x^{p-1}=\frac{x^p-1}{x-1}\,,$$

valamint hogy $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (3.3.18. Feladat).

3.5.9. Mutassuk meg, hogy $g(x)=x^n f(1/x)$.

3.5.14. Mutassuk meg, hogy $f\big(x+f(x)\big)$ osztható $f(x)$-szel.

3.5.15. Fogalmazzuk meg a Schönemann-Eisenstein kritériumot abban az esetben, amikor $\mathbb{Z}$ helyett a $\mathbb{C}[y]$ gyűrű fölötti polinomokat vizsgáljuk. Megy-e a 3.5.3. Gyakorlatban leírt bizonyítás ebben az esetben is?

3.5.16. Tegyük föl, hogy $\sqrt[3]{4}=a+b\sqrt[3]{2}$. Mi lehet az x^3-2 és az x^2-ax-b polinomok kitüntetett közös osztója? Van-e közös gyökük?

3.5.17. Ha az $f\in\mathbb{Z}[x]$ egy k-adfokú g osztóját keressük, akkor használjuk fel, hogy minden m egészre $g(m)\mid f(m)$, és alkalmazzunk interpolációt.

3.6.11. Az $f/(f,f')$ polinomnak mik a gyökei, és hányszorosak?

3.6.13. Mutassuk meg, hogy ha f irreducibilis, akkor (f,f') csak akkor lehet nem konstans, ha $f'=0$. Milyen f polinomokra teljesül ez $\mathbb{Z}_2$ fölött? Használjuk fel, hogy $\mathbb{Z}_2$ fölött tagonként lehet négyzetre emelni (3.3.18. Feladat).

3.6.15. Ha $f'(b)=0$, tudjuk-e módosítani f-et úgy, hogy b gyöke legyen?

3.6.16. Mutassuk meg, hogy ha c kivételes érték, akkor f'-nek és $f(x)-c$-nek van közös gyöke.

3.8.7. Az összes állítás közvetlen (de hosszadalmas) számolással igazolható a gyökök és együtthatók összefüggését fölhasználva. Ehelyett az α_1, α_2, α_3, α_4 gyököket a 3.7.2. Állítás bizonyításához hasonlóan képzeljük határozatlanoknak. (Ezt megtehetjük, hiszen (6) kivételével csupa azonosságot kell bizonyítani.) Ekkor az u_1, u_2, u_3 kifejezések páronként különbözők, és így (1)-hez elég azt belátni, hogy mindegyik u_i gyöke a harmadfokú rezolvensnek (hiszen a főegyüttható biztosan 8). Keressünk olyan $K_1(x)$ és $L_1(x)$ polinomokat, hogy $K_1(x)+L_1(x)=(x-\alpha_1)(x-\alpha_2)$ és $K_1(x)-L_1(x)=(x-\alpha_3)(x-\alpha_4)$ teljesüljön.

3.8.8. Használjuk föl a 3.8.7. Feladatot.

3.8.9. Használjuk föl a 3.8.7. Feladatot és a 3.8.3. Gyakorlatot.

3.8.12. Legyen $z = x + (1/x)$. Az $x + 1$ gyöktényező kiemelése után kapott polinomot osszuk le x^3-nel, és ezt írjuk föl z (harmadfokú) polinomjaként.

3.8.13. Teljes négyzet-e $\mathbb{C}$ fölött a $-(2x^2 + 4x + 2)$ polinom?

3.9.11. Használjuk föl az 1.5.18. Feladat eredményét.

3.9.13. Legyen η primitív m-edik egységgyök, ahol $m \mid n$. Számítsuk ki, hogy a feladatbeli szorzatban az $x - \eta$ hányadik hatványon szerepel, majd alkalmazzuk a A.4.6. Állítást.

3.9.14. Használjuk föl az előző feladatot.

3.9.16. Alkalmazzuk a gyökök és együtthatók közötti összefüggéseket az n-edik körosztási polinomra. Mutassuk meg, hogy az n-edik primitív egységgyökök összege $\mu(n)$ (ahol μ a Möbius-függvény), szorzatuk pedig 1, kivéve $n = 2$-re, amikor -1.

3.9.17. Osszuk le a $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggést $x - 1$-gyel, és azután helyettesítsünk $x = 1$-et.

3.9.18. Számítsuk ki a $\Phi_n(-x)$ polinomot a 3.9.14. Feladat, illetve a 3.9.11. Gyakorlat segítségével (attól függően, hogy n osztható-e néggyel), majd használjuk föl az előző feladat eredményét.

3.9.20. Az előző gyakorlat szerint Φ_{nm}-et felírhatjuk az $x - \eta\varepsilon$ gyöktényezők szorzataként, ahol $o(\eta) = m$ és $o(\varepsilon) = n$. Csoportosítsuk ezeket a gyöktényezőket η szerint.

3.9.22. A $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggésből kiindulva, n szerinti indukcióval bizonyítsunk. Számoljunk eleve $\mathbb{Z}_p$ fölött. Használjuk föl a 3.9.6. Gyakorlatot és a 3.3.18. Feladatot (azaz a tagonkénti p-edik hatványozás lehetőségét).

3.9.24. Térjünk át $\mathbb{Z}_p[x]$-re, alkalmazzuk a 3.9.22. Feladatot, majd a 3.6.12. Gyakorlat megoldásának azt az állítását, hogy $p \nmid m$ esetén $x^m - 1$-nek nincs többszörös tényezője $\mathbb{Z}_p[x]$-ben.

10.4. Csoportok

4.1.12. Mutassuk meg, hogy S minden x eleme $x = ze$ alakban írható alkalmas $z \in S$ segítségével (z választható x balinverze balinverzének).

4.2.26. Igazoljuk, hogy két transzpozíció szorzata mindig felírható hármasciklusok szorzataként.

4.2.27. Mutassuk meg j szerinti indukcióval, hogy ha $f(1) = i$, akkor $f(j) = j +_n (i - 1)$ (mod n összeadás).

4.2.28. Mutassuk meg a „bolhás” 1.5.8. Feladat felhasználásával, hogy az $(1, 2, \ldots, n)$ ciklus k-adik hatványa (n, k) darab $n/(n, k)$ hosszú diszjunkt ciklus szorzata.

4.2.29. Használjuk a 4.2.23. Gyakorlatban szereplő könyvespolc-modellt.

4.2.30. Vegyük az $(1, 2, \ldots, n)$ ciklus egy előállítását transzpozíciók szorzataként, és készítsük el ezekből az előző feladatban vizsgált gráfot. Mutassuk meg, hogy ez összefüggő lesz, majd alkalmazzuk az A.2.5. Tételt.

4.2.31. Készítsük el a megadott transzpozíciók halmazából a 4.2.29. Feladatban szereplő gráfot. Ha $k + t - 1 > n$, akkor ennek $n - 1$-nél kevesebb éle van, és így nem lehet összefüggő. Ha $k + t - 1 \leq n$, akkor alkalmazunk n szerinti indukciót az összefüggőség bizonyítására. Az indukció során a k, t, n hármasról a k, $t - k$, $n - k$ hármasra lépjünk (a $k < t$ esetben).

4.3.33. Induljunk ki az $(ab)^2 = 1$ összefüggésből. Negyedik hatványokra az állítás nem igaz, a D_4 diédercsoport például ellenpélda lesz (lásd 4.1.8. Állítás).

4.3.34. Igazoljuk, hogy ha $d = (a^n - 1, a^m - 1)$, akkor a $\mathbb{Z}_d^\times$ csoportban $o(a) \mid n$.

4.3.35. Használjuk föl a körosztási polinomokra ismert rekurziós képletet (3.9.5. Lemma), valamint azt, hogy az $x^n - 1$ polinomnak $p \nmid n$ esetén nincs többszörös gyöke $\mathbb{Z}_p$-ben (3.6.12. Gyakorlat).

4.3.36. Mutassuk meg, hogy $\Phi_n(nN)$ minden prímosztója $nk + 1$ alakú.

4.4.14. Feleltessük meg mindegyik bal oldali mellékosztálynak a komplexus-inverzét.

4.4.34. A második kérdéshez vizsgáljuk a $\mathbb{Z}_8^\times$ csoportot.

4.4.35. Párosítsunk minden elemet az inverzével. Mely elemek egyenlők a párjukkal?

4.4.36. Legyen d pozitív egész. A 2.4.7. Tétel miatt egy T test multiplikatív csoportjában az $x^d - 1$ polinomnak legfeljebb d gyöke lehet. Igazoljuk, hogy legfeljebb $\varphi(d)$ darab d rendű elem van. Alkalmazzuk a 3.9.6. Gyakorlat állítását.

4.4.42. Igazoljuk, hogy $\langle a/c, b/d \rangle = \langle (a, c)/[b, d] \rangle$.

4.4.43. Mutassuk meg, hogy a racionális számok egy X részhalmaza akkor és csak akkor generátorrendszer, ha minden q prímhatványhoz van olyan (már egyszerűsített alakban felírt) tört X-ben, melynek nevezője osztható q-val.

4.4.44. Legyen X egy k elemű generátorrendszer a G csoportban, feltehető, hogy X-be belevettük minden elemének az inverzét is. Legyen továbbá $|G : H| = n$, és válasszunk minden H szerinti bal mellékosztályból egy reprezentánselemet úgy, hogy H-ból az egységelemet választjuk. Jelölje R ezeknek a reprezentánselemeknek a halmazát. Ha $x \in X$ és $r \in R$, akkor xr is benne van valamelyik mellékosztályban, és így $r'h$ alakban írható alkalmas $r' \in R$ és $h \in H$ elemekre. Legyen Y az így kapott kn darab $h \in H$ elem halmaza. Mutassuk meg, hogy Y generálja H-t.

4.4.45. Készítsünk egy páros gráfot, melynek az A csúcshalmazát a H részcsoport szerinti összes bal mellékosztályok alkotják, a B csúcshalmazt pedig az összes jobb mellékosztályok. (Az egyszerre bal és jobb mellékosztályokat két példányban vesszük fel.) Kössünk össze két mellékosztályt, ha van közös elemük. Alkalmazzuk az A.2.7. König–Hall–Ore-tételt.

4.6.15. Számoljuk meg mindkét csoportban a másodrendű elemeket.

4.6.27. Legyen $\alpha(aH) = a * x$. Jóldefiniált ez a leképezés?

4.6.31. Tekintsük a kocka szimmetriacsoportjának a hatását a szemköztes lappárok alkotta háromelemű halmazon.

4.6.33. A G csoport alaphalmazán berajzolunk minden $g \in G$ elemhez $|G|$ darab g „színű" nyilat: tetszőleges x-ből g színű nyíl megy xg-be. Ennek a gráfnak a szimmetriái épp a G elemeivel való balszorzások (a Cayley-tételbeli G-vel izomorf csoport). Hogyan szüntethetjük meg a színeket és az irányítást?

4.6.39. Számoljuk meg kétféleképpen azokat a (g, x) párokat, melyekre $g * x = x$: egyszer rögzített g, egyszer pedig rögzített x mellett.

4.6.40. Legyen X az összes színezések halmaza, ahol a szimmetriával egymásba átvihetőket is különbözőnek tekintjük. Hasson a D_4 csoport az X halmazon a természetes módon, és alkalmazzuk a Burnside-lemmát (vagyis a 4.6.39. Feladat állítását).

4.6.41. Alkalmazzuk az előző feladatot. A tranzitivitás szükséges, keressünk a Klein-csoporttal izomorf ellenpéldát S_6-ban.

4.7.43. Használjuk fel, hogy egy homomorfizmust egy generátorrendszeren felvett értékei egyértelműen meghatároznak (4.4.28. Gyakorlat).

4.7.44. Mutassuk meg, hogy ha α fixpontmentes automorfizmus, akkor G minden eleme egyértelműen felírható $g^{-1}\alpha(g)$ alakban.

4.7.45. Tekintsük G hatását a H szerinti bal mellékosztályokon, és mutassuk meg, hogy ennek magja H.

4.7.48. Igazoljuk az $[x, y]^{-1} = [y, x]$ és $[x, yz] = [x, y]y[x, z]y^{-1}$ azonosságokat.

4.8.28. A kocka hat-hat alkalmas lapátlóját behúzva egy-egy (összesen két) szabályos tetraédert kapunk. Mutassuk meg, hogy azok az egybevágóságok, amelyek egy ilyen tetraédert önmagába visznek, S_4-gyel izomorf normálosztót alkotnak.

4.8.29. A $\mathbb{Z}_4^+$ csoportban értelmezzük a $\mathbb{Z}_2$ test elemeivel való szorzást úgy, hogy $0 * a = 0$ és $1 * a = 1$ legyen minden $a \in \mathbb{Z}_4^+$ elemre. Teljesülnek-e a vektortér-axiómák?

4.8.31. Használjuk fel, hogy véges sok szám legkisebb közös többszöröse akkor és csak akkor egyezik meg a szorzatukkal, ha a számok páronként relatív prímek.

Legyen G véges részcsoportja a T test multiplikatív csoportjának, és e a G exponense. Mutassuk meg, hogy G minden eleme gyöke az $x^e - 1$ polinomnak.

4.8.33. Legyen M maximális azon részcsoportok között, amelyekre $M \cap \langle a \rangle = \{0\}$ teljesül. Mutassuk meg, hogy $\langle a \rangle + M = A$. Ehhez válasszunk egy olyan minimális rendű c elemet, amely még nincs benne $\langle a \rangle + M$-ben, és vizsgáljuk pc-t. Az A helyett az A/M faktorcsoportban dolgozzunk.

4.9.6. Legyen N az F szabad csoportnak az a normálosztója amelyet az összes w^2 és $[u, v]$ szavak generálnak, ahol $u, v, w \in F$. Mutassuk meg, hogy az F/N csoport kommutatív, és minden elemének a négyzete az egységelem, így vektortérnek tekinthető a $\mathbb{Z}_2$ test fölött a 4.8.29. Feladat értelmében. Igazoljuk, alkalmas $F \to \mathbb{Z}_2^+$ homomorfizmusokat választva, hogy mind az X, mind az Y szabad generátorrendszerek képe bázis ebben a vektortérben.

4.9.7. Mutassuk meg, hogy ha u és v szabadon generálják az $F(u, v)$ csoportot, akkor az $u^i v u^{-i}$ $(i > 0)$ elemek szabad generátorrendszert alkotnak az általuk generált részcsoportban.

4.9.18. Használjuk föl a 4.3.33. Feladatot.

4.9.19. Mutassuk meg, hogy $B(k, 3)$-ban a konjugált elemek egymással felcserélhetők, és ezért minden elem benne van egy kommutatív normálosztóban. Bizonyítsunk k szerinti indukcióval.

4.9.20.

(7) Mutassuk meg, hogy $b = 1$.
(8) Ez a 4.8.32. Gyakorlat (2) pontjában szereplő csoport.
(9) Ez a 4.8.32. Gyakorlat (6) pontjában szereplő csoport.
(10) Mutassuk meg, hogy $f = ab$ és $t = a$ kielégíti D_3 definiáló relációit.
(12) Mutassuk meg, hogy $\{1, b, aba^{-1}, a^{-1}ba\}$ normálosztó.
(13) Mutassuk meg, hogy $u = a^2$ és $v = (ab)^2$ kielégítik az előző pontban szereplő definiáló relációkat, és az általuk generált részcsoport normálosztó.
(14) Mutassuk meg, hogy az a, b, cbc^{-1} elemek által generált részcsoport legfeljebb nyolcelemű, kommutatív normálosztó.

4.9.21. Legyen X az F szabad generátorrendszere, és válasszuk ki minden $x \in X$ esetén a $\varphi(x)$ elem egy tetszőleges ősképét α-nál. Legyen $\psi(x)$ ez az őskép. Mivel F szabad, ψ-t kiterjeszthetjük homomorfizmussá.

4.9.22. A szó hossza szerinti indukcióval igazoljuk, hogy minden nullösszegű szó benne van F kommutátor-részcsoportjában.

4.10.11. Mutassuk meg, hogy az $\alpha(x) = (p + 1)x$ leképezés p rendű automorfizmusa a $N = \mathbb{Z}_{p^2}^+$ csoportnak. Készítsünk ennek alapján az N normálosztóból és a $H = \mathbb{Z}_p^+$ részcsoportból nemkommutatív szemidirekt szorzatot.

4.10.24. Vegyünk egy olyan elemet, amely nincsen benne az egyetlen maximális részcsoportban. Mi lesz az általa generált részcsoport?

4.10.28. Elsőként az alábbi állításokat érdemes belátni. Az S_4 csoportban a 2-Sylow részcsoport nem lehet normálosztó, mert 8-nál több 2-hatvány rendű elem van. Az A_5 esetében minden pont stabilizátora tartalmaz egy 2-Sylow részcsoportot. A D_n-ben a forgatásokból álló normálosztó minden részcsoportja is normálosztó, és tartalmazza a páratlan prímekhez tartozó Sylowokat. Ha $n = 2^k m$, ahol m páratlan, akkor minden 2-Sylow 2^k tükrözésből, és az összes 2-hatvány rendű forgatásból áll.

4.10.30. Tegyük fel, hogy $p < q < r$. Mutassuk meg, hogy az r-Sylowok száma pq. Számoljuk össze a p, q, r rendű elemeket.

4.10.31. Ha bármely két p-Sylow metszete csak az egységelemből áll, akkor számoljuk meg a p-hatvány rendű elemeket. Ha nem, akkor mi lesz két p-Sylow p elemű metszetének a normalizátora?

4.10.32. Legyenek P_1 és P_2 olyan p-Sylowok, melyek D metszete a lehető legnagyobb elemszámú. Mutassuk meg, hogy D normálosztó G-ben. Ha $|D| = 1$, akkor számoljuk meg a p-hatvány rendű elemeket.

4.10.33. Legyen $g \in G$. Ekkor gPg^{-1} is p-Sylowja N-nek, ezért N-ben is konjugáltak. A második állítás bizonyításához mutassuk meg, hogy P normálosztó G mindegyik P-t tartalmazó p-Sylowjában.

4.10.34. A P részcsoport p-Sylow K-ban, ami normálosztó $N_G(K)$-ban. Alkalmazzuk a Frattini-elvet. A második állítás bizonyításához használjuk fel, hogy a p-Sylow részcsoportok száma K-ban is kongruens 1-gyel mod p.

4.10.35. Tegyük fel, hogy $q < p$, tehát $q \mid p - 1$. A 4.10.18. Következmény miatt minden nemkommutatív pq rendű G csoport egy $P \rtimes Q$ szemidirekt szorzat, ahol P-t egy p rendű a elem, Q-t egy q rendű b elem generálja. Legyen $bab^{-1} = a^t$. Ekkor a b-vel való konjugálás a $P \cong \mathbb{Z}_p^+$ normálosztónak az $\alpha_t : x \mapsto x^t$ automorfizmusa. Mivel b rendje q, ezért α_t rendje ennek osztója, vagyis 1 vagy q. De 1 nem lehet, mert akkor G kommutatív lenne, ezért α_t rendje q. Az $\mathrm{Aut}(\mathbb{Z}_p^+) \cong \mathbb{Z}_p^\times$ izomorfizmus miatt tehát t egy q rendű eleme $\mathbb{Z}_p^\times$-nek. A G csoportot izomorfia erejéig meghatározza a t szám.

Tegyük fel, hogy s egy másik q rendű eleme $\mathbb{Z}_p^\times$-nek. Mutassuk meg, hogy a b elem helyettesíthető egy alkalmas c hatványával úgy, hogy c az a elemet az s-edik hatványába konjugálja.

4.11.34. Mutassuk meg, hogy ha $\mathrm{Aut}(G)$ tranzitív a $G - \{1\}$ halmazon, akkor a csoport minden elemének rendje ugyanaz a p prím, a centruma pedig az egész csoport. Alkalmazzuk a véges Abel-csoportok alaptételét, majd a 4.8.30. Gyakorlatot.

4.11.36. Tegyük fel, hogy $\sim$ kongruencia X-en. Legyen $x \in X$, és K azon N-beli n elemek halmaza, melyekre $n(x) \sim x$. Mutassuk meg, hogy $K \lhd G$.

4.11.37. Kössük össze a b és c pontokat, ha $(bc) \in G$. Mutassuk meg, hogy a kapott gráf komponensei kongruenciát alkotnak.

4.11.38. Használjuk fel, hogy a -1 hatványa Q minden elemének, és ezért minden nem egyelemű stabilizátorban benne van.

4.11.39. Alkalmazzuk az 4.6.26. Gyakorlat (5) pontját.

4.11.40. Használjuk fel, hogy az A_n alternáló csoport az S_n mindegyik részcsoportját legfeljebb 2 indexű normálosztóban metszi az első izomorfizmus-tétel miatt.

4.11.41. A szokásos Sylow-tételt használó érvelés mellett alkalmazzuk a 4.11.39. Feladat állítását is. Amikor G rendje 180, akkor a 4.10.31. Feladat megoldásának ötletét is föl kell használni.

4.11.42. Használjuk fel, hogy a 4.11.40. Feladat szerint $4k+2$ rendű csoportban van kettő indexű normálosztó.

4.11.43. Alkalmazzuk a 4.6.26. Gyakorlatot és a 4.6.27. Feladatot.

4.12.18. Igazoljuk, hogy a kommutátorlánc minden eleme karakterisztikus részcsoport, és a faktorai mindig kommutatívak.

4.12.19. Azt kell belátni, hogy ha G feloldható csoport, és H részcsoport, N pedig normálosztó G-ben, akkor H és G/N is feloldható. Használjuk a feloldhatóság kommutátorlánccal való jellemzését (4.12.18. Feladat), valamint a 4.7.48. Feladatot.

4.12.20. Használjuk az izomorfizmus-tételeket.

4.12.21. Tekintsük G hatását egy p-Sylow részcsoport bal mellékosztályain. Mutassuk meg, hogy a hatás magja és képe is feloldható.

4.12.22. Jelölje U_k azoknak a T fölötti $n \times n$-es felső háromszög-mátrixoknak a halmazát, amelyekben a főátlótól számított, azzal párhuzamos ferde sorok közül k darab azonosan nulla (a főátlót is beleszámítva). Képletben: az $M = ((m_{i,j}))$ akkor eleme U_k-nak, ha $i > j-k$ esetén $m_{i,j} = 0$. Igazoljuk a következő állításokat (E az $n \times n$-es egységmátrix).

(1) Ha $M \in U_m$ és $K \in U_k$, akkor $MK \in U_{m+k}$.
(2) Ha $M \in U_1$, akkor $(E+M)^{-1} = E - M + M^2 - M^3 + \ldots + (-1)^{n-1}M^{n-1}$.
(3) Ha $M \in U_m$ és $K \in U_k$, akkor $[E+M, E+K] - E \in U_{m+k}$.

A fentieken kívül használjuk föl a 4.10.23. Gyakorlat állítását is.

4.12.23. Használjuk fel, hogy (a 4.7.20. Gyakorlat szerint) normálosztó karakterisztikus részcsoportja normálosztó.

4.12.24. Legyen M maximális részcsoport a G feloldható csoportban. Tekintsük G egy minimális N normálosztóját, és válasszunk szét két esetet aszerint, hogy N része-e M-nek.

4.13.6. Számoljuk meg az invertálható lineáris transzformációkat a következőképpen. Rögzítsünk egy bázist, és vizsgáljuk meg, hányféleképpen választhatók ki a bázisvektorok képei úgy, hogy függetlenek legyenek. A $\mathrm{PSL}(n, T)$ rendjének kiszámításához használjuk fel, hogy T multiplikatív csoportja ciklikus (4.3.16. Tétel).

4.13.13. Mutassuk meg, hogy két alkalmas 2-Sylow részcsoport metszetének normalizátora 5 indexű részcsoport lesz, és így létezik beágyazás A_5-be.

10.5. Gyűrűk

5.9.15.

5.10.12.

10.6. Galois-elmélet

6.5.12. A Galois-elmélet főtételének (6.6.7. Tétel) és a 6.5.11. Gyakorlatnak a felhasználásával igazoljuk, hogy $\sqrt{2}$ nincs benne az $x^4 - 5$ polinom $\mathbb{Q}$ fölötti felbontási testében.

6.2.8. Legyen θ nem valós gyöke az $x^3 - 2$ polinomnak. Határozzuk meg θ fokát $\mathbb{Q}(\sqrt[3]{2})$ fölött, és a $\mathbb{Q}(\theta) \cap \mathbb{R}$ testet.

6.10.6. Használjuk föl, hogy f irreducibilitása miatt G tranzitív részcsoportja S_4-nek (6.6.18. Gyakorlat), továbbá, hogy S_4 minden tranzitív részcsoportjának rendje néggyel osztható az orbit-stabilizátor tétel miatt (4.6.6. Tétel). Keressük meg az összes ilyen tranzitív részcsoportot. Használjuk a diszkriminánst annak eldöntésére, hogy G részcsoportja-e A_4-nek (6.10.3. Lemma). Végül gondoljuk meg, hogy a 3.8.7. Feladat megoldása tetszőleges nulla karakterisztikájú test fölött működik, és ezért f harmadfokú rezolvensének gyökei benne vannak f felbontási testében.

6.10.7. Használjuk föl, hogy a harmadfokú rezolvens gyökei $b/2$ és $\pm\sqrt{d}$. Legyenek f gyökei $\alpha_1, \alpha_2 = -\alpha_1, \alpha_3, \alpha_4 = -\alpha_2$. Fejezzük ki $d(b^2 - 4d)$-t az α_i gyökökkel.

6.10.8. Mutassuk meg, hogy ha f gyökei $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ és $u = (\alpha_1\alpha_2 + \alpha_3\alpha_4)/2$ (3.8.7. Feladat), akkor $(2u - b)(2u + b)^2 - 4c^2 = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2(\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_4)^2$.

10.7. Modulusok

7.2.20. Kövessük azokat az elemi bizonyításokat, amelyeket lineáris algebrában tanultunk.

7.2.21. Legyen $v \neq 0$ az $y = x$ egyenessel párhuzamos, $w \neq 0$ pedig egy rá merőleges vektor. Mutassuk meg, hogy v és w az $M = M(A, V)$ modulusnak gyenge bázisát alkotják. A második kérdés megválaszolásához vizsgáljuk a tükrözés helyett az origó körüli $+90$ fokos forgatást.

7.3.8. A (4) belátásához legyen $N \leq \langle m \rangle$, és tekintsük az $\{r \in R : rm \in N\}$ ideált (a 4.3.20. Lemma analógiájára). Mutassuk meg, hogy ha ezt az ideált az r elem generálja, akkor $N = \langle rm \rangle$.

7.4.13. Használjuk föl, hogy

$$\det(v_1 + ru, v_2, \ldots, v_i) = \det(v_1, v_2, \ldots, v_i) + r \det(u, v_2, \ldots, v_i)\,,$$

(itt a v_j és u oszlopvektorok), és a kitüntetett közös osztóra vonatkozó $(a + rb, b) = (a, b)$ azonosságot.

7.3.22. Álljon $M_i \leq T^{n\times n}$ azokból a mátrixokból, amelyeknek az i-edik oszlopban lévő elemek kivételével mindegyik eleme nulla. Keressünk egy olyan invertálható B_{ij} mátrixot, amelyre $M_i B_{ij} = M_j$, és igazoljuk, hogy a $B \mapsto BA_{ij}$ modulus-izomorfizmus.

7.3.23. A függetlenség 7.2.3. Gyakorlatban megadott jellemzése miatt részmodulusok egy rendszere akkor és csak akkor független, ha minden véges rész-rendszere az. Ezért ha tekintjük az I halmaz azon I' részhalmazait, amelyekre az M_j $(j \in I')$ modulus-rendszer független, akkor ezekre teljesül a Zorn-lemma (A.1.2. Tétel) feltétele.

7.3.26. Mutassuk meg, hogy a Jr balideálok összege, ahol r befutja R-et, kétoldali ideál.

7.3.27. A keresett k-féle egyszerű modulus a k darab teljes mátrixgyűrű egy-egy minimális balideálja lesz, mint R-modulus.

7.3.28. Igazoljuk a Zorn-lemma felhasználásával, hogy R minden valódi balideálja része egy maximális balideálnak.

7.4.14. Használjunk lineáris algebrát R hányadosteste fölött, pontosabban a determinánsok szorzástételét, illetve az inverz mátrixnak a determináns ferde kifejtéséből származó képletét.

7.4.15. Az előző feladat miatt $L^{-1} \in R^{k\times k}$. E mátrix elemeivel fejezzük ki a b_i vektorokat a c_i vektorok segítségével. A második állítás igazolásához használjuk föl, hogy L determinánsa nem nulla.

7.6.7. Használjuk föl a determinánsosztókról bizonyított állításokat (7.4.13. Feladat).

7.6.12. Ha csak véges sok invariáns altér van, hány dimenziós lehet egy sajátaltér? Mutassuk meg, hogy ha p prím $T[x]$-ben, és az $M(A, V)$ felbontásában két p-hatvány rendű direkt összeadandó is szerepel, akkor végtelen sok invariáns altér van. Használjuk föl a 7.4.10. Gyakorlatot.

7.7.11. Azt igazoljuk, hogy

$$\mathrm{Hom}_R\Big(\bigoplus_i M_i, K\Big) \cong \prod_i \mathrm{Hom}_R(M_i, K) \quad \text{és} \quad \mathrm{Hom}_R\Big(M, \prod_i K_i\Big) \cong \prod_i \mathrm{Hom}_R(M, K_i)\,.$$

7.7.19. Osszunk el egy maximális rendű elemet a rendjével.

7.7.21. Tegyük föl, hogy $b_1, \ldots, b_n$ bázis a T test fölötti V vektortérben, és tekintsük a $V^* = \mathrm{Hom}(V, T)$ duális tér *duális bázisát.* Ez azokból a b_i^* leképezésekből áll, melyekre $b_i^*(b_j) = 0$ ha $i \neq j$, és 1 ha $i = j$.

7.7.27.

7.8.23. A (3) pontban azt igazoljuk, hogy

$$\Big(\bigoplus_i M_i\Big) \otimes K \cong \bigoplus_i (M_i \otimes K)\,.$$

7.8.25.

7.8.26. Ha $t, s \in T$, akkor a $t \otimes m$ elemet megszorozhatjuk s-sel úgy, hogy az eredmény $(st) \otimes m$ legyen. Így ezeknek a tenzoroknak a véges lineáris kombinációit is meg tudjuk szorozni s-sel. Mutassuk meg, hogy ez a szorzás jóldefiniált. A többi állítást először az $R = \mathbb{Z}$ és $T = \mathbb{Q}$ esetben érdemes meggondolni.

10.8. Általános algebrák, hálók

8.1.17. Az $x \wedge \big(x \vee (x \wedge x)\big)$ kifejezést számítsuk ki a (4) segítségével kétféleképpen.

8.1.25. Legyen $x \equiv y$ akkor és csak akkor, ha x és y között van a feladatban leírt sorozat. Igazoljuk, hogy $\equiv$ ekvivalencia-reláció.

8.2.20. Három új jelölést is be kell vezetnünk. Csoportok esetében, ha H részcsoport és N normálosztó, akkor az első izomorfizmus-tételben HN-ről beszélünk. Ennek általános algebrák esetében a következő a megfelelője. Legyen B részalgebrája és θ kongruenciája az A algebrának. Ekkor $B[\theta]$-val jelöljük a θ azon osztályainak unióját, amelyeknek van B-vel közös eleme. Mutassuk meg, hogy $B[\theta]$ részalgebrája A-nak.

A $H \cap N$ csoportok esetében normálosztója lesz a H részcsoportnak. Az általános esetben jelölje $\theta|_B$ azt a partíciót a B halmazon, amelynek osztályai a θ osztályainak a B-vel való metszetei (az esetleges üres metszeteket elhagyva). Másképp fogalmazva B két eleme akkor és csak akkor kongruens $\theta|_B$-nél, ha θ-nál kongruensek. Mutassuk meg, hogy B egy kongruenciáját kaptuk. Ennek neve a θ-nak a B-re vett *megszorítása*.

Végül legyen $\rho \geq \theta$ is egy kongruencia az A algebrán. Ekkor mindegyik ρ-osztály θ-osztályok uniója. Foglaljuk ezeket a θ-osztályokat ρ-osztályonként egy-egy halmazba. A kapott halmazok az A/θ algebra egy partícióját adják, amit ρ/θ-val jelölünk. Másképp fogalmazva, az x/θ és y/θ akkor kongruens ρ/θ-nál, ha x és y kongruensek ρ-nál. Mutassuk meg, hogy ez a definíció nem függ az x és y reprezentánsok választásától, és tényleg A/ρ egy kongruenciáját kapjuk.

8.2.39. Tekintsük a $\{0, 1, 2, 3\}$ halmazon az $x * y = \min(x, y) +_4 1$ műveletet.

8.2.40. Egy elég sok tényezős szorzatnak tekintsük az első elemmel induló részletszorzatait. A kapott sorozatban a félcsoport végessége miatt van ismétlődés. Másrészt ha $se = s$, akkor e egy alkalmas hatványa nulla, és így s is nulla.

8.2.41. Haladjunk úgy, mint az M_3 egyszerűségének bizonyításában (8.2.37. Gyakorlat). Mutassuk meg, hogy ha egy nemtriviális kongruenciát veszünk, akkor van olyan atom (vagyis a nullának egy fedője), amely nullával kongruens. Ezután tekintsük ennek az atomnak a komplementumait, ezek mind 1-gyel kongruensek.

8.3.15. Először olyan függvényt gyártsunk az e (ÉS) és a $\neg$ (NEM) segítségével, amelynek értéke egy előre adott $(a_1, \ldots, a_n) \in A^n$ helyen 1, a többi helyen 0. Ezután a többi függvényt ezekből a v (VAGY) segítségével állítsuk össze.

8.3.16. A 8.3.15. Feladat megoldásához hasonlóan járjunk el.

8.3.28. Gondoljuk meg, hogy egy egy elemmel generált háló csakis egyelemű lehet, hiszen minden egyelemű részhalmaz részháló (a műveletek idempotenciája miatt). Hasonlóan, ha egy hálót az a és b elemek generálnak, akkor maximum négy eleme lehet: a, b, $a \wedge b$ és $a \vee b$ (hiszen ezek biztosan részhálót alkotnak).

8.3.30. Az első esetben a konstans tag nélküli egész együtthatós polinomokat, a másodikban az összes egész együtthatós polinomot tekintsük.

8.3.31. Tekintsük a $\{0, 1, 2, \ldots, k-1\}$ halmazon az $x * y = \min(x, y) +_k 1$ műveletet (vö. 8.2.39. Gyakorlat). Fejezzük ki ezzel az $x \mapsto x +_k 1$ függvényt, a $\min(x, y)$ függvényt, majd a konstans függvényeket. Haladjunk tovább a 8.3.15. Feladat megoldásának módszerével, ahol az ÉS műveletet a min, a VAGY műveletet a $v(x, y) = \min(x -_k 1, y -_k 1) +_k 1$ helyettesíti.

8.4.11. Konstruáljuk meg a végesen generált szabad algebrákat Birkhoff módszerével $\mathcal{K}$ fölött. Ezek végesek, és szabadok $\mathsf{V}(\mathcal{K})$ fölött is.

8.4.20. Mutassuk meg, hogy egy szubdirekt irreducibilis Abel-csoport minden nemtriviális részcsoportja szubdirekt irreducibilis, és ha véges, akkor a véges Abel-csoportok alaptétele miatt prímhatványrendű ciklikus.

8.4.21. Tekintsük a szabad Abel-csoportokat, illetve a szabad kommutatív gyűrűket (lásd 8.3.30. Feladat).

8.4.22. Igazoljuk, hogy $D_4 \in \mathsf{HS}(Q \times Q)$ és $Q \in \mathsf{HS}(D_4 \times D_4)$. Használjuk föl a két csoport definiáló relációit (4.9.15. Példa).

8.4.23. Használjuk az $x^6 = 1$ és $x^2y^2 = y^2x^2$ azonosságokat. Mutassuk meg, hogy minden ezeknek eleget tevő csoportban van egy olyan normálosztó, amely elemi Abel-féle 3-csoport, és a rá vett faktor elemi Abel-féle 2-csoport. Használjuk föl, hogy minden másodrendű lineáris transzformáció diagonalizálható, továbbá hogy ha A és B felcserélhető lineáris transzformációk, akkor A minden sajátaltere B-invariáns. Végül igazoljuk, hogy ha s és t másodrendű elemek egy G csoportban, $(st)^6 = 1$, és t felcserélhető $(st)^4$-nel, akkor s-sel is.

8.4.24. Legyenek A_i $(i \in I)$ az A algebra összes végesen generált részalgebrái, és B az A_i algebrák direkt szorzata. Ennek definiáljuk egy C részalgebráját a következőképpen. A $\mathbf{c} = (\ldots, c_i, \ldots)$ akkor van C-ben, ha van olyan i, hogy $c_j = c_i$ teljesül bármely olyan j-re, amelyre $A_j \supseteq A_i$ (ezek a „majdnem konstans" sorozatok). Legyen $\varphi(\mathbf{c}) = c_i$. Mutassuk meg, hogy a φ leképezés jóldefiniált, és szürjektív homomorfizmusa C-nek A-ra.

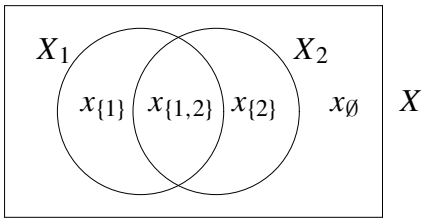
8.4.25. Tegyük föl, hogy az A algebrában teljesülnek a felsorolt azonosságok. Mutassuk meg, hogy A minden végesen generált részalgebrája homomorf képe egy végesen generált $\mathcal{K}$-beli szabad algebrának, majd alkalmazzuk a 8.4.24. Feladatot.

8.5.8. A (2) bizonyításához tegyük föl, hogy $x \vee c = y \vee c$ és $x \wedge f = y \wedge f$, ahol a feltétel miatt $c \leq f$ (itt $c \in I$ és $f \in F$). Számítsuk ki a disztributív azonosság segítségével az $(x \vee c) \wedge y$ kifejezést, és vezessük le, hogy $y \leq x$. A (3) esetében vegyünk egy $c \in L$ elemet, és legyen $I = (c]$ a c alatti, $F = [c)$ a c fölötti elemek halmaza.

8.5.23. Ha az R gyűrűben teljesül az $x^2 \approx x$ azonosság, akkor fejtsük ki a disztributivitás segítségével az $(x + y)^2$ kifejezést.

8.5.26. Tegyük föl, hogy C részalgebrája a $\mathcal{P}(X)$ Boole-algebrának, ahol X tetszőleges véges halmaz. Legyen az $x, y \in X$ elemekre $x \sim y$, ha C bármely Y elemére teljesül, hogy $x \in Y \iff y \in Y$. Igazoljuk, hogy $\sim$ ekvivalencia-reláció, és mutassuk meg, hogy $\sim$ osztályainak tetszőleges uniója eleme C-nek.

8.5.27. A 8.5.26. Feladat megoldásának mintájára mondjuk azt az $x, y \in X$ elemekre, hogy $x \sim y$, ha mindegyik i-re $x \in X_i \iff y \in X_i$. Ez is ekvivalencia-reláció, és ha X-et helyettesítjük a $\sim$ osztályaiból álló halmazzal (ahogy a 8.5.26. Feladat megoldásában is tettük), akkor az $X_1, \ldots, X_n$ halmazok továbbra is általános helyzetűek lesznek, de most már tetszőleges $I \subseteq \{1, 2, \ldots, n\}$ részhalmazhoz egyértelműen létezik olyan $x_I \in X$, amely akkor és csak akkor van benne az X_i halmazban, ha $i \in I$ (hiszen a $\sim$ relációval összevontuk az ilyen tulajdonságú elemeket). Így X elemszáma 2^n. A 10.1. Ábra mutatja ezt a helyzetet $n = 2$ esetén (ez a szokásos Venn-diagramm, amit egyszerű logikai feladatok megoldására is használunk).



10.1. Ábra. A két elemmel generált szabad Boole-algebra, mint halmazrendszer.

Megmutatjuk, hogy az X_i halmazok a teljes $\mathcal{P}(X)$ Boole-algebrát generálják. Az $\{x_I\}$ egyelemű halmaz megkapható úgy, hogy elmetsszük azokat az X_i halmazokat, ahol $i \in I$, és ehhez még hozzámetsszük azoknak az X_j halmazoknak a komplementumait, ahol $j \notin I$. Innen uniózással az X minden részhalmaza megkapható, tehát $|F| = 2^{2^n}$.

Legyen B egy Boole-algebra, és $b_1, \ldots, b_n \in B$. Rendeljük hozzá az x_I elemhez a

$$\varphi(x_I) = b_I = \Big(\bigwedge\nolimits_{i \in I} b_i\Big) \wedge \Big(\bigwedge\nolimits_{j \notin I} b'_j\Big)$$

elemet, és ha $Y \subseteq X$, akkor legyen

$$\varphi(Y) = \bigvee\nolimits_{y \in Y} \varphi(y)\,.$$

Ekkor $\varphi : F \to B$ homomorfizmus lesz, amelyre $\varphi(X_i) = b_i$ minden i-re. Mivel ennek igazolása eléggé számolós, egy másik utat is mutatunk (aminek a lényege az, hogy tetszőleges B helyett elég a kételemű Boole-algebrát venni).

Legyen $\mathcal{K}$ a kételemű Boole-algebrából álló egyelemű osztály. Készítsük el Birkhoff módszerével $\mathcal{K}$ fölött az n elemmel generált szabad algebrát. Ez a 8.4.10. Gyakorlat és a Stone-tétel miatt a Boole-algebrák varietása fölött is szabad lesz. Mutassuk meg, hogy az előzőekben leírt algebrával izomorf Boole-algebrát kapunk.

8.5.28. Igazoljuk, hogy az n elemmel generált szabad disztributív háló $f(n)$ elemszámára tetszőleges $0 \leq k \leq n$ esetén

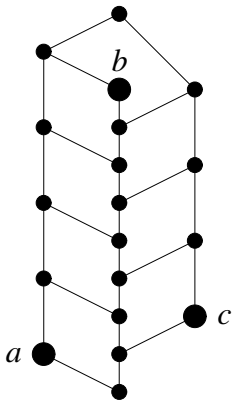
$$2^{\binom{n}{k}} \leq f(n) \leq 2^{2^n}$$

teljesül. A legjobb alsó becslést ebből akkor kapjuk, ha $k = \lfloor n/2 \rfloor$, vagyis páros n esetén n fele, páratlan n esetén az ennél $1/2$-del kisebb (egész) szám.

8.5.29. Tekintsük egy végtelen X halmaz összes részhalmazainak a $\mathcal{P}(X)$ Boole-algebráját. Legyen I az X véges részhalmazaiból álló ideál. Mutassuk meg, hogy a θ_I kongruencia (8.5.8. Gyakorlat) szerinti faktor atommentes.

8.5.30. Az (5) bizonyításához tegyük föl, hogy I valódi ideál. Legyen $d \in L - I$, és $F = [d)$ a d-nél nagyobb vagy egyenlő elemekből álló filter. Tekintsük az L azon ideáljait, amelyek I-t tartalmazzák. Mutassuk meg, hogy a Zorn-lemma miatt ezek között van maximális, és ez prímideál is, hiszen maximális az F filtertől diszjunkt ideálok között.

8.6.12. Mutassuk meg, hogy a 10.2. Ábrán látható hálót generálják az a, b, c elemei.



10.2. Ábra. A „halgerinc”-háló.

8.6.27. Tegyük föl, hogy $b = p_1 \wedge \ldots \wedge p_n = q_1 \wedge \ldots \wedge q_m$ két előállítás metszet-irreducibilisek metszeteként. Mutassuk meg a „kicserélési” tételt: mindegyik $1 \leq i \leq n$-hez van olyan $1 \leq j \leq m$, hogy az első felbontásban p_i-t q_j-re cserélve szintén a b egy felbontását kapjuk (vagyis ha $c = p_1 \wedge \ldots \wedge p_{i-1} \wedge p_{i+1} \wedge \ldots \wedge p_n$, akkor $c \wedge q_j = b$). Használjuk föl, hogy $c \wedge p_i = b$ miatt a $[b, c]$ és a $[p_i, p_i \vee c]$ intervallumok izomorfak.

8.6.33. Legyen $c \in L$. Vegyünk sorban a_i atomokat (addig, amíg lehet) úgy, hogy a_{i+1} ne legyen $c \vee a_1 \vee \ldots a_i$ alatt. Használjuk a dimenzió-egyenlőséget annak igazolására, hogy ez az eljárás véges sok lépésben véget ér, és a kapott atomok egyesítése c-nek komplementuma lesz.

8.6.34. Használjuk föl az $(x \vee y) \wedge (x \vee z) = x \vee \big((x \vee y) \wedge z\big)$ azonosságot (amely a modularitásból következik).

8.6.35. A 8.3.10. Gyakorlat miatt elég belátni, hogy a B szimmetrikus és tranzitív. Használjuk ehhez, hogy az A algebrának van Malcev-kifejezése (8.6.4. Tétel).

8.6.36. Definiáljuk a θ kétváltozós relációt a B algebrán a következőképpen: $(b_1, b_2) \in \theta$ akkor és csak akkor, ha van olyan $c \in C$, hogy $(b_1, c), (b_2, c) \in A$. Ez reflexív (mert A szubdirekt részalgebra) és nyilván kompatibilis, tehát a 8.6.35. Gyakorlat miatt kongruencia. Ugyanígy legyen $(c_1, c_2) \in \rho$ akkor és csak akkor, ha van olyan $b \in B$, hogy $(b, c_1), (b, c_2) \in A$, ez kongruencia a C algebrán. Végül értelmezzük a φ leképezést így: $\varphi(b/\theta) = c/\rho$ akkor és csak akkor, ha $(b, c) \in A$. Mutassuk meg, hogy φ jóldefiniált, izomorfizmus, és teljesül rá a feladat állítása.

8.6.37. Alkalmazzuk az előző 8.6.36. Feladatot, és indukciót a tényezők száma szerint.

8.6.38. Legyen H részcsoport G-ben, és N a H által generált normálosztó. Jelölje D a $G \times G$-ben a (g, g) alakú elemek részcsoportját, ahol g befutja G-t, B pedig a (g, h) alakú párokból álló részcsoportot, ahol $g^{-1}h \in N$ (tehát B az N-hez tartozó kongruencia). Alkalmazzuk a modularitást a $H \times \{1\} \leq N \times \{1\}$ és a D részcsoportokra. A D és a $H \times \{1\}$ egyesítésének kiszámításához használjuk föl a 8.6.35. Feladatot.

8.7.10. Mátrixok helyett dolgozzunk lineáris transzformációkkal. Ha L balideál, akkor jelölje $W = L^\sharp \leq T^n$ a hozzá tartozó alteret. Nyilván $W^\flat \supseteq L$, tehát csak a fordított tartalmazást kell igazolni. Ha C tetszőleges lineáris transzformáció, akkor a lineáris algebra előírhatósági tétele segítségével könnyű konstruálni olyan D lineáris transzformációt, hogy DC magtere ugyanaz, mint C magtere, de DC már identikusan hat a saját képterén, más szóval DC négyzete önmaga, vagyis DC idempotens transzformáció. Készítsünk ennek felhasználásával olyan L-beli transzformációt, amelynek magtere W.

8.7.11. Tekintsük a C fölötti szabad algebrák alaphalmazát, mint kompatibilis relációt.

8.7.12. Használjuk föl a 8.7.9. Gyakorlat állítását arra, hogy az állítást visszavezessük a 8.7.10. Feladatra.

8.8.3. Az injektivitás jellemzése minden varietásban igaz: használjuk az egy elemmel generált szabad algebrát. A szürjektivitásé nem: tekintsük a $\mathbb{Z} \to \mathbb{Q}$ identikus beágyazást a gyűrűk varietásában.

8.8.7. A (2) esetében legyen M az M_i modulusok direkt összege, és $m \in M_i$ esetén $\pi_i(m)$ az az elem, amelynek az i-edik koordinátája m, a többi nulla. A (3) esetében π_i úgy adódik, hogy az $X_i \to \bigcup X_i$ beágyazást kiterjesztjük egy $F(X_i) \to F(X)$ homomorfizmussá.

10.9. Hibajavító kódok

9.4.3. Legyen I a $v(x) + f(x)(x^n - 1) \in Q[x]$ alakú polinomok halmaza, ahol $v(x)$ befutja a C kódszavaihoz tartozó polinomokat, $f \in Q[x]$ pedig tetszőleges. Mutassuk meg, hogy I ideál, és használjuk föl, hogy test fölötti polinomgyűrű főideálgyűrű.

11. MEGOLDÁSOK, EREDMÉNYEK

11.1. Komplex számok

1.1. Műveletek és tulajdonságaik.

1.1.3. Vagdossunk le olyan darabokat a sakktábláról, ahol minden ráírt számból ugyanannyi van. Ilyenek például a 8×1-es téglalapok, vagy a 8×8-as négyzetek. A vagdosást végezzük úgy, hogy a végén a bal felső sarokban álló 4×4-es négyzet maradjon meg (ez az ábrán is látható). Ebben 0 szerepel, de 7 nem. Tehát a nullák és hetesek száma eredetileg sem lehetett egyenlő.

1.1.7. Jelölje felülvonás a modulo m maradékképzést. Ahhoz, hogy ez a leképezés szorzattartó, azt kell igazolni, hogy $\overline{xy}=\overline{x}*_m\overline{y}$. A maradékképzés definíciója miatt $x=mp+\overline{x}$ és $y=mq+\overline{y}$, alkalmas p,q egészekre. Ezért

$$xy=(mp+\overline{x})(mq+\overline{y})=m[mpq+p\overline{y}+\overline{x}q]+\overline{x}\ \overline{y}\,.$$

Tehát xy és $\overline{x}\ \overline{y}$ különbsége osztható m-mel, és ezért ez a két szám ugyanazt a maradékot adja m-mel osztva. De xy maradéka $\overline{xy}$, és $\overline{x}\ \overline{y}$ maradéka $\overline{x}*_m\overline{y}$ (a $*_m$ definíciója szerint). Tehát $\overline{xy}=\overline{x}*_m\overline{y}$.

Az összegtartás ugyanígy, de valamivel egyszerűbb számolással igazolható. Az 1.1.5-beli azonosságok igazolásához írjuk fel a megfelelő azonosságot egész számokra, majd vegyük mindkét oldal maradékát modulo m. Végül a kivonást definiáljuk az $x-_m y=x+_m(\overline{-y})$ képlettel (ellentett hozzáadása). A fenti módszerrel könnyű megmutatni, hogy $x-_m y=\overline{x-y}$, és hogy a felülvonás a kivonást is tartja.

1.1.8. Az osztás a szorzás inverz művelete, és így a $2:3$ (modulo 5 végzett) osztás eredménye akkor lesz x, ha $3*_5x=2$. A táblázat 3-hoz tartozó sorában a 2 maradék a 4 oszlopában szerepel, tehát a $2:3$ osztás eredménye 4. Általában a $b:a$ osztás modulo 5 elvégzése azt jelenti, hogy az $a,b\in\mathbb{Z}_5$ maradékokhoz olyan $x\in\mathbb{Z}_5$ maradékot keresünk, melyre $a*_5x=b$. Nullával nem tudunk osztani, hiszen ha $a=0$, akkor $b\neq0$ esetén nincs ilyen x, ha meg $b=0$, akkor minden x jó, tehát az eredmény nem egyértelmű. Ugyanakkor modulo 5 minden nem nulla maradékkal tudunk osztani. Ez abból következik, hogy minden nullától különböző maradéknak van reciproka, mint az a táblázatból leolvasható: az 1-nek és 4-nek önmaga, a 2 és 3 pedig egymás reciprokai modulo 5. De a táblázatból közvetlenül is láthatjuk, hogy minden nem nulla maradékkal lehet osztani, hiszen minden nem nulla elem sorában minden maradék előfordul.

Modulo 6 az $1/3$ osztás sem végezhető el, hiszen $3 *_6 x$ csak 0 vagy 3 lehet, 1 soha. Könnyű meggondolni, hogy modulo 6 csak az 1 és 5 maradékokkal tudunk korlátlanul osztani, mert csak ezeknek van inverze (mindkettőnek önmaga).

1.1.9. A modulo 5 táblázatban teljesül a nullosztómentesség, mert a nulla a szorzástáblának csak az első sorában és az első oszlopában fordul elő. Modulo 6 viszont nem teljesül, mert például $2 *_6 3 = 0$.

1.1.10. Egyik sem helyes.

(1) Abból, hogy modulo 5 van megoldás, még nem következik, hogy az eredeti egyenletnek is van megoldása. (Az eredeti egyenletnek nyilván nincs megoldása, hiszen x^2 és y^2 mindenképpen nemnegatív egész számok, és így $x^2 + 10y^2 < 10$ csak úgy lehetne, ha $y = 0$, de a 6 nem négyzetszám.)

(2) Ez a gondolatmenet azonos az előzővel, tehát még mindig rossz. Az csak véletlen szerencse, hogy az egyenletnek most van megoldása, például $x = y = 1$, de igaz állításra is adható helytelen bizonyítás. (Például ugyanezzel a gondolatmenettel kijönne, hogy az $x^2 + 5y^2 = 16$ egyenletnek is van megoldása, ami nem igaz.)

1.1.11. Csak az $a = 0, 1, 2, 3, 4$ értékeket kell végignézni. Ha mondjuk 3^5 értékét akarjuk kiszámítani modulo 5, akkor a 3^5 szám $\mathbb{Z}$-ben való kiszámítása helyett gyorsabb eljárás az, ha eleve modulo 5 maradékokkal számolunk. A $*_5$ szorzást $*$-gal jelölve a 3 négyzete $3*3 = 4$, a 3 köbe tehát $3*3*3 = 3*4 = 2$, negyedik hatványa $3*2 = 1$, ötödik hatványa $3*1 = 3$. Láthatjuk, hogy a hatványok ebben az esetben periodikusan ismétlődnek, tehát nagyon nagy kitevőkre is gyorsan kiszámíthatnánk őket. Ezzel a módszerrel könnyű ellenőrizni az első oszthatóságot, és ugyanígy számolhatjuk ki azt is, hogy a második oszthatóság pontosan akkor teljesül, ha a nem osztható öttel. Az első állításra közvetlen bizonyítást is nyerhetünk, ha az $a^5 - a = a(a+1)(a-1)(a^2+1)$ szorzat alakot felhasználjuk.

1.1.12. A feladat eredménye:

(1) $6 \mid a^6 - a \iff$ az a szám nem $6k+2$, sem nem $6k+5$ alakú.
(2) $6 \mid a^5 - 1 \iff$ az a szám $6k+1$ alakú.
(3) $6 \mid a^2 - 1 \iff$ az a szám $6k \pm 1$ alakú (azaz a relatív prím a 6-hoz).

1.1.13. Csak azt kell ellenőrizni, hogy $1, 3, 5, 7$ modulo 8 vett négyzete 1. Sőt, elég a négyzetre emelést elvégezni a ± 1 és ± 3 számokra, hiszen 5 és -3, illetve 7 és -1 ugyanazt a maradékot adják 8-cal osztva. A közvetlen bizonyítás: ha a páratlan számot $2k+1$ jelöli, akkor

$$(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1\,,$$

és itt a szomszédos k és $k+1$ valamelyike páros, azaz $4k(k+1)$ osztható 8-cal. Tanulságos, hogy ez utóbbi, némi ötletességet igénylő bizonyítást helyettesíthetjük az előbbi gondolatmenettel, ami a modulo 8 számolási apparátus birtokában teljesen mechanikusan felfedezhető.

1.1.14. Modulo 5 számolva azt kapjuk, hogy $3 *_5 \overline{y} = 2$. A táblázat 3-hoz tartozó sorából leolvashatjuk, hogy $\overline{y} = 4$ (valójában a $2 : 3$ osztást végeztük el). Tehát $y = 5k + 4$ alkalmas k egészre. Az eredeti egyenletbe visszahelyettesítve $x = -3k - 1$ adódik. Ez egész szám, tehát minden ilyen y-ra megoldást kaptunk. Így végtelen sok megoldás van, minden egész k-ra egy. Például $k = 0$ esetén $(x, y) = (-1, 4)$.

1.1.15. Az $x = 0, \ldots, 4$ értékeket végigpróbálva modulo 5 számolással azt kapjuk, hogy az első oszthatóság az $x = 5k + 3$ és $x = 5k + 4$ alakú számokra teljesül. A második oszthatóságot $x = 0, \ldots, 6$ helyettesítéssel modulo 7 vizsgálva kapjuk, hogy ez semmilyen x-re sem teljesül.

1.1.16. Itt már fárasztó volna a $0, \ldots, 100$ számokat mind behelyettesíteni. Helyette ki fogjuk használni, hogy a 101 *prímszám*, azaz ha osztója egy szorzatnak, akkor osztója valamelyik tényezőjének is. Ebből következik, hogy egy számnak legfeljebb két négyzetgyöke lehet modulo 101. Valóban, ha egy N számnak a is és b is négyzetgyöke modulo 101, akkor a^2 és b^2 ugyanazt a maradékot adja 101-gyel osztva, mint N. Ezért $101 \mid a^2 - b^2 = (a - b)(a + b)$, azaz $101 \mid a - b$, vagy $101 \mid a + b$. Az első esetben a és b egyenlők modulo 101, a másodikban ellentettek. Így az N számnak a-n kívül csak $-a$ lehet még négyzetgyöke modulo 101, más nem.

(1) Az oszthatóságot modulo 101 vizsgálva másodfokú egyenletet kapunk. Teljes négyzetté kiegészítéssel $x^2 - 2x + 2 = (x - 1)^2 + 1$. Legyen $y = x - 1$, ekkor $\overline{y}^2 = \overline{-1} = 100$. A 100-nak a 10 és a $\overline{-10} = 91$ négyzetgyöke, és a fentiek szerint több négyzetgyöke nincs modulo 101. Ezért $\overline{y} = 10$ vagy $\overline{y} = 91$. Tehát a megoldások: $x = 101k + 11$ és $x = 101k + 92$, ahol k egész.

(2) Most is az előző módszert akarjuk alkalmazni, de két lépés is nehézséget okoz. Az első a teljes négyzetté alakítás. Ehhez az x-es tag együtthatóját (ami most páratlan szám) el kellene tudni osztani kettővel. De ezt meg lehet tenni modulo 101, hiszen $13 = \overline{114}$, vagyis a feladatban 13 helyett 114-et írhatunk. Ekkor $x^2 - 114x - 3 = (x - 57)^2 - 3252$, és -3252 ugyanazt a maradékot adja 101-gyel osztva, mint -20. Tehát most az $(\overline{x} - 57)^2 = 20$ egyenletet kell megoldanunk. A második nehézség most következik: a 20-ból négyzetgyököt kell vonni modulo 101. Erre most nem tudunk más módszert, mint végigpróbálgatni a mod 101 maradékokat (amit el akartunk kerülni). Szerencsére azonban $20 = \overline{121}$, ami 11-nek a négyzete. Ezért a megoldások: $x = 101k + 46$ és $x = 101k + 68$.

A feladat tanulsága, hogy a másodfokú egyenlet „megoldóképlete” valójában csak annyit tesz, hogy az egyenletet négyzetgyökvonásra vezeti vissza. Ezt a valós számok esetében kalkulátorral vagy táblázatosan közelítőleg el tudjuk végezni, és ezért érezzük úgy, hogy ez egy megoldóképlet.

1.1.17. Nem fedhető le. A bizonyítás lényegében ugyanaz, mint a 100×100-as tábla esetén, csak most a modulo 2 maradékokat írjuk a sakktáblára a „szokásos" szabály szerint, és azt vesszük észre, hogy a két hiányzó mezőn ugyanaz a szám áll (tehát a maradékon különbözik a nullák és egyesek száma, márpedig ha létezne lefedés, akkor nem különbözne). Természetesen ezt a bizonyítást egyszerűbb úgy elmondani, hogy 0 és 1 felírása helyett a mezőket világosra és sötétre festjük, ahogy az a sakktáblán amúgy is szokásos.

1.1.18. Ha $m \mid k$, akkor a lefedés nyilván (például soronként) lehetséges. Ha nem, akkor számozzuk meg a sakktábla mezőit a szokásos módon a modulo m maradékokkal. Ha lenne jó lefedés, akkor most is az derülne ki, hogy a $0, 1, \ldots, m-1$ mindegyikét ugyanannyiszor írtuk fel a sakktáblára. Az 1.1.3. Gyakorlat megoldásában szereplő vagdosási eljárással azt kapjuk, hogy ha r az k szám m-mel való osztási maradéka, akkor a bal felső $r \times r$-es négyzetben is ugyanannyiszor szerepel a $0, 1, \ldots, m-1$ számok mindegyike. Az $r-1$-es szám ennek a kis négyzetnek minden sorában pont egyszer szerepel (a mellékátló áll csupa $r-1$-ekből), azaz összesen r-szer. Tehát mind az m szám ennyiszer kell, hogy szerepeljen, azaz $mr = r^2$, hiszen ebben a négyzetben összesen r^2 szám van. Ez ellentmondás, mert $r < m$. (Máshogy is befejezhetjük a bizonyítást, ha észrevesszük, hogy a 0 az $r \times r$-es négyzet mindegyik sorában legfeljebb egyszer szerepelhet, de a második sorban egyáltalán nincs 0, és így ebben a négyzetben legfeljebb $r-1$ darab 0 lehet.)

1.1.19. Vizsgáljuk p-t modulo 3. Ha a maradék 1 vagy 2, akkor p^2+2 maradéka 0, azaz $3 \mid p^2+2$. Mivel feltettük, hogy p^2+2 is prímszám, ez csak úgy lehet, ha $p^2+2 = \pm 3$, azaz $p^2 = 1$, vagy $p^2 = -5$, de mindkettő lehetetlen (hiszen ± 1 nem prím). Tehát a p maradéka hárommal osztva csak 0 lehet, és mivel p prím, azt kapjuk, hogy p más, mint ± 3, nem lehet. Ebben az esetben viszont p^3+4 vagy 31, vagy -23, és mindkettő tényleg prímszám.

Ha azt tesszük fel, hogy p is és p^2+5 is prímszám, akkor a fenti gondolatmenetből most is látszik, hogy p csak ± 3 lehet. De ekkor $p^2+5 = 14$, ami nem prím. Tehát nincs ilyen p, és így a második állítás is igaz! Hiszen az összes ilyen prímre teljesül, hogy p^3+4 is prímszám (mert nincs egy sem)! Senki sem vonja kétségbe, hogy e könyv minden Olvasója halandó, még akkor sem, ha történetesen senki sem olvassa el a könyvet. Sőt, az is igaz állítás, hogy ha p és p^2+5 is prímszám, akkor $2 \cdot 2 = 5$, hiszen hamis feltételből bármi következik.

Mindebből látszik, hogy az első megoldásban, amikor már kijött, hogy $p = \pm 3$, *nem kell ellenőrizni, hogy* p^2+2 *ilyenkor prímszám-e.* Ha nem lenne az, attól még az állítás érvényben maradna, legfeljebb csak még kevesebb p tenne eleget a feltételeknek.

1.2. A harmadfokú egyenlet megoldásának problémája.

1.2.1. Az y helyébe $x + w$-t írva $x^2 + (2w + p)x + (w^2 + pw + q) = 0$ adódik. Akkor tudjuk ezt közvetlenül, egy négyzetgyökvonással megoldani, ha nincs az egyenletben x-es tag, azaz ha $2w + p = 0$, vagyis $w = -p/2$. Ilyenkor $x^2 = p^2/4 - q$, ahonnan x, majd $y = x - p/2$ is kifejezhető, és a másodfokú egyenlet szokásos megoldóképletét kapjuk.

1.2.2. Az y helyébe $x + w$-t írva, és az $(x + w)^3 = x^3 + 3x^2w + 3xw^2 + w^3$ azonosságot használva azt kapjuk, hogy az x^2-es tag együtthatója $3aw+b$. Ez pontosan akkor lesz nulla, ha $w = -b/3a$. A helyettesítést elvégezve $p = 3aw^2+2bw+c$ és $q = aw^3+bw^2+cw+d$ adódik. (Azaz q az eredeti egyenlet bal oldalának a w helyen felvett értéke).

1.2.3. Nem láttuk be még azt sem, hogy az egyenletnek *van* ilyen gyöke. Azt mutattuk meg, hogy *ha* az x ilyen alakú, *akkor* megoldása az egyenletnek. Egyelőre csak reménykedünk, hogy a gyököket mind megkapjuk majd ezzel az eljárással.

A következő példa érzékelteti, hogy ezt az állítást nem láttuk be. Képzeljük el, hogy az $x^3 + x + 1 = 0$ egyenletet modulo 3 akarjuk megoldani. Mivel modulo 3 a szokásos szabályokkal számolhatunk, sőt a nem nulla maradékokkal könnyen láthatóan még osztani is lehet modulo 3, az $x^3 + px + q = 0$ megoldásához levezetett képletek modulo 3 is érvényesek. Az egyenletnek nyilván gyöke az 1 modulo 3. De $-3uv = p = 1$ soha nem teljesülhet, hiszen a bal oldal mindenképpen nulla lesz modulo 3.

1.2.4. Ha x és y megoldása az egyenletrendszernek, akkor az első egyenletből $y = a - x$, ezért $x(a-x) = b$, azaz $x^2 - ax + b = 0$, tehát x megoldása a $z^2 - az + b = 0$ másodfokú egyenletnek. Hasonló számolással (vagy annak kihasználásával, hogy az egyenletrendszer szimmetrikus x-ben és y-ban) látjuk, hogy y is megoldása ennek a másodfokú egyenletnek.

Megfordítva, ha u megoldása a $z^2 - az + b = 0$ egyenletnek, akkor $u^2 - au + b = 0$, így

$$z^2 - az + b = z^2 - az + b - (u^2 - au + b) = (z - u)(z - (a - u)) .$$

Két valós szám szorzata csak akkor lehet nulla, ha valamelyik tényező nulla. Tehát a $z^2 - az + b = 0$ egyenlet megoldásai u és $a - u$, és más megoldása nincs. Mivel $u + (a - u) = a$ és $u(a - u) = au - u^2 = b$, ezért tényleg az egyenletrendszer megoldását kaptuk.

Összefoglalva tehát a következő állítást láttuk be. A $z^2 - az + b = 0$ egyenletnek legfeljebb két valós megoldása van.

- Ha kettő van: $u_1 \neq u_2$, akkor az egyenletrendszernek is két megoldása van (és több nincs): $(x, y) = (u_1, u_2)$ és $(x, y) = (u_2, u_1)$.
- Ha csak egy van, és ez u (ilyenkor tehát $z^2 - az + b = (x - u)^2$ teljesül), akkor az egyenletrendszernek is egy megoldása van (és több nincs): $(x, y) = (u, u)$.
- Ha egy sincs, akkor az egyenletrendszernek sincs megoldása.

1.2.6. Ha az y-os tagot akarjuk eltüntetni, akkor olyan w-t kell választanunk, melyre $3aw^2 + 2bw + c = 0$. Ez másodfokú egyenlet w-re, aminek nem is biztos, hogy van valós megoldása, és ha van is, a kapott négyzetgyökös kifejezéssel nehezebb számolni, mint amikor az y^2-es tagot tüntetjük el.

Ha viszont a konstans tagot akarjuk eltüntetni, akkor olyan w-t kell keresni, melyre $aw^3 + bw^2 + cw + d = 0$. Vagyis w megoldása kell, hogy legyen az eredeti egyenletnek! Tehát ezt a helyettesítést már csak akkor tudjuk elvégezni, ha ismerünk egy megoldást, márpedig a cél éppen a megoldások megkeresése lenne. Ezért hangsúlyoztuk azt, hogy az y^2-es tag kiejtéséhez használt w (és az új egyenletben keletkező p és q) konkrétan kifejezhető az eredeti egyenlet együtthatóiból.

1.2.7. Ez a gondolatmenet az 1.2.4. Gyakorlat fenti megoldásnak csak az első bekezdését pótolja.

1.2.8. Legyen $u = \sqrt[3]{7+\sqrt{50}}$ és $v = \sqrt[3]{7-\sqrt{50}}$, továbbá $x = u + v$. Mint láttuk, $x^3 = u^3 + v^3 + 3uv(u + v)$. Mivel

$$u^3 + v^3 = (7 + \sqrt{50}) + (7 - \sqrt{50}) = 14$$

és

$$uv = \sqrt[3]{(7 + \sqrt{50})(7 - \sqrt{50})} = \sqrt[3]{-1} = -1\,,$$

ezért azt kapjuk, hogy $x^3 = 14 + 3 \cdot (-1) \cdot (u + v) = 14 - 3x$. Mivel x egész szám, osztója kell legyen a 14-nek. A ±1, ±2, ±7, ±14 értékeket kipróbálva azt kapjuk, hogy csak $x = 2$ teljesíti az $x^3 = 14 - 3x$ összefüggést. Ezzel azt láttuk be, hogy *ha* a kifejezés értéke egész szám, *akkor* csak 2 lehet, de még nem tudjuk, hogy x tényleg egész szám-e.

A $0 = x^3 - 14 + 3x = (x-2)(x^2+2x+7)$ szorzat alakból az adódik, hogy vagy $x = 2$, vagy $x^2 + 2x + 7 = 0$. Ez utóbbi összefüggést semmilyen valós x szám nem teljesíti, ezért beláttuk, hogy a feladatbeli kifejezés értéke 2.

Másik megoldásként vegyük észre, hogy $7+\sqrt{50} = (1+\sqrt{2})^3$ és $7-\sqrt{50} = (1-\sqrt{2})^3$, ahonnan ismét $x = 2$ adódik.

1.2.9. Az első állításhoz azt kell belátni, hogy $1 + \sqrt{-1}$ negyedik hatványa -4. Ez közvetlen számolással látható, akár azonnal negyedik hatványra emelve a kifejezést, akár azt észrevéve, hogy $(1 + \sqrt{-1})^2 = 2\sqrt{-1}$. Hasonlóan kapjuk, hogy az

$$1 - \sqrt{-1}, \qquad -1 + \sqrt{-1}, \qquad -1 - \sqrt{-1}$$

kifejezések negyedik hatványa is -4. Később majd bebizonyítjuk, hogy ezeken kívül más hasonló kifejezés nincs, aminek a negyedik hatványa -4 lenne.

1.2.10. A felsorolt négy esetből kettőben ugyanaz a szám jön ki (csak felcserélődik u és v), a másik két esetben azonban általában nem is kapunk megoldást (mert a képlet eredménye nem $u+v$ lesz, hanem $2u$, illetve $2v$). Vigyázzunk, u^3 és v^3 a $z^2+qz-(p/3)^3$ másodfokú egyenlet mindkét gyökét ki kell, hogy adja (lásd az 1.2.4. Gyakorlat megoldását), és ezért nem választhatjuk a négyzetgyök előjelét mindkétszer ugyanannak. A képlet mindazonáltal helyesen van felírva, mert valós számok körében az a megállapodás, hogy a négyzetgyök, ha elvégezhető, mindig a pozitív eredményt jelöli.

1.2.11. Nem, hanem csak azt jelenti, hogy nagyon gondosan meg kell vizsgálnunk, hogy az új kifejezésekkel milyen szabályok szerint számolhatunk. Ez az átalakítás mindössze azt mutatja, hogy a $\sqrt{ab}=\sqrt{a}\sqrt{b}$ összefüggés (amit felhasználtunk) nem fog érvényben maradni az új kifejezésekre.

1.2.12. A részletes megoldás (harmadfokú helyett tetszőleges páratlan fokú polinomra) elolvasható az A.3.4. Tétel bizonyításában.

1.3. Számolás komplex számokkal.

1.3.1. Ha lehetne, azaz egyenlők lennének, akkor a $2+3i=4+5i$ egyenlőségből átrendezéssel $2i=-2$ adódna, négyzetre emelve $-4=4$, ami ellentmondás. Ez mutatja, hogy általában az $a+bi$ és $c+di$ számokat különbözőnek kell definiálnunk, ha $a\neq b$ vagy $c\neq d$. Ha így teszünk, akkor még reménykedhetünk, hogy a komplex számokkal való számolás nem vezet majd ellentmondásra.

1.3.4. Legyen $x=a+bi$, $y=c+di$ és $z=e+fi$. Ekkor az összeadás és a szorzás definícióját alkalmazva

$$(x+y)z=((a+c)+(b+d)i)(e+fi)=$$
$$=(ae+ce-bf-df)+(af+cf+be+de)i\,.$$

Az $xz+yz$ kifejezést hasonlóan kiszámítva ugyanezt a végeredményt kapjuk.

1.3.5. A z számot $a+bi$ alakban kereshetjük. Ekkor

$$1=(a+bi)(1+i)=(a-b)+(a+b)i\,.$$

Két komplex szám akkor egyenlő, ha a valós és a képzetes részeik is egyenlők. A valós részek az $1=a-b$, a képzetes részek a $0=a+b$ egyenlőséget adják. Az egyenletrendszert megoldva $z=(1/2)-(1/2)i$ adódik.

1.3.8. Ha z valós, akkor $z\overline{z}=z^2$. Ezért pozitív z esetén $z\overline{z}$ négyzetgyöke maga z lesz. Ha viszont z negatív valós szám, akkor $z\overline{z}$ négyzetgyöke $-z$ lesz, hiszen valós szám esetében a négyzetgyökjel a négyzetgyök két értéke közül mindig a nemnegatívat jelöli.

1.3.11.

(1) Az eredmények $5+i$, $-i$, $(1/13)+(5/13)i$.
(2) Mindkét eredmény 1. Az első tört esetében ez még kiszámolható, a második esetében már nem igazán. Azt kell észrevenni, hogy a számláló és a nevező abszolút értéke ugyanaz, és az 1.3.16. Gyakorlat szerint az abszolút érték tartja az osztást.
(3) $(1+i)^2 = 2i$, ezért $(1+i)^4 = (2i)^2 = -4$. Mivel $1241 = 4\cdot 310+1$, az eredmény $(1+i)^{1241} = (-4)^{310}(1+i) = 2^{620}+2^{620}i$.

1.3.12.

(1) $0 = x^2+1 = (x+i)(x-i)$, tehát a nullosztómentesség miatt $x = i$ vagy $x = -i$.
(2) $x^2+12 = (x+2\sqrt{3}i)(x-2\sqrt{3}i)$, ezért $x = \pm 2\sqrt{3}i$.
(3) $0 = x^2+2x+2 = (x+1)^2+1$ (a másodfokú egyenlet megoldási módszerét alkalmaztuk). Innen (1) szerint $x+1 = \pm i$, tehát $x = -1\pm i$.
(4) $0 = x^2+2ix-1 = (x+i)^2$, tehát $x = -i$.

1.3.13. Ha $-21+20i = (c+di)^2 = c^2-d^2+2cdi$, akkor a valós és képzetes rész egyértelműsége miatt $c^2-d^2 = -21$ és $cd = 10$. Tehát $c = 10/d$, és a másik egyenletbe visszahelyettesítve, majd d^2-tel szorozva d^4-21d^2-100 adódik. Ez d^2-re másodfokú egyenlet, a megoldóképletből $d^2 = 25$ vagy $d^2 = -4$. Ez utóbbi lehetetlen, mert d valós. Tehát $d = \pm 5$, és akkor $c = 10/d$ miatt $c+di = \pm(2+5i)$.

Ez a gondolatmenet elmondható a $-21+20i$ helyett az általános $a+bi$-re is. A számolást elvégezve $d^2 = (-a\pm\sqrt{a^2+b^2})/2$ adódik. Amikor a négyzetgyök előtt negatív előjel van, akkor biztosan negatív eredményt kapunk d^2-re, mert $\sqrt{a^2+b^2} \geq |a|$, ez tehát hamis gyök. Amikor a négyzetgyök előtt pozitív előjel van, akkor ugyanezért d^2-re nemnegatív eredményt kapunk. A $2cd = b$ összefüggés alapján c értékét is megkaphatjuk. A nevezőbeli csúnya gyökös kifejezéstől megszabadulhatunk, ha a törtet $\sqrt{a+\sqrt{a^2+b^2}}$-tel bővítjük. De azt is megtehetjük, hogy inkább c értékét is a d-hez hasonlóan, a megfelelő másodfokú egyenletből kapjuk meg. Bármelyik módszerrel számolunk, a végeredmény a következő lesz:

$$\sqrt{a+bi} = \pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} \pm i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}\,.$$

Ez látszólag négy megoldás, ezért hozzá kell tenni, hogy a $2cd = b$ összefüggés miatt pozitív b esetén a két négyzetgyök előjelét egyformának, negatív b esetén különbözőnek kell választani. A képletből látszik, hogy *minden nem nulla komplex számnak pontosan két négyzetgyöke van a komplex számok között.* Ezt a következő pontban más módszerrel is be fogjuk látni. A most levezetett képletet nem érdemes megtanulni, inkább a levezetéséhez használt módszert (vagy a következő pontban tanulandókat) érdemes alkalmazni, ha négyzetgyököt kell vonni.

Az $x^2+(i-2)x+(6-6i) = 0$ egyenlet megoldásához vegyük észre, hogy **a másodfokú egyenlet megoldásakor használt módszerünk komplex számokra is ugyanúgy**

érvényes. Valóban, ellenőrizhetjük, hogy az 1.2.1. Kérdés megoldásakor csak a „szokásos” számolási szabályokat használtuk (amik az 1.3.3. Állításban vannak felsorolva), valamint azt, hogy a komplex számok között is lehet osztani. Tehát a fenti egyenlet megoldásához egyszerűen behelyettesíthetünk az ismert megoldóképletbe. A négyzetgyök alatt pontosan $-21+20i$ fog állni, amiből most vontunk négyzetgyököt. Az eredmény $2+2i$ és $-3i$.

1.3.14. Az első négy egyenlet mindegyikére alkalmazhatjuk a másodfokú egyenlet megoldóképletét, és az előző feladatban leírt négyzetgyökvonási eljárást.

(1) $(1\pm i)/\sqrt{2}$.
(2) $(-3\pm\sqrt{7}i)/2$.
(3) $3-i$ és $-1+2i$.
(4) $1-i$ és $(4-2i)/5$.
(5) Vegyük mindkét oldal abszolút értékét. Mivel $|x|=|\overline{x}|$, de $|3+2i|\neq 1$, csak az $x=0$ megoldás. Második (csúnyább, de mechanikus) megoldás: az $x=a+bi$ helyettesítéssel, a szorzást elvégezve
$$a+bi=(3a+2b)+(2a-3b)i$$
adódik. A valós részeket nézve innen $a=3a+2b$, a képzetes részeket nézve $b=2a-3b$. Ennek az egyenletrendszernek csak $a=b=0$ megoldása.
(6) Írjuk x-et $a+bi$ alakba. Ekkor $a+bi=2a$ adódik, tehát $a=2a$ és $b=0$. Vagyis csak az $x=0$ nulla megoldás. Eljárhattunk volna úgy is, hogy észrevesszük: x csak valós lehet, mert az egyenlet jobb oldala valós, de valós szám valós része önmaga, tehát az $x=2x$ egyenletet kell megoldanunk.

1.3.15. Legyen $z=a+bi$ és $w=c+di$. Ekkor $\overline{zw}=(ac-bd)-(ad+bc)i=\overline{z}\,\overline{w}$.

1.3.16.

(1) Igaz, azt kell belátni, hogy $\overline{z-w}=\overline{z}-\overline{w}$. Ez közvetlenül kiszámolható. Második megoldásként vegyük észre, hogy az összegtartás miatt $\overline{z-w}=\overline{z}+(\overline{-w})$. Így elég megmutatni, hogy a konjugálás az ellentettképzést tartja, azaz hogy $\overline{-w}=-\overline{w}$. Legyen $u=-w$, akkor ismét az összegtartás miatt $0=\overline{0}=\overline{u+w}=\overline{u}+\overline{w}$, amiből az állítás következik.
(2) Nem igaz, például $|1+(-1)|\neq|1|+|-1|$.
(3) Igaz, és bizonyítás teljesen analóg az (1)-beli második megoldással. Tekintsük a z/w hányadost, és legyen $u=1/w$. A szorzattartás miatt $|z/w|=|zu|=|z||u|$. Másfelől $uw=1$ miatt $|u||w|=1$, és így $|z|/|w|=|z||u|=|z/w|$.

1.4. A komplex számok trigonometrikus alakja.

1.4.3. Az világos, hogy $r = s \neq 0$, mert mindkettő $|z|$-kel egyenlő. Az egyenlőség mindkét oldalát szorozzuk be $\cos(-\alpha) + i\sin(-\alpha)$-val. Ekkor a szorzat képlete miatt

$$\cos(\alpha - \alpha) + i\sin(\alpha - \alpha) = \cos(\beta - \alpha) + i\sin(\beta - \alpha)$$

adódik. A valós és képzetes részeket összehasonlítva $\cos(\beta - \alpha) = 1$ és $\sin(\beta - \alpha) = 0$, ahonnan az állítást kapjuk. (Mindez geometriailag is látszik, hiszen egyenlő komplex számok hossza és szöge is egyenlő.) A megfordítás nyilvánvaló.

1.4.5. Legyen $z = r(\cos\alpha + i\sin\alpha)$ és $w = s(\cos\beta + i\sin\beta)$. Olyan u számot keresünk, amit w-vel megszorozva z-t kapunk. Keressük u-t is trigonometrikus alakban, azaz legyen $u = t(\cos\gamma + i\sin\gamma)$. Ekkor

$$r(\cos\alpha + i\sin\alpha) = z = uw = ts(\cos(\gamma + \beta) + i\sin(\gamma + \beta))\,.$$

A trigonometrikus alak egyértelműségéből következik, hogy $r = st$, és $\alpha = \beta + \gamma$ (pontosabban $\alpha - (\beta + \gamma)$ a 360° egész számú többszöröse). Ezért

$$z/w = (r/s)(\cos(\alpha - \beta) + i\sin(\alpha - \beta))\,.$$

Vagyis a hosszakat osztani kell, a szögeket pedig kivonni (modulo 360°).

1.4.6. A $\overline{z}$ a z tükörképe a valós tengelyre. A $z - w$ az a vektor, ami a w pontból a z pontba mutat, ennek abszolút értéke pedig a hossza, vagyis *a z és w távolsága.*

1.4.7. Az ilyen feladatok megoldásának kétféleképpen vághatunk neki. Megpróbálhatjuk, hogy z helyébe $x + yi$-t helyettesítünk. A műveletek elvégzése után olyan összefüggést kapunk x és y között, amit koordináta-geometriai módszerekkel érthetünk meg, például ráismerhetünk egy egyenes, vagy egy kör egyenletére. Ez a módszer azonban sok számolással jár. Ezért előbb érdemes meggondolni, hogy a feladatból nem olvashatunk-e le közvetlenül geometriai jelentést. Ha sikerül, akkor általában elegáns megoldást kapunk.

(1) Ha $z = x + yi$, akkor $z + 3 + 2i = x + yi + 3 + 2i = (x + 3) + (y + 2)i$. Mivel $x + 3$ és $y + 2$ valós számok, ennek a számnak a valós része $x + 3$. Tehát az $x + 3 \leq -2$ egyenlőtlenséget kapjuk. Innen $x \leq -5$, tehát a keresett alakzat egy félsík, amelyet az $x = -5$ egyenletű függőleges egyenes határol.

(2) Ha $z = x + yi$, akkor $x + 1 \geq y - 3$ adódik, vagyis $y \leq x + 4$. Ez is egy (zárt) félsík, ami az $y = x + 4$ egyenes alatt lévő pontokból áll, az egyenest is beleértve.

(3) Ha koordináta-geometriára vezetjük vissza az állítást egy kör egyenletét kell felismernünk. Jobb azonban, ha közvetlenül okoskodunk. A $|z - 1 - i|$ szám az előző feladat szerint a z és $1 + i$ pontok távolsága. Az egyenlőtlenség tehát azt fejezi ki, hogy a z pont az $1 + i$ ponttól legfeljebb 3 egység távolságra van. Vagyis egy zárt körlapot kapunk, melynek sugara 3, középpontja (1, 1).

(4) Ugyancsak az előző feladat szerint ez azon z pontok halmaza, amelyek a $3 - 2i$ és a $-4 + i$ pontoktól egyenlő távolságra vannak, azaz a két pontot összekötő szakasz felező merőlegese.

(5) Ez koordináta-geometriával egyszerűbb. Mondhatjuk azonban a következőt is: a $\overline{z}$ a z tükörképe a valós tengelyre. Ha e két vektor összege -1, akkor egy rombuszt kapunk, mely átlójának két végpontja 0 és -1. A lehetséges csúcsok tehát a $\mathrm{Re}(z) = -1/2$ függőleges egyenesen vannak.
(6) Az első halmaznál $|z|^2 = z\overline{z} = 1$, tehát az egységkört kapjuk. A második halmaz esetében átszorzással $1+8z = |z|^2$ adódik. Mivel $|z|$ valós, z is az, és így $|z|^2 = z^2$. A másodfokú egyenletet megoldva $z = 4 \pm \sqrt{17}$ adódik.
(7) Mivel $r = |z|$ nemnegatív valós, $iz = r$-et i-vel osztva $z = -ir$ adódik, azaz a keresett halmaz a képzetes tengely negatív része a nullával együtt. Ennek minden pontja jó, mert $|-ir| = r$.
(8) Végezzük el az osztást a $(z-1)/(z+1)$ tört esetében, azaz szorozzunk be a nevező konjugáltjával. Ekkor a számláló értéke $(z-1)(\overline{z}+1) = (|z|^2-1)+(z-\overline{z})$. Itt $|z|^2-1$ valós, $z-\overline{z}$ pedig tisztán képzetes. Tehát a $(z-1)/(z+1)$ valós része akkor és csak akkor nulla, ha $|z| = 1$, a képzetes része pedig akkor nulla, ha $z = \overline{z}$, vagyis ha z valós. Vagyis az első halmaz az egész valós egyenes, kivéve a -1 számot, a második halmaz pedig az egész egységkör, szintén kivéve a -1 számot.

1.4.8. Konkrét szám esetében a $z = a+bi$ trigonometrikus alak felírásához először érdemes azt meggondolni, hogy z szám melyik síknegyedbe esik, ezt a és b előjele dönti el. Ezután a $|z| = \sqrt{a^2+b^2}$ és a $\mathrm{tg}\,\alpha = b/a$ összefüggésből már könnyen megkapjuk a trigonometrikus alakot. Vigyázzunk, a $\cos\alpha - i\sin\alpha$ szám nincs trigonometrikus alakban, ennek szöge ugyanis $-\alpha$ (vagyis $2\pi-\alpha$). Az eredmények:

(1) $1+i = \sqrt{2}(\cos 45^\circ + i\sin 45^\circ)$ és $1-i = \sqrt{2}(\cos 315^\circ + i\sin 315^\circ)$.
(2) $\sqrt{3}+i = 2(\cos 30^\circ + i\sin 30^\circ)$ és $-1-\sqrt{3}i = 2(\cos 240^\circ + i\sin 240^\circ)$.
(3) $\cos 300^\circ + i\sin 300^\circ$.
(4) $(\sqrt{6}/2)(\cos 315^\circ + i\sin 315^\circ)$.

1.4.9.

(1) Az origóból való háromszorosra nyújtás, majd eltolás az x-tengely pozitív felének irányába két egységgel.
(2) Forgatva nyújtás az origóból: 45°-kal forgatunk és $\sqrt{2}$-szeresre nyújtunk. Ez az $1+i$ trigonometrikus alakjából olvasható le.
(3) A z pont képe a z-t az origóval összekötő félegyenesen van, és távolsága az origótól a z távolságának reciproka.

Ezt a transzformációt a geometriában az egységkörre vonatkozó *inverziónak* nevezik. Nevezetes tulajdonsága, hogy kört és egyenest is körbe vagy egyenesbe visz. Hasonló tulajdonságúak a $z \mapsto (az+b)/(cz+d)$, úgynevezett *törtlineáris transzformációk* is.

1.4.10.

(1) $(z+w)/2$. Ez leolvasható például az 1.1. ábráról, hiszen a paralelogramma átlói felezik egymást.
(2) $\{x \in \mathbb{C} : |x-z| = |x-w|\}$.
(3) $\{x \in \mathbb{C} : |x-z| = |w-z|\}$.
(4) iz.
(5) $i(z-w)$.
(6) A $z-w$ vektort kell $+90^\circ$-kal elforgatni, majd a kezdőpontját a w-be tenni, ami azt jelenti, hogy a végpontja (az origótól számítva) $i(z-w)+w$-ben lesz.
(7) Ha x a keresett pont, akkor az x-ből z-be mutató vektor $\pm 90^\circ$-kal történő elforgatottja x-ből w-be kell, hogy mutasson. Vagyis $(z-x)i = w-x$, illetve $(z-x)(-i) = w-x$. Innen x-re $(w-zi)/(1-i)$, illetve $(w+zi)/(1+i)$ adódik.
(8) Legyen $\varepsilon = \cos 120^\circ + i \sin 120^\circ$, ekkor $\varepsilon^2 = \overline{\varepsilon} = \cos 240^\circ + i \sin 240^\circ$. Az előzőhöz hasonló számolással $(w-\varepsilon z)/(1-\varepsilon)$, illetve $(w-\varepsilon^2 z)/(1-\varepsilon^2)$ adódik.

1.4.11. A négyzet négy csúcsa legyen A, B, C, D, pozitív körüljárás szerint. Ekkor az AB oldalra kifelé írt négyzet középpontja az előző feladat (7) pontjának megoldását felhasználva $(B+Ai)/(1+i)$. A másik három négyzet középpontját ugyanígy kapjuk. A szemközti négyzetek középpontját összekötő két vektor tehát

$$\frac{1}{1+i}\big((B+Ai)-(D+Ci)\big),$$

illetve

$$\frac{1}{1+i}\big((C+Bi)-(A+Di)\big).$$

Az első vektor i-szerese a második, ezért a két vektor egyenlő hosszú, és merőleges.

1.4.12. Legyen $\varepsilon = \cos 120^\circ + i \sin 120^\circ$ és $\eta = \cos 60^\circ + i \sin 60^\circ$. A szabályos hatszöget felrajzolva látjuk, hogy $\eta = 1+\varepsilon$ és $1+\varepsilon+\varepsilon^2 = 0$, továbbá nyilván $\eta^2 = \varepsilon$ és $\varepsilon\eta = -1$. Ha a háromszög csúcsai A, B, C, akkor az 1.4.10. Gyakorlat (8) pontja miatt az AB csúcsra kifelé írt szabályos háromszög középpontja

$$X = \frac{1}{1-\varepsilon}(A-\varepsilon B).$$

Analóg módon írhatjuk fel a másik két szabályos háromszög középpontját is, jelölje ezeket Y és Z. Azt kell belátni, hogy az $\overrightarrow{XY}$ vektort 60°-kal elforgatva az $\overrightarrow{XZ}$-t kapjuk, azaz $(Y-X)\eta-(Z-X)=0$. Behelyettesítve, $1-\varepsilon$-nal szorozva, és A, B, C szerint rendezve a következőt kapjuk:

$$A(-\eta+\varepsilon+1)+B(\eta+\varepsilon\eta-\varepsilon)+C(-\varepsilon\eta-1).$$

A fenti összefüggések miatt itt A, B és C együtthatója is nulla.

1.4.13. Csak a megoldás ötletét mondjuk el, a diszkussziót az Olvasóra hagyjuk. Két komplex szám hányadosának szöge a szögek különbsége. Ez a hányados tehát akkor lesz pozitív valós, ha a két vektor szöge ugyanaz (hiszen a pozitív valós számok szöge 0°), és akkor lesz negatív valós, ha a két vektor iránya ellentétes (hiszen a negatív valós számok szöge 180°). Rögzítsük a z_1 és z_2 pontokat. Ekkor $(z_3 - z_1)/(z_3 - z_2)$ szöge a $z_1z_2z_3$ háromszögnek a z_3-nál levő szöge. A kettősviszony tehát akkor pozitív valós, ha a z_1z_2 szakasz a z_3 és z_4 pontokból ugyanolyan szögben látszik, vagyis ha z_3 és z_4 ugyanazon a látóköríven van. A kettősviszony akkor lesz negatív valós, ha z_3 és z_4 ugyanazon a látókörön van, de ellentétes íveken. Az egyenest azért kell megengedni, mert a vizsgált háromszögek el is fajulhatnak.

1.4.14. Legyenek a négyszög csúcsai A, B, C, D. Ekkor

$$(A - B)(C - D) + (A - D)(B - C) = (A - C)(B - D)\,,$$

hiszen ez azonosság. A háromszög-egyenlőtlenség miatt innen

$$|(A - C)(B - D)| \le |(A - B)(C - D)| + |(A - D)(B - C)|\,.$$

De a bal oldalon ef, a jobb oldalon $ac + bd$ áll. Egyenlőség akkor van, ha $(A - B)(C - D)$ és $(A - D)(B - C)$ párhuzamos, és egyenlő állású, vagyis ha a hányadosuk pozitív valós szám. Az előző feladat szerint ilyenkor $ABCD$ húrnégyszög. Megfordítva, ha $ABCD$ konvex húrnégyszög, akkor az A és C csúcsoknál levő szögek összege 180°, ahonnan az előző feladat megoldása szerint következik, hogy $(A - B)(C - D)$ és $(A - D)(B - C)$ hányadosa pozitív valós. A diszkussziót most is az Olvasóra hagyjuk.

1.4.15. Legyen $\varepsilon = \cos(x/2) + i\sin(x/2)$, akkor a keresett összeg az $\varepsilon^2 + \varepsilon^4 + \ldots + \varepsilon^{2n}$ képzetes része. A mértani sort összeadva az eredmény

$$\varepsilon^2\frac{\varepsilon^{2n} - 1}{\varepsilon^2 - 1} = \varepsilon^{n+1}\frac{\varepsilon^n - (1/\varepsilon^n)}{\varepsilon - (1/\varepsilon)}\,.$$

Ez az átírás azért jó, mert $\varepsilon - (1/\varepsilon) = -2i\sin(x/2)$ és $\varepsilon^n - (1/\varepsilon)^n = -2i\sin(nx/2)$. Így

$$\sin x + \sin 2x + \ldots + \sin nx = \frac{\sin((n+1)x/2)\sin(nx/2)}{\sin(x/2)}\,,$$

és

$$\cos x + \cos 2x + \ldots + \cos nx = \frac{\cos((n+1)x/2)\sin(nx/2)}{\sin(x/2)}\,.$$

A végeredmény birtokában természetesen az állítás már komplex számok nélkül is igazolható, például n szerinti indukcióval.

1.5. Egységgyökök és rendjeik.

1.5.1. Az r pozitív valós szám, és az n-edik gyökét is a pozitív valós számok között keressük. Az analízis eredményei szerint ilyen n-edik gyök mindig pontosan egy van.

1.5.2. Keressük az n-edik gyököket $w = s(\cos\beta + i\sin\beta)$ alakban, ekkor

$$w^n = s^n(\cos n\beta + i\sin n\beta) = r(\cos\alpha + i\sin\alpha)\,,$$

ahonnan a trigonometrikus alak egyértelműsége miatt $s = \sqrt[n]{r}$, és $n\beta - \alpha = 2k\pi$, ahol k egész szám. A k számot helyettesíthetjük az n-nel való osztási maradékával, mert ez a $\beta = (\alpha + 2k\pi)/n$ szöget csak modulo 2π változtatja meg.

1.5.5. Ha $|z| > 1$, akkor $1 < |z| < |z|^2 < |z|^3 < \ldots$ egyre nagyobb lesz, soha nem lesz közöttük egyenlő. Sőt a negatív kitevőkre sem, mert $1 = |z|^0 > |z|^{-1} > \ldots$ meg egyre kisebb lesz. Ugyanez a helyzet akkor, ha $|z| < 1$, mert akkor minden fordítva van. (Elegánsabban: a z helyett az $1/z$-re mondható el a fenti gondolatmenet, aminek már 1-nél nagyobb az abszolút értéke, viszont a hatványai ugyanazok, mint a z hatványai.) Tehát csak $|z| = 1$ jön szóba, vagyis $z = 1$ vagy -1. Az 1 hatványai egyesével, a -1 hatványai kettesével ismétlődnek. Valójában az 1 első, a -1 második egységgyök.

1.5.8. Képzeljük azt, hogy kettesével ugrál. Ha n páratlan, akkor az első körben pont átugorja a kiindulópontot, és így n lépést megtéve, minden csúcsot érintve, két kör után ér haza. Ha viszont az n páros, akkor már $n/2$ lépés, és egy kör megtétele után hazaér, miközben a csúcsok felét kihagyja.

Általában, ha k-asával ugrál, akkor m lépést megtéve a km-edik csúcson lesz. Ez akkor a kiindulópont, ha $n \mid km$. A legkisebb ilyen m számot keressük. Nyilván

$$n \mid km \iff \frac{n}{(n,k)} \,\Big|\, \frac{k}{(n,k)}m$$

(itt az (n,k) legnagyobb közös osztót jelöl). Mivel $n/(n,k)$ és $k/(n,k)$ relatív prímek, ez az oszthatóság akkor és csak akkor érvényes, ha

$$\frac{n}{(n,k)} \,\Big|\, m\,.$$

A *legkisebb* ilyen (pozitív) m természetesen maga az $n/(n,k)$. Ezért a bolha ennyi lépést tesz meg, amikor először visszaér (és ennyi csúcsot is érint). Ezalatt k-szor ennyi „távolságot" tesz meg, és mivel a kör hossza n, a megtett körök száma a megtett távolság n-edrésze, vagyis $k/(n,k)$.

Megjegyezzük, hogy a fenti gondolatmenet negatív egész k számokra is érvényes, ebben az esetben a bolha visszafelé ugrál.

1.5.13. A megoldáshoz felhasználjuk a gyökvonás képletét (1.5.2. Gyakorlat). Néhány esetben egyszerűbb csak egy gyököt megkeresni, és azt az egységgyökökkel végigszorozni.

(1) A harmadik egységgyökök, algebrai alakban 1 és $-1/2 \pm i\sqrt{3}/2$.
(2) A -4 trigonometrikus alakja $4(\cos 180^\circ + i \sin 180^\circ)$. A negyedik gyökök $\pm 1 \pm i$.
(3) $\sqrt{3} - i = 2(\cos 330^\circ + i \sin 330^\circ)$, a képlet szerint a 8-adik gyökök hossza $\sqrt[8]{2}$, szögeik $41, 25^\circ + k \cdot 45^\circ$, ahol $0 \leq k < 8$.
(4) Ezek azok a $2n$-edik egységgyökök, amelyek nem n-edik egységgyökök. Szögeik a $2\pi/2n$ páratlan többszörösei, hosszuk 1.

1.5.14. Elég meghatározni a rendeket, mert ezután a válasz a következő gyakorlat megoldásából leolvasható. Az 1.5.10. Állítást használjuk. Az $1 + i$ és a $\cos(\sqrt{2}\pi) + i \sin(\sqrt{2}\pi)$ rendje végtelen, az $(1 + i)/\sqrt{2}$ szöge $360^\circ/8$, tehát rendje 8, végül $\cos(336^\circ) + i \sin(336^\circ)$ rendje a $336/360$ tört egyszerűsített alakjának nevezője, azaz 15.

1.5.15. Ha egy egységgyök rendje d, akkor csak az $n = d$ esetben lesz primitív n-edik egységgyök, és pontosan a $d \mid n$ számokra lesz lesz n-edik egységgyök, hiszen ezek a jó kitevői.

1.5.16. Ha $\varepsilon^n = i$, akkor $\varepsilon^{4n} = i^4 = 1$, ezért ε rendje véges, és $4n$-nek osztója. Ha $o(\varepsilon) = d$, akkor $\varepsilon^d = 1$. Innen $1 = \varepsilon^{dn} = i^d$, és így $4 = o(i) \mid d$.

1.5.17. Mivel $\varepsilon^{512} = 1$, ezért $(-i\varepsilon)^{512} = 1$. Így $o(-i\varepsilon) \mid 512$. De $512 = 2^9$, tehát ha $o(-i\varepsilon) \neq 512$, akkor már $o(-i\varepsilon) \mid 256$ is teljesül. De ez lehetetlen, mert $(-i\varepsilon)^{256} = \varepsilon^{256}$, ami nem 1, mert 512 a legkisebb pozitív jó kitevője ε-nak. Tehát $o(-i\varepsilon) = 512$.

Második megoldás. Az 1.5.10. Állítást fogjuk használni. Az ε szám szöge 360°-nak $k/512$-szerese, ahol $(k, 512)$=1, vagyis k páratlan. Mivel $-i$ szöge 360°-nak $-1/4$-szerese, ezért $-i\varepsilon$ szöge 360°-nak $(k/512) - (1/4) = (k-128)/512$-szöröse. Ez egyszerűsíthetetlen tört, hiszen a nevező 2-hatvány, a számláló pedig páratlan. Ezért $-i\varepsilon$ rendje is 512.

1.5.18. Ha ε rendje 4-gyel osztható, akkor $o(-\varepsilon) = o(\varepsilon)$. Ha csak kettővel osztható, de 4-gyel nem, akkor $o(-\varepsilon) = o(\varepsilon)/2$. Végül ha $o(\varepsilon)$ páratlan, akkor $o(-\varepsilon) = 2 \cdot o(\varepsilon)$. Minderre két bizonyítást is adunk. Legyen $o(\varepsilon) = n$.

Első megoldás. Keressük meg a $-\varepsilon$ jó kitevőit. Nyilván $(-\varepsilon)^k = (-1)^k \varepsilon^k$. Ez akkor lesz 1, ha $\varepsilon^k = (-1)^k$. Speciálisan $k = 2n$ jó kitevő. Négyzetre emelve $\varepsilon^{2k} = 1$, azaz $n \mid 2k$ minden k jó kitevőre. Vagyis ha $d = o(-\varepsilon)$, akkor $n \mid 2d$ és $d \mid 2n$. Tehát $nx = 2d$ és $dy = 2n$ alkalmas x, y pozitív egészekre, ahonnan $xy = 4$ adódik. Így d/n (ami $x/2$) csak 1, 2, vagy $1/2$ lehet.

Ha n páratlan, akkor innen $n \mid d$, és mivel n nem jó kitevő ilyenkor, $d = 2n$. Ha n páros, akkor már n is jó kitevő, tehát $d \mid n$, és így az a kérdés, hogy $n/2$ mikor jó kitevő. Nyilván $(\varepsilon)^{n/2} = -1$ (mert $(\varepsilon)^{n/2}$ négyzete 1, de önmaga nem 1). Tehát $n/2$ akkor jó kitevő, ha $(-1)^{n/2} = -1$, azaz ha $4 \nmid n$. Ilyenkor $d = n/2$, különben csak $d = n$ lehet.

Második megoldás. Ismét az 1.5.10. Állítást használjuk. Legyen ε szöge 360°-nak k/n-szerese, ahol $(k, n) = 1$. Mivel -1 szöge $360^\circ/2$, a $-\varepsilon$ szöge 360°-nak $(k/n) + (1/2) = (2k + n)/(2n)$-szerese. Azt kell megvizsgálnunk, hogy ennek a törtnek mennyi a nevezője

az egyszerűsítés után. Könnyű meggondolni, hogy a számlálónak és a nevezőnek nem lehet 2-től különböző prímosztója. Tehát az a kérdés, hogy a 2 melyik hatványával lehet egyszerűsíteni. Ha n páratlan, akkor már 2-vel sem lehet egyszerűsíteni, mert a számláló páratlan. Ha n páros, akkor $(k, n) = 1$ miatt k páratlan. Ilyenkor 2-vel lehet egyszerűsíteni, és a számláló $k + n/2$ lesz. Ha $4 \mid n$, akkor ez páratlan, tehát nem lehet tovább egyszerűsíteni. Ha $4 \nmid n$, akkor még 2-vel egyszerűsíthetünk, de tovább már nem, a nevező miatt.

1.5.19. Az első esetben a tizenkettedik egységgyököket kapjuk, mindegyiket kétszer. A másodikban a negyvenkettedik egységgyököket kapjuk, mindegyiket egyszer.

1.5.20.

(1) A közös gyökök azok az ε számok, melyekre $\varepsilon^n = 1 = \varepsilon^m$, vagyis amelyek rendje osztója m-nek is és n-nek is. Ezek tehát pontosan az (m, n)-edik egységgyökök, így számuk (m, n).

(2) Ha $\varepsilon^m = 1$ és $\eta^n = 1$, akkor nyilván $(\varepsilon\eta)^{mn} = 1$.

(3) Legyen $o(\varepsilon) = m$ és $o(\eta) = n$. Ha m és n nem relatív prímek, akkor legkisebb közös többszörösük, amit $[m, n]$ jelöl, kisebb, mint a szorzatuk. De $(\varepsilon\eta)^{[m,n]} = 1$, tehát $\varepsilon\eta$ rendje kisebb, mint mn.

Tegyük most fel, hogy m és n relatív prímek. Legyen $d = o(\varepsilon\eta)$, be kell látni, hogy $d = mn$. A (2) miatt ehhez elég, hogy $mn \mid d$, ehhez pedig, hogy $m \mid d$ és $n \mid d$ (hiszen m és n relatív prímek). Szimmetriaokokból elég csak az első oszthatóságot megmutatni.

Nyilván $(\varepsilon\eta)^d = 1$. Ezt n-edik hatványra emelve $1 = \varepsilon^{nd}\eta^{nd} = \varepsilon^{nd}$. Ezért $m = o(\varepsilon) \mid nd$. Mivel $(n, m) = 1$, ebből következik a kívánt állítás.

1.5.21. Elsőnek az n-edik egységgyökök összegét számítjuk ki. Hogyan fogná fel ezt a feladatot egy fizikus? Azt mondaná, hogy egy szabályos sokszög csúcsaiba mutató vektorok s átlaga a súlypontba, vagyis a sokszög középpontjába mutat. Azért a középpontjába, mert a sokszög szimmetrikus. Ha nem a középpontba mutatna, akkor el lehetne forgatni a sokszöget úgy, hogy önmagába menjen, de s elforduljon, ami lehetetlen.

Második megoldásként ezt a gondolatmenetet modellezzük algebrailag. Jelölje S az n-edik egységgyökök összegét, és legyen ε az az egységgyök, melynek szöge $2\pi/n$. Ezzel a szöggel „forgassuk el" az S összeget, azaz szorozzuk meg ε-nal. Ekkor az összeg tagjai ugyanazok maradnak, csak más sorrendben lesznek felírva. Ezért $S\varepsilon = S$. Innen $S = 0$ vagy $\varepsilon = 1$ következik. De $\varepsilon = 1$ pontosan akkor, ha $n = 1$. Tehát a keresett összeg nulla, kivéve ha $n = 1$, amikor az összeg értéke 1.

Amikor az n-edik egységgyökök szorzatát vizsgáljuk, akkor másik ötlet segít. Párosítsuk mindegyik egységgyököt a konjugáltjával. Ez azért hasznos, mert $\varepsilon\overline{\varepsilon} = |\varepsilon|^2 = 1$, vagyis a konjugáltak kiejtik egymást. Marad azoknak az egységgyököknek a szorzata, amelyeknek a párja önmaga, azaz amelyek valósak. Ilyen egységgyök csak az 1 és a -1 lehet. Ha n páros, akkor a -1 is szerepel az n-edik egységgyökök között, ezért az eredmény -1. Ha n páratlan, akkor viszont 1 a keresett szorzat értéke.

Megjegyezzük, hogy az egységgyökök összegét és szorzatát is kiszámolhattuk volna közvetlenül a trigonometrikus alakból. Az összeghez mértani sort kell összeadni, a szorzásnál meg a szögek adódnak össze, és itt számtani sort kapunk. Ez a módszer hasznos a négyzetösszeg kiszámítására is. A mértani sor összegképlete alapján

$$\varepsilon_1^2+\varepsilon_2^2+\ldots+\varepsilon_n^2=\varepsilon_1^2+\varepsilon_1^4+\ldots+\varepsilon_1^{2n}=\frac{\varepsilon_1^{2n}-1}{\varepsilon_1^2-1}\,.$$

A számláló nulla, és így az eredmény is az, kivéve ha a nevezőben nulla van, vagyis ha $\varepsilon_1^2=1$. Ez csak úgy lehet, ha $n=1$ vagy $n=2$. Ezekben az esetekben közvetlenül láthatjuk, hogy a négyzetösszeg 1, illetve 2.

1.5.22. A binomiális tételt alkalmazzuk először az $(1+1)^n$ összegre.

$$2^n=\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{n}.$$

Hasonlóan felírva az $(1-1)^n$ összeget, azt kapjuk, hogy

$$0=\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\ldots+(-1)^n\binom{n}{n}.$$

Legyen

$$A=\binom{n}{0}+\binom{n}{2}+\ldots\qquad\text{és}\qquad B=\binom{n}{1}+\binom{n}{3}+\ldots$$

(az összegezést akár a végtelenségig is folytathatjuk, mert egy binomiális együttható értéke nulla lesz, ha az alul álló szám már meghaladja a felül állót). Ekkor a fenti képletek szerint $A+B=2^n$ és $A-B=0$, vagyis $A=B=2^{n-1}$. Végül írjuk fel az $(1+i)^n$ összeget.

$$(1+i)^n=\binom{n}{0}+i\binom{n}{1}-\binom{n}{2}-i\binom{n}{3}+\binom{n}{4}+i\binom{n}{5}-\binom{n}{6}-i\binom{n}{7}+\binom{n}{8}\ldots.$$

Ezért

$$\mathrm{Re}((1+i)^n)=\binom{n}{0}-\binom{n}{2}+\binom{n}{4}-\binom{n}{6}+\binom{n}{8}-+\ldots.$$

Ha most

$$X=\binom{n}{0}+\binom{n}{4}+\binom{n}{8}+\ldots\qquad\text{és}\qquad Y=\binom{n}{2}+\binom{n}{6}+\binom{n}{10}+\ldots,$$

akkor $X-Y=\mathrm{Re}((1+i)^n)$ és $X+Y=B=2^{n-1}$. Innen pedig a keresett X kifejezhető: $X=(2^{n-1}+\mathrm{Re}((1+i)^n))/2$. Az $(1+i)^n$ értékét trigonometrikus alakban számíthatjuk ki, az eredmény $2^{n/2}(\cos(2n\pi/8)+i\sin(2n\pi/8))$, aminek a valós része $2^{n/2}\cos(2n\pi/8)$. A feladatban $n=1867$, így a végeredmény $X=2^{1865}-2^{932}$.

1.5.23. Egyrészt

$$(\cos x + i \sin x)^n = \cos(nx) + i \sin(nx)\,,$$

másrészt a binomiális tétel miatt

$$(\cos x + i \sin x)^n = \sum_{j=0}^{n} i^j \binom{n}{j} \cos^{n-j} x \sin^j x$$

(az itt használt, úgynevezett szumma jelölés magyarázata a 2.1.8. Definícióban található). Innen valós és képzetes részt véve

$$\cos(nx) = \cos^n x - \binom{n}{2} \cos^{n-2} x \sin^2 x + \binom{n}{4} \cos^{n-4} x \sin^4 x - \binom{n}{6} \cos^{n-6} x \sin^6 x \ldots$$

(itt $\sin^2 x$ helyére $1 - \cos^2 x$-et írva $\sin x$ teljesen eltüntethető), és

$$\sin(nx) = \binom{n}{1} \cos^{n-1} x \sin x - \binom{n}{3} \cos^{n-3} x \sin^3 x + \binom{n}{5} \cos^{n-5} x \sin^5 x \ldots$$

11.2. Polinomok

2.1. A polinom fogalma.

2.1.3. Az eredmény

$$a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 +$$
$$+(a_0b_3 + a_1b_2 + a_2b_1)x^3 + (a_1b_3 + a_2b_2)x^4 + a_2b_3x^5\,.$$

Amennyiben a_2 és b_3 sem nulla, a szorzat foka 5.

2.1.4. Először a bal oldali zárójelet bontjuk föl:

$$(a_1 + \ldots + a_n)(b_1 + \ldots + b_m) = a_1(b_1 + \ldots + b_m) + \ldots + a_n(b_1 + \ldots + b_m)\,.$$

Ha most mindegyik zárójelben beszorzunk, az állítást kapjuk.

2.1.9. Az eredmények

$$(x^3 + 3x^2 + 2) - (x^3 + 3x - 4) = 3x^2 - 3x + 6\,,$$
$$(x^2 + ix + 3)(x^2 + i) = x^4 + ix^3 + (3 + i)x^2 - x + 3i\,.$$

Az első polinom másodfokú, a második negyedfokú.

2.1.10. Ha $n = 3$, akkor az eredmény

$$a_1a_2a_3 + a_1a_2b_3 + a_1b_2a_3 + a_1b_2b_3 + b_1a_2a_3 + b_1a_2b_3 + b_1b_2a_3 + b_1b_2b_3\,.$$

Az általános $(a_1+b_1)\dots(a_n+b_n)$ szorzatot több lépésben fejthetjük ki (és közben mindig felhasználhatjuk a 2.1.4. Gyakorlatot). A végeredmény egy 2^n tagú összeg lesz, amelynek mindegyik tagja egy n-tényezős $x_1x_2\dots x_n$ szorzat, ahol az x betű helyére a vagy b betűt kell írni az összes lehetséges kombinációban. Általában *ha több soktagú összeget szorzunk össze, akkor mindegyik tényezőből ki kell venni egy tagot az összes lehetséges módon egymástól függetlenül, ezeket össze kell szorozni, és a kapott szorzatokat összeadni.*

2.1.11. Írjuk be az a_{ij}-ket egy táblázatba: az a_{ij} az i-edik sor j-edik helyére kerüljön (tehát n sor lesz, és m oszlop). Ekkor mindkét szumma a táblázatban álló számok összege, csak az elsőben először az oszlopokat adjuk össze, a másodikban pedig először a sorokat.

2.2. A szokásos számolási szabályok.

2.2.2. A tényezők száma szerinti indukcióval bizonyítunk, azaz feltesszük, hogy az n-nél kevesebb tényezős szorzatok értéke már független a zárójelezéstől. Ha adott egy n-tényezős szorzat, akkor az $A*B$ alakú, ahol A és B már rövidebb szorzatok. Ha A nem egytényezős, akkor az indukciós feltevés miatt $A = a_1*C$ alakban írható. Az asszociativitást alkalmazva $A*B = (a_1*C)*B = a_1*(C*B)$. Vagyis mindegyik n-tényezős szorzat a_1*D alakra hozható. Az indukciós feltevés miatt D értéke független a zárójelezéstől, tehát tényleg bármely két zárójelezés ugyanazt az eredményt adja.

2.2.4. Legyenek f, g, h az X halmazon értelmezett, X-be vezető függvények. Azt kell belátni, hogy $f\circ(g\circ h) = (f\circ g)\circ h$. Két függvény akkor egyenlő, ha minden helyen megegyezik az értékük. De ha $x\in X$ tetszőleges, akkor a kompozíció definícióját ismételten felhasználva

$$\big(f\circ(g\circ h)\big)(x) = f\big((g\circ h)(x)\big) = f\Big(g\big(h(x)\big)\Big)\,,$$

és

$$\big((f\circ g)\circ h\big)(x) = \big(f\circ g\big)\big(h(x)\big) = f\Big(g\big(h(x)\big)\Big)\,.$$

A két érték tehát tényleg ugyanaz.

Ha vesszük az x-tengelyre való T tengelyes tükrözést, illetve az origó körüli 90 fokos F forgatást, akkor ez a két transzformáció nem cserélhető fel. Ezt a legegyszerűbben komplex számokkal láthatjuk be: $T(z) = \overline{z}$, és $F(z) = iz$, de $(T\circ F)(z) = \overline{iz} = -i\overline{z}$ nem egyenlő $(F\circ T)(z) = i\overline{z}$-tal, kivéve ha $z = 0$.

2.2.5. Az útmutatásban szereplő állítás igazolása a következő. Keressük meg azt a könyvet, ami a legbaloldalra való, és addig cseréljük meg mindig a bal oldali szomszédjával, amíg a helyére nem kerül. Ezután ugyanezt végigcsináljuk a balról második helyre való könyvvel, és így tovább.

Ha adott az $a_1 * \ldots * a_n$ szorzat, akkor a 2.2.2. Feladat miatt a zárójelezéssel nem kell foglalkoznunk, a kommutativitás viszont lehetővé teszi bármely két szomszédos tényező cseréjét. Ennek ismételgetésével pedig a tényezők bármelyik sorrendje megkapható.

2.2.7. Az *identikus leképezés* az az *id* függvény, amely X minden eleméhez saját magát rendeli. Nyilvánvalóan $f \circ id = id \circ f = f$ tetszőleges f függvényre (aki nem hiszi, helyettesítsen be tetszőleges $x \in X$-et). Más függvény nem lehet neutrális elem. Ha ugyanis e ilyen, akkor az $e \circ id = id$ egyenletbe x-et helyettesítve $e(x) = x$ adódik.

2.2.8. Ha e bal oldali, f jobb oldali neutrális elem, akkor $e * f = f$ (mert e bal oldali neutrális elem), ugyanakkor $e * f = e$ (mert f jobb oldali neutrális elem). Tehát $e = f$. Vagyis ha van bal oldali, és van jobb oldali neutrális elem is, akkor mindkét fajtából csak egy lehet, és az kétoldali neutrális elem lesz.

2.2.10.

(1) Tegyük fel, hogy v balinverze, és w jobbinverze u-nak. A $*$ asszociativitása miatt $v * (u * w) = (v * u) * w$. De $v * (u * w) = v * e = v$, és $(v * u) * w = e * w = w$. Ezért $v = w$.

(2) $u * v * v^{-1} * u^{-1} = u * e * u^{-1} = e$, és $v^{-1} * u^{-1} * u * v = v^{-1} * e * v = e$.

2.2.11. Az f és g függvényekről akkor mondjuk, hogy egymás inverzei (a hagyományos értelemben) ha mindkettő „visszacsinálja a másik hatását", vagyis ha minden $x \in X$-re $f\big(g(x)\big) = x$ és $g\big(f(x)\big) = x$. A kompozíció nyelvére lefordítva ez azt jelenti, hogy $f \circ g = g \circ f = e$, és pontosan ezt kellett bizonyítani.

Ha f-nek van balinverze, azaz olyan g, melyre $g \circ f = e$, akkor f *injektív* (más néven 1–1-értelmű) függvény, ami azt jelenti, hogy X bármely két különböző x és y elemét f különböző elemekbe viszi. Valóban, ha $f(x) = f(y)$, akkor g-t alkalmazva mindkét oldalra $x = g\big(f(x)\big) = g\big(f(y)\big) = y$ adódik. Megfordítva, minden injektív függvénynek van balinverze. Egy ilyen g balinverzet úgy gyárthatunk, hogy g-t az $f(x)$ elemen x-nek definiáljuk (és ha az $f(x)$ alakú elemek nem merítik ki X-et, akkor a fennmaradó helyeken g tetszőleges lehet). Tehát egy függvény akkor és csak akkor balinvertálható, ha injektív.

Ha f-nek van jobbinverze, azaz olyan g, melyre $f \circ g = e$, akkor f *szürjektív* függvény (másképp fogalmazva az egész X-re képez), ami azt jelenti, hogy X bármely x eleme előáll X egy alkalmas y elemének f-nél vett képeként. Valóban, $y = g(x)$ jó választás, hiszen $x = f\big(g(x)\big) = f(y)$. Megfordítva, minden szürjektív függvénynek van jobbinverze. Egy ilyen g jobbinverzet úgy gyárthatunk, hogy X minden x eleméhez kiválasztunk tetszőlegesen egy olyan $y \in X$-et, amelyre $f(y) = x$, és $g(x)$-nek ezt az y elemet definiáljuk. Tehát egy függvény akkor és csak akkor jobbinvertálható, ha szürjektív.

Ezt a két állítást összetéve látjuk, hogy f akkor és csak akkor invertálható, ha *bijektív*, azaz ha kölcsönösen egyértelmű.

2.2.16. Ha egy H részhalmaz teljesíti a felsorolt tulajdonságokat, akkor maga is csoport G műveletére nézve (hiszen az asszociativitás azonosság, ami öröklődik G-ből H-ra, a többi csoporttulajdonságot pedig felsoroltuk). Megfordítva, ha H maga is csoport a G műveletére nézve, akkor a G műveletének értelmezve kell lennie H-ban is, azaz (1) teljesül. A többi állításhoz elég belátni, hogy G és H neutrális eleme ugyanaz, és egy h-beli elem inverze H-ban kiszámítva ugyanaz lesz, mintha G-ben számítanánk ki.

Legyen a H csoport egységeleme f, a G csoporté e. Jelölje f^{-1} az f elemnek a G csoportbeli inverzét. Ekkor $f*f=f$, mert f egységeleme H-nak. Ezért $(f*f)*f^{-1}=f*f^{-1}=e$. Ugyanakkor $f*(f*f^{-1})=f*e=f$, hiszen e egységeleme G-nek. Az asszociativitás miatt tehát $e=f$. Az, hogy az inverzképzés ugyanaz H-ben, mint G-ben, az inverz egyértelműségéből következik (2.2.10. Feladat), hiszen egy H-beli elem H-beli inverze nyilván inverz G-ben is (mert $e=f$).

Megjegyezzük, hogy (2) helyett elegendő föltenni azt, hogy a H részhalmaz nem üres. Ha ugyanis $h\in H$, akkor ezt a G-beli inverzével megszorozva látjuk, hogy (1) és (3) miatt G egységeleme is H-ban van.

2.2.18. Tegyük fel először, hogy a szereplő m és n kitevők pozitívak. Ekkor a (2), (3), (4) állításokat egyszerű leszámlálással tudjuk bizonyítani. Például $a^m a^n$ és a^{m+n} esetében is nyilván $m+n$ darab a betűt írtunk le egymás mellé, $(a^m)^n$ és a^{mn} esetében pedig mn darabot. A (4) állításban a és b egymással szabadon cserélgethető, és nyilván mindkét oldalon n darab a és n darab b szerepel.

Ezután az (1) állítást is be tudjuk látni pozitív n esetén. Azt kell megmutatni, hogy $a^{-n}a^n=e=a^n a^{-n}$. Ha a inverzét b jelöli, akkor az a^{-n} definíció szerint b^n-nel egyenlő. Tudjuk, hogy $ba=e=ab$, azaz a és b felcserélhetők. Ezért a (4) állítás már bizonyított része szerint $a^{-n}a^n=b^n a^n=(ba)^n=e$, és hasonlóan $a^n a^{-n}=e$.

Ha most m és n nulla, vagy negatív is lehet, akkor esetszétválasztással okoskodunk, a negatív kitevőjű hatvány definícióját használva. Példaként a (2) állítást bizonyítjuk, a többi (hasonló) gondolatmenetet az Olvasóra hagyjuk.

Ha $m=0$, akkor $a^m=e$ és $m+n=n$, tehát az állítás tetszőleges egész n-re teljesül. Ha m negatív, mondjuk $m=-k$, ahol k pozitív egész, akkor jelölje ismét b az a inverzét. Ekkor $a^m=a^{-k}=b^k$. Tehát azt kell megmutatni, hogy $b^k a^n=a^{-k+n}$. Ha $n\geq k$, akkor a bal és a jobb oldalon is $n-k$ darab a betű marad (hiszen $ba=e$). Ha viszont $n<k$, akkor a bal oldalon $k-n$ darab b betű marad, a jobb oldal pedig $a^{-(k-n)}$, ami a negatív kitevőjű hatvány definíciója miatt szintén b^{k-n}.

2.2.20. A disztributivitás (és $0+0=0$) miatt $0r=(0+0)r=0r+0r$. Mindkét oldalhoz $0r$ ellentettjét adva $0=0r$ adódik. Ugyanígy láthatjuk be, hogy $r0=0$ minden r elemre.

Ha u invertálható, azaz $uv=1$, akkor természetesen u nem lehet nulla, mert akkor $uv=1$ is nulla lenne. Ekkor tetszőleges r elemre $r=r1=r0=0$, vagyis a gyűrű a

nullgyűrű, amit kizártunk az egységelemes gyűrűk közül. Végül

$$0 = r0 = r\big(s + (-s)\big) = rs + r(-s)$$

miatt rs ellentettje, ami definíció szerint $-(rs)$, tényleg $r(-s)$-sel egyenlő. Analóg módon igazolható a $(-r)s = -(rs)$ azonosság is.

2.2.24. Ha az R additív csoportjára alkalmazzuk a 2.2.16. Feladatot, akkor az állítás első felét kapjuk. Ha R test, akkor az R multiplikatív csoportjára (aminek elemei most R nem nulla elemei) is alkalmazhatjuk ezt a feladatot, és akkor az állítás másik felét kapjuk.

2.2.26. Ha $ur = us$, akkor $u(r-s) = 0$. Mivel u nem bal oldali nullosztó, innen $r - s = 0$, vagyis $r = s$.

Megjegyezzük, hogy ebben a megoldásban nem csak a disztributivitást használtuk fel, abból ugyanis csak annyi következne, hogy $u(r - s) = ur + u(-s)$. Szükség volt a 2.2.20. Feladatban bizonyított $u(-s) = -(us)$ összefüggésre is.

Megfordítva, tegyük fel, hogy az u elemmel szabad balról egyszerűsíteni. Ha $uv = 0$ lenne, akkor az $uv = u0$ egyenletet u-val balról egyszerűsítve $v = 0$ adódik. Ezért az u nem bal oldali nullosztó. Tehát az állítás megfordítása is igaz.

2.2.28. Ez pontosan ugyanaz a gondolatmenet, mint a 2.2.27. Tétel bizonyítása. Ha r-nek balinverze s, akkor az $ru = 0$ egyenletet balról s-sel megszorozva $0 = sru = 1u = u$ adódik. Ezért r nem lehet bal oldali nullosztó.

2.2.30. Ha u invertálható eleme $\mathbb{Z}_m$-nek, akkor van olyan v, hogy $u *_m v = 1$, vagyis $uv - 1$ osztható m-mel. Így u és m minden közös osztója osztja az 1-et is, vagyis u relatív prím az m-hez.

A megfordításhoz legyenek $u_1, \ldots, u_k$ a $\mathbb{Z}_m$-nek az m-hez relatív prím elemei, és u ezek egyike. Ha $u *_m u_j = u *_m u_k$, akkor $m \mid u(u_j - u_k)$. Mivel azonban m és u relatív prímek, innen $m \mid u_j - u_k$, tehát u_j és u_k ugyanazt a maradékot adja m-mel osztva, vagyis ($\mathbb{Z}_m$ elemei lévén) egyenlőek. Beláttuk tehát, hogy $u *_m u_1, \ldots, u *_m u_k$ páronként különbözők. De nyilván $u *_m u_j$ is relatív prím m-hez, tehát az $u *_m u_1, \ldots, u *_m u_k$ számok ugyanazok, mint $u_1, \ldots, u_k$ (csak esetleg más sorrendben). Speciálisan tehát az 1 is szerepel az $u *_m u_j$ számok között, azaz u invertálható.

Ez a bizonyítás elegáns, de némileg csalásnak tekinthető. Kihasználtuk ugyanis a számelmélet relatív prím számokról szóló elemi eredményeit. Márpedig ezek bizonyítása az euklideszi algoritmuson alapszik, amelyből az elsők között következik az, hogy ha u és m relatív prímek, akkor van olyan x és y egész, hogy $ux + my = 1$. Ha ezt szabad használnunk, akkor az x szám mod m maradéka inverze lesz u-nak, tehát a fenti gondolatmenet fölöslegessé válik.

Annak, hogy a fenti megoldást mégis szerepeltettük, két oka van. Egyrészt a relatív prím számok felhasznált tulajdonságai (sőt a számelmélet alaptétele is) ismerős már középiskolából (bár esetleg bizonyítás nélkül), ismerősebb, mint az előző bekezdésben használt állítás. Másrészt a fenti megoldás ötletét általánosítani lehet majd olyan algebrai állítások bizonyítására, ahol a számelméletet már közvetlenül nem alkalmazhatjuk.

A $\mathbb{Z}_m$ nullosztói azok a nem nulla elemek, amelyek nem relatív prímek m-hez. Valóban, ha $d = (a, m) > 1$, akkor $a *_m (m/d) = 0$, és itt egyik tényező sem nulla (mert $d > 1$ miatt $m/d < m$). Megfordítva, ha $(a, m) = 1$, akkor az előzőek szerint a invertálható, és így nem nullosztó.

2.2.33. A művelet asszociatív, mert $a*(b*c) = a = (a*b)*c$ (sőt, bárhogyan zárójelezünk egy szorzatot, az eredmény mindig a legbaloldali tényező lesz). Nyilván S minden eleme jobb oldali neutrális elem. Ha S egyelemű, akkor az egyetlen eleme kétoldali neutrális elem. Ha azonban S legalább kételemű, akkor egyetlen bal oldali neutrális eleme sincs.

2.2.34. Ha a megadott halmaz egy gyűrűnek része, és a műveletek is „ugyanazok", akkor elegendő a 2.2.24. Feladatban megadott tulajdonságokat ellenőrizni. Ezt nagyon sokszor használjuk majd az alábbiakban.

(1) Ez részteste $\mathbb{C}$-nek. Ennek ellenőrzéséhez először is vegyük észre, hogy az összeadás és a szorzás sem vezet ki a megadott halmazból: ha $z = a + bi$ és $w = c + di$ olyan komplex számok, hogy a, b, c, d racionális, akkor

$$z + w = (a + c) + (b + d)i \quad \text{és} \quad zw = (ac - bd) + (ad + bc)i$$

is az adott halmazban van, hiszen $a + c$, $b + d$, $ac - bd$, $ad + bc$ úgyszintén racionális számok. Nyilván a $0 = 0 + 0i$ és az $1 = 1 + 0i$ is a megadott halmazban van (hiszen 0 és 1 is racionális számok). Ha $z = a + bi$ a halmazban van, akkor ellentettje, $(-a) + (-b)i$ is. Végül ha $a + bi \neq 0$, akkor

$$\frac{1}{a + bi} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \,,$$

és ha a, b racionális akkor nyilván $a/(a^2 + b^2)$ és $-b/(a^2 + b^2)$ is racionális. Tehát testről van szó, és ez persze nullosztómentes is. A nullosztómentesség már abból is következik, hogy a $\mathbb{C}$ nullosztómentes, és annak egy részgyűrűjéről van szó.

(2) Ez az előzőhöz mindenben hasonlít, egyetlen kivétellel: a reciprokképzésre kapott képlet kivezet az egész számok közül. Tehát nullosztómentes gyűrűről van szó, amelyben meg kell határoznunk az invertálható elemeket. Ha $a + bi$ invertálható, akkor van olyan $c + di$ ebben a halmazban, hogy $(a + bi)(c + di) = 1$. Szorozzuk meg ezt az egyenlőséget konjugáltjával. A $z\overline{z} = |z|^2$ összefüggés miatt azt kapjuk, hogy $(a^2 + b^2)(c^2 + d^2) = 1$. De mindkét tényező nemnegatív egész szám, és így szorzatuk csak úgy lehet 1, ha mindkettő értéke 1. Tehát $a^2 + b^2 = 1$, és mivel a^2 és b^2 is nemnegatív, ez csak úgy lehet, ha $a = \pm 1$ és $b = 0$, vagy $a = 0$ és $b = \pm 1$. Ekkor az $a + bi$ komplex számra az $1, -1, i, -i$ értékeket kapjuk. Vagyis csak ezek lehetnek invertálhatók. Ezek tényleg invertálhatók is: 1 és -1 inverze önmaga, az i és a $-i$ pedig egymás inverzei.

(3) Ez is részteste $\mathbb{C}$-nek. A számolás hasonló ahhoz, ahogy az (1)-et oldottuk meg, csak az inverzképzés változik egy kicsit: most a törtet $a - b\sqrt{2}$-vel kell bővíteni:

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}\,.$$

Ellenőriznünk kell, hogy a nevező csak akkor lehet nulla, ha $a+b\sqrt{2}=0$. A nevező $(a+b\sqrt{2})(a-b\sqrt{2})$, és noha $\mathbb{C}$ nullosztómentes, ez lehetne nulla akkor is, amikor $a - b\sqrt{2} = 0$. De ebben az esetben $b = 0$, hiszen különben $\sqrt{2} = a/b$ lenne, márpedig $\sqrt{2}$ irracionális szám. De ha $b = 0$, akkor $a = b\sqrt{2} = 0$, és így $a + b\sqrt{2}$ is nulla. Igazából azt láttuk be, hogy az $a + b\sqrt{2}$ egyértelműen meghatározza az a és b racionális számokat.

(4) Ez nem gyűrű, a szorzás nincs jól definiálva, mert kivezet a halmazból. Tegyük fel ugyanis, hogy

$$\sqrt[3]{2}\sqrt[3]{2} = \sqrt[3]{4} = a + b\sqrt[3]{2}$$

alkalmas a és b racionális számokra. Ezt az egyenletet szorozzuk meg $b + \sqrt[3]{2}$-vel, ekkor kiesik a $b\sqrt[3]{4}$, és a rendezés után

$$2 - ab = \sqrt[3]{2}(a + b^2)$$

adódik. Mivel $\sqrt[3]{2}$ irracionális, innen $a + b^2 = 0 = 2 - ab$, ahonnan $b^3 = -2$, ami egyetlen racionális számra sem teljesül. Egy másik, elegáns megoldást mutatunk majd a 3.5.16. Feladatban.

(5) Ez nyilvánvalóan kommutatív gyűrű, aminek nincs egységeleme, és minden nem nulla eleme kétoldali nullosztó.

(6) Ez kommutatív, egységelemes gyűrű, a nullelem az üres halmaz, az egységelem pedig maga az X. Minden a nullától és az egységelemtől különböző elem nullosztó, és így nem is invertálható. Pontosan akkor kapunk testet, ha az X halmaz egyelemű. Erről a gyűrűről lesz még szó a Boole-algebrákról szóló fejezetben.

Ezeket az állításokat könnyen be lehet látni, ha az összeadás és a szorzás definícióját alkalmazzuk. Mintabizonyításként megmutatjuk a disztributivitást, azaz hogy $(A + B)C = AC + BC$. Két halmaz akkor egyenlő, ha kölcsönösen tartalmazzák egymást. Tegyük fel először, hogy $x \in (A + B)C$. Ez azt jelenti, hogy $x \in C$ (hiszen a szorzás a metszetképzés), és $x \in A+B$, vagyis $x \in A$ de $x \notin B$, vagy fordítva, $x \notin A$ de $x \in B$. Az első esetben $x \in AC$ de $x \notin BC$, és így $x \in AC + BC$. A másik esetben $x \notin AC$ de $x \in BC$, és így ismét $x \in AC + BC$. Ezzel beláttuk, hogy $(A + B)C \subseteq AC + BC$. A másik irányú tartalmazás hasonlóan igazolható.

2.2.35. Könnyű ellenőrizni, hogy R zárt a $\mathbb{Z}_6$-beli összeadásra, szorzásra és ellentettképzésre, tehát részgyűrű. Azt gondolhatnánk, hogy mivel az 1 nincs benne, nem lesz egységelemes. De ez nem így van! Ugyanis a 4 egységelem: $4 *_6 4 = 4$, továbbá $4 *_6 2 = 2$ és

persze $4 *_6 0 = 0$. Sőt, testet kaptunk, hiszen a 4 és a 2 inverze is önmaga. (A 2.4.24. Feladat megoldásában látni fogjuk, hogy nullosztómentes gyűrűben egy részgyűrű egységeleme csak az eredeti gyűrű egységeleme lehet.)

2.2.36. Az (1) – (4) állításokat a 2.2.18. Gyakorlatban már beláttuk (csak a művelet jele ott szorzás volt; a (4) állításban persze fel kell használni, hogy egy gyűrűben az összeadás kommutatív). Így csak az (5) állítást kell belátni. Ha n pozitív, akkor a disztributivitás miatt az n tagú

$$n(rs) = rs + rs + \ldots + rs$$

összegből balról kiemelhetünk r-et (ekkor $r(ns)$-et kapunk), de jobbról kiemelhetünk s-et is (és ekkor az eredmény $(nr)s$ lesz). Ha $n = 0$, akkor mindhárom kifejezés értéke nulla a 2.2.20. Feladat miatt. Végül ha n negatív, akkor az $m = -n$ pozitív egészre már tudjuk, hogy $m(rs) = (mr)s = r(ms)$. Az (1) állítás, és ismét a 2.2.20. Feladat segítségével az egyenlőség $n = -m$-re is adódik.

2.2.37. A 2.1.10. Gyakorlat szerint $(a+b)^n$ olyan összeg, amelynek tagjai az a és b néhány (összesen n) példányának szorzatai, vagyis $a^{n-j}b^j$ alakúak. Ez a szorzat annyiféleképpen jöhet létre, ahányféleképpen az n darab $(a + b)$ „zárójelből" ki lehet választani azt a j darabot, amelyből b-t választunk (és akkor a többi $n - j$ zárójelből a-t választunk). A A.2.2. Tétel szerint ez $\binom{n}{k}$-féleképpen történhet meg.

A bizonyítás ugyanez tetszőleges kommutatív gyűrű fölött. Ebben az esetben a binomiális együtthatókkal való szorzás azt jelenti, mint bármely egész számmal való szorzás: az elemet ennyi példányban össze kell adni (lásd a 2.2.17. Definíció utáni megjegyzéseket).

2.2.38. A $(\sqrt{2} - 1)^n(\sqrt{2} + 1)^n = 1$ összefüggésből látszik, hogy $\sqrt{2} + 1$ mindegyik hatványa invertálható. Ez végtelen sok különböző szám, hiszen $\sqrt{2} + 1 > 1$.

2.2.39. Mivel $\mathbb{Z}_3$ és $\mathbb{Z}_5$ is test, a komplex számoknál látottakhoz hasonlóan világos, hogy ha $a^2 + b^2 \neq 0$, akkor $a + bi$ invertálható. A $\mathbb{Z}_3$ mindegyik elemének a négyzete 0 vagy 1, és így $a^2 + b^2 = 0$ csak úgy lehet, ha $a = b = 0$. Ezért $\mathbb{Z}_3$-at i-vel kibővítve testet kapunk (amely kilenc elemű). Ugyanakkor $2^2 + 1^2 = 5$, vagyis ha $\mathbb{Z}_5$-ből indulunk ki, akkor $(2 + i)(2 - i) = 0$. Tehát a nullosztómentesség nem teljesül, és így nem kapunk testet.

2.2.40.

(1) Igen, mert $\varphi(x + y) = 2^{x+y} = 2^x 2^y = \varphi(x)\varphi(y)$.
(2) Igen, mert komplex számok szorzásakor a szögek összeadódnak: $\varphi(x + y) = \cos(x + y) + i \sin(x + y) = (\cos x + i \sin x)(\cos y + i \sin y) = \varphi(x)\varphi(y)$.
(3) Nem, például $|-1 + 1| \neq |-1| + |1|$.
(4) Igen, $\varphi(x + y) = 60 *_{100} (x + y) = 60 *_{100} x + 60 *_{100} y = \varphi(x) + \varphi(y)$, mert a $\mathbb{Z}_{100}$ gyűrűben igaz a disztributivitás. (Mindegyik $+$ jel igazából $+_{100}$, csak az olvashatóság kedvéért lehagytuk ezeket az indexeket.)

(5) Vigyázzunk, ez formailag másik kérdés, mint az előző, mert a $60x$ úgy van definiálva, hogy az x-et összeadjuk önmagával 60 példányban. Ez a leképezés is művelettartó, mert igazából $60x = 60 *_{100} x$ teljesül. Ugyanis a $\mathbb{Z}_{100}$ gyűrűben igaz a disztributivitás, és ezért

$$60x = x + x + \ldots + x = (1 + 1 + \ldots + 1) *_{100} x = 60 *_{100} x\,.$$

Érdemes azonban meggondolni, hogy tetszőleges gyűrűben a $\varphi(x) = nx$ leképezés minden n egészre tartja az összeadást (a 2.2.18. Gyakorlat miatt).

2.2.41. Legyen a G_1 csoport egységeleme e_1, a G_2 csoport egységeleme e_2. Ekkor $e_1^2 = e_1$, és φ szorzattartása miatt

$$\varphi(e_1) = \varphi(e_1^2) = \varphi(e_1)^2\,.$$

Mindkét oldalt $\varphi(e_1)$ inverzével megszorozva (magyarán $\varphi(e_1)$-gyel egyszerűsítve) azt kapjuk, hogy $e_1 = \varphi(e_1)$.

Ha ezután $g \in G_1$ inverze h, akkor $gh = e_1$-re φ-t alkalmazva

$$\varphi(g)\varphi(h) = \varphi(gh) = \varphi(e_1) = e_2\,.$$

Ezért $\varphi(h)$ (a g inverzének a képe) tényleg g képének, azaz $\varphi(g)$-nek az inverze lesz. (Igazából balinverzre láttuk be az állítást. Ugyanígy beláthatjuk jobbinverzre, és ezáltal kétoldali inverzre is, vagy felhasználhatjuk, hogy csoportban a balinverz a 2.2.10. Feladat miatt kétoldali inverz is mindig.)

2.2.42. Bár a feladat szempontjából ez nem lényeges, a 2.2.34. Gyakorlat szerint itt tényleg két testről van szó. Legyen φ kölcsönösen egyértelmű művelettartó leképezés az első testből a másodikba. Az előző 2.2.41. Feladatot az additív csoportra alkalmazva azt kapjuk, hogy $\varphi(0) = 0$. Mivel φ kölcsönösen egyértelmű, ebből következik, hogy a nem nulla elemek halmazát a nem nulla elemek halmazára képzi, és így használhatjuk ezt a feladatot még egyszer, most a multiplikatív csoportra. Az eredmény az, hogy $\varphi(1) = 1$. Ismét az előző feladat szerint φ az ellentettképzést is tartja, és így $\varphi(-1) = -1$ is teljesül. Ezután alkalmazzuk φ-t az $i^2 = -1$ összefüggésre. Azt kapjuk, hogy

$$-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2\,.$$

Tehát az $u = \varphi(i)$ négyzete -1. De ilyen u nincs az $a + b\sqrt{2}$ alakú számok között, hiszen ezek valósak.

2.2.43. Az $(a_1 + \ldots + a_k) + (a_{k+1} + \ldots + a_n) = a_1 + \ldots + a_n$ képletet nyilván elfogadjuk. Ha $k = n-1$, akkor az $(a_1 + \ldots + a_{n-1}) + x = a_1 + \ldots + a_n$ összefüggésből $x = a_n$, vagyis az egytagú a_n összeget úgy érdemes értelmezni, hogy az egyetlen tagjával, a_n-nel egyenlő. Ha viszont $k = 0$, akkor az $(a_1 + \ldots + a_n) + x = a_1 + \ldots + a_n$ összefüggést kapjuk, ahol x most az üres összeg (egyáltalán nincs tagja). De ebből az egyenletből világos, hogy $x = 0$, vagyis az üres összeget nullának érdemes definiálni. Ha ugyanezt összeg helyett szorzással írjuk föl, akkor az derül ki, hogy az üres szorzat értékét 1-nek érdemes venni. (Ennek speciális esete az $a^0 = 1$ megállapodás.)

Az üres összeg és szorzat fogalma első ránézésre erőltetettnek tűnhet. Ugyanígy érezhettek az emberek akkor is, amikor először fogadták el a nullát számnak, majd később az üres halmazt halmaznak. Időről időre látni fogjuk, hogy az üres összeg és szorzat fogalma is rengeteg felesleges esetszétválasztást, extra megjegyzést fog megspórolni.

2.3. A polinomok alaptulajdonságai.

2.3.4. Legyen

$$f(x)=\sum_{i=0}^{n} a_i x_i\,, \quad g(x)=\sum_{i=0}^{m} b_i x_i\,, \quad h(x)=\sum_{i=0}^{\ell} c_i x_i\,.$$

Az összeadás és a szorzás szabályai szerint x^k együtthatója $f(g+h)$-ban

$$\sum_{i+j=k} a_i(b_j+c_j)$$

$fg+fh$-ban pedig

$$\sum_{i+j=k} a_i b_j + a_i c_j\,.$$

Láthatjuk, hogy ez a két összeg egyenlő.

2.3.5.

(1) Nem alkotnak részgyűrűt, az összeadás kivezet, például $x^{20}+x$ és $-x^{20}$ is páros fokú, de az összegük x, ami páratlan fokú. (Azok a polinomok, amelyben minden nem nulla együtthatójú tag kitevője páros, részgyűrűt alkotnak, de az egy másik feladat.)

(2) Nem alkotnak részgyűrűt, az (1)-beli példa szerint az összeadás innen is kivezet.

2.3.6. Nem alkotnak gyűrűt. Az egyetlen tulajdonság, ami nem teljesül, a bal oldali disztributivitás: $f\circ(g+h)=f\circ g+f\circ h$. Például ha $f(x)=x^2$, $g(x)=x$ és $h(x)=1$, akkor x^2-be $x+1$-et helyettesítve $(x+1)^2$ adódik, ami nem egyenlő x^2+1^2-nel.

2.3.7. Jelölje $\overline{a}$ az $a\in\mathbb{Z}$ maradékát mod m. Legyen $f(x)=a_0+a_1x+\ldots+a_nx^n$ és $h(x)=c_0+c_1x+\ldots+c_\ell x^\ell$. Ekkor $\overline{f}\;\overline{h}$-ban az x^k-os tag együtthatója

$$\overline{a_0}\;\overline{c_k}+\ldots+\overline{a_k}\;\overline{c_0}\,,$$

az $\overline{fh}$-ban az x^k-os tag együtthatója pedig

$$\overline{a_0c_k+\ldots+a_kc_0}\,.$$

Ez a két együttható tényleg egyenlő, hiszen a felülvonás leképezés összeg- és szorzattartó (1.1.6. Állítás). Beláttuk tehát, hogy $\overline{f}\;\overline{h}=\overline{fh}$. Hasonlóan, de egyszerűbb számolással igazolható, hogy $\overline{f}+\overline{h}=\overline{f+h}$.

2.3.8. Ez az előző gyakorlat általánosítása, és a megoldás is ugyanúgy megy, csak $\overline{c}$ helyett mindenütt $\varphi(c)$-t kell írni.

2.4. Polinomfüggvények és gyökök.

2.4.2. Legyen $f(x) = a_0 + a_1x + \ldots + a_nx^n$ és $g(x) = c_0 + c_1x + \ldots + c_nx^n$. Ekkor

$$(f+g)^*(b) = (a_0 + c_0) + (a_1 + c_1)b + \ldots + (a_n + c_n)b^n\,,$$

és

$$f^*(b) + g^*(b) = (a_0 + a_1b + \ldots + a_nb^n) + (c_0 + c_1b + \ldots + c_nb^n)\,.$$

Ez a két összeg nyilván egyenlő. Hasonlóan, bár picit bonyolultabb számolással igazolható az $(fg)^*(b) = f^*(b)g^*(b)$ összefüggés is.

2.4.4. Jelölje B a Horner-elrendezés utolsó cellájában szereplő $c_0b + a_0$ értéket (amiről meg kell mutatnunk, hogy $f^*(b)$-vel egyenlő). Beszorzással, és x szerint rendezve:

$$(x-b)(c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_jx^j + \ldots + c_1x + c_0) + B =$$
$$= c_{n-1}x^n + \ldots + (c_{j-1} - bc_j)x^j + \ldots + (c_0 - bc_1)x - bc_0 + B\,.$$

A Horner-elrendezés táblázatából tudjuk, hogy $c_{n-1} = a_n$, továbbá $c_{j-1} - bc_j = a_j$ (ha $1 \le j < n$), és végül $-bc_0 + B = a_0$. Tehát tényleg az eredeti f polinomot kapjuk. A b-t behelyettesítve pedig $f^*(b) = B$ adódik (hiszen $x - b$ nullává válik).

2.4.8. Mivel egy gyöktényező főegyütthatója 1, ami soha nem lehet nullosztó, gyöktényezővel való szorzáskor a fokszám mindig eggyel nő. Tehát az igaz nullosztómentesség nélkül is, hogy ha $f(x) = (x-b_1)\ldots(x-b_k)q(x)$, akkor $k \le \mathrm{gr}(f)$. Csak az nem biztos, hogy minden gyök szerepel az itt felsoroltak között (amire mutattunk is példát).

2.4.9. Ha f a c értéket végtelen sok helyen felveszi, akkor ezek mind gyökei az $f - c$ polinomnak, és így $f - c$ a 2.4.7. Tétel miatt azonosan nulla. Ezért f a konstans c polinom.

2.4.12.

(1) Ezekből (egyszerre) kiemelhető az $n-1$ darab $(x-a_i)$ gyöktényező mindegyike, ahol $i \ne j$. Mivel a polinom $n-1$-edfokú, már csak egy konstans szorzó maradhat.

(2) Az a_j-t behelyettesítve e konstans értékét meghatározhatjuk. Az eredmény:

$$f_j(x) = \frac{(x-a_1)\ldots(x-a_{j-1})(x-a_{j+1})\ldots(x-a_n)}{(a_j-a_1)\ldots(a_j-a_{j-1})(a_j-a_{j+1})\ldots(a_j-a_n)}\,.$$

Ezek a *Lagrange-féle alappolinomok*.

(3) $f(x) = b_1f_1(x) + \ldots + b_nf_n(x)$ jó lesz. Ha ugyanis a_j-t behelyettesítjük, akkor egy kivétellel az összeg mindegyik tagja nullává válik (hiszen $f_i(a_j) = 0$ ha $i \ne j$), a megmaradó tag pedig $b_jf_j(a_j) = b_j$ lesz, hiszen $f_j(a_j) = 1$.

2.4.13.

(1) Mivel $(f+g)(a_j) = b_j = f(a_j)$, ezért a g polinomnak gyöke az $a_1, a_2, \ldots a_{n-1}$. De g foka $n-1$, ezért

$$g(x) = c(x-a_1)\ldots(x-a_{n-1})$$

alkalmas c konstansra.

(2) A b_n-et behelyettesítve

$$c = \frac{b_n - f(a_n)}{(a_n-a_1)\ldots(a_n-a_{n-1})}$$

adódik.

2.4.14. A Horner-elrendezés táblázata a következő lesz:

	1	0	−4	1	−1	0	4
2	1	2	0	1	1	2	$\boxed{8}$

Ezért a 2 nem gyöke f-nek, és $f(x) = (x-2)(x^5+2x^4+x^2+x+2)+8$.

2.4.15. Ha $f(x) = a_n x^n + \ldots + a_0$, akkor

$$f(x) - f^*(b) = \sum_{j=0}^{n} a_j(x^j - b^j)\,.$$

A zárójelben álló kifejezések mindegyikéből kiemelhető $(x-b)$, és ami marad, az x-nek egy polinomja lesz.

2.4.16. Az Útmutatóban leírt megoldást folytatva $q_0(x) = (x-b)q_1(x) + b_1$, ahonnan az $f(x) = (x-b)q_0(x) + b_0$ egyenlőségbe visszahelyettesítve

$$f(x) = b_0 + b_1(x-b) + q_1(x)(x-b)^2$$

adódik. Az eljárást folytassuk tovább. A kapott q_i polinomok foka minden lépésben eggyel csökken, ezért $q_{n-1}(x) = b_n$ már konstans polinom lesz, ahol n az f foka. Ekkor

$$f(x) = b_0 + b_1(x-b) + b_2(x-b)^2 + \ldots + b_n(x-b)^n\,.$$

Az egyértelműség bizonyításához az Útmutatóban írtak alapján tegyük föl, hogy

$$d_0 + d_1(x-b) + d_2(x-b)^2 + \ldots + d_n(x-b)^n$$

a nullapolinom, ahol nem mindegyik d_i nulla, és n a legkisebb olyan egész, amelyre ez lehetséges. Az $x = b$ helyettesítésel $d_0 = 0$ adódik. Mivel $T[x]$ nullosztómentes, és $x-b$ nem a nullapolinom, azt kapjuk, hogy

$$d_1 + d_2(x-b) + \ldots + d_n(x-b)^{n-1} = 0\,.$$

Az n minimalitása miatt itt már mindegyik együttható nulla.

2.4.17. Akkor és csak akkor, ha m összetett szám. Ha ugyanis $m = ab$, ahol $1 < a, b < m$, akkor az ax elsőfokú polinomnak (legalább) két gyöke van: a 0 és a b. Ha viszont m prímszám, akkor $\mathbb{Z}_m$ nullosztómentes (2.2.29. Állítás), és így a 2.4.7. Tétel miatt minden polinomnak legfeljebb annyi gyöke van, mint a foka.

2.4.18. Az eredmény $(1/2)x^3 - (3/2)x^2 + x + 3$ (például Newton-interpolációval).

2.4.19. Legyen f egy n-edfokú polinom, amely minden racionális helyen racionális értéket vesz föl. Válasszunk ki $n + 1$ racionális helyet bárhogy, például az $1, 2, \ldots, n + 1$ helyeket, és készítsük el azt a g interpolációs polinomot, amely ezeken a helyeken ugyanazt az értéket veszi föl, mint az f. Persze a g racionális együtthatós (ez például a Lagrange-interpolációnál használt képletekből látszik, de elegánsabban azt mondhatnánk, hogy mivel $\mathbb{Q}$ test, ezért $\mathbb{Q}$ fölött elvégezhető az interpoláció, és az eredmény persze $\mathbb{Q}[x]$-beli). Ekkor f és g két legfeljebb n-edfokú polinom, amelyek $n + 1$ helyen megegyeznek. A polinomok azonossági tételét (2.4.10. Következmény) a komplex test fölött alkalmazva azt kapjuk, hogy $f = g$, tehát g is racionális együtthatós.

A második állítás nem igaz, például $x(x + 1)/2$ nem egész együtthatós, de egész helyen egész értéket vesz föl, hiszen két szomszédos egész szám közül az egyik mindig páros. Tetszőleges k-ra van ilyen k-adfokú polinom is, például az

$$\frac{x(x-1)\ldots(x-k+1)}{k!}$$

„binomiális együttható".

2.4.20. Mivel $f(14) = 440$, az f-et kereshetjük $(x - 14)g(x) + 440$ alakban, ahol g is egész együtthatós polinom. A másik két feltételt behelyettesítve átrendezéssel $g(10) = 10$ és $g(18) = 20$ adódik. Innen akár az $a - b \mid g(a) - g(b)$ összefüggést felhasználva (2.4.15. Gyakorlat), akár g-t $(x - 10)h(x) + 10$ alakban felírva a $8 \mid 10$ ellentmondás adódik. Ilyen polinom tehát nem létezik. Megjegyezzük, hogy a következő feladat állítása segítségével is megmutatható, hogy nincs ilyen polinom.

2.4.21. Legyenek a_i és b_i egészek, ahol $1 \leq i \leq n$, és g az a legfeljebb $n - 1$-ed fokú interpolációs polinom, melyre $g(a_i) = b_i$ minden i-re. Tegyük fel, hogy van olyan f egész együtthatós polinom, amelyre $f(a_i) = b_i$ minden i-re. Meg kell mutatni, hogy g is egész együtthatós.

Osszuk el f-et maradékosan az $(x - a_1)\ldots(x - a_n)$ polinommal:

$$f(x) = (x - a_1)\ldots(x - a_n)q(x) + r(x)\,.$$

Mivel $(x - a_1)\ldots(x - a_n)$ főegyütthatója 1, a maradékos osztás nem vezet ki $\mathbb{Z}[x]$-ből, vagyis q és r is egész együtthatós. A fenti egyenletből $r(a_i) = b_i$ minden i-re, azaz r is interpolál az a_i helyeken. Mivel r foka legfeljebb $n - 1$, az interpoláció egyértelműsége miatt $r = g$. Tehát g tényleg egész együtthatós.

2.4.22. Legyen $r \neq 0$ eleme R-nek. Ha $f \in R[x]$ olyan, hogy $f(0) = 0$ és $f(r) = 1$, akkor az $f(x)$-ből az $x - 0$ gyöktényezőt kiemelve $f(x) = xg(x)$ adódik. Ide r-et helyettesítve azt kapjuk, hogy $1 = rg(r)$, azaz $g(r)$ inverze r-nek.

2.4.23. Az, hogy az $R \to R$ függvények kommutatív gyűrűt alkotnak a pontonkénti összeadásra és a szorzásra, könnyen ellenőrizhető (és később lesz róla szó, amikor a gyűrűk direkt szorzatát tárgyaljuk). Az azonosságok azért teljesülnek, mert minden egyes r behelyettesítésekor teljesülnek a kapott értékekre. Például az $f(g+h) = fg + fh$ disztributív szabály igazolásához azt kell megmutatni, hogy e két függvény minden $r \in R$ helyen megegyezik. A pontonkénti összeadás és szorzás definíciója miatt ez azt jelenti, hogy

$$f(r)\big(g(r) + h(r)\big) = f(r)g(r) + f(r)h(r)\,,$$

ami valóban teljesül, hiszen R gyűrű. A nullelem a konstans nulla függvény, az ellentett pedig a *pontonkénti ellentett*:

$$(-f)(r) = -f(r)\,.$$

Az egységelem a konstans 1 függvény lesz.

Az R azért nem nullosztómentes, mert ha a (legalább kételemű) alaphalmazát két részre osztjuk, az f függvény az első részen nulla, és a másikon nem, a g függvény pedig a másik részen nulla, és az elsőn nem, akkor fg már azonosan nulla lesz. Az (1) állítás tehát igaz.

A 2.4.2. Gyakorlat szerint

$$(f+g)^*(b) = f^*(b) + g^*(b) \qquad \text{és} \qquad (fg)^*(b) = f^*(b)g^*(b)\,,$$

ami maga a (3) állítás. De ez azt is jelenti, hogy

$$(f+g)^* = f^* + g^* \qquad \text{és} \qquad (fg)^* = f^*g^*\,,$$

ahol a két egyenlőség bal oldalán polinom-műveletek, a jobb oldalukon pontonkénti műveletek állnak. Így az $f \mapsto f^*$ leképezés összeg- és szorzattartó (ami a (4) állítás). Innen az is látszik, hogy a polinomfüggvények halmaza zárt a pontonkénti műveletekre. Nyilván a nullapolinomhoz az azonosan nulla függvény, a konstans 1 polinomhoz pedig az azonosan 1 függvény tartozik, és a $(-f)^*$ az f^* pontonkénti ellentettje. Így a polinomfüggvények részgyűrűt alkotnak az $R \to R$ függvények gyűrűjében, amely az egységelemet is tartalmazza, és ezzel a (2) állítást is beláttuk.

2.4.24. Álljon S azokból a függvényekből, melyeknek a 2 szám gyöke. Ez a 2.2.24. Feladatbeli tulajdonságok (azaz az összeadásra, szorzásra és ellentettképzésre való zártság) ellenőrzésével könnyen láthatóan részgyűrű. E részgyűrű egységeleme az a függvény, amely a 2 helyen nullát, a többi helyen 1-et vesz föl. Ezzel szemben R egységeleme a konstans 1 függvény.

Legyen most R nullosztómentes gyűrű, melynek egységelemét e jelöli, és S egységelemes részgyűrű, melynek egységeleme legyen f. Mivel az egységelemes gyűrűk közül kizártuk a nullgyűrűt, $f \neq 0$. Nyilván $ff = f = fe$ (az első egyenlőség azért igaz, mert f egységelem S-ben, a második pedig azért, mert e egységelem R-ben). Az egyszerűsítési szabály (2.2.26. Gyakorlat) miatt innen $e = f$.

2.5. A gyöktényezős alak.

2.5.1. Mivel szorzáskor a fokszámok összeadódnak, egy konstans foka nulla, egy gyöktényező foka pedig 1, ezért a gyöktényezők száma tényleg a polinom foka lesz (ezt a gondolatmenetet már használtuk a 2.4.7. Tételben, lásd a 2.4.8. Gyakorlat megoldását is).

A c konstans kiszámításához használjuk föl, hogy polinomok szorzatának főtagja a főtagok szorzata. Így a gyöktényezős alakot beszorozva a főtag $c \cdot x \cdot x \cdot \ldots \cdot x = cx^n$ lesz. Vagyis c tényleg a főegyüttható.

2.5.2. Legyen $r \neq 0$ eleme R-nek. Ekkor az $rx - 1$ polinom elsőfokú, és ezért van gyöke, ami nyilván r inverze lesz. Tehát minden nem nulla elem invertálható.

2.5.6. Tegyük fel, hogy $(x-b)^k g(x) = (x-b)^m h(x)$, ahol sem $g(b)$, sem $h(b)$ nem nulla. Mivel az $x - b$ nem a nullapolinom, egyszerűsíthetünk vele a 2.2.20. Feladat szerint. Ha $k < m$, akkor tehát $g(b) = (x-b)^{m-k} h(x)$ marad, ami nem lehet, mert g-nek b nem gyöke. Ugyanígy zárható ki a $k > m$ lehetőség is. Tehát $k = m$, azaz k egyértelműen meghatározott.

Ha ezután f-et kanonikus alakban írjuk fel:

$$f(x) = c(x-d_1)^{k_1}(x-d_2)^{k_2} \ldots (x-d_m)^{k_m} ,$$

akkor a d_j tényleg k_j-szoros gyök lesz az új értelemben is, hiszen $(x-d_j)^{k_j}$ kiemelhető, a megmaradó polinomnak pedig a d_j már nem gyöke (a nullosztómentesség miatt).

2.5.7. Az $(x-b_1)(x-b_2)(x-b_3)$ beszorozva és rendezve az

$$x^3 - (b_1+b_2+b_3)x^2 + (b_1b_2+b_1b_3+b_2b_3)x - b_1b_2b_3$$

alakot ölti. Az $(x-b_1)(x-b_2)(x-b_3)(x-b_4)$ beszorzását a 2.1.10. Gyakorlat felhasználásával végezzük el. Mindegyik zárójelből egy tagot kell választanunk, ezeket összeszorozni, és a kapott szorzatokat összeadni. Rögtön rendezünk is x hatványai szerint.

Az x^4 csak úgy keletkezhet, ha mindegyik zárójelből x-et választunk. Egy ilyen tag van, amelynek tehát az együtthatója 1. Az x^3 akkor keletkezik, ha három zárójelből választunk x-et, a negyedikből tehát $-b_j$-t kell választanunk. Ez négyféleképpen lehetséges, és így x^3 együtthatója

$$-(b_1+b_2+b_3+b_4) .$$

Az x^2 úgy keletkezhet, hogy két zárójelből x-et, a másik kettőből $-b_j$-t választunk. Négy zárójelből kettőt hatféleképpen lehet kiválasztani, tehát hat ilyen tag lesz. Az x^2 együtthatója tehát

$$b_1b_2 + b_1b_3 + b_1b_4 + b_2b_3 + b_2b_4 + b_3b_4$$

(az előjel persze $+$, hiszen $(-b_i)(-b_j) = b_ib_j$). Az x úgy keletkezik, hogy három zárójelből választunk $-b_j$-t, tehát x együtthatója

$$-(b_1b_2b_3 + b_1b_2b_4 + b_1b_3b_4 + b_2b_3b_4) .$$

Végül a konstans tag esetében mindegyik zárójelből a $-b_j$-t választjuk, tehát ez $b_1b_2b_3b_4$.

2.5.10. Az $x^4 = 4$ egyenlet gyökei a -4 szám negyedik gyökei. Ezeket már meghatároztuk az 1.5.13 (2) (sőt az 1.2.9.) Gyakorlatban, az eredmény $\pm 1 \pm i$ lett. Mivel $x^4 + 4$ főegyütthatója 1, a gyöktényezős alak a következő:

$$x^4 + 4 = 1 \cdot \big(x - (1+i)\big)\big(x - (1-i)\big)\big(x - (-1+i)\big)\big(x - (-1-i)\big)\,.$$

A beszorzást ügyesen elvégezhetjük, ha felhasználjuk az $(a-b)(a+b) = a^2 - b^2$ azonosságot. Az első két tényező szorzata ugyanis

$$(x - 1 - i)(x - 1 + i) = (x-1)^2 - i^2 = x^2 - 2x + 2\,.$$

Ugyanígy kapjuk, hogy a második két tényező szorzata $x^2 + 2x + 2$. Tehát

$$x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$$

valós (sőt egész) együtthatós polinomok szorzatára való felbontás. (Az, hogy az i kiesett, azon múlt, hogy ügyesen párosítottuk a gyöktényezőket: minden gyököt a konjugáltjával.) Folytassuk most a beszorzást, újra felhasználva az $(a-b)(a+b) = a^2 - b^2$ azonosságot:

$$(x^2 - 2x + 2)(x^2 + 2x + 2) = (x^2 + 2)^2 - (2x)^2 = x^4 + 4\,.$$

Tehát tényleg visszakaptuk az eredeti polinomot.

2.5.11. Az $x - 1$ gyöktényező kiemelése után maradó polinom a Horner-elrendezés alsó sorában található. Erre ismét a Horner-elrendezést kell alkalmaznunk, és ezt addig folytatjuk, amíg az 1 már nem lesz gyök. Ezért a legegyszerűbb egy táblázatot készíteni több sorral:

	1	−1	0	−1	1
1	1	0	0	−1	**0**
1	1	1	1	**0**	
1	1	2	**3**		

$$x^4 - x^3 - x + 1 = (x-1)(x^3 - 1) = (x-1)^2(x^2 + x + 1)\,.$$

Mivel a táblázat utolsó sora szerint $x^2 + x + 1$-nek az 1 már nem gyöke, ezért az eredeti polinomnak az 1 pontosan kétszeres gyöke.

2.5.12. A polinomok azonossági tételének (2.4.10. Következmény) a bizonyítását módosítjuk. Legyen f és g a két polinom. Ekkor $f - g$-ből kiesik a főtag, és ezért ez a különbség legfeljebb $n-1$-edfokú. De legalább n gyöke van, és így csak a nullapolinom lehet.

2.5.13. Emeljük négyzetre a $\sigma_1 = x_1 + \ldots + x_n$ összeget. Ekkor (a 2.1.4. Gyakorlat szerint) egy olyan összeget kapunk, amelynek tagjai az összes lehetséges $x_i x_j$ szorzatok. Ha $i = j$, akkor ez x_i^2, ezek együtt a keresett négyzetösszeget adják. Ha $i \neq j$, akkor viszont $x_i x_j$ és $x_j x_i$ is szerepel, tehát az ilyen tagokból σ_2 kétszeresét kapjuk. Így végülis

$$x_1^2 + \ldots + x_n^2 = \sigma_1^2 - 2\sigma_2 \quad (\text{ha } n \geq 2).$$

Ezt az összefüggést általánosítjuk majd a 2.7.8. Tételben.

2.5.14. Alkalmazzuk a gyökök és együtthatók összefüggését (2.5.9. Következmény). Ha

$$f(x) = 2x^4 + 2x + 3 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0\,,$$

akkor $a_4 = 2$, $a_3 = a_2 = 0$, $a_1 = 2$ és $a_0 = 3$. Ezért

$$\sigma_1 = b_1 + b_2 + b_3 + b_4 = (-1)^1 a_3/a_4 = 0\,,$$
$$\sigma_2 = b_1b_2 + b_1b_3 + b_1b_4 + b_2b_3 + b_2b_4 + b_3b_4 = (-1)^2 a_2/a_4 = 0\,,$$
$$\sigma_3 = b_1b_2b_3 + b_1b_2b_4 + b_1b_3b_4 + b_2b_3b_4 = (-1)^3 a_1/a_4 = -1\,,$$
$$\sigma_4 = b_1b_2b_3b_4 = (-1)^4 a_0/a_4 = 3/2\,.$$

Tehát a gyökök összege nulla, szorzata $3/2$, négyzetösszege az előző 2.5.13. Gyakorlat szerint $\sigma_1^2 - 2\sigma_2 = 0$, végül a gyökök reciprokainak összege

$$\frac{1}{b_1} + \frac{1}{b_2} + \frac{1}{b_3} + \frac{1}{b_4} = \frac{b_1b_2b_3 + b_1b_2b_4 + b_1b_3b_4 + b_2b_3b_4}{b_1b_2b_3b_4} = \frac{\sigma_3}{\sigma_4} = -\frac{2}{3}\,.$$

Megjegyezzük, hogy fel tudunk írni közvetlenül is egy olyan polinomot, aminek a gyökei az f polinom gyökeinek reciprokai, ez

$$g(x) = x^4 f(1/x) = 3x^4 + 2x^3 + 2$$

lesz. A $f(x)$ polinom gyökei reciprokainak összegét tehát a $g(x)$ polinomból mint a gyökök összegét olvashatjuk le.

2.5.15. Az $x^n - 1$ polinom főegyütthatója 1, gyökei pontosan az n-edik egységgyökök, és ezért valóban

$$x^n - 1 = (x - \varepsilon_1)\dots(x - \varepsilon_n)\,.$$

Speciálisan $x^4 - 1 = (x - 1)(x - i)(x + 1)(x + i)$.

Az n-edik egységgyökök összegét, szorzatát és négyzetösszegét már meghatároztuk az 1.5.21. Gyakorlatban, a mostani eszköztárunk azonban gyorsabb megoldást kínál. Az $\varepsilon_1 \dots \varepsilon_n$ szorzatot a gyökök és együtthatók összefüggése (a 2.5.9. Következmény) felhasználásával megkaphatjuk az $x^n - 1$ polinomból. Ennek a polinomnak a konstans tagja $a_0 = -1$, főegyütthatója $a_n = 1$, és így

$$\varepsilon_1 \dots \varepsilon_n = \sigma_n(\varepsilon_1, \dots \varepsilon_n) = (-1)^n a_0/a_n = (-1)^n \cdot (-1)/1 = (-1)^{n+1}$$

(sőt ez a 0 behelyettesítésével is azonnal adódik). Ugyanígy olvasható le az $\varepsilon_1 + \ldots + \varepsilon_n$ összeg az $x^n - 1$ polinomban az x^{n-1}-es tag a_{n-1} együtthatójáról:

$$\varepsilon_1 + \ldots + \varepsilon_n = \sigma_1(\varepsilon_1, \dots \varepsilon_n) = (-1)^1 a_{n-1}/a_n.$$

De $a_{n-1} = 0$ ha $n \geq 2$ (és így az n-edik egységgyökök összege is nulla ilyenkor), ha viszont $n = 1$, akkor ez az együttható -1, és ekkor eredményül $(-1)^1(-1) = 1$ adódik. Végül a gyökök négyzetösszegének kiszámításához a 2.5.13. Gyakorlatot használjuk fel. Az $x^n - 1$ polinomban az x^{n-2}-es tag a_{n-2} együtthatója nulla ha $n > 2$, ezért $\sigma_2(\varepsilon_1, \dots \varepsilon_n)$ is nulla, és így

$$\varepsilon_1^2 + \ldots + \varepsilon_n^2 = \sigma_1^2 - 2\sigma_2 = 0\,.$$

Ha $n = 2$, akkor az eredmény 2 lesz (ami közvetlenül is világos: $1^2 + (-1)^2 = 2$). Végül $n = 1$-re a négyzetösszeg $1^2 = 1$ (ekkor már a σ_2 nincs is értelmezve).

Végül (4) igazolásához helyezzük el a sokszöget úgy, hogy csúcsai pont az n-edik egységgyökök legyenek, és az $\varepsilon_n = 1$-hez tartozó csúcsból húzzuk meg az átlókat. Mivel két pont távolsága a különbségük abszolút értéke (1.4.6. Gyakorlat), és $\varepsilon_n = 1$, ezért az

$$|(1 - \varepsilon_1)| \cdot \ldots \cdot |(1 - \varepsilon_{n-1})|$$

szorzatot kell kiszámítani. Az ismert azonosság (a mértani sor összegképlete) szerint

$$x^n - 1 = (x - 1)(x^{n-1} + \ldots + x + 1)$$

Ezt vessük össze az $x^n - 1$ gyöktényezős alakjával, és egyszerűsítsünk az $x - 1$ polinommal (ezt szabad a 2.2.20. Feladat szerint, hiszen $x - 1$ nem a nullapolinom). Azt kapjuk, hogy

$$(x - \varepsilon_1) \ldots (x - \varepsilon_{n-1}) = x^{n-1} + \ldots + x + 1\,.$$

Az x helyébe 1-et helyettesítve, és mindkét oldal abszolút értékét véve az állítást kapjuk (hiszen az abszolút érték szorzattartó).

Nem osztottunk ebben a bizonyításban nullával? Hiszen $x - 1$-gyel egyszerűsítettünk, és ezután x helyére 1-et írtunk. Több ismert tréfás gondolatmenetben hasonló trükkel ellentmondást lehet kihozni!

A válasz az, hogy az $x - 1$ *polinommal* egyszerűsítettünk, ami nem a nullapolinom, vagyis $\mathbb{C}[x]$ nullosztómentességét használtuk fel. De érdemes máshogy is meggondolni ezt a problémát. A fenti gondolatmenet mintája az, hogy az

$$f(x)(x - 1) = g(x)(x - 1)$$

polinomegyenlőségből következtettünk arra, hogy $f(1) = g(1)$. Ha polinomfüggvényekkel akarunk számolni, akkor annyi biztosan igaz, hogy $f^*(b) = g^*(b)$ minden $b \neq 1$-re. Az f és g polinomokhoz tartozó polinomfüggvények tehát végtelen sok helyen megegyeznek (minden $b \neq 1$ komplex számra), és így az f és g polinomok az azonossági tétel miatt egyenlők (együtthatóról együtthatóra), vagyis már a $b = 1$ helyen is egyenlők.

Ez a gondolatmenet komplex felett működik, de véges testek fölött nem biztos, mert annak a testnek esetleg kevesebb eleme van, mint a szereplő polinomok foka. Az első gondolatmenetünk, amikor $x - 1$-gyel egyszerűsítettünk, ennyiben jobb: az minden test fölött működik.

2.5.16. Nem. A legegyszerűbb ellenpélda az, hogy a $\mathbb{Z}_2$ test fölött az x^k polinomokhoz $k \geq 1$ esetén ugyanaz a polinomfüggvény tartozik: az identikus leképezés. Ezen polinomok esetében a 0 gyök multiplicitása más és más. Tehát a polinomfüggvény nem határozza meg a gyökök multiplicitását (hanem csak a gyökök halmazát).

2.5.17. Legyenek a test elemei $a_1, \ldots, a_n$. Ekkor az

$$(x - a_1) \ldots (x - a_n) + 1$$

nem konstans polinomnak nyilván nincs gyöke ebben a testben. (Az 1 a test egységeleme, de bármelyik nem nulla elemet írhatnánk a helyére.)

2.6. Többhatározatlanú polinomok.

2.6.3. A 2.1.4. Gyakorlat szerint szorozzuk össze az f és g polinomokat, azaz minden tagot minden taggal. Ha f egy i-edfokú P tagját g egy j-edfokú Q tagjával szorozzuk, akkor a PQ eredmény nyilván $i+j$-ed fokú lesz. Azokat a PQ tagokat keressük, amikor $i+j=k$, tehát $j=k-i$. Az i-edfokú P tagok az f_i-ben vannak összegyűjtve, ezeket tehát a g polinom $k-i$-edfokú tagjaival, azaz g_{k-i}-vel kell megszorozni, hogy k-adfokú tagokat kapjunk.

Legyen f foka n, és g foka m. Ekkor az előzőek szerint fg-ben nincsen $m+n$-nél magasabb fokú tag, az $m+n$-edfokú tagok pedig az $f_n g_m$ szorzat tagjai. Azt kell tehát megmutatni, hogy $f_n g_m \neq 0$. Ez azonban világos, hiszen a 2.6.2. Állítás szerint a többhatározatlanú polinomok szorzása nullosztómentes.

2.6.5. Először egy konkrét példát mutatunk.

$$f(x_1,x_2,x_3)=x_1x_2^4-x_1x_2x_3-3x_2^3+x_3^2+2x_1^2+x_1x_2x_3^3\,.$$

Első lépésben x_1 szerint rendezünk:

$$(-3x_2^3+x_3^2)+(x_2^4-x_2x_3+x_2x_3^3)x_1+2x_1^2\,,$$

majd a zárójeleken belül x_2 szerint:

$$(x_3^2-3x_2^3)+\big((-x_3+x_3^3)x_2+1\cdot x_2^4\big)x_1+2x_1^2\,,$$

és a legbelső zárójelben már x_3 szerint is rendezve van a polinom. Beszorozva, de a sorrendet nem megváltoztatva a következőt kapjuk:

$$x_3^2-3x_2^3-x_1x_2x_3+x_1x_2x_3^3+x_1x_2^4+2x_1^2\,.$$

Ez pedig tényleg a lexikografikusan növekvő sorrend.

Az alábbi általános gondolatmenetet a fenti példán érdemes nyomon követni. Tegyük fel, hogy az eredeti polinomnak tagja $P=rx_1^{m_1}\dots x_n^{m_n}$ és $Q=sx_1^{k_1}\dots x_n^{k_n}$, és ezek közül az első a lexikografikusan kisebb, azaz van olyan j index, hogy $m_i=k_i$ minden $i<j$ esetén, de $m_j<k_j$. (Gondoljunk a fenti példában az $x_1x_2x_3^3$ és az $x_1x_2^4$ tagokra.) Amikor a polinomot először x_1 hatványai szerint rendezzük, akkor mind P-ből, mind Q-ból $x_1^{m_1}$-et emelünk ki, és ami megmarad, az az $x_1^{m_1}$ együtthatójában fog szerepelni (a fenti példában ez az együttható $x_2^4-x_2x_3+x_2x_3^3$). Mostantól kezdve már csak ezt az együtthatót vizsgáljuk, és x_2 hatványai szerint rendezzük. Egészen addig „együtt marad” P és Q, amíg el nem érünk az x_j szerinti rendezéshez (a fenti példában $j=2$). Ennél a lépésnél a P-nek megfelelő tag az $x_j^{m_j}$ együtthatójába kerül (jelölje ezt az együtthatót p, a fenti példában $m_j=1$, $p=-x_3+x_3^3$, ebben a P-nek megfelelő tag x_3^3, hiszen $P=x_1x_2x_3^3$), a Q-nak megfelelő tag pedig az $x_j^{k_j}$ együtthatójába (jelölje ezt q, a fenti példában $k_j=4$, $q=1$, hiszen $Q=x_1x_2^4\cdot 1$). Mivel $m_j<k_j$, a p együtthatót írjuk le „előbb”, vagyis a q-hoz képest a „bal oldalra”. Amikor a még magasabb indexű változók szerint rendezünk (a fenti

példában az x_3 szerint), akkor már a p és q együtthatókon belül cserélgetünk csak, tehát P és Q sorrendje már nem változik meg.

2.6.8. A homogén komponensek a következők:

$$p_5 = ix_1x_2x_3x_4^2 - x_1^2x_3^3 + 2x_1^2x_2x_3x_4 - 6x_1^2x_2^2x_4 - x_1^2x_2^2x_3 + \pi x_1^2x_2^3$$
$$p_4 = 3x_1^3x_2$$
$$p_1 = x_4\,,$$

itt p_5 tagjai már lexikografikusan növő sorrendben vannak felírva. A p polinom főtagja $3x_1^3x_2$, ezért p^7 főtagja $3^7x_1^{21}x_2^7$. Viszont p^7 foka $7\cdot5 = 35$, és így a legnagyobb fokú tagok között a lexikografikusan legnagyobb a 2.6.3. Gyakorlat szerint $(\pi x_1^2x_2^3)^7 = \pi^7x_1^{14}x_2^{21}$ lesz.

2.6.9. Legyen $f \in R[x_1, \ldots, x_n]$. Ebbe a polinomba n darab R-beli elemet akarunk behelyettesíteni: x_i helyére b_i-t, ahol $1 \le i \le n$. Ezt röviden úgy fogjuk mondani, hogy az f polinomba a $\mathbf{b} = (b_1, \ldots, b_n)$-et helyettesítjük be, ezeknek az R-beli elem-n-eseknek a halmazát R^n jelöli majd, és b_i-t a $\mathbf{b}$ „pont” i-edik *koordinátájának* nevezzük (az elnevezés és a szemlélet persze a geometriából származik).

Az $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ definíció szerint tetszőleges n-határozatlanú polinom

$$f = g_0 + g_1x_n + \ldots + g_kx_n^k$$

alakban írható, ahol $g_0, \ldots, g_k \in R[x_1, \ldots, x_{n-1}]$. Az $f(b_1, \ldots, b_n)$ értékét tehát n szerinti indukcióval definiálhatjuk, azaz feltehetjük, hogy $n-1$-változós polinomba már be tudunk helyettesíteni. Eszerint az $a_i = g_i(b_1, \ldots, b_{n-1})$ már ismert. Legyen

$$f(\mathbf{b}) = a_0 + a_1b_n + \ldots + a_kb_n^k\,.$$

A gyakorlat többi állítását is a fenti módon, n szerinti indukcióval igazolhatjuk.

2.6.10. Bizonyítsunk n szerinti indukcióval. Egyváltozós polinomokra tudjuk az állítást az azonossági tétel miatt (2.4.10. Következmény). Tegyük föl, hogy $f \in R[x_1, \ldots, x_n]$, és az f-hez tartozó polinomfüggvény azonosan nulla. Legyen

$$f = g_0 + g_1x_n + \ldots + g_mx_n^m\,,$$

ahol $g_i \in R[x_1, \ldots, x_{n-1}]$. Helyettesítsünk az első $n-1$ változóba tetszőleges, de rögzített R-beli elemeket. Ekkor f-ből egy $R[x_n]$-beli polinom keletkezik, amelyhez az azonosan nulla polinomfüggvény tartozik. Az azonossági tétel miatt f minden együtthatója nulla, vagyis mindegyik g_i polinom értéke nulla ennél a rögzített helyettesítésnél. Ez minden helyettesítésre igaz, és ezért a g_i polinomokhoz is az azonosan nulla polinomfüggvény tartozik. Az indukciós feltevés szerint mindegyik g_i a nullapolinom, de akkor f is az.

Az indukció kezdő lépése lehetett volna az $n = 0$ is, hiszen az $n-1$-ről n-re lépés bizonyítása az $n = 1$ esetben is működik. Ehhez mindössze abban kell megállapodni, hogy a nulla változós polinomok a konstansok, vagyis R elemei.

2.6.11. Legyen T test, az előző gyakorlatban bevezetett jelöléseket használjuk. Adottak tehát az $\mathbf{a}^1, \ldots, \mathbf{a}^k \in T^n$ páronként különböző „pontok", és a $b_1, \ldots, b_k$ értékek. Olyan $f \in T[x_1, \ldots, x_n]$ polinomot keresünk, amelyre $f(\mathbf{a}^i) = b_i$, ha $1 \leq i \leq k$.

A Newton-interpolációt modellezzük, azaz k szerinti indukciót alkalmazunk. Egy pont esetében nyilván jól interpolál egy konstans polinom. Tegyük fel, hogy van olyan f, ami már az első $k-1$ helyen a megadott értéket veszi föl. Ha találunk olyan g polinomot, amelyre $g(\mathbf{a}^i) = 0$, ha $1 \leq i \leq k-1$, de $g(\mathbf{a}^k) \neq 0$ akkor az $f + cg$ nyilván megoldása a feladatnak, ahol $c = b_k / g(\mathbf{a}^k)$.

Mivel az alappontok különbözők, az $\mathbf{a}^k = (a_1^k, \ldots, a_n^k)$ és $\mathbf{a}^i = (a_1^i, \ldots, a_n^i)$ sem egyenlő, azaz valamelyik koordinátájuk különbözik. Jelölje a megfelelő indexet $u(i)$, tehát akkor tudjuk, hogy $a^i_{u(i)} \neq a^k_{u(i)}$. Behelyettesítéssel azonnal láthatjuk, hogy

$$g(x_1, \ldots, x_n) = (x_{u(1)} - a^1_{u(1)}) \ldots (x_{u(k-1)} - a^{k-1}_{u(k-1)})$$

megfelel a kívánalmaknak.

Legyen most T egy q elemű véges test, és f egy n-változós függvény T-n. Ekkor az összes T-beli n-esek száma q^n, azaz véges, és így van olyan polinom, ami f-et az összes helyen interpolálja. Tehát f (az ehhez a polinomhoz tartozó) polinomfüggvény.

2.7. Szimmetrikus polinomok.

2.7.4. A σ_k főtagja $x_1 \ldots x_k$ (hiszen azok között az n jegyű „telefonszámok" között, amelyekben k darab 1-es van, és a többi számjegy nulla, nyilván az a legnagyobb, ahol az 1-es számjegyek a legnagyobb helyiértékeket foglalják el). Mivel szorzat főtagja a főtagok szorzata, ezért $r\sigma_1^{k_1}\sigma_2^{k_2} \ldots \sigma_n^{k_n}$ főtagja

$$r(x_1)^{k_1}(x_1x_2)^{k_2} \ldots (x_1 \ldots x_{n-1})^{k_{n-1}}(x_1 \ldots x_{n-1}x_n)^{k_n} = \\ = r x_1^{k_1+\ldots+k_n} x_2^{k_2+\ldots+k_n} \ldots x_{n-1}^{k_{n-1}+k_n} x_n^{k_n}.$$

2.7.5. Tegyük fel, hogy $m_1 \geq m_2 \geq \ldots \geq m_n$ nem igaz, hanem mondjuk $m_j < m_{j+1}$ teljesül valamelyik j indexre. Cseréljük meg a főtagban az x_j és az x_{j+1} változókat. Mivel a polinom szimmetrikus, a kapott

$$r x_1^{m_1} x_2^{m_2} \ldots x_{j-1}^{m_{j-1}} x_j^{m_{j+1}} x_{j+1}^{m_j} x_{j+2}^{m_{j+2}} \ldots x_n^{m_n}$$

is tagja a polinomunknak, de ez lexikografikusan nagyobb a főtagnál, ami ellentmondás. Ezért a főtag kitevői tényleg egyre kisebbednek.

Ha a polinom valamelyik tagjában szerepelne egy $x_j^{k_j}$, ahol $k_j > m_1$, akkor az x_1 és x_j cseréjével olyan tagot kapnánk, amelyben az x_1 kitevője nagyobb m_1-nél. De ez lehetetlen, mert akkor ez a tag lexikografikusan nagyobb lenne a főtagnál.

Ezek szerint valamennyi tagban valamennyi határozatlan kitevője legfeljebb $m_1 + 1$-féle lehet: $0, 1, \ldots, m_1$ valamelyike. Ezeket a kitevőket függetlenül választhatjuk minden tagban, és így a tagok száma tényleg legfeljebb $(m_1 + 1)^n$ lehet.

2.7.6. A $H(\sigma_1, \sigma_2, \sigma_3)$ polinom összes tagját kiszámolni túlságosan nagy munka lenne, ennél gazdaságosabban is eljárhatunk. Amikor H egy-egy tagjába a σ_i-ket behelyettesítjük, akkor a kapott polinomnak csak a főtagját számítsuk ki. Az $y_1y_3^3$-ből a helyettesítés után $\sigma_1\sigma_3^3 = (x_1 + x_2 + x_3)(x_1x_2x_3)^3$ keletkezik. Ennek főtagja

$$P = x_1^{1+3}x_2^3x_3^3\,.$$

Hasonlóképpen az y_2^5-ből $\sigma_2^5 = (x_1x_2 + x_1x_3 + x_2x_3)^5$ lesz, aminek főtagja

$$Q = x_1^5x_2^5\,.$$

A H polinom főtagja $30y_1y_3^3$, az ebből keletkező $30P$ azonban ki fog esni! Valóban, a másik tagból keletkező $-\sigma_2^5$ polinomban a

$$P = x_1^4x_2^3x_3^3 = (x_1x_2)^2(x_1x_3)^2(x_2x_3)$$

pontosan -30-as együtthatóval fog szerepelni.

Ugyanakkor a H második tagjából keletkező $-Q$ nem eshet ki. Valóban, a $-\sigma_2^5$-nek ez a főtagja, tehát a $-\sigma_2^5$ többi tagja nem ejtheti ki. Az első tagból kapott $30\sigma_1\sigma_3^3$ kifejtésekor keletkező tagok szintén nem ejthetik ki $-Q$-t, mert ezek mind lexikografikusan P-nél kisebb vagy egyenlők, viszont $P \prec Q$. (A $H(\sigma_1, \sigma_2, \sigma_3)$ polinom főtagja tehát $-Q$ lesz.)

2.7.9. Az s_i és σ_i polinomokat beírva a kiindulási képlet a következő lesz:

$$(x_1^2 + x_2^2 + x_3^2) - (x_1 + x_2 + x_3)(x_1 + x_2 + x_3) + 2(x_1x_2 + x_1x_3 + x_2x_3) = 0\,.$$

Ha $x_3 = 0$, akkor

$$(x_1^2 + x_2^2) - (x_1 + x_2)(x_1 + x_2) + 2(x_1x_2) = 0$$

adódik, vagyis

$$s_2(x_1, x_2) - \sigma_1(x_1, x_2)s_1(x_1, x_2) + 2\sigma_2(x_1, x_2) = 0\,.$$

Ez pedig a már bizonyított $n = k = 2$ eset.

Általában is nyilvánvaló, hogy $s_i(x_1, \ldots, x_n)$-be x_n helyére nullát írva az eggyel kevesebb változós $s_i(x_1, \ldots, x_{n-1})$ adódik. Mi történik, ha $\sigma_i(x_1, \ldots, x_n)$-be írunk x_n helyére nullát? Tudjuk, hogy $\sigma_i(x_1, \ldots, x_n)$ az összes olyan i-tényezős szorzatok összege, ahol a (csupa különböző) tényezők az $x_1, \ldots, x_n$ változók közül kerülnek ki. Ha $x_n = 0$, akkor eltűnnek azok a szorzatok, ahol x_n is szerepel. A megmaradó polinom így az eggyel kevesebb változós $\sigma_i(x_1, \ldots, x_{n-1})$.

2.7.11. Igaz. Ha ugyanis két változót megcserélünk, akkor egy k-adfokú P tag egy szintén k-adfokú Q tagba fog átmenni. Mivel a polinom szimmetrikus, Q is tagja lesz, és persze ugyanabban a homogén komponensben lesz, mint P. Tehát a k-adfokú homogén komponens is szimmetrikus.

2.7.12. Az $x_1x_2^3x_3$ nem lehet tag, mert akkor a szimmetria miatt tag lenne $x_1^3x_2x_3$ is, ami a főtagnál lexikografikusan nagyobb. Tehát minden kitevő legfeljebb 2 lehet (mint azt a 2.7.5. Gyakorlatban is láttuk). Emiatt hatodfokú tag csak $rx_1^2x_2^2x_3^2$ lehetne, de ez sem szerepelhet, mert ez is lexikografikusan nagyobb lenne a főtagnál. Vagyis minden tag $x_1^{m_1}x_2^{m_2}x_3^{m_3}$ alakú lesz, ahol az m_1, m_2, m_3 kitevők mindegyike legfeljebb 2 (vagyis háromféle), és az egyik legfeljebb 1. A tagok száma így maximum $3 \cdot 3 \cdot 3 - 1 = 26$ lehet (azért 1-et kell levonni, mert $x_1^2x_2^2x_3^2$ az egyetlen, ahol mindegyik kitevő legfeljebb 2, de egyik sem legfeljebb 1). Ilyen polinom létezik is, például adjuk össze 1 együtthatóval a most leírt tulajdonságú 26 tagot.

Az eljárás első lépése az, hogy le kell vonni a $\sigma_1^{2-2}\sigma_2^{2-1}\sigma_3^1 = \sigma_2\sigma_3$ tagot.

2.7.13. Az alaptétel bizonyításának egyértelműségre vonatkozó része alapján először ki kell számolni minden tagban a kitevők összegét, azaz a tagok fokát, és csak a legnagyobb fokú tagokat megtartani. Ezt már megtettük a 2.6.8. Gyakorlat megoldásában, ekkor a p_5 polinomot kapjuk. A második lépésben p_5 minden tagjában az x_2, x_3, x_4 fokait kell összeadni. Ennek legnagyobb értéke 4 lesz, és ezt csak egyetlen tagban, az $ix_1x_2x_3x_4^2$-ben érjük el. Amikor tehát x_i helyére σ_i-t írunk, akkor $i\sigma_1\sigma_2\sigma_3\sigma_4^2$ főtagja (ami a 2.7.4. Gyakorlat szerint $ix_1^5x_2^4x_3^3x_4^2$) biztosan nem fog kiesni.

2.7.14. A polinom főtagja $x_1^2x_2$, tehát első lépésben $\sigma_1^{2-1}\sigma_2^{1-0} = \sigma_1\sigma_2$-t kell levonnunk. Ehhez el kell végezni a 2.1.4. Gyakorlat alapján a $\sigma_1\sigma_2$ szorzást. Az eredmény $x_ix_jx_k$ alakú tagok összege, ahol x_i-t σ_1-ből, x_jx_k-t σ_2-ből választjuk. Így biztosan $j \neq k$. Ha i különbözik j-től is és k-tól is, akkor σ_3 egy tagját kapjuk, de hányszor? Például az $x_1x_2x_3$ tag fellép úgy is, hogy x_1-et választjuk σ_1-ből, és x_2x_3-at σ_2-ből, de felléphet úgy is, hogy σ_1-ből az x_2-t, vagy az x_3-at választjuk. Tehát $x_1x_2x_3$ (és minden ugyanilyen tag) háromszor lép fel. A másik lehetőség az, hogy i megegyezik j vagy k valamelyikével. Most tehát azt kell megszámolni, hogy mondjuk az $x_1x_2^2$ hányféleképpen kapható meg. Látjuk, hogy ez csakis $x_2(x_1x_2)$ alakban keletkezhet (hiszen a σ_2-beli tagok két indexe mindenképpen különböző). Odáig jutottunk tehát, hogy

$$\sigma_1\sigma_2 = 3\sigma_3 + f(x_1, \ldots, x_n)\,.$$

Így $f(x_1, \ldots, x_n) = \sigma_1\sigma_2 - 3\sigma_3$.

Megjegyezzük, hogy a kapott képlet $n = 2$ esetén is érvényes, ha ekkor σ_3 értékét nullának tekintjük. Ha $n = 1$, akkor a feladatban üres összeg szerepel, de a képletünk ilyenkor is helyes (ekkor σ_2 is nulla).

2.7.15. A reciprokösszeg σ_{n-1}/σ_n (ezt közös nevezőre hozással már a 2.5.14. Gyakorlatban láttuk az $n = 4$ speciális esetben). A gyökök és együtthatók összefüggése (a 2.5.9. Következmény) miatt az $x^n + x + 1$ polinom esetében $\sigma_n = (-1)^n$ és $\sigma_{n-1} = (-1)^{n-1}$, vagyis a gyökök reciprokösszege -1.

A köbösszeg meghatározására két megoldást is mutatunk. Az első megoldásban közvetlenül alkalmazzuk az alaptétel bizonyításában tanult algoritmust. Mivel a köbösszeg

főtagja x^3, első lépésben a σ_1^3-t kell levonni belőle. Emeljük tehát köbre az $(x_1 + \ldots + x_n)$ összeget. Ezt a 2.1.10. Gyakorlat szerint úgy tehetjük meg, hogy az $x_1, \ldots, x_n$ közül kiválasztunk tetszőleges módon hármat, ezeket összeszorozzuk, és a kapott szorzatokat összeadjuk. Ilyenkor háromféle szorzat keletkezik. Az x_i^3 csak egyszer, az $x_i^2 x_j$ (ahol $i \neq j$) háromszor (úgy, mint $x_i x_i x_j$, $x_i x_j x_i$, $x_j x_i x_i$), végük az $x_i x_j x_k$ (ahol az i, j, k páronként különböző) hatszor (az indexeknek ugyanis hatféle lehetséges sorrendje van). De az $x_i^2 x_j$ alakú tagok összegét meghatároztuk az előző feladatban. Ennek eredményét felhasználva

$$\sigma_1^3 = s_3 + 3(\sigma_1\sigma_2 - 3\sigma_3) + 6\sigma_3\,,$$

és így $s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. Itt vigyázni kell az $n = 2$ esettel, amikor a képlet csak abban az értelemben marad helyes, ha ilyenkor σ_3 értékét nullának tekintjük. Az $x^n + x + 1$ polinomból ennek alapján leolvasható, hogy a gyökök köbeinek összege $n = 2$-re 2, $n = 3$-ra és 4-re -3, $n \geq 5$-re 0.

A második megoldásban a Newton-Girard formulákat (2.7.8. Tétel) alkalmazzuk:

$$s_3 - \sigma_1 s_2 + \sigma_2 s_1 - 3\sigma_3 = 0\,.$$

Tudjuk, hogy $s_1 = \sigma_1$, továbbá akár a Newton-Girard formulákból, akár a 2.5.13. Gyakorlatból, hogy $s_2 = \sigma_1^2 - 2\sigma_2$. Ezeket behelyettesítve s_3-ra az imént már kiszámított eredmény adódik. A köbösszeget még egy harmadik módon is meghatározzuk majd a 2.7.17. Feladat megoldásában.

2.7.16. Az első keresett polinom nyilván az

$$(x - a^2)(x - b^2)(x - c^2) = x^3 - (a^2 + b^2 + c^2)x^2 + (a^2b^2 + a^2c^2 + b^2c^2)x - a^2b^2c^2$$

lesz. Az $x^3 + 3x + 1$ polinomból a gyökök és együtthatók összefüggése alapján leolvashatjuk, hogy $a + b + c = 0$, $ab + ac + bc = 3$, és $abc = -1$. Ezért nyilván $a^2b^2c^2 = (abc)^2 = 1$, és a 2.5.13. Gyakorlat alapján $a^2 + b^2 + c^2 = 0^2 - 2 \cdot 3 = -6$. Az $a^2b^2 + a^2c^2 + b^2c^2$ meghatározásához ismét az alaptétel algoritmusát használjuk fel. A főtag a^2b^2, ezért első lépésben $\sigma_2^2 = (ab + ac + bc)^2$-t kell levonni. De a négyzetösszeget ki tudjuk számítani:

$$(ab + ac + bc)^2 = a^2b^2 + a^2c^2 + b^2c^2 - 2(abac + abbc + acbc)\,,$$

és az utolsó tag nyilván $-2abc(a + b + c) = 0$. A végeredmény tehát $x^3 + 6x^2 + 9x - 1$.

A másik egyenlet esetében is okoskodhatnánk hasonlóan, de a számolás nagyon bonyolult lenne. Vegyük ehelyett észre, hogy $a + b + c = 0$ miatt $a + b = -c$, $b + c = -a$, $c + a = -b$, és ezért a

$$g(x) = (x + a)(x + b)(x + c)$$

polinomot kell csak meghatároznunk. De tudjuk, hogy

$$(x - a)(x - b)(x - c) = x^3 + 3x + 1\,.$$

Ide x helyébe $-x$-et helyettesítve, és $(-1)^3$-nel szorozva $g(x) = x^3 + 3x - 1$ adódik.

2.7.17. A 2.6.3. Gyakorlat szerint homogén polinomok szorzata is homogén, és szorzáskor a fokok összeadódnak. Ezért $\sigma_1^{k_1} \dots \sigma_n^{k_n}$ is homogén, és foka $k_1+2k_2+\dots+nk_n$. Amikor az alaptétel bizonyításában megadott algoritmust végezzük, akkor tehát mindig egy homogén polinomot vonunk ki f-ből, melynek a foka szükségképpen annyi, mint f foka (hiszen a levont polinomot úgy választjuk, hogy a főtag mindig kiessen). Vagyis az eljárásban végig olyan tagokat vonunk le, melyekre $k_1 + 2k_2 + \dots + nk_n = k$, és így f tényleg felírható ilyen tagok összegeként. Ha f főtagja $x_1^{m_1} \dots x_n^{m_n}$, akkor végig minden változó kitevője legfeljebb $m_1 \le m$ lesz. A 2.7.4. Gyakorlat szerint $\sigma_1^{k_1} \dots \sigma_n^{k_n}$-ben x_1 kitevője $k_1 + k_2 + \dots + k_n$, ezért minden levont tagra fenn kell álljon a $k_1 + k_2 + \dots + k_n \le m$ egyenlőtlenség is.

A most kapott képletek behatárolják, hogy egy adott f felírásakor az F polinomban milyen tagok szerepelhetnek egyáltalán (persze f homogén komponenseivel külön-külön kell elbánni). Illusztrációként ezzel a módszerrel is meghatározzuk az s_3 köbösszeg felírását az elemi szimmetrikus polinomokkal.

Most tehát $m = 3 = k$, és így $k_1 + 2k_2 + \dots + nk_n = 3$ (továbbá $k_1 + \dots + k_n \le 3$, de ez kevesebbet mond ebben az esetben, mint az előző feltétel). Mivel mindegyik k_i egész szám, látjuk, hogy $k_4 = \dots = k_n = 0$, továbbá $k_3 \le 1$ (és ha $k_3 = 1$, akkor $k_2 = k_1 = 0$). Ugyanígy kapunk korlátokat k_2-re és k_1-re is, és a végén a következő lehetőségek maradnak:

$$s_3 = a\sigma_3 + b\sigma_2\sigma_1 + c\sigma_1^3\,,$$

ahol az a, b, c együtthatók ismeretlenek. Ezeket azonban meghatározhatjuk alkalmas helyettesítésekkel is. Ha x_1 helyére 1-et, a többi határozatlan helyére nullát írunk, akkor s_3-ból és σ_1-ből 1 lesz, σ_2 és σ_3 pedig nullává válik. Ezért $c = 1$. Ha $x_1 = x_2 = 1$, és a többi változó nulla, akkor $s_3 = \sigma_1 = 2$, $\sigma_2 = 1$, $\sigma_3 = 0$, és így a $2 = 2b + 8$ egyenletet kapjuk, ahonnan $b = -3$. Végül x_3-at is 1-re változtatva $s_3 = \sigma_1 = \sigma_2 = 3$, $\sigma_3 = 1$, és a $3 = a - 3 \cdot 3 \cdot 3 + 27$ egyenletből $a = 3$.

11.3. A polinomok számelmélete

3.1. Számelméleti alapfogalmak.

3.1.1. Az $x^2 + 1$ polinom vizsgálatához hasonlóan járunk el. Mivel $\pm\sqrt{2}$ irracionális, $\mathbb{Q}$ fölött csakis a „triviális” $x^2 - 2 = c(x^2/c - 2/c)$ felbontás létezik, ahol $c \neq 0$ racionális szám. Ezek a triviális felbontások valós c esetén $\mathbb{R}[x]$-ben is megvannak. Ugyanakkor $\mathbb{R}$ fölött $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, és ezt a felbontást is módosíthatjuk úgy, hogy az egyik tényezőt egy valós $c \neq 0$ számmal megszorozzuk, a másikat pedig c-vel elosztjuk.

3.1.2. Ugyanúgy járunk el, mint amikor a polinomot $\mathbb{C}$ és $\mathbb{R}$ fölött vizsgáltuk. Mivel másodfokú polinomról van szó, vagy két elsőfokú szorzatára bonthatjuk, vagy pedig egy konstans, és egy másodfokú szorzatára. Ha az egyik elsőfokú tényező $ax + b$, akkor $-b/a$ gyöke a polinomnak.

A $\mathbb{Z}_2$ elemeit végigpróbálgatva azt kapjuk, hogy $x^2 + 1$ egyetlen gyöke az 1, és így $x^2 + 1 = (x + 1)(x + 1)$. Ezt a felbontást módosíthatnánk még úgy, hogy az egyik tényezőt egy nem nulla konstanssal megszorozzuk, a másikat pedig ugyanezzel elosztjuk. Csakhogy $\mathbb{Z}_2$ egyetlen nem nulla eleme az 1, és így ezen a módon most nem kapunk új felbontást. Ugyanezért az $x^2 + 1$-et egy konstans és egy másodfokú polinom szorzatára is csak egyféleképpen bonthatjuk: $x^2 + 1 = 1(x^2 + 1)$.

A $\mathbb{Z}_3$ elemeit végigpróbálgatva azt kapjuk, hogy $x^2 + 1$-nek ebben a testben nincsen gyöke. Ezért itt az $x^2 + 1$-et csakis egy nem nulla konstans és egy másodfokú polinom szorzatára bonthatjuk: $x^2 + 1 = 1(x^2 + 1) = 2(2x^2 + 2)$.

3.1.4. Mintabizonyításként csak a (3) állítást mutatjuk meg, a többi hasonlóan igazolható. Mivel $r \mid s$, az oszthatóság definíciója szerint van olyan $a \in R$, melyre $ra = s$. Ugyanígy $s \mid t$ miatt van olyan $b \in R$, hogy $sb = t$. De akkor $t = sb = (ra)b = r(ab)$, és így $r \mid t$.

3.1.5. Ha $0 \mid s$, akkor van olyan $a \in R$, melyre $a \cdot 0 = s$. De (a 2.2.20. Gyakorlat miatt) $a \cdot 0 = 0$, tehát $s = 0$. Ugyanakkor $r \cdot 0 = 0$ miatt $r \mid 0$ tetszőleges R esetén. Ha R test, akkor $r \mid t$ mindig teljesül, kivéve ha $r = 0$ de $t \neq 0$. Valóban, ha $r \neq 0$, akkor $r(t/r) = t$, ha pedig $t = 0$, akkor az imént bizonyított állítás szerint t-nek minden elem osztója.

3.1.6. Ha R egységelemes, kommutatív gyűrű, akkor egy $r \in R$ (mint konstans polinom) akkor és csak akkor osztója egy $f \in R[x]$ polinomnak, ha osztója f mindegyik együtthatójának. Valóban, ha $r \mid f$, akkor van olyan $g(x) = b_0 + \ldots + b_n x^n \in R[x]$, melyre

$$f(x) = rg(x) = rb_0 + \ldots + rb_n x^n .$$

Tehát f minden együtthatója r-nek többszöröse. A megfordítás igazolásához tegyük fel, hogy $f(x) = a_0 + \ldots + a_n x^n$ minden együtthatója r-rel osztható. Ekkor $a_j = rb_j$ alkalmas $b_0, \ldots, b_n \in R$ elemekre. Így

$$f(x) = r(b_0 + \ldots + b_n x^n) ,$$

vagyis $r \mid f$.

3.1.8. A három állítás azonnal adódik az oszthatóság elemi tulajdonságaiból (3.1.4. Gyakorlat): a tranzitivitás a (3)-ból, a reflexivitás a (4)-ből, a szimmetria pedig közvetlenül a definícióból.

3.1.11. Ezt már beláttuk a 2.3.2. Tételben (vagyis igazából a 2.1.7. Állításban).

3.1.16. Pozitív egész számok esetében két felbonthatatlan akkor és csak akkor asszociált, ha egyenlő. Így minden pozitív egész felírható kanonikus alakban úgy is, hogy nem szerepel egységtényező: az egyenlő felbonthatatlanokat összevonjuk. Speciálisan az 1 üres szorzatként írható (2.2.43. Gyakorlat).

Ha egy negatív egész számban egy p felbonthatatlan páratlan kitevőn szerepel, akkor p-nek a negatív asszociáltját (azaz $-|p|$-t), az összes többi szereplő felbonthatatlannak pedig a pozitív asszociáltját választva a kanonikus alakban nem lesz egységre szükség (például $-72 = (-2)^3 3^2$). A fennmaradó esetekben, vagyis ha a szám egy négyzetszám ellentettje, mindenképpen -1 lesz az egységtényező.

3.1.17. A kanonikus alak egyértelműsége precízen a következőt jelenti. Tegyük fel, hogy

$$ep_1^{\alpha_1} \dots p_m^{\alpha_m} = fq_1^{\beta_1} \dots q_n^{\beta_n},$$

ahol e, f egységek, $p_1, \dots, p_m$ páronként nem asszociált felbonthatatlanok, és $q_1, \dots, q_n$ is páronként nem asszociált felbonthatatlanok. Ekkor a $\{p_1, \dots, p_m\}$ és a $\{q_1, \dots, q_n\}$ halmazok között létezik egy kölcsönösen egyértelmű megfeleltetés úgy, hogy az egymásnak megfelelő felbonthatatlanok asszociáltak, és a kitevőik megegyeznek (speciálisan $m = n$). Vagyis ha p_i és q_j egymásnak felelnek meg, akkor $p_i \sim q_j$, és $\alpha_i = \beta_j$.

Az állítás bizonyításához az alaptétel egyértelműségi állítását használjuk fel. Mindkét oldalon felbonthatatlanok szorzata szerepel (ha az e, illetve f egységeket „beolvasztjuk" valamelyik felbonthatatlanba, például az egyik p_1 helyett ep_1-et írunk). Ezért a szereplő felbonthatatlanok között van egy kölcsönösen egyértelmű φ megfeleltetés úgy, hogy az egymásnak megfelelő felbonthatatlanok asszociáltak.

Húzzunk egy vonalat p_i és q_j között akkor, ha asszociáltak. Ekkor a φ megfeleltetés miatt minden p_i-ből és minden q_j-ből indul ki vonal. Egyikből sem indulhat ki két vonal, mert ha például p_1-ből q_1-hez és q_2-höz is vezetne vonal, akkor q_1 és q_2 asszociáltak lennének, ami nem igaz. Tehát a vonalak kölcsönösen egyértelmű megfeleltetést létesítenek $\{p_1, \dots, p_m\}$ és $\{q_1, \dots, q_n\}$ között. Be kell még látni, hogy ha $p_i \sim q_j$, akkor $\alpha_i = \beta_j$.

Ha r tetszőleges felbonthatatlan, amelynek α darab asszociáltja van a bal oldalon, akkor pontosan az ezeknek φ-nél megfelelő jobb oldali felbonthatatlanok lesznek r asszociáltjai a jobb oldalon, és így a jobb oldalon is α darab asszociáltja van r-nek. Ha tehát r asszociáltja a bal oldalon p_i, a jobb oldalon meg q_j, akkor $p_1 \sim q_i$, és $\alpha_i = \beta_j = \alpha$.

3.1.19. Tegyük fel, hogy az r és s elemeknek u és v is kitüntetett közös osztója. Ekkor u közös osztó, és ezért v kitüntetettsége miatt $u \mid v$. Az u és v szerepét megcserélve $v \mid u$, és így $u \sim v$.

3.1.20. Ha adott egy p felbonthatatlan, akkor bármely $r \in R$ esetében megtehetjük, hogy az r kanonikus alakjában p asszociáltjai közül éppen p-t szerepeltetjük (vagyis ha r felbontásában eredetileg p-nek egy pe asszociáltja szerepel, akkor az e egységtényezőt kivisszük a kanonikus alak elejére, és beleolvasztjuk az ottani egységbe). Az sem akadály, ha p nem is osztója r-nek, ebben az esetben p kitevője r kanonikus alakjában nulla lesz. Például ha

$p = -2$, akkor $24 = (-1)(-2)^3 3^1$ és $15 = 1 \cdot (-2)^0 3^1 5^1$. Így tetszőleges két elem, r és s kanonikus alakja felírható

$$r = e p_1^{\alpha_1} \dots p_m^{\alpha_m} \quad \text{és} \quad s = f p_1^{\beta_1} \dots p_m^{\beta_m}$$

alakban, amivel az (1)-et beláttuk.

Ezekre az elemekre $r \mid s$ akkor és csak akkor, ha $\alpha_i \leq \beta_i$ minden $1 \leq i \leq m$ esetén. Valóban, ha ez a feltétel teljesül, akkor

$$s = r(f/e) p_1^{\beta_1 - \alpha_1} \dots p_m^{\beta_m - \alpha_m},$$

és itt f/e egy értelmes eleme R-nek, hiszen e egység, és így lehet vele R-ben osztani. Megfordítva, ha $r \mid s$, akkor van olyan $t \in R$, melyre $rt = s$. Így t minden felbonthatatlan osztója osztója s-nek, és így t kanonikus alakja is felírható $t = g p_1^{\gamma_1} \dots p_m^{\gamma_m}$ alakban, ahol $g \in R$ egység. A szorzást elvégezve a kanonikus alak egyértelműsége miatt $\alpha_i + \gamma_i = \beta_i$ adódik, vagyis $\alpha_i \leq \beta_i$ tényleg teljesül. Így (2) is igaz. Ha az asszociált osztókat nem különböztetjük meg egymástól, akkor ezek száma

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1)$$

(ugyanúgy, mint pozitív egészekre), hiszen a β_i kitevő $0, 1, \dots, \alpha_i$, vagyis $\alpha_i + 1$-féle lehet, és ezek a választások egymástól függetlenek.

Most már meg tudjuk mutatni, hogy ha $\delta_i = \min(\alpha_i, \beta_i)$, akkor a fenti r és s elemeknek az $u = p_1^{\delta_1} \dots p_m^{\delta_m}$ kitüntetett közös osztója lesz. A (2) állítás szerint u közös osztó, mert a kanonikus alakjában szereplő δ_i kitevőkre $\delta_i \leq \alpha_i$ és $\delta_i \leq \beta_i$ is teljesül. Ha viszont v is közös osztója r-nek és s-nek, akkor v-nek is minden felbonthatatlan osztója valamelyik p_i asszociáltja, és így v kanonikus alakja is felírható $v = g p_1^{\gamma_1} \dots p_m^{\gamma_m}$ alakban, ahol $g \in R$ egység. Így (2) miatt $\gamma_i \leq \alpha_i$ és $\gamma_i \leq \beta_i$ minden i-re, de akkor γ_i legfeljebb akkora lehet, mint α_i és β_i közül a nem nagyobb, vagyis δ_i. Tehát (2) miatt $v \mid u$. Ezzel a kitüntetett közös osztó létezését, azaz a (3) állítást beláttuk.

Azt mondjuk, hogy az $u \in R$ elem az r és s elemek *kitüntetett közös többszöröse*, ha $r \mid u$ és $s \mid u$ (azaz u közös többszörös), és ha v tetszőleges közös többszöröse r-nek és s-nek, akkor $u \mid v$. Az eddig bizonyítottakhoz teljesen hasonlóan igazolható, hogy a fenti r és s elemeknek

$$p_1^{\max(\alpha_1, \beta_1)} \dots p_m^{\max(\alpha_m, \beta_m)}$$

kitüntetett közös többszöröse lesz. Az, hogy a kitüntetett közös többszörös asszociáltság erejéig egyértelmű, ugyanúgy igazolható, mint ahogy a kitüntetett közös osztó esetében történt a 3.1.19. Gyakorlatban.

Végül ha kettőnél több, de véges sok elem adott, akkor ezeknek is van közös kanonikus alakja. Kitüntetett közös osztót úgy kapunk, hogy minden p felbonthatatlan esetében az előforduló kitevők minimumát vesszük. Ha a maximumot vesszük, akkor az eredmény kitüntetett közös többszörös lesz.

Végtelen sok elem esetében megtehetjük, hogy a közös kanonikus alakot „végtelen sok tényezős” szorzatnak képzeljük, amelyben azonban véges sok kivétellel minden kitevő nulla.

Ezzel a konvencióval érvényben marad a kitüntetett közös osztó képlete, és így az mindig létezik. A kitüntetett közös többszörös esetében azonban előfordulhat, hogy egy p prím kitevője az egyes elemekben egyre nagyobb, és így nincsen maximumuk. Előfordulhat továbbá az is, hogy ugyan minden p-re létezik ez a maximum, de az eredményben végtelen sok prím szerepel nem nulla kitevővel, és ezeket nem tudjuk összeszorozni. Ebben a két esetben az eredeti számoknak már közös többszöröse sincs. Ha viszont nem ez a helyzet, akkor a képlet kitüntetett közös többszöröst szolgáltat.

3.1.22. Legyen R szokásos gyűrű, és $p \in R$ prím. Meg kell mutatni, hogy p felbonthatatlan. Mivel p prím, p nem nulla, és nem egység. Tegyük fel, hogy $p = rs$. Ekkor r és s is osztója p-nek. Másrészt $p \mid rs$, és így p prímtulajdonsága miatt $p \mid r$ vagy $p \mid s$. Az első esetben tehát r és p asszociáltak, a másodikban pedig s és p asszociáltak. A $p = rs$ felbontás tehát csak triviális lehet, és így p tényleg felbonthatatlan.

Most legyen R alaptételes gyűrű, és p egy felbonthatatlan eleme R-nek. Ekkor p nem nulla és nem egység, meg kell mutatni, hogy prímtulajdonságú. Tegyük fel, hogy $p \mid rs$, azaz $rs = pt$ alkalmas $t \in R$ esetén. Ha r (vagy s) nulla, akkor ennek osztója a p, ha pedig r és s valamelyike egység, akkor p nyilván osztója a másiknak. Ha t egység, akkor p felbonthatatlansága miatt r és s egyike p-nek asszociáltja. A fennmaradó esetekben az r, s és t elemeket felírhatjuk felbonthatatlanok szorzataként. Ha $r = p_1 \dots p_m$ és $s = q_1 \dots q_n$, akkor

$$pt = rs = p_1 \dots p_m q_1 \dots q_n \,.$$

Az R gyűrű alaptételes, így az rs elemnek a felbontása egyértelmű. Mivel p szerepel a bal oldalon, ezért a jobb oldalon álló tényezők valamelyike p-nek asszociáltja. Ha ez valamelyik p_i, akkor $p \mid r$, ha meg valamelyik q_j, akkor $p \mid s$. Tehát p tényleg prím.

3.1.23. Az oszthatóság akkor teljesül, ha van olyan $f(x) = a_0 + \ldots + a_n x^n$ polinom, melyre

$$3x^2 = 2x(a_0 + \ldots + a_n x^n) = 2a_0 x + 2a_1 x^2 + \ldots + 2a_n x^{n+1} \,.$$

Két polinom akkor egyenlő, ha a megfelelő együtthatóik megegyeznek. Ezért $2a_1 = 3$, és $2a_i = 0$ ha $i \neq 1$. A $2a_1 = 3$ egyenletnek a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ testekben van megoldása ($a_1 = 3/2$), $\mathbb{Z}$-ben azonban nincs. Tehát az oszthatóság nem igaz $\mathbb{Z}[x]$-ben, a másik három esetben azonban igen: $3x^2 = (2x)\big((3/2)x\big)$.

Megjegyezzük, hogy polinomok között az oszthatóságot általában nem ezzel a módszerrel érdemes eldönteni, hanem a következő, 3.2. Szakaszban tárgyalt maradékos osztási eljárás segítségével (lásd a 3.2.17. Gyakorlatot is).

3.1.24. Ha $r \mid s$, akkor (r, s) (asszociáltság erejéig) r lesz, hiszen r közös osztó, és ha t is közös osztó, akkor $t \mid r$ miatt r kitüntetett is. Speciálisan r és 0 kitüntetett közös osztója r (és r asszociáltjai), hiszen $r \mid 0$.

3.1.25. Ez a gyakorlat azt járja körül, hogy a felbonthatatlan illetve prím elemek definíciójában (3.1.13, illetve 3.1.21) mennyire volt szükséges külön kikötni, hogy a szóbanforgó elem nem lehet sem nulla, sem egység.

Triviális felbontást eleve csak nem nulla elem esetében definiáltunk. A nulla ugyanis túl „furcsán" viselkedik: a $0 = 0 \cdot 0$ felbontásban például mindkét tényező a 0-nak asszociáltja, de egyik tényező sem egység. Nullosztómentes gyűrűben az igaz, hogy a nulla minden felbontásában az egyik tényező a nullának asszociáltja lesz (tudniillik önmaga). Egy egység minden felbontása triviális, hiszen minden tényező egység lesz.

Egy R gyűrűben a $0 \mid rs$-ből akkor és csak akkor következik, hogy $0 \mid r$ vagy $0 \mid s$, ha R nullosztómentes (hiszen $0 \mid t$ akkor és csak akkor, ha $t = 0$). Minden egységre teljesül, hogy ha osztója egy szorzatnak, akkor osztója valamelyik (sőt mindegyik) tényezőnek.

3.1.26. Tegyük fel, hogy R alaptételes. Írjuk fel az r, s, t számokat közös kanonikus alakban:

$$r = ep_1^{\alpha_1} \dots p_m^{\alpha_m}, \quad s = fp_1^{\beta_1} \dots p_m^{\beta_m}, \quad t = gp_1^{\gamma_1} \dots p_m^{\gamma_m}.$$

A 3.1.20. Gyakorlatban a kitüntetett közös osztóra kapott képlet szerint ekkor a p_i kitevője az $(r, s)t$-ben $\min(\alpha_i, \beta_i) + \gamma_i$, az (rt, st)-ben pedig $\min(\alpha_i + \gamma_i, \beta_i + \gamma_i)$ lesz. Elég tehát belátni a

$$\min(\alpha, \beta) + \gamma = \min(\alpha + \gamma, \beta + \gamma)$$

azonosságot. Ez könnyen ellenőrizhető esetszétválasztással: ha $\alpha \leq \beta$, akkor mindkét oldal $\alpha + \gamma$, egyébként pedig mindkét oldal $\beta + \gamma$.

Az minden szokásos gyűrűben igaz, hogy $(r, s)t$ osztója (rt, st)-nek. Valóban, $(r, s) \mid r$ miatt $(r, s)t \mid rt$, ugyanígy $(r, s)t \mid st$, és így (rt, st) kitüntetettsége miatt $(r, s)t \mid (rt, st)$. Ha viszont tudjuk, hogy $(r, s) = rx + sy$, akkor innen $(r, s)t = rtx + sty$. Ezt pedig osztja (rt, st), hiszen osztja rt-t és st-t is. Így tehát $(r, s)t$ és (rt, st) egymás osztói, vagyis asszociáltak.

3.1.27.

Akinek még nehézséget okoz általános gyűrűben gondolkozni, az az alábbi megoldásban nyugodtan gondoljon pozitív egészekre, és ennek megfelelően helyettesítse a $\sim$ jelet $=$ jellel (tehát asszociáltság helyett mondjon egyenlőséget), egység helyett pedig 1-et.

Tegyük fel, hogy $r \mid st$ és $(r, s) \sim 1$. A kitüntetett közös osztó kiemelési tulajdonsága miatt (rt, st) és $(r, s)t$ asszociáltak. Mivel r és s relatív prímek, $(r, s)t \sim t$. Másfelől r közös osztója rt-nek és st-nek, vagyis $r \mid (rt, st) \sim (r, s)t \sim t$. Tehát tényleg $r \mid t$, és így (1)-et beláttuk.

Most legyen p irreducibilis elem. Ekkor p nem nulla, nem egység, és mindegyik osztója vagy egység, vagy p-nek asszociáltja. Tegyük fel, hogy $p \mid rs$, de $p \nmid r$. Ekkor (p, r) osztója p-nek, de nem lehet p-nek asszociáltja (mert akkor $p \sim (p, r) \mid r$ miatt $p \mid r$ teljesülne). Mivel p irreducibilis, $(p, r) \mid p$ csak egység lehet. Az (1) tulajdonság szerint tehát $p \mid t$.

3.1.28. Tegyük fel, hogy $f = p_1 \dots p_k = q_1 \dots q_\ell$ az $f \in R$ elem két felbontása irreducibilisek szorzatára. A feltevés szerint p_1 prím, és mivel osztója a $q_1 \dots q_\ell$ szorzatnak, osztója valamelyik q_j-nek. De q_j irreducibilis, p_1 pedig nem egység, és így $p_1 \sim q_j$. Vagyis $q_j = p_1 e_1$ valamilyen e_1 egységre. Rendeljük hozzá p_1-hez q_j-t, és mindkét oldalt egyszerűsítsük p_1-gyel. Ezután p_2-vel folytatjuk az eljárást. Amikor az összes p_i elfogyott, akkor a bal oldalon 1 marad, a jobb oldalon pedig az e_i egységeknek és még esetleg néhány q_j-nek a szorzata. De minden ilyen megmaradó q_j osztója lenne 1-nek, ami nem lehet (hiszen q_j irreducibilis, tehát nem egység). Ezért a p_i-k és a q_j-k egyszerre fogynak el, és így a közöttük most felépített leképezés kölcsönösen egyértelmű.

3.1.29. Ismét a 3.1.20. Gyakorlatban a kitüntetett közös osztóra és a kitüntetett közös többszörösre kapott képlet segítségével számolunk, ekkor mindegyik kitevőben a

$$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$$

azonosságot kell igazolni. Ez pedig teljesül, hiszen ha két szám közül a kisebbet hozzáadjuk a nagyobbhoz, akkor a két szám összegét kapjuk.

3.1.30. Tudjuk a 2.2.34. (2) Gyakorlat megoldásából, hogy a Gauss-egészek között négy egység van: a ± 1 és a $\pm i$. Határozzuk meg a 2 osztóit ugyanezzel a gondolatmenettel. Ha $(a + bi)(c + di) = 2$, akkor ezt az egyenletet a konjugáltjával megszorozva

$$(a^2 + b^2)(c^2 + d^2) = 4$$

adódik. Ha itt $a^2 + b^2 = 1$, akkor az idézett megoldásban láttuk, hogy $a + bi$ egység. Ugyanígy ha $c^2 + d^2 = 1$, akkor $c + di$ egység, és akkor $a + bi$ értéke $2, -2, 2i$, vagy $-2i$ lesz. Ezek tehát a 2 triviális felbontásai. Az egyetlen további lehetőség, ha $a^2 + b^2 = 2$. Ekkor a és b is csak ± 1 lehet, és $a + bi$-re $1 + i,\ 1 - i,\ -1 + i,\ -1 - i$ adódik (vagyis az $1 + i$ négy asszociáltja). Így végülis 2 osztói $1, 1 + i, 2$, és ezek asszociáltjai.

Most meg kell néznünk, hogy ezek közül melyek osztják $1 + 3i$-t. Az 1 nyilván osztja, a 2 nem, mert ha $2(u + vi) = 1 + 3i$, akkor innen $2u = 1$ (és $2v = 3$), ami u és v egészekre lehetetlen. Végül az $(1 + 3i)/(1 + i)$ osztást elvégezve $2 + i$ adódik, ami Gauss-egész. Tehát $1 + i \mid 1 + 3i$, és így a 2 és az $1 + 3i$ kitüntetett közös osztói $1 + i$ asszociáltjai.

A fenti meggondolást praktikusan csak kis számokra lehet végrehajtani. Azonban a Gauss-egészek között is el lehet végezni a maradékos osztást, és az euklideszi algoritmust is, amivel általában is meg tudjuk határozni két Gauss-egész kitüntetett közös osztóját. Érvényes az alaptétel is, és ez az egyik kiindulópontja érdekes, egész számokra vonatkozó tételek bizonyításának. Az érdeklődő Olvasó ezzel a témával a [**11**] könyv 7.4. és 7.5. Szakaszában ismerkedhet meg.

3.1.31. Legyen R kommutatív, nullosztómentes gyűrű. Belátjuk, hogy ha egy $r \neq 0$ elem osztója önmagának, akkor R egységelemes. Valóban, ekkor van olyan $x \in R$, hogy $rx = r$. A 2.4.24. Gyakorlat megoldásához hasonlóan innen $rxs = rs$, majd r-rel egyszerűsítve $xs = s$ teljesül minden $s \in R$ esetén, azaz x egységeleme R-nek.

Ha tehát $e \in R$ minden elemnek osztója, akkor $e \mid e$ miatt R egységelemes, kivéve ha $e = 0$, amikor a 2.2.20. Feladat szerint R a nullgyűrű. Ha $p \in R$ prím, akkor $p \mid p^2$-ből a prímtulajdonság miatt $p \mid p$ következik, és így most is azt kapjuk, hogy R egységelemes. Ha r és s asszociáltak, akkor $r \mid s \mid r$ miatt $r \mid r$, és így ha R nem egységelemes, akkor $r = 0$. Így $r \mid s$ miatt $s = 0$, vagyis az egyetlen asszociált elempár a $(0, 0)$.

A páros számok nyilván részgyűrűt alkotnak $\mathbb{Z}$-ben, amely nem egységelemes, hiszen a $2x = 2$ egyenletnek $\mathbb{Z}$-ben is csak az 1 szám megoldása. A felbonthatatlanok a néggyel ($\mathbb{Z}$-ben) nem osztható számok (vagyis a $4k + 2$ alakú számok, ahol $k \in \mathbb{Z}$). Ezek valóban felbonthatatlanok, hiszen két páros szám szorzata biztosan osztható néggyel. Megfordítva, ha egy nem nulla szám néggyel osztható $\mathbb{Z}$-ben, vagyis $4k$ alakú, akkor $2(2k)$ a páros számok körében készített felbontása, amely nemtriviális (hiszen nem nulla számnak ebben a gyűrűben nincs is asszociáltja).

Ezek szerint minden páros szám felbontható a páros számok gyűrűjében felbonthatatlanok szorzatára: ha a $\mathbb{Z}$-beli kanonikus alakjában 2^n szerepel, akkor $n - 1$ darab kettest kiemelve a megmaradó tényező is felbonthatatlan lesz. A felbontás nem egyértelmű, hiszen például $36 = 2 \cdot 18 = 6 \cdot 6$ két lényegesen különböző felbontás felbonthatatlanok szorzatára (mert a 2 nem asszociáltja a 6-nak).

Ha a 3.1.7. Definíció utáni megjegyzésben leírt asszociáltság-fogalmat használjuk, akkor a páros számok gyűrűjében két elem akkor és csak akkor lesz asszociált, ha egyenlők, vagy egymás ellentettjei.

3.1.32. A 2 konstans polinom osztói $\mathbb{Z}[x]$-ben csak ± 1 és ± 2 (hiszen ha $2 = pq$, akkor p és q is csak nulladfokú lehet). Ezek közül x-et ± 1 osztja, ± 2 nem. Tehát 2 és x közös osztói csak ± 1, és így ezek kitüntetettek is. Ha $2p(x) + xq(x) = 1$ lenne alkalmas $p, q \in \mathbb{Z}[x]$-re, akkor $x = 0$-t helyettesítve $2p(0) = 1$, ami lehetetlen, mert $p(0)$ egész szám.

3.1.33. Ha a 3 prím lenne R-ben, akkor a $3 \cdot 3 = 9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ összefüggés miatt osztaná $2 + i\sqrt{5}$ és $2 - i\sqrt{5}$ valamelyikét. De ha például $3(a + bi\sqrt{5}) = 2 + i\sqrt{5}$ lenne, akkor a valós részeket véve $3a = 2$, ami egész a-ra nem teljesül. Tehát a 3 nem prím.

A 3 osztóinak megkereséséhez a 3.1.30. Gyakorlat mintájára járunk el. Tegyük fel, hogy

$$(a + bi\sqrt{5})(c + di\sqrt{5}) = 3\,.$$

Ezt az egyenletet a konjugáltjával megszorozva

$$(a^2 + 5b^2)(c^2 + 5d^2) = 9$$

adódik (és e két tényező pozitív egész). Tehát csak a $9 = 1 \cdot 9 = 3 \cdot 3 = 9 \cdot 1$ felbontás jön szóba. De $a^2 + 5b^2 \geq 5$, ha $b \neq 0$. Ezért $a^2 + 5b^2$ soha nem lesz 3 (mert az nem

négyzetszám), és 1 is csak úgy lehet, ha $a + bi\sqrt{5} = \pm 1$. Mivel a ± 1 egységek, a 3 mindegyik felbontása triviális.

Tehát 3 osztói csak ± 1 és ± 3 lesznek. Láttuk, hogy ± 3 nem osztója $2 + i\sqrt{5}$-nek. Így csak a ± 1 közös osztója 3-nak és $2 + i\sqrt{5}$-nek, ezek persze kitüntetettek is. Tegyük fel, hogy R-ben teljesül a kitüntetett közös osztó kiemelési tulajdonsága. Ekkor

$$\big((2 - i\sqrt{5})3,\, (2 - i\sqrt{5})(2 + i\sqrt{5})\big) \sim (2 - i\sqrt{5})\big(3,\, 2 + i\sqrt{5}\big) = \pm(2 - i\sqrt{5})\,.$$

De ez nem igaz: $\big((2 - i\sqrt{5})3,\, (2 - i\sqrt{5})(2 + i\sqrt{5})\big) = \big((2 - i\sqrt{5})3,\, 9\big)$ osztható 3-mal (hiszen a 3 közös osztója $(2 - i\sqrt{5})3$-nak és 9-nek), $2 - i\sqrt{5}$ pedig nem osztható 3-mal.

3.1.34. Ez a halmaz nyilván zárt az összeadásra és az ellentettképzésre, és tartalmazza a konstans polinomokat is. Ha két ilyen polinomot összeszorzunk, akkor a szorzatban a konstans tagon kívül csak harmadfokú, továbbá legalább $3 + 3 = 6$-odfokú tagok lehetnek, és így a szorzat is benne van a halmazban. A 2.2.24. Feladat miatt tehát R tényleg részgyűrű. De $1 \in R$, és mivel $\mathbb{R}[x, y]$ szokásos gyűrű, R is nullosztómentes és kommutatív.

Belátjuk, hogy az x^5y^2 és az x^2y^5 polinomoknak nincs kitüntetett közös osztója. Tegyük fel ugyanis, hogy $p \in R$ kitüntetett közös osztó. Ekkor p osztója x^5y^2-nek $\mathbb{R}[x, y]$-ban is, és ezért könnyen láthatóan cx^ny^m alakú, ahol $c \in \mathbb{R}$, $n \le 5$ és $m \le 2$. Mivel $p \mid x^2y^5$, ezért $n \le 2$ is teljesül. Másrészt viszont x^2y közös osztója x^5y^2-nek és x^2y^5-nak az R gyűrűben (hiszen $x^5y^2/x^2y = x^3y$ és $x^2y^5/x^2y = y^4$ is elemei R-nek), ezért $x^2y \mid p$. Ez azt jelenti, hogy $n \ge 2$. Ugyanígy $xy^2 \mid p$, és így $m \ge 2$. De akkor $p = cx^2y^2$, ami lehetetlen, mert $cx^2y^2 \notin R$.

3.1.35. Azt, hogy R szokásos gyűrű, ugyanúgy láthatjuk be, mint ahogy $\mathbb{R}[x]$-ről megmutattuk, hogy szokásos gyűrű: itt is igaz lesz, hogy a főtagok szorzata a szorzat főtagja. Megmutatjuk, hogy x-nek minden osztója cx^r alakú, ahol $c \in \mathbb{R}$, és $0 \le r \le 1$ valós szám.

Valóban, ha $pq = x$, akkor a főtagokat összeszorozva x-et kell, hogy kapjunk, és így ha p főtagja cx^r, q főtagja pedig dx^s, akkor $cd = 1$ és $r + s = 1$. Legyen p, illetve q „altagja”, azaz legalacsonyabb „fokú” tagja $c'x^{r'}$, illetve $d'x^{s'}$. A szorzatpolinom képletéből láthatjuk, ugyanúgy, mint a főtagok esetében, hogy a pq szorzat „altagja” $c'd'x^{r'+s'}$ lesz, és ez most szintén x. Emiatt $r' + s' = 1$, de $r' \le r$ és $s' \le s$ miatt ez csak úgy lehetséges, ha $r' = r$ és $s' = s$. Vagyis a p és a q polinom is csak egyetlen tagból állhat.

Így viszont x-et nemhogy nem tudjuk felbonthatatlanok szorzatára bontani, de még felbonthatatlan osztója sincs! Ugyanis cx^r felírható $cx^{r/2}$ és $x^{r/2}$ szorzataként, és (ha $r > 0$, akkor) ez nemtriviális felbontás, hiszen R egységei a nem nulla konstans polinomok. (Ha $r = 0$, akkor viszont cx^r egység, tehát ismét nem felbonthatatlan.)

3.2. A maradékos osztás.

3.2.3. Ugyanígy bizonyítunk, mint az egész számok számelméletében. A 86. oldalon található jelöléseket használjuk. Elsőnek azt mutatjuk meg, hogy r_n közös osztója f-nek és g-nek. Az utolsó sorból látszik, hogy $r_n \mid r_{n-1}$. Az utolsó előtti sor szerint $r_n \mid r_{n-2}$. Ugyanígy haladunk tovább felfelé: ha már tudjuk, hogy r_n osztója r_{j+1}-nek és r_j-nek is, akkor azt a sort használva, amelynek a bal oldalán r_{j-1} áll, azt kapjuk, hogy $r_n \mid r_{j-1}$. A második sorhoz érve $r_n \mid g$, végül az első sorból $r_n \mid f$ adódik.

Az r_n kitüntetettségének igazolásához tegyük fel, hogy $h \mid f$ és $h \mid g$ is teljesül. Az első sorból ekkor $h \mid r_1$. A második sorból ezt felhasználva $h \mid r_2$. Lefelé haladva sorban látjuk, hogy $h \mid r_j$ minden j-re, végül az utolsó előtti sor adja a kívánt $h \mid r_n$ összefüggést.

Végül az r_n-et előállítjuk $fp + gq$ alakban. Ismét alulról fölfelé haladunk. Az utolsó előtti sor szerint $r_n = r_{n-2} - r_{n-1}q_n$. Ide behelyettesítjük az r_{n-1}-nek az alulról a harmadik sorból kapott $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$ előállítását:

$$r_n = r_{n-2} - r_{n-1}q_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = r_{n-3}(-q_n) + r_{n-2}(1 + q_{n-1}q_n)\,.$$

Vagyis az r_n-et most már r_{n-3} és r_{n-2} segítségével állítottuk elő. Ha most r_{n-2}-t fejezzük ki az alulról számított negyedik sorból, és ide behelyettesítünk, akkor r_n-nek az r_{n-4} és r_{n-3} segítségével kapott előállítását kapjuk. Az eljárást folytatva végül r_n-et f és g segítségével felírva kapjuk meg.

Azt tanácsoljuk az Olvasónak, hogy ezt a *visszahelyettesítési eljárást* ne általában próbálja megérteni, hanem először két konkrét pozitív egész számra végezze el. Ezután érdemes ugyanezt polinomokkal is kipróbálni, erre szolgál a 3.2.15. Gyakorlat. A most leírt eljárás hangsúlyozottan a p és q megkeresésére szolgál, ha csak azt akarjuk megmutatni, hogy létezik ilyen p és q, akkor inkább a 3.2.6. Tétel bizonyítását érdemes követni.

3.2.4. Először praktikusan vizsgáljuk a kérdést. Ha f és g valamelyike nulla, akkor persze a kitüntetett közös osztójuk a másik lesz. Általánosabban, ha az egyik osztója a másiknak, például $g \mid f$, akkor a kitüntetett közös osztó g lesz. Ez persze nem látszik ránézésre, csak ha az osztást elvégezzük. Természetesen a nagyobb fokút érdemes osztani a kisebb fokúval, vagyis ha véletlenül $\mathrm{gr}(f) < \mathrm{gr}(g)$, akkor meg kell cserélni a két polinomot. Ha már az első osztás maradéka, $r_1 = 0$, akkor a kitüntetett közös osztó g lesz.

A fenti diszkusszió nagy részét elkerülhetjük, ha a $g = r_0$ (sőt $f = r_{-1}$) jelölést bevezetjük. Ez azonban, bár formálisan megoldaná a problémákat, a szőnyeg alá söpörné az előző bekezdésben megvizsgált kérdéseket.

3.2.5. Az euklideszi algoritmus elvégzése során minden számítás ugyanaz lesz, akár $\mathbb{Q}$, akár $\mathbb{C}$ fölött gondolkozunk (hiszen a számításokban csak a négy alapműveletet használjuk), ezért a végeredmény, azaz a kitüntetett közös osztó is ugyanaz. Természetesen a kitüntetett közös osztó csak konstansszoros erejéig egyértelmű, vagyis a kapott racionális együtthatós polinom nem nulla racionális konstansszorosai lesznek kitüntetett közös osztók $\mathbb{Q}[x]$-ben, és a nem nulla komplex konstansszorosai lesznek kitüntetett közös osztók $\mathbb{C}[x]$-ben. Ezért *minden* $\mathbb{Q}$ fölötti kitüntetett közös osztó egyben $\mathbb{C}$ fölött is az.

Az általánosítás a következő. Legyen T test, és S részteste T-nek. Ha h kitüntetett közös osztója az $f, g \in S[x]$ polinomoknak $S[x]$-ben, akkor h az f és g kitüntetett közös osztója $T[x]$-ben is. A bizonyítás ugyanaz, mint az előző bekezdésben.

3.2.7. Elképzelhető, hogy I csak a nullapolinomból áll, és ekkor nincsen benne legalacsonyabb fokú polinom (mert az egyetlen elemének nincs foka). De ebben az esetben a $h_0 = 0$ választás megfelelő lesz, hiszen ennek többszörösei kiadják I összes elemét. Természetesen $f, g \in I$ miatt ez az eset csak akkor fordulhat elő, ha $f = g = 0$, amikor a Tétel állítása közvetlenül is nyilvánvaló.

3.2.9. Nem irreducibilis, a $2x = 2 \cdot x$ nemtriviális felbontás. Ugyanis $\mathbb{Z}[x]$ egységei a 3.1.11. Gyakorlat szerint csak ± 1, és így sem 2, sem x nem lesz egység.

3.2.11. A 3.2.3. Gyakorlat (vagy a 3.2.6. Tétel) szerint egy T test feletti $T[x]$ polinomgyűrűben f és g kitüntetett közös osztója felírható $fp + gq$ alakban alkalmas p, q polinomokra. A 3.1.26. Gyakorlat miatt tehát érvényes a kitüntetett közös osztó kiemelési tulajdonsága, és így a 3.1.27. Gyakorlat mutatja, hogy $T[x]$ minden irreducibilis eleme prím. Végül a 3.1.28. Feladat adja az alaptétel egyértelműségi állítását.

3.2.12. Tegyük fel, hogy van olyan nem konstans polinom $T[x]$-ben, amely nem bontható fel irreducibilisek szorzatára. Válasszunk ezek közül egy minimális fokszámú f polinomot. A minimalitás tehát azt jelenti, hogy az f-nél kisebb fokú polinomok már mind felbomlanak irreducibilisek szorzatára. Az f nem lehet irreducibilis, hiszen akkor önmaga, mint egytényezős szorzat az f-nek irreducibilisekre való felbontása lenne. Ezért f felbomlik az f-nél alacsonyabb fokú g és h polinomok szorzatára. Az f fokának a minimalitása miatt g és h már felbomlik irreducibilisek szorzatára: $g = p_1 \dots p_n$ és $h = q_1 \dots q_m$. De akkor $f = p_1 \dots p_n q_1 \dots q_m$ az f-nek irreducibilisek szorzatára való felbontása. Ez ellentmondás, ezért ilyen f polinom nincs, és így minden nem konstans $T[x]$-beli polinom irreducibilis polinomok szorzatára bomlik.

3.2.14. A hányados $x/2 - 1/2$, a maradék $(5/2)x - (7/2)$.

3.2.15. Az eredmények a következők.

(1) A kitüntetett közös osztó $x^2 + x + 1$ (illetve ennek bármelyik konstansszorosa), és

$$x^2 + x + 1 = \big(-(1/9)x + (2/9) \big) f(x) + (1/6) g(x) \,.$$

(2) Itt három osztást kell elvégezni. A kitüntetett közös osztó

$$x - 1 = (-x)(x^5 - 1) + (1 + x^3)(x^3 - 1) \,.$$

3.2.16. Nem végezhető el. Az osztónak, vagyis a konstans 2 polinomnak a foka 0, ennél r foka kisebb nem lehet. Ezért r a nullapolinom, vagyis $x = 2q(x)$. De ez lehetetlen: az x polinom nem osztható 2-vel $\mathbb{Z}[x]$-ben, mert egy polinom itt akkor és csak akkor osztható 2-vel, ha mindegyik együtthatója páros (3.1.6. Gyakorlat).

3.2.17. Igaz, a maradékos osztás $\mathbb{Q}[x]$-beli egyértelműsége miatt. Ha ugyanis $g = fh$, ahol $h \in \mathbb{Z}[x]$, akkor $g = fh + 0$ egy maradékos osztás $\mathbb{Q}[x]$-ben, tehát az eljárásnak ezt kell kihoznia.

3.2.18. A lényeg most is az, hogy az osztási eljárás során végig minden együttható S-ben lesz, hiszen most g főegyütthatójával lehet S-ben osztani. A 3.2.2. Állítás bizonyításához hasonlóan tehát a következőképpen haladhatunk. Mivel g főegyütthatója invertálható S-ben, ezért itt lehet vele maradékosan osztani: $f = gq_1 + r_1$, ahol $q_1, r_1 \in S[x]$, és $r_1 = 0$, vagy r_1 foka kisebb g fokánál. Ugyanakkor $f = gq + 0$ alkalmas $q \in T[x]$ polinomra, hiszen g osztója f-nek $T[x]$-ben. A maradékos osztás egyértelműségét $T[x]$-ben alkalmazva ($q = q_1$ és) $0 = r_1$ adódik, azaz g osztója f-nek $S[x]$-ben is.

3.2.19. Az f polinomot $x - b$-vel osztva $f(x) = (x - b)q(x) + r$ adódik, ahol r konstans. Az x helyére b-t helyettesítve $r = f(b)$. Speciálisan $f(b) = 0$ akkor és csak akkor, ha f osztható $x - b$-vel.

3.2.20. Nulla lesz a maradék. Ha csak a maradékra vagyunk kíváncsiak, és az osztó nagyon kis fokú polinom, melynek a gyökeit ismerjük, akkor ezeknek a gyököknek a behelyettesítése segíthet a maradék megkeresésében. A legegyszerűbb példát erre az előző gyakorlatban láttuk: f-et $x - b$-vel osztva a maradék $f(b)$ lesz.

Most másodfokú polinommal osztunk, ezért a maradék $ax + b$ alakú polinom:

$$x^4 + x^2 + 1 = (x^2 + x + 1)q(x) + (ax + b)$$

(ahol a és b valós, sőt racionális számok, hiszen az osztandó és az osztó is racionális együtthatós). Az $x^2+x+1 = (x^3-1)/(x-1)$ polinom gyökei a primitív harmadik egységgyökök: $\varepsilon_1 = \cos 120^\circ + i \sin 120^\circ$, és $\varepsilon_2 = \cos 240^\circ + i \sin 240^\circ$. Mivel $\varepsilon_i^4 = \varepsilon_i$, ezek gyökei az $x^4 + x^2 + 1$ polinomnak is. Ezért behelyettesítve $a\varepsilon_i + b = 0$ adódik. A két egyenletet kivonva $a(\varepsilon_1 - \varepsilon_2) = 0$, és mivel $\varepsilon_1 - \varepsilon_2 \neq 0$, ezért $a = 0$, és $a\varepsilon_i + b = 0$-ból $b = 0$.

Ezt az észrevételt többféleképpen is általánosíthatjuk. Például az $x^4 + x^2 + 1$ helyett vehetjük az $f(x) = x^{2n} + x^n + 1$ polinomot. Ha n nem osztható 3-mal, akkor f-nek is gyöke lesz ε_1 és ε_2, és így a leírt gondolatmenet alapján f is osztható $x^2 + x + 1$-gyel.

3.2.21. Itt már nem praktikus a maradékos osztás elvégzése, az előző gyakorlat megoldásában látott technikát alkalmazzuk. Legyen

$$x^{64} + x^{54} + x^{14} + 1 = (x^2 - 1)q(x) + (ax + b)\,.$$

Az x helyébe 1-et és -1-et helyettesítve $a + b = 4$ és $-a + b = 4$ adódik, ahonnan $a = 0$, $b = 4$, tehát a maradék 4.

Az $x^2 + 1$-gyel való osztáskor i-t és $-i$-t érdemes helyettesíteni. Az i-t behelyettesítve $ai + b = 0$ adódik. Itt a, b valós (sőt mellesleg egész, hiszen az osztó, $x^2 + 1$ főegyütthatója

invertálható $\mathbb{Z}$-ben). Ezért $ai + b = 0$-ból azt kapjuk, hogy $a = b = 0$, vagyis az osztásnál a maradék nulla.

3.2.22. A b gyök h-beli multiplicitása az f-beli és a g-beli multiplicitások minimuma lesz. Ha ugyanis b multiplicitása f-ben k és g-ben ℓ, ahol mondjuk $k \leq \ell$, akkor $(x-b)^k$ közös osztója f-nek és g-nek, és így osztója h-nak is. De h-ban nem lehet b multiplicitása k-nál nagyobb, hiszen $h \mid f$. Megjegyezzük, hogy ha $R[x]$ alaptételes, akkor f és g kanonikus alakját felírva a kitüntetett közös osztó képletéből (3.1.20. Gyakorlat (3)) is ezt az eredményt kapjuk.

3.2.23. Ezek azok a részhalmazok, amelyek egy adott szám összes többszöröséből állnak. Egy d szám többszöröseinek halmaza nyilván zárt az összeadásra, és nyilván minden elemének minden többszörösét is tartalmazza.

Megfordítva, legyen $I \subseteq \mathbb{Z}$ ilyen tulajdonságú, nem üres halmaz. Ha I csak a nullából áll, akkor ez a nulla összes többszöröseinek halmaza. Ha nem, akkor van I-ben pozitív szám is, hiszen ha $-k \in I$, akkor $k \in I$ (mert k többszöröse $-k$-nak). Legyen d az I halmaz legkisebb pozitív eleme. Megmutatjuk, hogy I pontosan a d többszöröseiből áll. Az a feltételből nyilvánvaló, hogy d többesei benne vannak I-ben. Legyen most $n \in I$, és osszuk el n-et maradékosan d-vel:

$$n = dq + r\,,$$

ahol $0 \leq r < d$. Innen $r = n + (-q)d \in I$, hiszen I zárt az összeadásra. Mivel I-ben nincs d-nél kisebb pozitív szám, $r = 0$, és így $d \mid n$. Vagyis I tényleg d többszöröseiből áll.

A 1.5.7. Tétel bizonyításában egy z komplex szám jó kitevőinek halmazát vizsgáltuk. Nyilvánvaló, hogy ez az I halmaz a feladatban leírt tulajdonságú: ha $z^n = 1 = z^m$, akkor $z^{n+m} = 1$, és minden k egészre $z^{nk} = 1$. Tehát az I halmaz egy pozitív d többszöröseiből áll (és ez a d pontosan a z rendje lesz).

3.3. Gyökök és irreducibilitás.

3.3.10. A polinomot (hacsak nem a nullapolinomról van szó) felírhatjuk $g(x)x^k$ alakban, ahol g konstans tagja már nem nulla, és a g polinomra alkalmazhatjuk a tesztet. Az eredeti polinomnak g gyökei mellett még a nulla lesz gyöke.

3.3.12. Az első három polinom esetében úgy érdemes eljárni, hogy a polinomot $\mathbb{C}$ felett gyöktényezők szorzatára bontjuk, majd a nem valós gyökökhöz tartozó gyöktényezőket párosítjuk a konjugáltjukkal. A gyökvonást trigonometrikus alakban célszerű elvégezni. A módszert részletesen bemutattuk a 2.5.10. Gyakorlat megoldásában, ezért most csak az eredményeket közöljük:

$$x^4 - 1 = (x-1)(x+1)(x^2+1)\,,$$
$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)\,,$$
$$x^4 + 9 = (x^2 - \sqrt{6}x + 3)(x^2 + \sqrt{6}x + 3)\,.$$

Az $x^6 - 4x^3 + 3 = 0$ egyenletet az $y = x^3$ helyettesítéssel oldhatjuk meg, ez y-ban másodfokú egyenletre vezet, melynek gyökei 1 és 3. Tehát $x^6-4x^3+3 = (x^3-1)(x^3-3)$. Mindkét tényezőnek egyetlen valós gyöke van, tehát az eredmény:

$$x^6 - 4x^3 + 3 = (x-1)(x^2+x+1)(x-\sqrt[3]{3})(x^2+\sqrt[3]{3}x+\sqrt[3]{9})\,.$$

3.3.13. Figyelnünk kell arra, hogy a felsorolt négy gyűrű felett nemcsak az irreducibilis polinomok mások, hanem az egységek is. Ennek megfelelően egy $\mathbb{C}$ feletti felbontás

$$(6x+6\sqrt{2})(x-\sqrt{2})(x+i)(x-i)$$

(a 6 itt egység, tehát külön tényezőként nem szerepelhet, de bármelyik másik irreducibilis tényezőbe is beolvaszthattuk volna). Amikor $\mathbb{R}$ fölött dolgozunk, akkor x^2+1 már irreducibilis lesz, mert másodfokú, és nincsen valós gyöke. Így az $\mathbb{R}$ fölött jó felbontások például a következők:

$$(2x+2\sqrt{2})(3x-3\sqrt{2})(x^2+1) = (x+\sqrt{2})(x-\sqrt{2})(6x^2+6)\,.$$

A $\mathbb{Q}$ fölött az x^2-2 is irreducibilis, hiszen másodfokú, és nincs racionális gyöke, és így a következőt kapjuk:

$$(x^2-2)(6x^2+6)\,.$$

Végül $\mathbb{Z}$ fölött az egységek csak a ± 1, tehát 2 és 3 is felbonthatatlan polinomok. Az x^2-2 és x^2+1 polinomokat $\mathbb{Z}$ fölött nem lehet alacsonyabb fokúak szorzatára bontani, hiszen láttuk, hogy $\mathbb{Q}$ fölött is irreducibilisek. De nem lehet őket $\mathbb{Z}$ fölött egy nulladfokú (azaz konstans polinom) és egy másodfokú polinom szorzatára sem nemtriviálisan felbontani, hiszen semmilyen ± 1-től különböző konstans nem emelhető ki belőlük. Ezért a $\mathbb{Z}$ feletti felbontás:

$$2\cdot 3\cdot (x^2-2)\cdot (x^2+1)\,.$$

Ezt csak úgy variálhatjuk, hogy néhány (páros sok) tényezőt -1-gyel beszorzunk.

3.3.14. A 3.3.6. Lemma miatt a polinomnak $1-i$ is hatszoros gyöke, és ezért

$$(x-1-i)^6(x-1+i)^6 g(x) = (x^2-2x+2)^6 g(x)$$

alakban írható. Mivel $(x^2-2x+2)^6$ valós együtthatós, g is az (a 3.2.2. Állítás miatt). Ez a szorzat akkor lesz tizenkettedfokú, ha g konstans. Tehát a keresett polinomok pontosan az $r(x^2-2x+2)^6$ polinomok, ahol $r \neq 0$ valós szám.

3.3.15. A racionális gyöktesztet alkalmazzuk (3.3.9. Tétel). Ha p/q racionális gyöke ennek a polinomnak, ahol p és q relatív prím egészek, akkor $p \mid 5$ és $q \mid 2$. A lehetséges gyökök tehát

$$1,\ \ -1,\ \ 1/2,\ \ -1/2,\ \ 5,\ \ -5,\ \ 5/2,\ \ -5/2\,.$$

Ezeket végig kell próbálgatni. Az rögtön látszik, hogy pozitív gyök nem lehet, a negatívakat behelyettesítve azt kapjuk, hogy csak a -1 lesz racionális gyök. A gyöktényezőt (például a Horner-elrendezéssel) kiemelve

$$2x^3 + 3x + 5 = (x+1)(2x^2 - 2x + 5)$$

adódik. A $2x^2 - 2x + 5$ polinomnak racionális gyöke más, mint -1, nem lehet, mert az gyöke lenne az eredeti polinomnak is. Látjuk, hogy -1 nem gyök, és mivel ez másodfokú polinom, irreducibilis $\mathbb{Q}$ fölött (miként az elsőfokú $x+1$ is).

3.3.16. Ha $c > 0$, akkor $\mathbb{C}$ fölött gyöktényezős alakra bontva, a 3.3.12. Gyakorlat mintájára

$$x^4 + c = (x^2 - \sqrt{2}\sqrt[4]{c}x + \sqrt{c})(x^2 + \sqrt{2}\sqrt[4]{c}x + \sqrt{c})\,.$$

Már megvizsgáltuk azt az esetet (a 3.3.11. Példában), amikor $c = 36$. Ugyanez a gondolatmenet általában is azt adja, hogy az $x^4 + c$ polinom akkor és csak akkor lesz reducibilis $\mathbb{Q}$ fölött, ha $\sqrt{2}\sqrt[4]{c}$ és $\sqrt{c}$ is racionális szám, és ebben az esetben a fenti két másodfokú tényező $\mathbb{Q}$, sőt $\mathbb{R}$ fölött is irreducibilis, hiszen másodfokúak, és nincs valós gyökük (mert $x^4 + c$-nek sincs). Megjegyezzük, hogy ha $\sqrt{2}\sqrt[4]{c}$ racionális szám, akkor a négyzete, azaz $2\sqrt{c}$ is az, és így $\sqrt{c}$ is. Könnyű meggondolni, hogy (egész c esetén) $\sqrt{2}\sqrt[4]{c}$ akkor és csak akkor racionális, ha c kanonikus alakjában minden $p > 2$ prím kitevője néggyel osztható, a 2 kitevője pedig $4k-2$ alakú.

Ha $c < 0$, akkor legyen $d = -c > 0$. Ebben az esetben, ismét a $\mathbb{C}$ feletti gyöktényezős alakból kiindulva, az $\mathbb{R}$ fölötti felbontás

$$x^4 - d = (x - \sqrt[4]{d})(x + \sqrt[4]{d})(x^2 + \sqrt{d})\,.$$

Belátjuk, hogy $x^4 - d$ akkor és csak akkor irreducibilis $\mathbb{Q}$ fölött, ha $\sqrt{d}$ irracionális szám. Valóban, $x^4 - d$-nek akkor és csak akkor van racionális gyöke, ha $\sqrt[4]{d}$ racionális szám (ekkor a négyzete, azaz $\sqrt{d}$ is racionális). Ha nincs racionális gyöke, akkor csak két másodfokú, racionális együtthatós polinom szorzatára bomolhat. Ezek közül valamelyiknek gyöke lesz $i\sqrt[4]{d}$, és akkor a konjugáltja is, tehát ez a tényező $q(x^2+\sqrt{d})$ alakú, ahol $q \in \mathbb{C}$. Mivel $q(x^2 + \sqrt{d}) \in \mathbb{Q}[x]$, ezért q és $q\sqrt{d}$ is racionális, tehát $\sqrt{d}$ is az. Megfordítva, ha $\sqrt{d}$ racionális, akkor $(x^2 - \sqrt{d})(x^2 + \sqrt{d})$ jó felbontás.

3.3.17. Test fölött konstans polinom sosem, elsőfokú polinom mindig irreducibilis. A $\mathbb{Z}_2$ fölött összesen két elsőfokú polinom van: x és $x+1$. Mivel $\mathbb{Z}_2$ test, ezek irreducibilisek.

Test fölött egy másod- vagy harmadfokú polinom akkor és csak akkor irreducibilis, ha nincs az adott testben gyöke. A $\mathbb{Z}_2$ elemei 0 és 1, ezek nem szabad tehát, hogy gyökök legyenek. A négy $\mathbb{Z}_2$ fölötti másodfokú polinom közül x^2-nek és x^2+x-nek gyöke a nulla, x^2+1-nek pedig az 1. Tehát az egyetlen másodfokú irreducibilis polinom az x^2+x+1.

Érdemes itt egy pillanatra megállni, és megvizsgálni, hogyan is bomlik fel az x^2+1 polinom alacsonyabb fokúak szorzatára. Mivel az x^2+1-nek az 1 gyöke, az $x-1$ gyöktényező kiemelhető. Már itt problémánk lehet: polinom ez? Hiszen egy $\mathbb{Z}_2[x]$-beli polinomnak minden együtthatója 0 és 1 lehet csak. De tudjuk, hogy a -1 jelentése az 1 ellentettje, vagyis $\mathbb{Z}_2$-ben $-1=1$ (más szóval, pongyolán fogalmazva: „az előjelek nem számítanak"). Vagyis $x-1$ helyett $x+1$-et is írhatunk. A kiemelést például a Horner-eljárással végezve

$$x^2+1=(x+1)(x+1)$$

adódik. Ezt beszorzással is ellenőrizhetjük:

$$(x+1)(x+1)=x^2+x+x+1=x^2+(1+_2 1)x+1=x^2+0\cdot x+1=x^2+1\,.$$

(Ha valaki e számolást nem érzi egészen precíznek, az használja a szorzás elvégzésekor a szorzatpolinom együtthatóját megadó (2.1) képletet a 38. oldalon.) Ugyanígy az is kijön, hogy tetszőleges $f, g \in \mathbb{Z}_2[x]$ polinomokra

$$(f+g)^2=f^2+g^2\,,$$

hiszen $fg+gf=(1+_2 1)fg=0$. Vagyis $\mathbb{Z}_2$ *fölött tagonként lehet négyzetre emelni.* Ezt a hasznos tulajdonságot sokszor kiaknázzuk majd.

Mivel a harmadfokú irreducibilisek is azok, amelyeknek nincs gyöke, ezeket is könnyen felsorolhatjuk. A polinom főtagja x^3, konstans tagja, mivel a 0 nem gyök, csakis 1 lehet. Végül a polinom (nem nulla) tagjainak száma páratlan, különben az 1 gyöke lenne. Így $\mathbb{Z}_2$ fölött két harmadfokú irreducibilis polinom van:

$$x^3+x+1 \qquad \text{és} \qquad x^3+x^2+1\,.$$

A negyedfokú irreducibilis polinomok megkeresése már nem ilyen egyszerű. Persze ezeknek sem lehet $\mathbb{Z}_2$-ben gyöke. Az olyan polinomokat, amelyeknek nincs gyöke, a harmadfokú esethez hasonlóan felsorolhatjuk:

$$x^4+x+1\,, \qquad x^4+x^2+1\,, \qquad x^4+x^3+1\,, \qquad x^4+x^3+x^2+x+1\,.$$

Ezek azonban nem feltétlenül irreducibilisek $\mathbb{Z}_2$ fölött. Tudjuk, hogy a gyök létezése elsőfokú tényezőt jelent, vagyis ha a felsorolt polinomok valamelyike reducibilis, akkor csakis két másodfokú f és g polinom szorzatára bomolhat. Itt f-nek és g-nek nincs gyöke $\mathbb{Z}_2$-ben (hiszen szorzatuknak sincs), és ezért ők irreducibilis, másodfokú polinomok. De már felsoroltuk a másodfokú irreducibilis polinomokat, ezek szerint f és g is csak x^2+x+1 lehet. Szorzatuk,

$$f(x)g(x)=(x^2+x+1)^2=x^4+x^2+1$$

(a négyzetre emelést természetesen tagonként végeztük). Tehát a felsorolt négy polinomból ez az egy nem irreducibilis, a másik három igen.

3.3.18. Ha $0 < i < p$, akkor a

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{1\cdot 2\cdot \dots \cdot i}$$

binomiális együttható p-vel osztható, hiszen a számláló osztható p-vel, a nevező viszont nem (mert p prím, de a nevező egyik tényezőjének sem osztója). Ha egy n szám osztható p-vel, azaz $n = pm$, akkor tetszőleges $r \in R$ elemre

$$nr = (mp)r = m(pr) = m \cdot 0 = 0$$

(felhasználtuk a hatványozásnak a 2.2.18. Gyakorlat (3) pontjában leírt tulajdonságát a többszörös fogalmára átalakítva). A binomiális tételből azt kapjuk, hogy

$$(r+s)^p = r^p + \binom{p}{1} r^{p-1}s + \dots + \binom{p}{p-1} rs^{p-1} + s^p\,.$$

A szereplő binomiális együtthatók a fentiek szerint p-vel oszthatók, és így az összegből csak $r^p + s^p$ marad meg, a többi tag nulla lesz. (Itt természetesen a binomiális tételnek az általános gyűrűkre vonatkozó változatát alkalmaztuk, amelyet a 2.2.37. Gyakorlatban fogalmaztunk meg).

A most bizonyított állításból persze azonnal következik (például a tagok száma szerinti indukcióval), hogy kettőnél több tagú összeget is tagonként emelhetünk p-edik hatványra. A kis Fermat-tétel bizonyításához (modulo p számolva) elég azt megmutatni, hogy $b \in \mathbb{Z}_p$ esetén $b^p = b$. Emeljük p-edik hatványra a b darab 1-esből álló összeget:

$$(1+1+\dots+1)^p = 1^p + 1^p + \dots + 1^p\,.$$

A bal oldalon b^p áll, a jobb oldalon pedig b.

Végül ha $f(x) = a_0 + \dots + a_n x^n \in \mathbb{Z}_p[x]$, akkor, mivel tagonként lehet p-edik hatványra emelni, $f(x)^p = a_0^p + \dots + a_n^p (x^p)^n$. De $a_i \in \mathbb{Z}_p$ miatt $a_i^p = a_i$, és így ez tényleg $f(x^p)$.

3.3.19. A $\mathbb{Z}_2$ fölötti irreducibilitás vizsgálatához érdemes átfutni a 3.3.17. Gyakorlat megoldását, amelyben felsoroltuk a legfeljebb negyedfokú irreducibilis polinomokat, és amelyből kiderül, hogy itt tagonként lehet négyzetre emelni. Ezeket az eredményeket az alábbiakban felhasználjuk.

$x^8 + x^2 + 1 = (x^4 + x + 1)^2$ (tagonkénti „négyzetgyökvonással”), vagyis ez egy irreducibilis polinom négyzete.

$x^5 + x + 1$-nek nincs $\mathbb{Z}_2$-ben gyöke (sem a 0, sem az 1 nem gyök), ezért nincs elsőfokú tényezője. Ha felbomlik, akkor tehát csak egy másod- és egy harmadfokú irreducibilis szorzata lehet. Az egyetlen másodfokú irreducibilis polinom az $x^2 + x + 1$, ezzel osztva a maradék nulla lesz, és $x^5 + x + 1 = (x^3 + x^2 + 1)(x^2 + x + 1)$ adódik.

$x^5 + x^3 + 1$-nek nincs $\mathbb{Z}_2$-ben gyöke, és $x^2 + x + 1$-gyel sem osztható, vagyis irreducibilis.

$x^5 + x^4 + x^3 + 1$-nek gyöke az 1, a gyöktényezőt (például a Horner-elrendezéssel) kiemelve az $(x+1)(x^4+x^2+x+1)$ felbontás adódik. Ez utóbbi tényezőnek ismét gyöke az 1, vagyis $x^5+x^4+x^3+1 = (x+1)^2(x^3+x^2+1)$ a felbontás irreducibilisek szorzatára.

A $\mathbb{Z}_{17}$ fölött a támpontunk a 3.3.18. Feladat, mely szerint $\mathbb{Z}_{17}[x]$-ben tagonként lehet 17-edik hatványra emelni.

$x^2 + 1$ másodfokú, tehát csak a gyökeit kell ellenőrizni, vagyis -1-ből, azaz 16-ból kell négyzetgyököt vonni. Az eredmény nyilván ± 4 ezért $x^2 + 1 = (x + 4)(x - 4) = (x + 4)(x + 13)$.

$x^4 + 1$ ezek szerint $(x^2 + 4)(x^2 - 4)$ alakban írható. A tényezők másodfokúak, tehát ismét a gyökeiket kell megvizsgálni. Nyilván $x^2 - 4 = (x + 2)(x - 2)$. Másfelől a -1 négyzetgyökei ± 4, tehát -4 négyzetgyökei ± 8. Így $x^4+1 = (x+2)(x-2)(x+8)(x-8)$.

$x^8 + 1$ az előzőek szerint $(x^2 + 2)(x^2 - 2)(x^2 + 8)(x^2 - 8)$. Itt is mindegyik négyzetgyökvonás elvégezhető: $x^8+1 = (x+7)(x-7)(x+6)(x-6)(x+3)(x-3)(x+5)(x-5)$.

$x^{17} + 1 = (x + 1)^{17}$, tagonkénti 17-edik hatványra emeléssel.

$x^{17} + 2 = x^{17} + 1 + 1$. Tagonkénti 17-edik „gyökvonással” ez $(x + 2)^{17}$. A kis Fermat-tétel miatt igazából $x^{17} + c = (x + c)^{17}$ minden $c \in \mathbb{Z}_{17}$ esetén.

3.3.20. Ez is hasonló a 3.3.11. Példa megoldásához, azonban van benne egy extra csavar. Az $x^4 - 10x^2 + 1$ polinom négy gyöke $\pm\sqrt{2} \pm \sqrt{3}$, amit a legegyszerűbb úgy ellenőrizni, hogy az

$$(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$$

gyöktényezős felbontásban elvégezzük a beszorzást (ezt mindjárt meg is tesszük majd). Ez tehát az $\mathbb{R}$ feletti felbontás irreducibilisek szorzatára.

A racionális gyökteszt segítségével megállapíthatjuk, hogy az $x^4 - 10x^2 + 1$ polinomnak nincs racionális gyöke (ennél számolósabb közvetlenül kihozni, hogy $\pm\sqrt{2} \pm \sqrt{3}$ irracionális szám). Ha tehát ez a polinom nem lenne irreducibilis $\mathbb{Q}$ fölött, akkor két másodfokú, irreducibilis polinom szorzatára bomolhatna csak.

A 3.3.11. Példa megoldásában két konjugált komplex gyökpár szerepelt, és így egy másodfokú, valós együtthatós tényező gyökei konjugáltak voltak. Most azonban négy valós gyök van, és így elvileg bármely kettőből gyárthatnánk egy másodfokú, racionális együtthatós tényezőt. Nem tehetünk mást, mint hogy ezeket a gyöktényezőket minden lehetséges módon párosítjuk egymással, és elvégezzük a beszorzást. Összesen háromféle párosítás lehetséges. Mindhárom esetben ismét az $(a-b)(a+b) = a^2-b^2$ azonosság felhasználásával egyszerűsíthetjük a számolást. A három eredmény a következő lesz:

$$\begin{aligned}(x^2 - 2\sqrt{2}x - 1)(x^2 + 2\sqrt{2}x - 1) = \\ = (x^2 - 2\sqrt{3}x + 1)(x^2 + 2\sqrt{3}x + 1) = \\ = (x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6})\,.\end{aligned}$$

Mindhárom felbontásban normált, de nem racionális együtthatós polinomok szerepelnek, és így a 3.3.11. Példa gondolatmenete szerint egyik sem ad $\mathbb{Q}$ feletti felbontást. Beláttuk tehát, hogy $x^4 - 10x^2 + 1$ irreducibilis $\mathbb{Q}$ fölött.

Ha $\mathbb{Z}_5$ felett dolgozunk, akkor $\sqrt{6}$ értéke 1 lesz, és így a fenti felbontások közül a harmadik működni fog:

$$x^4 - 10x^2 + 1 = (x^2 - 5 - 2)(x^2 - 5 + 2) = (x^2 - 2)(x^2 + 2)\,.$$

E két tényező már irreducibilis $\mathbb{Z}_5$ felett, hiszen másodfokúak, és $\mathbb{Z}_5$ elemeit végigpróbálhatva látjuk, hogy nincs gyökük. A $\mathbb{Z}_7$ fölött a ±1, ±2, ±3 számokat négyzetre emelve látjuk, hogy a 2-ből vonható négyzetgyök (az eredmény ±3), a 3-ból viszont nem. Ezért ebben az esetben a fenti első felbontás fog működni:

$$x^4 - 10x^2 + 1 = (x^2 - 6x - 1)(x^2 + 6x - 1)\,.$$

E két tényező ismét irreducibilis. Végül $\mathbb{Z}_{11}$ fölött a 3-nak lesz négyzetgyöke (a ±5), és így itt a fenti második felbontás adja a megoldást:

$$x^4 - 10x^2 + 1 = (x^2 - 10x + 1)(x^2 + 10x + 1)\,.$$

Aki ismeri számelméletből a kvadratikus maradékok elméletét (tud bánni az úgynevezett Legendre-szimbólumokkal), az könnyen végiggondolhatja, hogy tetszőleges $p > 3$ prím esetén a 2, 3, 6 számok közül mindig lesz legalább egy, amelyből négyzetgyök vonható modulo p. Így a fenti három felbontás egyike mindig működni fog, vagyis az $x^4 - 10x^2 + 1 \in \mathbb{Z}_p[x]$ polinom minden p-re reducibilis.

Ez azért érdekes, mert a későbbiekben látni fogjuk, hogy egy polinom modulo p vizsgálata sokszor segít az irreducibilitás eldöntésében. A 104. oldalon található táblázatban szerepel több ilyen módszer is, de a fenti polinom irreducibilitását egyik sem bizonyítja (például az eddigiek alapján könnyű belátni, hogy $x^4 - 10x^2 + 1$ semmilyen eltoltjára sem alkalmazható az úgynevezett Schönemann-Eisenstein-kritérium).

3.4. Egész együtthatós polinomok.

3.4.2. Legyen p felbonthatatlan egész szám. Ekkor p nem nulla és nem egység $\mathbb{Z}$-ben (azaz nem ±1). Mivel $\mathbb{Z}[x]$ egységei is ±1 (3.1.11. Gyakorlat), ezért p nem nulla és nem egység $\mathbb{Z}[x]$-ben sem. Meg kell még mutatni, hogy a $\mathbb{Z}[x]$-beli felbontásai is triviálisak. Ha $p = fg$, ahol $f, g \in \mathbb{Z}[x]$, akkor f és g fokainak összege nulla, ezért f és g is konstans polinom. Így a $\mathbb{Z}[x]$-beli és a $\mathbb{Z}$-beli felbontások ugyanazok. Mivel az egységek is ugyanazok ebben a két gyűrűben, a triviális felbontások is ugyanazok lesznek.

3.4.6. Azt a 3.4.5. Következmény bizonyításában láttuk, hogy minden racionális együtthatós polinom felírható rf alakban, ahol r racionális szám, és f primitív, egész együtthatós polinom. Tegyük fel, hogy $rf = sh$, ahol s is racionális szám, és h is primitív, egész együtthatós polinom. Ekkor $h = (r/s)f$, vagyis f osztója h-nak $\mathbb{Q}[x]$-ben. A 3.4.5. Következmény miatt $f \mid h$ teljesül $\mathbb{Z}[x]$-ben is. A szerepeket felcserélve a $h \mid f$ oszthatóságot kapjuk, szintén $\mathbb{Z}[x]$-ben. Tehát f és h tényleg asszociáltak $\mathbb{Z}[x]$-ben. Ebből az is következik, hogy r és s vagy egyenlők, vagy egymás ellentettjei.

3.4.13. $30x^3 - 30 = 2 \cdot 3 \cdot 5 \cdot (x-1) \cdot (x^2 + x + 1)$. Az itt szereplő tényezők közül 2, 3, 5 irreducibilis $\mathbb{Z}$ fölött, mert $\mathbb{Z}$-beli prímek, $x - 1$ mert primitív, és $\mathbb{Q}$ fölött irreducibilis (lévén elsőfokú), végül $x^2 + x + 1$ szintén, azért, mert primitív és $\mathbb{Q}$ fölött irreducibilis (hiszen másodfokú, és nincs racionális gyöke).

3.4.14. A 3.1.11. Gyakorlat szerint R és $R[x]$ egységei ugyanazok. Mivel R nullosztómentes, egy nem nulla konstans R-beli polinom minden felbontása csakis nulladfokú, azaz konstans polinomok szorzatára történhet. Egy ilyen felbontás akkor és csak akkor triviális R-ben, ha $R[x]$-ben az (mert ugyanazok az egységek).

Ezek az észrevételek először is azt mutatják, hogy egy konstans polinom akkor és csak akkor irreducibilis R-ben, amikor $R[x]$-ben. Ha tehát R egy elemét $R[x]$-ben irreducibilisek szorzatára bontjuk, akkor ez egyben egy R-ben irreducibilisek szorzatára történő felbontás is lesz. Így R-ben minden nem nulla és nem egység elem irreducibilisek szorzatára bontható. Mivel az egységek ugyanazok R-ben és $R[x]$-ben, két R-beli elem akkor és csak akkor asszociált R-ben, ha $R[x]$-ben az. Emiatt a felbontás $R[x]$-beli egyértelműségéből az R-beli egyértelműség adódik.

3.4.15. Legyen f nem nulla és nem egység polinom $\mathbb{Z}[x]$-ben. Ha f konstans, akkor a $\mathbb{Z}$-beli irreducibilisekre való felbontása megfelelő lesz. Ha nem konstans, akkor felírható $\mathbb{Q}[x]$-beli irreducibilisek szorzataként. A második Gauss-lemma (3.4.7. Lemma) miatt feltehető, hogy ezek a tényezők egész együtthatósak (és továbbra is irreducibilisek, hiszen ezen egy racionális számmal való szorzás nem változtat). Tehát elég belátni, hogy egy egész együtthatós, $\mathbb{Q}[x]$-ben irreducibilis g polinom felbontható $\mathbb{Z}[x]$-ben irreducibilisek szorzatára.

Írjuk fel a g polinomot nh alakban, ahol n egész szám, és h primitív, egész együtthatós polinom. Az n-et felbonthatjuk a $\mathbb{Z}$-beli alaptétel szerint, a h pedig irreducibilis lesz $\mathbb{Z}$ fölött, mert primitív, és $\mathbb{Q}$ fölött irreducibilis.

3.4.16. Legyen $f = mf_0$ és $g = kg_0$, ahol f_0 és g_0 primitív polinomok. Az m és k egész számokat $\mathbb{Z}$-ben, az f_0 és g_0 polinomokat $\mathbb{Z}[x]$-ben felbonthatjuk irreducibilisek szorzatára, ez utóbbiak tényezői is primitív polinomok lesznek. A 3.1.20. Gyakorlatban láttuk, hogy a kanonikus alakból hogyan lehet megkapni a kitüntetett közös osztót. Ezt alkalmazva adódik, hogy f és g kitüntetett közös osztója nh lesz, ahol n az m és k egész számok legnagyobb közös osztója, h pedig (az első Gauss-lemma első következménye miatt) egy primitív polinom (az f_0 és a g_0 közös irreducibilis tényezőinek a szorzata). Mindezt $\mathbb{Q}$ fölött nézve a konstans szorzók nem számítanak, tehát itt h lesz a kitüntetett közös osztó. Ezért

kapható meg h és n is a leírt módon (itt felhasználtuk, hogy az nh felbontás lényegében egyértelmű a 3.4.6. Gyakorlat miatt).

A $\mathbb{C}[x, y]$-ban is működik ugyanez, csak nem racionális törtekkel, hanem racionális törtfüggvényekkel kell számolni. Vagyis $\mathbb{C}[x, y]$ elemeit x polinomjának képzelve elvégezhetjük az euklideszi algoritmust, az eljárásban fellépő polinomok együtthatói $p(y)/q(y)$ alakú törtek lesznek, ahol $p, q \in \mathbb{C}[y]$. Az f és g együtthatóit is $\mathbb{C}[y]$-beli polinomoknak képzeljük, és így keressük meg a kitüntetett közös osztójukat. Általában ha R alaptételes gyűrű, akkor $R[x]$-ben működik a leírt eljárás, feltéve, hogy R elemeinek már ki tudjuk számítani a kitüntetett közös osztóját.

3.4.17. Ha T test, akkor minden nem nulla eleme egység. Így nincs benne sem irreducibilis, sem prím, de az igaz, hogy minden nullától és egységtől különböző eleme egyértelműen felbontható irreducibilisek szorzatára. (Aki nem hiszi, hozzon ellenpéldát: mutasson egy olyan nem nulla és nem egység elemet T-ben, amely nem bontható fel, vagy a felbontása nem egyértelmű. Senki nem tud ilyen ellenpéldát hozni, mert már nem nulla és nem egység elemet sem fog találni egy testben.)

Annak bizonyításában, hogy alaptételes gyűrű feletti polinomgyűrű is alaptételes, kihasználtuk, hogy test fölötti polinomgyűrű alaptételes (a $\mathbb{Q}[x]$-ben használtuk az alaptételt, amikor $\mathbb{Z}[x]$-et vizsgáltuk), tehát erre nem kaptunk új bizonyítást.

3.5. Irreducibilitás a racionális számtest fölött.

3.5.1. Az állítás közvetlen számolással is igazolható (egy $rx^n = fg$ felbontás tényezőiben a legmagasabb és legalacsonyabb fokú tagok vizsgálatával, a 3.1.35. Gyakorlat mintájára). Elegánsabb azonban a következő gondolatmenet. A $T[x]$ alaptételes gyűrű, amelyben az x irreducibilis polinom (hiszen elsőfokú). Tehát rx^n kanonikus alakban van, és így osztói az x legfeljebb n-edik hatványainak asszociáltjai (lásd 3.1.20. Gyakorlat, (2) pont).

3.5.3. Tegyük fel, hogy az $f(x) = a_0 + \ldots + a_n x^n$ polinom és a p prímszám teljesítik a feltételeket, de f mégsem irreducibilis $\mathbb{Q}$ fölött, vagyis az f-nél alacsonyabb fokú, racionális együtthatós $g(x) = b_0 + \ldots + b_k x^k$ és $h(x) = c_0 + \ldots + c_\ell x^\ell$ polinomok szorzatára bontható (így $k, \ell < n$). A második Gauss-lemma (3.4.7. Lemma) miatt feltehetjük, hogy g és h egész együtthatós.

Mivel $a_n = b_k c_\ell$, a b_k és c_ℓ egészek egyike sem osztható p-vel. Ugyanakkor $a_0 = b_0 c_0$, és mivel a_0 osztható p-vel, de p^2-tel nem, a b_0 és c_0 számok közül pontosan az egyik osztható p-vel. Szimmetriaokokból (g és h esetleges cseréjével) feltehetjük, hogy ez a b_0.

Haladjunk végig a g polinom együtthatóin a b_0-tól kezdve addig, amíg p-vel osztható számot látunk. Legyen i az első olyan index, amelyre b_i nem osztható p-vel. Ilyen i van, hiszen b_0 osztható p-vel, de b_k nem, és persze $0 < i \leq k$. Ekkor az $f = gh$ polinomban az

$$a_i = b_0 c_i + b_1 c_{i-1} + \ldots + b_{i-1} c_1 + b_i c_0$$

együttható nem osztható p-vel, mert az összeg mindegyik tagja osztható vele, kivéve az utolsó tagot. A feltétel szerint f együtthatói oszthatók p-vel, kivéve a_n-et. Ezért $i = n$, azaz $i \le k$ miatt $k \ge n$. Ez ellentmond a $k < n$ feltételnek.

3.5.4. A felsorolt állítások közül csak (4) és (6) igaz!

(1) Ellenpélda: $x^2 + 1$ mod 2 véve.
(2) Ellenpélda: $2x^2 + x$ mod 2 véve.
(3) Ellenpélda: $3x$ mod 5 véve.
(4) Ez az állítás igaz, és a jelenség már a Schönemann-Eisenstein kritérium bizonyításában is előjött. Tegyük fel, hogy f reducibilis, ekkor a második Gauss-lemma miatt felbontható a nála alacsonyabb fokú, egész együtthatós g és h polinomok szorzatára. Amikor egy polinomot mod p veszünk, akkor a fokszáma nem nőhet (de csökkenhet, ha a főegyütthatója p-vel osztható). Tehát ha az $f = gh$ felbontást mod p vesszük, akkor
$$\mathrm{gr}(\overline{g}) \le \mathrm{gr}(g) < \mathrm{gr}(f) = \mathrm{gr}(\overline{f}),$$
és ugyanígy $\mathrm{gr}(\overline{h}) < \mathrm{gr}(\overline{f})$. Tehát mod p is nemtriviális felbontást kapunk.
(5) Ellenpélda: $2x + 1$ mod 2 véve, $k = 1$.
(6) Ez igaz, és a bizonyítás ugyanaz, mint a (4) pontban.

3.5.5. Ha az f polinomot szorzattá lehet bontani: $f = gh$, akkor az összes eltoltjait is ugyanúgy szorzattá bonthatjuk, hiszen $f(x+c) = g(x+c)h(x+c)$ is teljesül. Megfordítva, ha $f(x + c)$ felbontható, akkor az $x \to x - c$ helyettesítéssel f egy felbontását kapjuk.

Általában egy T test fölött az $x \to ax + b$ helyettesítésről is ugyanezt mondhatjuk el. Ennek is van „inverze”: az $f(ax + b)$ polinom egy felbontásából az x helyébe $x/a - b/a$-t írva az f egy felbontását kapjuk. Fontos megjegyezni, hogy eközben a szereplő polinomok foka nem változik, és így nemtriviális felbontásból mindig nemtriviális felbontás adódik.

Az állítás azon múlik, hogy $f(x) \to f(ax + b)$ a $T[x]$ polinomgyűrűnek önmagára menő, kölcsönösen egyértelmű, művelettartó leképezése (azaz izomorfizmusa). Ez a megközelítés azért kényelmesebb a fentinél, mert nem kell azzal foglalkoznunk, hogy a felbontások triviálisak-e! Csak ennyit kell mondanunk: az irreducibilis elem fogalmát a gyűrű műveletei segítségével definiáltuk, tehát izomorfizmusnál irreducibilis elem képe irreducibilis lesz.

Ezen a módon azt is láthatjuk, hogy ha nem test fölött vagyunk, hanem például $\mathbb{Z}[x]$-ben, akkor az „invertálható” helyettesítések, például az $x \to x + c$, megőrzik az irreducibilitást.

3.5.6. Az $f(x) = 1 + x + \ldots + x^{p-1}$ polinomba $x + 1$-et helyettesítve a főegyütthatója nem változik, továbbra is 1 marad. Az $f(x + 1)$ konstans tagját az $x = 0$ helyettesítéssel kaphatjuk meg, látjuk, hogy ez $f(1) = p$, ami p-vel osztható, de p^2-tel nem. Azt kell még belátni, hogy az $f(x + 1)$ polinom összes nem fő együtthatója p-vel osztható, vagyis hogy ezt a polinomot mod p véve x^{p-1} adódik. Ezért áttérünk $\mathbb{Z}_p[x]$-re.

Az ismert azonosság (vagy a mértani sor összegképlete) miatt
$$1 + (x + 1) + \ldots + (x + 1)^{p-1} = \frac{(x + 1)^p - 1}{(x + 1) - 1}.$$

Mivel $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (3.3.18. Feladat), ez tovább így alakítható:

$$\frac{(x+1)^p-1}{(x+1)-1}=\frac{x^p+1^p-1}{x}=x^{p-1}\,.$$

Így az állítást beláttuk.

3.5.7. Tegyük fel, hogy $6x^4+3x+1=f(x)g(x)$, ahol f és g legfeljebb harmadfokú, nem konstans polinomok; a második Gauss-lemma miatt feltehető, hogy egész együtthatósak. Vegyük ezt a felbontást modulo 3. Ekkor a bal oldal a konstans 1 polinom lesz. Mivel $\mathbb{Z}_3$ nullosztómentes, az f és g is nem nulla konstans polinommá válik mod 3 véve. Egyik sem volt konstans eredetileg, tehát mindkettő főegyütthatója hárommal osztható kell, hogy legyen. De akkor szorzatuk főegyütthatója osztható kilenccel, ami nem igaz: ez a főegyüttható ugyanis 6.

3.5.8. Az előző gyakorlat megoldása szó szerint elmondható. Az f-et mod p véve konstans polinomot kapunk, mert minden együtthatója p-vel osztható. Ez a konstans nem nulla, mert az f konstans tagja nem osztható p-vel. Az előző gyakorlat gondolatmenete szerint ekkor f főegyütthatója p^2-tel osztható lenne.

3.5.9. Mindkét állítás bizonyításának kulcsa a következő észrevétel:

$$x^n f(1/x)=x^n(a_n/x^n+\ldots+a_1/x+a_0)=a_n+\ldots+a_1x^{n-1}+a_0x^n=g(x)\,.$$

Innen azonnal látszik, hogy a g gyökei pont az f gyökeinek a reciprokai (a nulla egyik polinomnak sem gyöke, mert a_0 és a_n nem nulla). Ha $b\in T$ az f-nek k-szoros gyöke, és így $f(x)=(x-b)^k h(x)$, akkor

$$g(x)=x^n f(1/x)=x^k\big((1/x)-b\big)^k x^{n-k}h(1/x)=\big((1/b)-x\big)^k b^k x^{n-k}h(1/x)\,,$$

ahol $b^k x^{n-k}h(1/x)$ is polinom, mert h foka $n-k$. Ezért $1/b$ legalább k-szoros gyöke g-nek. Ha $1/b$ a g-nek ℓ-szeres gyöke, akkor tehát $\ell\geq k$. Mivel f és g szerepe szimmetrikus, ugyanígy adódik, hogy $k\geq\ell$, és így a két multiplicitás megegyezik.

Ha $f(x)=p(x)q(x)$, ahol $p\in T[x]$ foka $k<n$, és $q\in T[x]$ foka $\ell<n$, akkor

$$g(x)=x^k p(1/x)\cdot x^\ell q(1/x)$$

a g-nek lesz felbontása ugyanilyen fokú polinomok szorzatára, és így g is reducibilis. Az f és g szimmetriája miatt tehát ez a két polinom ugyanakkor irreducibilis.

3.5.11. A megoldás ugyanaz, mint az x^4+x^2+x+1 polinom esetében, mert annál a számolásnál az x^2-es tag együtthatójából kapott egyenletet nem használtuk ki. De most más megoldás is kínálkozik: ez a polinom $\mathbb{Z}_2$ fölött irreducibilis (3.3.17. Gyakorlat), és mivel a főegyütthatója páratlan, irreducibilis $\mathbb{Q}$ fölött is (lásd 3.5.4. Gyakorlat, (4) pont).

3.5.12. Csak olyan prímszámokat érdemes nézni, amelyek a polinom nem fő együtthatóinak közös osztói. Így az $x^{11} + 2x + 18$ esetében csak a $p = 2$ jön szóba, és ez meg is felel, mert a 18 is páros, de nem osztható $p^2 = 4$-gyel. Ezért ez a polinom irreducibilis $\mathbb{Q}$ fölött (és mivel primitív, $\mathbb{Z}$ fölött is). Az $x^{11} + 2x + 12$ polinomnál is csak a $p = 2$ jön szóba, de ez sem megfelelő, mert 4 osztója a konstans tagnak, azaz 12-nek. Erre a polinomra tehát nem alkalmazható a Schönemann-Eisenstein-kritérium. ***Ebből azonban nem következik, hogy a polinom reducibilis!*** Az irreducibilitást ezen a módon nem sikerült eldönteni, tehát egy másik módszerrel kell próbálkoznunk.

Ugyanígy folytatva látjuk, hogy $x^{11} + 12x + 5$ esetében sem alkalmazható a kritérium (most nincs is közös prímosztója a nem fő együtthatóknak). Az $x^{11} + n$ polinomra akkor és csak akkor alkalmazható a kritérium, ha az n szám kanonikus alakjában van olyan prím, ami az első kitevőn szerepel. Vagyis $n = 24$ megfelelő ($p = 3$), de $n = 72$ nem.

3.5.13. Komplex fölött pontosan az elsőfokú polinomok irreducibilisek, tehát a három felsorolt polinom egyike sem az. Valós fölött az elsőfokú polinomok mellett azok a másodfokúak irreducibilisek, amelyeknek nincs valós gyöke. Ezért $x^2 + x + 1$ irreducibilis, de $x^7 + x + 1$ és $x^2 - 2$ nem az.

Mivel $\mathbb{Z}$ fölött egy nem konstans polinom akkor irreducibilis, ha primitív, és irreducibilis $\mathbb{Q}$ fölött, $3x^7 + 6x - 18$ nem irreducibilis $\mathbb{Z}$ fölött. A többi (3)-beli polinom primitív, és így a feladatban felsorolt összes polinomot a $\mathbb{Q}$ fölötti irreducibilitás szempontjából kell megvizsgálni; a megoldás hátralévő részében az „irreducibilis" és „reducibilis" szavakat ebben az értelemben használjuk.

Noha körosztási polinomokról még nem volt szó, egy esetleges későbbi ismétlés kedvéért megjegyezzük, hogy az alábbiakban szereplő polinomok közül $\Phi_{32}(x) = x^{16} + 1$, $\Phi_{12}(x) = x^4 - x^2 + 1$ és $\Phi_8(x) = x^4 + 1$ körosztási polinomok, és így a 3.9.8. Tétel miatt (is) irreducibilisek.

$3x^7 - 6x^6 + 6x^2 + 3x - 2$: irreducibilis, fordított Schönemann-Eisenstein ($p = 3$).

$3x^7 + x^6 + 6x^2 + 2x - 2$: reducibilis, a -1 gyöke (ez a racionális gyökteszt segítségével található meg).

$3x^7 - 6x^6 + 6x^2 + 2x - 2$: irreducibilis, Schönemann-Eisenstein ($p = 2$).

$x^{16} + 1$: irreducibilis, $x \to x + 1$ helyettesítés után Schönemann-Eisenstein $p = 2$-re. Ennek kiszámítását a 3.5.6. Feladat mintájára érdemes elvégezni (lásd 3.9.23. Gyakorlat).

$x^{16} + 2$: irreducibilis, Schönemann-Eisenstein ($p = 2$).

$x^4 - 14x^2 + 9$: irreducibilis, a 3.3.20. Feladat módszerével. A gyökei $\pm\sqrt{2} \pm \sqrt{5}$.

$x^4 - x^2 + 1$: irreducibilis, a 3.3.16. Gyakorlat módszerével. A gyökei a tizenkettedik primitív egységgyökök, az $\mathbb{R}$ feletti felbontása $(x^2 - \sqrt{3}x + 1)(x^2 + \sqrt{3}x + 1)$.

$3x^7 + 6x - 18$: irreducibilis, Schönemann-Eisenstein ($p = 2$).

$x^5 + 4$: irreducibilis, $x \to x + 1$ helyettesítés után Schönemann-Eisenstein ($p = 5$).

$x^3 + 9$: irreducibilis, mert harmadfokú, és nincs racionális gyöke (az egyetlen valós gyöke a $-\sqrt[3]{9}$, irracionális szám).

$x^3 + 3$: irreducibilis, Schönemann-Eisenstein $p = 3$-ra.

$x^{10}-x^5+1$: reducibilis, x^2-x+1 osztója. Ezt úgy lehet megtalálni, hogy $y=x^5$ helyettesítéssel megkeressük a gyököket. Mivel $y^2-y+1=0$, az y a két primitív hatodik egységgyök, η_1 és η_2 egyike lesz, ezekből kell ötödik gyököt vonni. De $\eta_1^5=\eta_2$ és $\eta_2^5=\eta_1$, így $x^{10}-x^5+1$-nek is gyöke η_1 és η_2, tehát osztható $(x-\eta_1)(x-\eta_2)=x^2-x+1$-gyel.

$x^{10}+10$: irreducibilis, Schönemann-Eisenstein ($p=2$).

x^4+25: irreducibilis, a 3.3.16. Gyakorlat eredménye szerint.

x^4+2: irreducibilis, Schönemann-Eisenstein ($p=2$).

x^4+4x+1: irreducibilis, $x\to x+1$ helyettesítés után Schönemann-Eisenstein ($p=2$).

x^4-2x+1: reducibilis, az 1 gyöke.

$2x^4+2x^2+1$: irreducibilis, fordított Schönemann-Eisenstein ($p=2$).

$x^6-10x+10$: irreducibilis, Schönemann-Eisenstein ($p=5$).

$x^4+x^3+x^2+1$: irreducibilis, ez a 3.5.10. Példában szereplő polinomhoz tartozó reciprok polinom (lásd 3.5.9. Feladat).

$x^4+2x+27$: irreducibilis, $x\to x+1$ helyettesítés után Schönemann-Eisenstein ($p=2$).

x^6+1: reducibilis, az ismert azonosság szerint $(x^2+1)(x^4-x^2+1)$.

x^3+7x-3: irreducibilis, mert harmadfokú, és a racionális gyökteszt miatt nincs racionális gyöke.

$x^4+3x^3+x^2+1$: reducibilis, a -1 gyöke.

3.5.14. Legyen h többszöröse f-nek $\mathbb{Z}[x]$-ben. Megmutatjuk, hogy $f(x)\mid f\big(x+h(x)\big)$. Valóban, ha $f(x)=a_0+\ldots+a_nx^n$, akkor

$$f\big(x+h(x)\big)-f(x)=(a_0-a_0)+\ldots+a_n\big(x+h(x)\big)^n-a_nx^n\,.$$

Az $a-b\mid a^k-b^k$ összefüggés miatt $\big(x+h(x)\big)^k-x^k$ osztható $x+h(x)-x=h(x)$-szel, és így $f(x)$-szel is. Ezért $f(x)\mid f\big(x+h(x)\big)-f(x)$, ahonnan $f(x)\mid f\big(x+h(x)\big)$.

Ebből már láthatjuk, hogy a keresett f polinom nem létezik. Az f nem lehet konstans, mert akkor $f\big(g(x)\big)$ is az, és így nem irreducibilis $\mathbb{Q}$ fölött. Ha viszont f nem konstans, akkor az előző bekezdésben bizonyított állítás $h(x)=xf(x)$ és $g(x)=x+h(x)$ választással ellentmondásra vezet: ekkor $f\big(g(x)\big)=f\big(x+h(x)\big)$ osztható f-fel, és így csak akkor lehetne irreducibilis, ha f konstansszorosa lenne, de a foka nagyobb f fokánál: pontosan $(\mathrm{gr}(f)+1)\mathrm{gr}(f)$, mert kompozíció foka a tényezők fokainak szorzata.

3.5.15. Az $f(x,y)=x^9+x^3y^3+(y^2+y)$ már rendezve van x hatványai szerint, a nem nulla együtthatók 1, y^3, y^2+y relatív prím polinomok $\mathbb{C}[y]$-ban, hiszen az 1 közöttük van: minden normált polinom nyilvánvalóan primitív.

A Schönemann-Eisenstein alkalmazható f-re, mint x polinomjára, a $p=y$ választással. Ez a p prím lesz $\mathbb{C}[y]$-ban, hiszen a $\mathbb{C}[y]$ alaptételes gyűrű, amelyben az y elsőfokú, és így irreducibilis polinom (hiszen $\mathbb{C}$ test). A fenti együtthatók mindegyike y-nal osztható, kivéve a főegyütthatót, vagyis az 1-et, és y^2 nem osztója a konstans tagnak, azaz y^2+y-nak. A Schönemann-Eisenstein tétel minden alaptételes gyűrű fölött ugyanúgy bizonyítható, és így f irreducibilis a $\mathbb{C}[y]$ elemeinek a hányadosaiból álló gyűrű fölött.

Mivel f, mint x polinomja, primitív, a 3.4.8. Tétel általános változata miatt f irreducibilis lesz $\mathbb{C}[y]$ fölött is, azaz $\mathbb{C}[x, y]$-nak ez egy irreducibilis eleme.

3.5.16. Tegyük föl, hogy $\sqrt[3]{4} = a + b\sqrt[3]{2}$, és legyen f az $x^3 - 2$ és az $x^2 - ax - b$ polinomok kitüntetett közös osztója. Mivel $x^3 - 2$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és $f \mid x^3 - 2$, ezért f vagy konstans, vagy $x^3 - 2$ konstansszorosa. Ez utóbbi lehetetlen, mert f osztója a másodfokú $x^2 - ax - b$ polinomnak, és így foka legfeljebb kettő. Tehát f nem nulla konstans polinom.

Az f polinom $\mathbb{C}$ fölött is kitüntetett közös osztó (3.2.5. Gyakorlat). Az $x^3 - 2$ és az $x^2 - ax - b$ polinomoknak $\sqrt[3]{2}$ közös gyöke, és ezért ez gyöke f-nek is (3.2.13. Állítás). Ez lehetetlen, mert f konstans polinom.

3.5.17. Keressük meg az $f \in \mathbb{Z}[x]$ összes legfeljebb k-adfokú g osztóját $\mathbb{Z}[x]$-ben a következőképpen. Mivel $f = gh$ alkalmas $h \in \mathbb{Z}[x]$ polinomra, $f(m) = g(m)h(m)$ minden m egészre, és így $g(m) \mid f(m)$. Ez azt jelenti, hogy $g(m)$ értékére csak annyi lehetőségünk van, amennyi az $f(m)$ osztóinak a száma, azaz $f(m) \neq 0$ esetén véges sok.

Rögzítsük tehát az $a_0, \ldots, a_k$ egész helyeket úgy, hogy egyikük se legyen gyöke az f polinomnak. Az összes lehetséges módon válasszuk ki a $b_0, \ldots, b_k$ értékeket úgy, hogy $b_i \mid f(a_i)$ minden i-re teljesüljön. Minden ilyen $b_0, \ldots, b_k$ értékrendszerhez írjuk fel azt az (egyértelműen meghatározott, legfeljebb k-adfokú) $g \in \mathbb{Q}[x]$ interpolációs polinomot, amelyre $g(a_i) = b_i$. Ellenőrizzük, hogy a kapott g egész együtthatós-e, illetve hogy osztója-e f-nek. Így megkapjuk az összes lehetséges legfeljebb k-adfokú osztót. Természetesen a keletkező $b_0, \ldots, b_k$ értékrendszerek hatalmas száma miatt az eljárás nem hatékony, és akkor még nem is beszéltünk arról a (szintén nagyon sok számolással járó) problémáról, amit az egyes $f(a_i)$ számok összes osztójának meghatározása jelent. De annyit beláttunk, hogy a kívánt eljárás *létezik*.

Az eljárással meg tudjuk állapítani a $\mathbb{Q}$ fölötti irreducibilitást is. Valóban, legyen f egy nem konstans, racionális együtthatós polinom. Ekkor alkalmas $n \in \mathbb{Z}$-re nf már egész együtthatós, ami ugyanakkor irreducibilis, mint az f. A második Gauss-lemma miatt viszont nf akkor és csak akkor irreducibilis $\mathbb{Q}$ fölött, ha nem bomlik alacsonyabb fokú, egész együtthatós polinomok szorzatára.

3.6. A derivált és a többszörös gyökök.

3.6.6. A deriváltja $6x^5 + 5x^4 + 20x^2 + 12x^2 + 16x + 4$, ennek és az eredeti polinomnak a kitüntetett közös osztója az euklideszi algoritmussal kiszámolva $x^2 + 2$. Tehát f-nek két többszörös gyöke van, ezek $x^2 + 2$ gyökei, vagyis $\pm\sqrt{2}i$, mindegyik kétszeres.

3.6.7. A $3x^2$ jelentése $x^2 + x^2 + x^2$. Ezt a polinomok közötti műveletek definíciója szerint úgy kell kiszámítani, hogy az x^2 együtthatóját (amit nem írtunk ki, mert az értéke 1), önmagával kell háromszor összeadni. Ez az együttható a $\mathbb{Z}_2$ gyűrű eleme, amelyben $1 +_2 1 +_2 1 = 1$. Ezért $3x^2 = 1x^2 = x^2$. Szó sincs tehát arról, hogy $3x^2$ azért lenne x-szel egyenlő, mert mindegyik $x \in \mathbb{Z}_2$-re ugyanazt az értéket veszi föl.

A második gondolatmenetben az a hiba, hogy összekeveredik a polinom és a polinomfüggvény fogalma. Az idézőjeles gondolatmenet csak azt bizonyítja, hogy az x^2 és x polinomokhoz tartozó *polinomfüggvények* egyenlőek. A $\mathbb{Z}_2[x]$ polinomgyűrűben az x határozatlannal formálisan, az együtthatóival modulo 2 kell számolni.

Ez a példa azt is mutatja, hogy $\mathbb{Z}_2$ fölött nincs értelme polinomfüggvény deriváltjáról beszélni. Hiszen mi is lenne az identikus leképezésnek, mint polinomfüggvénynek a deriváltja? Ezt a polinomfüggvényt az x és az x^2 polinom is megvalósítja. Ezeknek a deriváltja 1, illetve $2x = 0$, és az ezekhez tartozó polinomfüggvények különbözők. Szóval akkor az identitás deriváltja konstans 1, vagy konstans 0 legyen?

3.6.8. Ilyen például $x^9 + x^8$ a $\mathbb{Z}_2$ fölött. A 3.6.3. Állítás bizonyításából látszik, hogy általában olyan $f(x) = (x - b)^8 q(x)$ polinomot érdemes keresni, amelyre $8q(b) = 0$ (de $q(b)$ és $q'(b)$ nem nulla).

3.6.9. Tegyük fel, hogy b az f-nek pontosan ℓ-szeres gyöke, ahol tehát $\ell \geq 1$. Ekkor (a 3.6.4. Tétel szerint) f'-nek a b pontosan $\ell - 1$-szeres gyöke. Tehát $\ell - 1 = k - 1$, vagyis $\ell = k$. Ez a tétel tehát „önmagában hordja a megfordítását".

Az állítás $\mathbb{Z}_2$ fölött nem igaz: az $x^3 + x^2$ polinomnak csak kétszeres gyöke a nulla, annak ellenére, hogy ez a polinom deriváltjának is kétszeres gyöke.

3.6.10. A 3.6.4. Tétel ismételt alkalmazásával világos, hogy ha b az f-nek legalább k-szoros gyöke, akkor a $k - 1$-edik deriváltjának legalább egyszeres gyöke, és így közös gyöke f-nek és a $k - 1$-edik deriváltjának.

Az állítás megfordítása még $\mathbb{C}$ fölött sem igaz. Például az $x^3 + x$ polinomnak az x csak egyszeres gyöke, de a második deriváltnak szintén gyöke.

Ha azt tesszük fel, hogy b gyöke az f első $k - 1$ deriváltjának, és $\mathbb{C}$ fölött vagyunk, akkor az előző gyakorlat állításának az ismételt alkalmazásával adódik, hogy f-nek b legalább k-szoros gyöke. Ugyanez $\mathbb{Z}_2$ fölött nem igaz: ismét $x^3 + x^2$ lesz ellenpélda $k = 3$ esetén.

3.6.11. Ha egy b komplex szám az f-nek k-szoros gyöke, akkor f'-nek $k-1$-szeres gyöke. Vagyis az $x-b$ irreducibilis polinom kitevője az f kanonikus alakjában k, az f'-ében $k-1$. A kitüntetett közös osztó képlete szerint tehát $x - b$ kitevője (f, f')-ben is $k - 1$, azaz b az (f, f')-nek is pontosan $k-1$-szeres gyöke. Így $f_1 = f/(f, f')$-ben az $(x-b)$ irreducibilis tényező kitevője $k - (k - 1) = 1$ lesz. Más szóval f_1 gyökei ugyanazok, mint az f gyökei, de mindegyik egyszeres, és persze f_1 is racionális együtthatós (a 3.2.5. Gyakorlat miatt).

Ezt a gondolatot alkalmazhatjuk f helyett az (f, f') polinomra is. Mivel ennek gyökei éppen az f legalább kétszeres gyökei, ezért egy szintén racionális együtthatós f_2 polinomot kapunk, amelynek gyökei az f legalább kétszeres gyökei, de mindegyik csak egyszer.

Nyilván $g_1(x) = f_1(x)/f_2(x)$ egy olyan racionális együtthatós polinom, amelynek gyökei az f egyszeres gyökei, mindegyik egyszer.

Ezután az állítást k szerinti indukcióval bizonyíthatjuk, a $k = 1$ esetet most láttuk be. Ha $k-1$-re már tudjuk az állítást, akkor alkalmazzuk ezt az (f, f') polinomra. Így egy olyan $h(x) \in \mathbb{Q}[x]$ polinomot kapunk, amelynek gyökei pont az (f, f') polinom $k-1$-szeres gyökei, mindegyik egyszer. De akkor h a keresett g_k polinom, hiszen egy komplex szám akkor és csak akkor k-szoros gyöke f-nek, ha $k-1$-szeres gyöke (f, f')-nek.

3.6.12. Ha $f = g^2h$, akkor a szorzat deriválási szabálya szerint $(g^2)' = 2gg'$, és így

$$f' = (g^2)'h + g^2h' = g(2g'h + gh') .$$

Ezért g közös osztója f-nek és f'-nek.

Az $x^n - 1$ deriváltja nx^{n-1}. Ha p nem osztója n-nek, akkor ez nem a nullapolinom $\mathbb{Z}_p[x]$-ben, és így minden osztója sx^k alakú, ahol $0 \neq s \in \mathbb{Z}_p$ (lásd 3.5.1. Gyakorlat). De sx^k csak akkor lehet osztója $x^n - 1$-nek, ha konstans (azaz ha $k = 0$), mert $x^n - 1$-nek nem gyöke a 0. Ezért ($p \nmid n$ esetén) $x^n - 1$ relatív prím a deriváltjához, és így nem lehet többszörös tényezője.

Ha viszont $p \mid n$, mondjuk $n = pm$, akkor $\mathbb{Z}_p[x]$-ben

$$x^n - 1 = (x^m - 1)^p .$$

Ez közvetlenül adódik abból, hogy $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (3.3.18. Feladat). Ugyanis ekkor $(x^m - 1)^p = x^n + (-1)^p$, és $p > 2$ esetén $(-1)^p = -1$, mert p páratlan, ha meg $p = 2$, akkor $(-1)^2 = 1$, de ez -1 is, mert $\mathbb{Z}_2$-ben $-1 = 1$. Vagyis $x^n - 1$-nek pontosan $p \mid n$ esetén van többszörös tényezője.

3.6.13. Legyen $f \in S[x]$ egy S fölött irreducibilis polinom, ahol S test, és legyen $h \in S[x]$ az f és f' kitüntetett közös osztója. Tegyük fel, hogy f-nek van többszörös gyöke egy S-nél bővebb T testben. Ekkor (f, f') ebben a nagyobb testben kiszámítva nem konstans. A 3.2.5. Gyakorlat szerint azonban f és f' kitüntetett közös osztója nem függ attól, hogy melyik testben számítjuk ki. Tehát h nem konstans, és mivel osztója az irreducibilis f polinomnak, h és f asszociáltak $S[x]$-ben. Ugyanakkor $h \mid f'$, vagyis beláttuk, hogy $f \mid f'$. Ha $f' \neq 0$, akkor f' foka kisebb f foknál, és így f nem oszthatja f'-t. Tehát csak az $f' = 0$ eset az, ami egyáltalán előfordulhat.

Ha $S = \mathbb{Q}$, akkor ez lehetetlen, hiszen ekkor f konstans polinom lenne, márpedig f-ről föltettük, hogy nem konstans (hiszen irreducibilis).

Ha $S = \mathbb{Z}_2$, és $f(x) = a_0 + \ldots + a_nx^n$, akkor

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1} = 0$$

akkor és csak akkor teljesül, hogy f páratlan indexű együtthatói nullával egyenlők, vagyis

$$f(x) = a_0 + a_2x^2 + \ldots + a_{2k}x^{2k}$$

alakú. Vegyük észre, hogy $a_i^2 = a_i$ (hiszen $a_i \in \mathbb{Z}_2$). Mivel $\mathbb{Z}_2$ fölött tagonként lehet négyzetre emelni (3.3.18. Feladat),

$$f(x) = (a_0 + a_2x + \ldots + a_{2k}x^k)^2 .$$

Ez ellentmond annak, hogy f irreducibilis. Tehát ilyen f polinom $\mathbb{Z}_2$ fölött sincs. Megjegyezzük, hogy ugyanez a gondolatmenet $\mathbb{Z}_2$ helyett szó szerint ugyanígy $\mathbb{Z}_p[x]$-ben is elmondható.

3.6.14. Érdemes általában meggondolni (például n szerinti indukcióval), hogy

$$(f_1 f_2 \ldots f_n)' = \sum_{i=1}^{n} f_1 \ldots f_{i-1} f_i' f_{i+1} \ldots f_n .$$

Ennek az állítás speciális esete, amikor $f_i(x) = x - b_i$ (pontosabban még minden meg van szorozva c-vel). A második állítás az elsőből a b_i behelyettesítésével adódik, hiszen csak egyetlen tagja lesz az összegnek, ami nem (feltétlenül) válik nullává.

3.6.15. Mivel f legalább másodfokú, f' legalább elsőfokú, és így az algebra alaptétele miatt van egy komplex b gyöke. Ekkor $c = -f(b)$ megfelelő lesz. Ehhez a 3.6.5. Következmény miatt elég megmutatni, hogy b közös gyöke $f(x) - f(b)$-nek és a deriváltjának. Ez azonban nyilvánvaló, hiszen ez a derivált $f'(x)$.

3.6.16. Az $f(x)$ a c értéket akkor és csak akkor veszi fel n-nél kevesebb helyen, ha az $f(x) - c$ polinomnak n-nél kevesebb komplex gyöke van, azaz ha van többszörös gyöke. Ez azt jelenti, hogy van egy közös b gyöke a deriváltjával, ami $f'(x)$. Tehát $f'(b) = 0$, és $f(b) = c$. Tehát a kivételes c értékek száma legfeljebb annyi, mint f' komplex gyökeinek a száma, ami legfeljebb $n - 1$, hiszen f' egy $n - 1$-edfokú polinom.

3.7. A rezultáns és a diszkrimináns.

3.7.3. Ott használtuk ki, amikor f-et $f(x) = a_n(x - \alpha_1) \ldots (x - \alpha_n)$ alakban írtuk fel, később már nem.

Legyen $f(x) = 0x^2 + x - 1$ és $g(x) = x + 1$. E két polinom rezultánsa nem nulla. Ugyanakkor f egyetlen gyöke az $\alpha_1 = 1$, továbbá $n = 2$, $m = 1$, $a_n = 0$, és a $0^1 g(1)$ képlet nullát ad eredményül, vagyis az Állítás nem teljesül.

3.7.10. A determinánst például az utolsó sora szerint kifejtve

$$R(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = (-2a)(-2ac) + b(ab - 2ab) = 4a^2c - ab^2 .$$

A diszkrimináns a 3.7.7. Definíció szerint ennek $(-1)^1/a$-szorosa, azaz tényleg $b^2 - 4ac$. A 3.7.9. Állítás szerint ez akkor és csak akkor pozitív, ha minden gyök egyszeres, és a nem valós gyökök száma néggyel osztható. Mivel maximum két gyök van, ez a szám csak úgy lehet néggyel osztható, ha nulla, vagyis mindkét gyök valós. A diszkrimináns akkor és csak

akkor nulla, ha a polinomnak egyetlen, kétszeres gyöke van. Ez természetesen csak valós szám lehet, hiszen különben a konjugáltja egy újabb gyöke lenne a polinomnak.

3.7.11. A diszkrimináns (a sok nulla miatt a determinánst ismételt kifejtéssel kiszámolva)

$$(-1)^3 R(f, f') = -\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = -4p^3 - 27q^2 .$$

Ennek a diszkussziója a 3.8.2. Tételben található.

3.7.13. Az első egyenletrendszerben a két egyenletet y polinomjának tekintve a rezultánsuk

$$r(x) = \begin{vmatrix} x-1 & x+1 & -2 & 0 \\ 0 & x-1 & x+1 & -2 \\ x-1 & x & -1 & 0 \\ 0 & x-1 & x & -1 \end{vmatrix} = 2(x-1)^2 .$$

Tudjuk, hogy ha (x_1, y_1) közös gyöke az eredeti két egyenletnek, akkor x_1 gyöke a rezultánsnak. A rezultánsnak csak az $x = 1$ gyöke. Azonban ez nem biztos, hogy közös gyökből származik, hiszen a rezultáns akkor is nulla, ha $a_n = b_m = 0$ (és jelenleg ez teljesül, hiszen $a_n = b_m = x - 1$). Tehát az $x = 1$ értéket „kézzel" kell megvizsgálni. Ha $x = 1$, akkor az első egyenlet a $2y - 2 = 0$, a második az $y - 1 = 0$ alakot ölti. Ezeknek $y = 1$ közös gyöke, és így az egyenletrendszer egyetlen megoldása $(x, y) = (1, 1)$.

A második egyenletrendszer esetében a rezultáns $1 - x$ lesz. Az érvelés most is ugyanaz, de most az $x = 1$ hamis gyök, mert ezt visszahelyettesítve a $2y = 1$ és $y = 1$ egyenleteket kapjuk, és ezeknek nincs közös gyöke. A második egyenletrendszernek tehát nincs megoldása.

A harmadik egyenletrendszerben először x-et tekintjük változónak. Az első két egyenlet rezultánsa $f(y, z) = y^4 - (2z + 2)y^2 - y + (z^2 + z)$. Szimmetriaokokból az első és a harmadik egyenlet rezultánsa (y és z cseréjével) $g(y, z) = y^2 + (-2z^2 + 1)y + (z^4 - 2z^2 - z)$. Az f és g rezultánsa, rögtön szorzattá alakítva

$$z^5(z + 1)^4(z - 1)^2(z - 2)(z^2 + 2z + 2)(z^2 - 2z - 1) .$$

Azt gondolhatnánk, hogy ennek mindegyik gyöke megoldáshoz vezet, hiszen végig normált polinomok rezultánsát vettük, a főegyütthatóknak nem volt gyöke, és így nem jöhetett be „hamis" gyök. De ez tévedés! Például a $z = 2$ gyöke a fenti polinomnak. Ez annyit jelent, hogy az $f(y, 2)$ és a $g(y, 2)$ polinomoknak van közös gyöke. Valóban van: az $y = 1$ (és csak ez). Tehát ha $y = 1$ és $z = 2$, akkor az egyenletrendszer első két egyenletének is kell legyen közös gyöke x-re. Van is: az $x = -2$ (és más nem). Ugyanígy a második két egyenletnek is kell legyen közös gyöke, ez viszont csak az $x = -2$ lesz. Ez az oka annak, hogy a $z = 2$ végülis nem vezet az egyenletrendszer megoldásához.

Az összes gyököt ugyanígy végigszámolni nagyon fáradságos volna. Egyszerűbb megoldáshoz vezet, ha az f polinom helyett az egyenletrendszer második és harmadik egyenletének a rezultánsát számoljuk ki, ez $h(x, y) = y^2 + y - (z^2 + z)$. A g és a h rezultánsa ugyanis

$$z^4(z+1)^2(z^2-2z-1)$$

(ezt szorzattá alakítani is sokkal egyszerűbb, mint a fenti polinomot, hiszen csak a racionális gyöktesztre van ehhez szükség). A fentiek szerint ennek is valamennyi gyökét ellenőrizni kell. A végeredmény a következő: a megoldások egyrészt azok, ahol két ismeretlen értéke nulla, a harmadik pedig -1, másrészt azok, ahol $x = y = z$ a $z^2 - 2z - 1$ egyenlet valamelyik gyökével (azaz $1 \pm \sqrt{2}$-vel) egyenlő.

3.8. A harmad- és negyedfokú egyenlet.

3.8.3. Tegyük föl először, hogy $q^2 - 4pr = 0$. Ha $p \neq 0$, akkor $p^2 - 4qr$ a polinom diszkriminánsa. Mivel ez nulla, van kétszeres gyök, így a polinom $p(x-\alpha)^2$ alakú. Itt persze a $p \in \mathbb{C}$ számból is vonható négyzetgyök. Ha viszont $p = 0$, akkor $p^2 = 4qr$ miatt $q = 0$, vagyis a polinom konstans, és így ismét teljes négyzet.

Megfordítva, ha a polinom teljes négyzet, akkor vagy egy konstans polinom négyzete, vagy egy elsőfokúé. Az első esetben konstans polinomról van szó, tehát $q^2 = 4pr = 0$. A második esetben a polinom másodfokú, és mivel egy elsőfokú polinom négyzete, van kétszeres gyöke. Ezért a diszkriminánsa nulla kell, hogy legyen.

Ha $\mathbb{C}$ helyett $\mathbb{Q}$ fölött vizsgáljuk a kérdést, akkor az állítás a következőképpen módosul. A $px^2 + qx + r \in \mathbb{Q}[x]$ polinom akkor és csak akkor négyzete egy $\mathbb{Q}[x]$-beli polinomnak, ha vagy $p = q = 0$ és r egy $\mathbb{Q}$-beli elem négyzete, vagy $p \neq 0$ egy $\mathbb{Q}$-beli elem négyzete és $q^2 - 4pr = 0$. A bizonyítás ugyanaz, mint az előbb, csak most figyelni kell arra is, hogy nem minden racionális számból vonható négyzetgyök.

3.8.5. A szokásos módon D jelöli a Cardano-képletben a négyzetgyök alatti kifejezést.

(1) $x^3 - 6ix - i + 8 = 0$: ennél az egyenletnél D szerencsére teljes négyzet, hiszen $D = (8 - i/2)^2 - (2i)^3 = (8 + i/2)^2$. Innen azt kapjuk, hogy $u = \cos 30^\circ + i \sin 30^\circ$ és $v = 2i/u = 2(\cos 60^\circ + i \sin 60^\circ)$, a gyökök $(1 + \sqrt{3}/2) + (1/2 + \sqrt{3})i$, $(1 - \sqrt{3}/2) + (1/2 - \sqrt{3})i$ és $-2 - i$.

(2) $x^3 + 12x - 16i = 0$: ebben az esetben $D = 0$, innen $u = 2(\cos 30^\circ + i \sin 30^\circ)$, $v = -4/u = 2(\cos 150^\circ + i \sin 150^\circ)$, $x^3 + 12x - 16i = (x - 2i)^2(x + 4i)$, azaz a $2i$ kétszeres gyök.

(3) $x^3 - 21x + 20 = 0$: ennél az egyenletnél $D = -243$, és így nemtriviális feladat a köbgyökvonás. Trigonometrikus alakban közelítőleg elvégezhetjük (kalkulátorral végezve a trigonometrikus alakra való oda- és visszakonvertálást), ekkor $u = \sqrt{7}(\cos\alpha + i \sin\alpha)$ adódik, ahol $\alpha \approx 40,893^\circ$. Az 1.2. Szakaszban ezt az egyenletet megoldottuk: u értéke valójában $2 + i\sqrt{3}$, a gyökök 4, 1 és -5.

(4) $x^4 + x^2 + 4x - 3 = 0$: a harmadfokú rezolvens $8u^3 - 4u^2 + 24u - 28$, aminek szerencsére gyöke az 1. Ennek alapján az egyenlet két másodfokú polinom szorzataként $(x^2+1)^2 - (x-2)^2 = (x^2 - x + 3)(x^2 + x - 1)$ alakban írható, gyökei tehát $(1 \pm i\sqrt{11})/2$ és $(-1 \pm \sqrt{5})/2$.

3.8.6. A harmadfokú rezolvens $(8u + 40)(u^2 - 1)$, ennek gyökei $u = 1$, $u = -1$, $u = -5$. Ezekből rendre az $x^4 - 10x^2 + 1$ polinom következő felbontásait kapjuk:

$$(x^2+1)^2 - 12x^2 = (x^2 - 2\sqrt{3}x + 1)(x^2 + 2\sqrt{3}x + 1)$$
$$(x^2-1)^2 - 8x^2 = (x^2 - 2\sqrt{2}x - 1)(x^2 + 2\sqrt{2}x - 1)$$
$$(x^2-5)^2 - 24 = (x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6})\,.$$

Ezek pontosan a 3.3.20. Feladatban használt felbontások. A kapott észrevételt a 3.8.8. Gyakorlatban általánosítjuk.

3.8.7. Az Útmutató utolsó mondatában szereplő két egyenletet összeadva

$$K_1(x) = \frac{(x-\alpha_1)(x-\alpha_2) + (x-\alpha_3)(x-\alpha_4)}{2} = x^2 - \frac{\alpha_1+\alpha_2+\alpha_3+\alpha_4}{2} + u_1$$

adódik, ahol $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = -a$ a gyökök és együtthatók összefüggése miatt. A két egyenletet kivonva

$$L_1(x) = \frac{(x-\alpha_1)(x-\alpha_2) - (x-\alpha_3)(x-\alpha_4)}{2} = \frac{\alpha_3+\alpha_4-\alpha_1-\alpha_2}{2}x + \frac{\alpha_1\alpha_2 - \alpha_3\alpha_4}{2}\,.$$

Nyilván

$$f(x) = \big(K_1(x) + L_1(x)\big)\big(K_1(x) - L_1(x)\big) = K_1(x)^2 - L_1(x)^2\,.$$

A 3.8.4. Tétel bizonyításában szereplő $K(x) = x^2 + (a/2)x + u$ polinom tehát ugyanaz, mint a fenti K_1, ha az u helyére u_1-et helyettesítünk. A fenti összefüggés szerint erre az u értékre $K^2 - f = K_1^2 - f = L_1^2$, vagyis teljes négyzet. Ezért $u = u_1$ gyöke a harmadfokú rezolvensnek. A 3.8.4. Tétel bizonyításában szereplő L polinomra $u = u_1$ esetén tehát $L^2 = K^2 - f^2 = K_1^2 - f^2 = L_1^2$ teljesül, ahonnan $L = \pm L_1$.

Innen (1) és (2) is következik. Az α_i határozatlanok alkalmas cserélgetésével látjuk, hogy u_2 és u_3 is gyöke a harmadfokú rezolvensnek. Az Útmutatóban leírtak miatt így a rezolvens tényleg $8(x-u_1)(x-u_2)(x-u_3)$ lesz, azaz (1) igaz. A (2) is világos: ha $L = L_1$, akkor $K(x) + L(x) = (x-\alpha_1)(x-\alpha_2)$ és $K(x) - L(x) = (x-\alpha_3)(x-\alpha_4)$, különben pedig fordítva.

A 3.8.4. Tétel bizonyításában megadtuk az L^2 polinom alakját az f együtthatóival és u-val kifejezve, fent pedig szerepel az L_1 polinom az α_i számokkal kifejezve. Ezt négyzetre emelve és az együtthatókat összehasonlítva rendre (3), (4), (5) adódik. Végül (6) egyszerű azonos átalakítással kapható (5)-ből.

3.8.8. A 3.8.7. Feladat mutatja, hogy ha a harmadfokú rezolvensnek az u_1 gyökét használjuk, akkor $f(x)$ az $(x-\alpha_1)(x-\alpha_2)$ és az $(x-\alpha_3)(x-\alpha_4)$ polinomok szorzatára bomlik. Ugyanez a számolás az α_i gyökök cserélgetésével azt adja, hogy ha az u_2 gyököt használjuk, akkor a két tényező $(x-\alpha_1)(x-\alpha_3)$ és $(x-\alpha_2)(x-\alpha_4)$ lesz, az u_3 esetében pedig $(x-\alpha_1)(x-\alpha_4)$ és $(x-\alpha_2)(x-\alpha_3)$.

3.8.9. Az f-nek akkor és csak akkor van racionális gyöke, ha felbomlik egy első és egy harmadfokú racionális együtthatós polinom szorzatára. Megmutatjuk, hogy f két másodfokú $\mathbb{Q}[x]$-beli polinomra való felbontásai pontosan a (2) és (3) esetben keletkeznek.

Alkalmazzuk a 3.8.3. Gyakorlat megoldásában szereplő, racionális együtthatós polinomokról szóló állítást arra a $K(x)^2 - f(x) = px^2 + qx + r$ polinomra, amit a harmadfokú g rezolvens levezetésekor kaptunk. Ha u gyöke g-nek, akkor $q^2 - 4pr = 0$, és ha u racionális, akkor $p, q, r \in \mathbb{Q}$. A (2) és (3) pontban megfogalmazott feltétel azt adja, hogy $K(x)^2 - f(x)$ egy racionális együtthatós $L(x)$ polinom négyzete (a (2) a $p \neq 0$, a (3) a $p = 0$ eset), és így az f polinomot sikerült felbontani két racionális együtthatós, másodfokú polinom szorzatára.

Megfordítva, tegyük föl, hogy f két másodfokú, racionális együtthatós polinom szorzatára bomlik. Feltehető, hogy ezek normáltak, vagyis $v(x) = (x-\alpha_1)(x-\alpha_2)$ és $w(x) = (x-\alpha_3)(x-\alpha_4)$ (ahol az α_i gyökök komplex számok). A gyökök és együtthatók összefüggése miatt $\alpha_1\alpha_2$ és $\alpha_3\alpha_4$ e polinomok konstans tagjai, tehát racionálisak. A 3.8.7. Feladat szerint az $u_1 = (\alpha_1\alpha_2 + \alpha_3\alpha_4)/2$ racionális szám gyöke a harmadfokú rezolvensnek, és az ebből kapott K és L polinomokra $K + L = v$ és $K - L = w$. Innen kivonással kapjuk, hogy L is racionális együtthatós, tehát $K^2 - f = L^2 = px^2 + qx + r$ egy elsőfokú, racionális együtthatós polinom négyzete. A 3.8.3. Gyakorlat szerint erre teljesül a (2) és (3) pontban megfogalmazott feltételek egyike.

Végül ha $a = 0$, akkor $au = c$ azzal ekvivalens, hogy $c = 0$. Továbbá $u = b/2$, és így $u^2 - d = b^2/4 - d$, ami pontosan akkor négyzetszám, ha a négyszerese, vagyis $b^2 - 4d$ az.

3.8.10. A harmadfokú rezolvens most $(8u - 4b)(u^2 - d)$, amiből (1) azonnal következik. A (2) állítás következménye a 3.8.9. Feladatnak. Valóban, tegyük föl először, hogy f irreducibilis. Ekkor a 3.8.9. Feladat (3) állítása nem teljesülhet, és mivel $c = 0$, ezért $b^2 - 4d$ nem négyzetszám. Nem teljesülhet továbbá a a 3.8.9. Feladat (2) állítása sem. Ez azt jelenti, hogy az $u = \pm\sqrt{d}$ értékekre $2u - b$ sem négyzetszám. Ezzel a (2) egyik irányát igazoltuk.

Megfordítva, ha a $\sqrt{b^2 - 4d} = e_1 \in \mathbb{Q}$, akkor

$$f(x) = \left(x^2 - (-b + e_1)/2\right)\left(x^2 - (-b - e_1)/2\right),$$

ha $\sqrt{2\sqrt{d} - b} = e_2 \in \mathbb{Q}$, akkor a 3.8.9. Feladat megoldását végigszámolva

$$f(x) = \left(x^2 - e_2x + \sqrt{d}\right)\left(x^2 + e_2x + \sqrt{d}\right),$$

végül ha $\sqrt{-2\sqrt{d} - b} = e_3 \in \mathbb{Q}$, akkor

$$f(x) = \left(x^2 - e_3x - \sqrt{d}\right)\left(x^2 + e_3x - \sqrt{d}\right).$$

3.8.11. Az x^4-2 esetében $b=0$ és $d=-2$, ami nem négyzetszám, és ezért $\pm 2\sqrt{d}-b$ nemhogy egy racionális szám négyzete, de még racionális sem lehet. Mivel $b^2-4d=8$ sem négyzetszám, az x^4-2 irreducibilis $\mathbb{Q}$ fölött (ezt persze a Schönemann–Eisenstein-kritériumból is tudjuk).

Az x^4+4 esetében $b^2-4d=-16$ és $-2\sqrt{d}-b=-8$ nem négyzetszám, de $2\sqrt{d}-b=4$ igen, ebből az előző gyakorlat megoldása alapján $e_2=2$, és az $(x^2-2x+2)(x^2+2x+2)$ felbontást kapjuk (amit ismerünk a 2.5.10. Gyakorlatból).

Az x^4-10x^2+1 polinomról is tudjuk már, hogy irreducibilis $\mathbb{Q}$ fölött (3.3.20. Feladat). Ebben az esetben a 24, 12 és 8 értékek adódnak, amelyek nem négyzetszámok.

3.8.12. A 3.5.9. Feladat szerint minden n-edfokú $f(x)=a_nx^n+\ldots+a_0$ reciprok polinom szimmetrikus a „közepére", vagyis $a_n=a_0$, $a_{n-1}=a_1$, és így tovább, általában $a_i=a_{n-i}$. Ha f foka páratlan, akkor i és $n-i$ közül egy páros, egy páratlan, és így $a_ix^i+a_{n-i}x^{n-i}$-nek gyöke a -1. A polinom ilyen tagok összege, tehát annak is gyöke a -1.

A feladatban szereplő $x^7+2x^6-x^4-x^3+2x+1$ polinomból az $x+1$ gyöktényezőt kiemelve $x^6+x^5-x^4-x^2+x+1$ marad. Ennek nem gyöke a nulla, és így gyökvesztés nélkül eloszthatjuk x^3-nel, vagyis egyenletünk a következőképpen alakul:

$$0=\frac{x^6+x^5-x^4-x^2+x+1}{x^3}=\left(x^3+\frac{1}{x^3}\right)+\left(x^2+\frac{1}{x^2}\right)-\left(x+\frac{1}{x}\right).$$

Legyen $z=x+(1/x)$, ekkor négyzetre illetve köbre emeléssel

$$z^2=\left(x^2+\frac{1}{x^2}\right)+2\quad\text{és}\quad z^3=\left(x^3+\frac{1}{x^3}\right)+3\left(x+\frac{1}{x}\right).$$

Ezért egyenletünk a $z^3-3z+z^2-2-z=0$ alakot ölti. Ez harmadfokú, tehát meg tudjuk oldani gyökjelekkel. Innen az eredeti polinom gyökeit is megkapjuk, mert ha $z=u$ a fenti harmadfokú egyenlet valamelyik gyöke (ahol u már ismert szám), akkor az $x+(1/x)=u$ egyenletet x-szel átszorozva másodfokú egyenletet kapunk.

Általában is könnyen belátható, hogy egy páros fokú reciprok polinom mindig felírható a $z=x+(1/x)$ polinomjaként. Ezért a gyökeinek a meghatározása visszavezethető egy feleakkora fokú egyenlet megoldására.

3.8.13. Ezt az egyenletet, a negyedfokú egyenlet megoldási ötletéhez hasonlóan, két négyzet különbségére bonthatjuk. Mivel $-2x^2-4x-2=-2(x+1)^2=(i\sqrt{2})^2(x+1)$, ezért

$$x^8+2x^2+4x+2=(x^4)^2-(i\sqrt{2}x+i\sqrt{2})^2=$$
$$=(x^4-i\sqrt{2}x-i\sqrt{2})(x^4+i\sqrt{2}x+i\sqrt{2}).$$

Tehát csak két negyedfokú egyenletet kell megoldani.

3.9. A körosztási polinom.

3.9.2. A harmadik primitív egységgyökök $-1/2 \pm i\sqrt{3}/2$, a hatodikak $1/2 \pm i\sqrt{3}/2$, a tizenkettedikek $\pm\sqrt{3}/2 \pm i/2$. Innen az állítás beszorzással adódik.

3.9.3. A p darab p-edik egységgyök az $x^p - 1$ polinom összes gyöke (és mindegyik egyszeres, lásd 2.5.15. Feladat). A 1.5.12. Tétel szerint ezek közül az 1 kivételével mindegyik primitív p-edik egységgyök is, hiszen az $1, \ldots, p-1$ számok relatív prímek p-hez. Ezért

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + \ldots + x^{p-1}\,.$$

3.9.4. Ha $o(\eta) = 12$, akkor hatványai között négy tizenkettedrendű, két hatodrendű, két negyedrendű, két harmadrendű, egy másodrendű és egy elsőrendű szám van. Az adódik, hogy $\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) = x^{12} - 1$. Az osztás elvégzésekor érdemes a nevezőben minél több tényezőt összevonni, mert ezzel a számolást rövidíthetjük. A 6 osztóihoz tartozó körosztási polinomok szorzata $x^6 - 1$, ezért

$$\Phi_{12}(x) = \frac{x^{12} - 1}{\Phi_1\Phi_2\Phi_3\Phi_6\Phi_4} = \frac{x^{12} - 1}{(x^6 - 1)\Phi_4(x)} = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1\,.$$

3.9.6. Tekintsük a $\prod_{d|n} \Phi_d(x) = x^n - 1$ képletben a fokszámokat.

3.9.10. A rekurziós képlet alapján, ha p prím, akkor

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{\Phi_1\Phi_p \ldots \Phi_{p^{k-1}}} = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1}\,,$$

hiszen a nevezőben szereplő indexek éppen p^{k-1} osztói. Az $y = x^{p^{k-1}}$ helyettesítéssel azonnal látszik, hogy mennyi ennek a törtnek az értéke:

$$\Phi_{p^k}(x) = \frac{y^p - 1}{y - 1} = 1 + y + \ldots + y^{p-1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \ldots + x^{(p-1)p^{k-1}}\,.$$

3.9.11. Legyen n pozitív, páratlan egész. A 1.5.18. Feladat szerint ha $o(\varepsilon) = n$, akkor $o(-\varepsilon) = 2n$, és ha $o(\varepsilon) = 2n$, akkor $o(-\varepsilon) = n$. Ez azt jelenti, hogy $\varepsilon \mapsto -\varepsilon$ kölcsönösen egyértelmű megfeleltetést létesít Φ_n és Φ_{2n} gyökei között. Más szóval $\Phi_n(-x)$ és $\Phi_{2n}(x)$ gyökei ugyanazok (és mindegyik egyszeres). Ezért e két polinom egymás konstansszorosa. A Φ_{2n} polinom normált, tehát a két polinom egyenlőségéhez már csak azt kell megmutatni, hogy (páratlan $n > 1$ esetén) $\Phi_n(-x)$ is az. De ez igaz: a $\Phi_n(-x)$ főegyütthatója $(-1)^{\varphi(n)} = 1$, mert a A.4.3. Állítás szerint $\varphi(n)$ páros szám (kivéve ha $n = 1$ vagy 2).

3.9.12. Láttuk, hogy $\Phi_1(x) = x - 1$. Ha p prímszám, akkor a 3.9.3. Gyakorlat miatt $\Phi_p(x) = 1 + x + \ldots + x^{p-1}$. A további prímhatvány-indexű körosztási polinomok 20-ig a 3.9.10. Gyakorlat alapján a következők: $\Phi_4(x) = x^2 + 1$, $\Phi_8(x) = x^4 + 1$, $\Phi_{16}(x) = x^8 + 1$, $\Phi_9(x) = x^6 + x^3 + 1$. Ha az index egy páratlan szám kétszerese, akkor az előző feladat miatt $\Phi_6(x) = x^2 - x + 1$, $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$, $\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$, $\Phi_{18}(x) = x^6 - x^3 + 1$. Korábban kiszámoltuk már azt is, hogy $\Phi_{12}(x) = x^4 - x^2 + 1$. A megmaradt esetek: $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ (ezt a rekurziós képletből osztással kaphatjuk), és $\Phi_{20}(x) = \Phi_{10}(x^2)$ (lásd a 3.9.14. Feladatot).

3.9.13. Tudjuk, hogy $x^{n/d} - 1$ azoknak az $x - \eta$ gyöktényezőknek a szorzata, ahol η rendje osztója n/d-nek. Azt kell belátnunk, hogy a $\prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$ képletben $o(\eta) = n$ esetén $x - \eta$ az első hatványon szerepel, egyébként pedig a nulladikon. Legyen $o(\eta) = m$. Ekkor $x^{n/d} - 1$-ben $x - \eta$ az első hatványon szerepel, ha $m \mid (n/d)$, egyébként pedig a nulladikon. Persze $m \mid (n/d) \iff d \mid (n/m)$. Ezért a $\prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$ képletben $x - \eta$ kitevője $\sum_{d|(n/m)} \mu(d)$. A A.4.6. Állítás miatt ez az összeg 1, ha $n/m = 1$, és nulla egyébként.

3.9.14. A feladatra két megoldást adunk. Az első rövid számolás, ami felhasználja a 3.9.13. Feladatban bizonyított összefüggést. A második bizonyítás hosszabb, de nagyon tanulságos, mert gyakoroljuk általa az elemrend fogalmát.

Az első bizonyításban tehát induljunk ki abból, hogy $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$. Ebben a szorzatban eltekinthetünk azoktól a tényezőktől, amelyekre a $\mu(d)$ kitevő nulla, hiszen az ilyen tényezők értéke 1. Tehát csak azok a $d \mid n$ számok az érdekesek, amelyek csupa különböző prímek szorzatai. Mivel n minden prímosztója osztója m-nek is, az ilyen d számok m-nek is osztói. Ezért

$$\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)} = \prod_{d|m}\left((x^{n/m})^{m/d} - 1\right)^{\mu(d)} = \Phi_m(x^{n/m})$$

(az utolsó lépésben m-re alkalmaztuk a 3.9.13. Feladatban bizonyított formulát).

A második, közvetlen bizonyításban a

$$\Phi_n(x) = \prod_{o(\eta)=n}(x - \eta) \quad \text{és} \quad \Phi_m(x^{n/m}) = \prod_{o(\varepsilon)=m}(x^{n/m} - \varepsilon)$$

képletekből indulunk ki. Mindkét képletben könnyen láthatóan minden gyök egyszeres, tehát azt kell megmutatni, hogy a két oldalnak ugyanazok a gyökei. Más szóval, hogy $o(\eta) = n$ akkor és csak akkor, ha $o(\eta^{n/m}) = m$.

A hatvány rendjének képlete szerint $o(\eta^{n/m}) = o(\eta)/(o(\eta), n/m)$. Ha $o(\eta) = n$, akkor ez $n/(n, n/m) = n/(n/m) = m$. Megfordítva, tegyük fel, hogy $o(\eta)/(o(\eta), n/m) = m$. Azaz

$$o(\eta) = (o(\eta), n/m)m = (o(\eta)m, n) = (m, n/o(\eta))o(\eta)\,.$$

Itt kétszer használtuk a kitüntetett közös osztó kiemelési tulajdonságát. (A második esetben is szabad ezt megtenni, azaz $o(\eta) \mid n$, hiszen ez már az $o(\eta) = (o(\eta)m, n)$ összefüggésből következik.) Azt kaptuk tehát, hogy $(m, n/o(\eta)) = 1$. Ha az $n/o(\eta)$ számnak lenne egy

p prímosztója, akkor persze $p \mid n$, és a feltételünk szerint n prímosztói mind osztják m-et, azaz $p \mid m$, ahonnan a $p \mid (m, n/o(\eta)) = 1$ ellentmondás adódik. Ezért az $n/o(\eta)$ egész számnak nincs prímosztója, vagyis $n/o(\eta) = 1$, ami a kívánt $o(\eta) = n$ állítást bizonyítja.

3.9.15. Az előző feladat alapján elég a négyzetmentes indexű körosztási polinomokat ismerni. Ha ugyanis az n szám tetszőleges, és az m az n prímosztóinak a szorzata, akkor m négyzetmentes, és Φ_m ismeretében $\Phi_n(x) = \Phi_m(x^{n/m})$ is kiszámítható. Speciálisan $\Phi_{36}(x) = \Phi_6(x^6) = x^{12} - x^6 + 1$, $\Phi_{72}(x) = \Phi_6(x^{12}) = x^{24} - x^{12} + 1$, $\Phi_{144}(x) = \Phi_6(x^{24}) = x^{48} - x^{24} + 1$, $\Phi_{100}(x) = \Phi_{10}(x^{10}) = x^{40} - x^{30} + x^{20} - x^{10} + 1$ (itt felhasználtuk a 3.9.12. Gyakorlat eredményét).

3.9.16. Belátjuk, hogy az n-edik primitív egységgyökök összege $\mu(n)$, ahol μ a Möbius-függvény (A.4.5. Definíció), szorzatuk pedig mindig 1, kivéve az $n = 2$ esetet, amikor -1. Az utóbbi állítást az Olvasónak érdemes bebizonyítania úgy is, hogy minden primitív n-edik egységgyököt párosít az inverzével (ami szintén primitív n-edik egységgyök). Mi mindkét állítást a gyökök és együtthatók összefüggésének felhasználásával igazoljuk. Ezek alapján ugyanis a primitív n-edik egységgyökök $S(n)$ összege a $\Phi_n(x)$ körosztási polinomban a „felülről második tag", vagyis az $x^{\varphi(n)-1}$-es tag együtthatójának ellentettje, szorzatuk pedig a konstans tag $(-1)^{\varphi(n)}$-szerese.

A $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggésben nézzük meg, mi az x^{n-1} együtthatója a két oldalon. A jobb oldalon ez 0, kivéve az $n = 1$ esetet, amikor -1. A másik oldalon x^{n-1}-es tagot csak úgy kaphatunk, ha egy kivételével mindegyik polinomból a legmagasabb fokú tagot vesszük, a kivételesből pedig a második legmagasabb fokút (hiszen $n - 1$ csak eggyel kevesebb, mint a szorzatpolinom foka). Mivel $\Phi_d(x)$-ben a második legmagasabb fokú tag együtthatója $-S(d)$, és az összes Φ_d polinom normált, a bal oldalon az x^{n-1} együtthatója a $-S(d)$ számok összege lesz. A két oldalt egybevetve tehát beláttuk, hogy

$$\sum_{d|n} S(d) = \begin{cases} 1 & \text{ha } n = 1, \\ 0 & \text{ha } n \neq 1. \end{cases}$$

Ez ugyanaz az összefüggés, amit a A.4.6. Állításban igazoltunk S helyett μ-re. Ezért n szerinti indukcióval azonnal látjuk, hogy $S(n) = \mu(n)$. (Valójában arról van szó, hogy ez a rekurzív összefüggés az S függvényt egyértelműen definiálja. Az indukciót most is ugyanazzal a logikával végezzük, mint a 3.9.7. Következmény bizonyításában.)

A szorzatra vonatkozó összefüggést levezetéséhez a $\prod_{d|n} \Phi_d(x) = x^n - 1$ konstans tagját kell tekinteni (azaz nullát helyettesíteni). Ekkor $\prod_{d|n} \Phi_d(0) = -1$ adódik, és innen indukcióval látszik, hogy $\Phi_n(0)$ értéke mindig 1, kivéve $n = 1$-re, amikor -1. Tudjuk, hogy $\varphi(n)$ akkor és csak akkor páros, ha $n > 2$ (lásd A.4.3. Állítás). Az n-edik primitív egységgyökök szorzata, ami $(-1)^{\varphi(n)}\Phi_n(0)$, tehát tényleg 1 ha $n \neq 2$, és -1, ha $n = 2$.

3.9.17. A $\Phi_n(1)$ értéket kell meghatároznunk. A $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggésbe közvetlenül 1-et helyettesíteni nem érdemes, hiszen a Φ_1 miatt nullát kapunk. Ezért előbb osszunk le $\Phi_1(x) = x - 1$-gyel. Az eredmény:

$$\prod_{\substack{d|n \\ d\neq 1}} \Phi_d(x) = \frac{x^n - 1}{x - 1} = 1 + x + x^2 + \ldots + x^{n-1} .$$

Ebbe az azonosságba $x = 1$-et helyettesítve

$$\prod_{\substack{d|n \\ d\neq 1}} \Phi_d(1) = n .$$

Innen könnyen látható n szerinti indukcióval, hogy ha n egy p prím hatványa, de nem 1, akkor $\Phi_n(1) = p$, ha pedig n nem prímhatvány, akkor $\Phi_n(1) = 1$. Természetesen $n = 1$-re közvetlenül látszik, hogy az eredmény nulla.

Felmerül a kérdés, hogy szabad-e a fenti egyenlőségbe $x = 1$-et helyettesíteni, nem jelentené-e ez azt, hogy $1 - 1 = 0$-val osztottunk. A válasz megtalálható a 2.5.15. Feladat megoldását követő diszkusszióban.

3.9.18. Eljárhatnánk az előző feladat megoldásában használt módon is, $\Phi_2(x) = x+1$-gyel leosztva a rekurziót páros n esetén. Ennél egyszerűbb azonban, ha ennek a feladatnak az *eredményét* használjuk fel. Ha $n = 4m$, akkor a 3.9.14. Feladat miatt $\Phi_n(x) = \Phi_{2m}(x^2)$, és így $\Phi_n(-1) = \Phi_{2m}(1)$, ami 2, ha m kettő-hatvány, különben 1. Ha n nem osztható néggyel, akkor a 3.9.11. Gyakorlat miatt páratlan $n > 1$ esetén az eredmény $\Phi_{2n}(1) = 1$, ha viszont $n = 2k > 2$, akkor $\Phi_n(-1) = \Phi_k(1)$. A fennmaradó „kis" eseteket kézzel kiszámolhatjuk. A végeredmény a következő: $\Phi_1(-1) = -2$, $\Phi_2(-1) = 0$, $\Phi_n(-1) = 2$, ha $n > 2$ kettő-hatvány, $\Phi_n(-1) = p$, ha $n = 2p^k > 2$ (p prím), a többi esetben az eredmény 1.

3.9.19. Legyen θ egy mn-edik primitív egységgyök. Mivel m és n relatív prímek, vannak olyan x és y egészek, melyekre $nx + my = 1$. Ekkor $\theta = \theta^{nx+my} = \theta^{nx}\theta^{my}$. A hatvány rendjének képlete szerint $o(\theta^{nx}) = mn/(mn, nx)$. Nyilván $(mn, nx) = n(m, x)$, és az $nx + my = 1$ összefüggés miatt $(m, x) = 1$. Ezért $o(\theta^{nx}) = m$. Hasonlóan $o(\theta^{my}) = n$. Ezért θ tényleg előáll egy primitív m-edik és egy primitív n-edik egységgyök szorzataként.

Most belátjuk, hogy ez az előállítás egyértelmű. Tegyük fel, hogy $o(\eta) = o(\eta') = m$ és $o(\varepsilon) = o(\varepsilon') = n$. Ha $\eta\varepsilon = \eta'\varepsilon'$, akkor innen $\eta/\eta' = \varepsilon'/\varepsilon$. A bal oldalon egy m-edik, a jobb oldalon egy n-edik egységgyök van, azaz a bal oldal rendje m-nek, a jobb oldalé n-nek osztója. Mivel $(m, n) = 1$, ez csak úgy lehet, hogy az egyenlőség mindkét oldalán 1 rendű szám áll, azaz $\eta = \eta'$ és $\varepsilon = \varepsilon'$.

Az Euler-függvény multiplikativitásának bizonyításához tekintsük az összes $\eta\varepsilon$ szorzatot, ahol $o(\eta) = m$ és $o(\varepsilon) = n$. Az előző bekezdésben bizonyított állítás szerint az ilyen szorzatok száma $\varphi(m)\varphi(n)$. Az 1.5.20. Gyakorlat (3) pontja szerint az így kapott $\eta\varepsilon$ szorzatok mind mn rendű számok, és az első bekezdés szerint minden mn rendű szám előáll

egy ilyen szorzatként. Ezért ezek a szorzatok éppen az mn-edik primitív egységgyököket adják, és így számuk $\varphi(mn)$.

3.9.20. Az előző gyakorlat miatt

$$\Phi_{mn}(x) = \prod_{o(\eta)=m,\ o(\varepsilon)=n} (x-\eta\varepsilon) = \left(\prod_{o(\eta)=m} \eta\right)^{\varphi(n)} \prod_{o(\eta)=m,\ o(\varepsilon)=n} (x/\eta-\varepsilon)\,.$$

A zárójelben álló szorzat a 3.9.16. Feladat miatt 1, kivéve az $m=2$ esetet, amikor -1, ez adja a minusz előjelet az $m=2, n=1$ esetben. Csoportosítsunk η szerint:

$$\prod_{o(\eta)=m,\ o(\varepsilon)=n} (x/\eta-\varepsilon) = \prod_{o(\eta)=m} \left(\prod_{o(\varepsilon)=n} (x/\eta-\varepsilon)\right) = \prod_{o(\eta)=m} \Phi_n(x/\eta)\,.$$

Tudjuk, hogy ha η befutja az m-edik primitív egységgyököket, akkor $1/\eta$ is, és ezért ha x/η helyett ηx-et írunk, azzal csak a tényezők sorrendjét változtatjuk.

3.9.21. $\mathbb{Z}$ fölött a körosztási polinomok az irreducibilis tényezők:

$$x^{12}-1 = \Phi_1(x)\ \Phi_2(x)\ \Phi_3(x)\ \Phi_4(x)\ \Phi_6(x)\ \Phi_{12}(x) = (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1)\,.$$

A $\mathbb{Z}_2$ fölött ez tovább bomlik a következőképpen:

$$\Phi_4(x) = (x+1)^2\,, \quad \Phi_{12}(x) = (x^2+x+1)^2\,,$$

azaz $x^{12}-1 = (x+1)^4(x^2+x+1)^4$. A $\mathbb{Z}_3$ fölött

$$\Phi_3(x) = (x-1)^2\,, \quad \Phi_6(x) = (x+1)^2\,, \quad \Phi_{12}(x) = (x^2+1)^2\,,$$

azaz $x^{12}-1 = (x-1)^3(x+1)^3(x^2+1)^3$ (az x^2+1 irreducibilis $\mathbb{Z}_3$ fölött, hiszen másodfokú, és nincs gyöke $\mathbb{Z}_3$-ban). Végül $\mathbb{Z}_5$ fölött

$$\Phi_4(x) = (x-2)(x+2)\,, \quad \Phi_{12}(x) = (x^2+2x-1)(x^2-2x-1)\,.$$

A kapott eredményeket érdemes összevetni a 3.9.22. Feladat állításával.

3.9.22. Tegyük fel, hogy n a legkisebb ellenpélda az állításra. Végig $\mathbb{Z}_p[x]$-ben számolunk (de nem írjuk ki a felülvonásokat). Tekintsük a $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggést. A d szám egyértelműen felírható $d = p^j m'$ alakban, ahol $0 \le j \le k$ és $m' \mid m$. Az indukciós feltevés szerint $d < m$ esetén teljesül $\mathbb{Z}_p$ fölött, hogy $\Phi_d = \Phi_{m'}^{\varphi(p^j)}$. Gyűjtsük össze rögzített m' mellett ezeket a tényezőket. Az eredmény

$$\Phi_{m'}^{\varphi(p^0)+\varphi(p^1)+\ldots+\varphi(p^k)} = \Phi_{m'}^{p^k}$$

(a kitevőben a 3.9.6. Gyakorlatban bizonyított $\sum_{d|p^k} \varphi(d) = p^k$ összefüggést használtuk). Ha a $\Phi_d = \Phi_{m'}^{\varphi(p^j)}$ összefüggést a $d = n$ esetben is tudnánk (ez a bizonyítandó állítás),

akkor a fentieket összeszorozva, és felhasználva, hogy $\prod_{m'|m}\Phi_{m'}(x)=x^m-1$,

$$\prod_{d|n}\Phi_d(x)=\left(\prod_{m'|m}\Phi_{m'}(x)\right)^{p^k}=(x^m-1)^{p^k}=x^{mp^k}-1=x^n-1$$

adódna (hiszen mod p szabad tagonként p^k-adik hatványra emelni, és $(-1)^{p^k}=-1$ páratlan p prímre is, meg $p=2$-re is igaz, utóbbi azért, mert $\mathbb{Z}_2$-ben $-1=1$). Ha most úgy számolunk, hogy a $\Phi_n=\Phi_m^{\varphi(p^k)}$ összefüggést nem használjuk, akkor ugyanez a gondolatmenet azt adja, hogy

$$\frac{\Phi_m(x)^{\varphi(p^k)}}{\Phi_n(x)}\prod_{d|n}\Phi_d(x)=x^n-1\,.$$

Felhasználva, hogy $\prod_{d|n}\Phi_d(x)=x^n-1$, azt kapjuk, hogy a bal oldali tört értéke 1, vagyis $\Phi_n(x)=\Phi_m(x)^{\varphi(p^k)}$, amit bizonyítani kellett. Valamivel talán egyszerűbb a számolás, ha a fenti módszerrel csak az $n=pm$ esetet intézzük el, majd alkalmazzuk a 3.9.14. Feladatot.

3.9.23. A 3.9.10. Gyakorlat képlete alapján

$$\Phi_{p^k}(x)=\frac{x^{p^k}-1}{x^{p^{k-1}}-1}=1+x^{p^{k-1}}+x^{2p^{k-1}}+\ldots+x^{(p-1)p^{k-1}}\,.$$

Ezért $\Phi_{p^k}(x+1)$ konstans tagja az $x=0$ helyen vett helyettesítési érték, vagyis p. Továbbá $\mathbb{Z}_p[x]$-ben számolva

$$\Phi_{p^k}(x+1)=\frac{(x+1)^{p^k}-1}{(x+1)^{p^{k-1}}-1}=\frac{x^{p^k}+1-1}{x^{p^{k-1}}+1-1}=x^{p^k-p^{k-1}}\,.$$

Ez $\mathbb{Z}$-ben azt jelenti, hogy $\Phi_{p^k}(x+1)$ minden együtthatója osztható p-vel, kivéve a főegyütthatót. A Schönemann-Eisenstein kritérium tehát teljesül.

3.9.24. A 3.9.23. Gyakorlat és a 3.9.11. Feladat alapján látjuk, hogy prímhatványra, illetve páratlan prímhatvány kétszeresére a körosztási polinom egy eltoltja tényleg teljesíti a Schönemann-Eisenstein kritérium feltételét. Megfordítva, tegyük fel, hogy $\Phi_n(x+c)$ a p prímre teljesíti a kritériumot. Áttérve $\mathbb{Z}_p$-re azt kapjuk, hogy $\overline{\Phi_n}(x+\overline{c})=x^{\varphi(n)}$, hiszen a főegyüttható kivételével minden együttható eltűnik (nullává válik) mod p. Ebbe az azonosságba $y=x-\overline{c}$-t írva adódik, hogy $\overline{\Phi_n}(y)=(y-\overline{c})^{\varphi(n)}$.

Legyen $n=p^km$, ahol már $p\nmid n$. A 3.9.22. Feladat szerint $\overline{\Phi_n}(y)=\overline{\Phi_m}(y)^{\varphi(p^k)}$, és így

$$\overline{\Phi_m}(y)=(y-\overline{c})^{\frac{\varphi(n)}{\varphi(p^k)}}=(y-\overline{c})^{\varphi(m)}\,.$$

Tudjuk, hogy $\Phi_m(y)\mid y^m-1$. Mivel $p\nmid m$, az y^m-1 polinomnak nincs többszörös tényezője $\mathbb{Z}_p[x]$-ben (lásd 3.6.12. Gyakorlat). Így $\varphi(m)=1$, ahonnan (a A.4.3. Állítás szerint) $m=1$ vagy 2.

3.9.25. Még a primitív

```
with(numtheory):
for n from 3 by 2 do
  if issqrfree(n) and not isprime(n) then
    s := coeffs(cyclotomic(n,x));
    for i in s do
      if i > 4 or i < -4 then
        print(n, sort(cyclotomic(n,x)));
        break
      fi
    od
  fi
od;
```

MAPLE-program is gyorsan kiszámolja a mai asztali számítógépeken, hogy a legkisebb n az $1785 = 3 \cdot 5 \cdot 7 \cdot 17$, melyre Φ_n-ben van legalább 5 abszolút értékű együttható. Az $n = 385 = 5 \cdot 7 \cdot 11$ a legkisebb olyan érték, melyre Φ_n-ben előfordul legalább 3 abszolút értékű együttható, és $n = 1365 = 3 \cdot 5 \cdot 7 \cdot 13$ esetén fordul elő először legalább 4 abszolút értékű együttható.

11.4. Csoportok

4.1. Bevezető példák.

4.1.4. Hová viszi $f \circ f$ az 1-et? Az f elviszi 2-be, ha még egyszer alkalmazzuk f-et, akkor az továbbviszi $f(2) = 4$-be. Tehát $(f \circ f)(1) = 4$. A többi elem képét hasonlóan kiszámolva

$$g = f \circ f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix}$$

adódik. Ugyanígy ellenőrizhető, hogy $f \circ g = g \circ f$ az identitás.

4.1.5. A 2.2.4. Gyakorlat szerint a kompozíció művelete asszociatív. A 2.2.7. Gyakorlat szerint az identikus leképezés neutrális elem. Végül a 2.2.11. Gyakorlat szerint a kétoldali inverz is létezik.

4.1.9. Könnyű kiszámolni, hogy

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad \text{és} \quad g \circ f = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

Ezek különböző permutációk, és így az f és g nem cserélhetők fel. Emiatt S_3 nem kommutatív csoport. Ha $n > 3$, akkor az f permutációt kiterjeszthetjük az $\{1, 2, \dots, n\}$ halmazra, ha $i > 3$ esetén $f(i)$-t i-nek definiáljuk. Ugyanezt tegyük meg g-vel is. Ekkor a fenti számolás lényege nem változik, és továbbra is két nem felcserélhető elemet kapunk. Ezért $n \geq 3$ esetén S_n nem kommutatív. As S_1 és S_2 csoportok viszont Abel-félék. Ez közvetlenül is ellenőrizhető, de be is látjuk majd, hogy a kételemű (általában a prímelemű) csoportok mind kommutatívak.

4.1.10. Akkor és csak akkor, ha $n = 1$. Ha $n = 1$, akkor 1×1-es mátrixokról van szó, amelyek nyilván felcserélhetők. Ha $n \geq 2$, akkor az (egy determinánsú)

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{és} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

mátrixokat a kétféle sorrendben összeszorozva két különböző mátrixot kapunk. Elég a bal felső sarokban levő elemet kiszámolni, ami az egyik szorzatban 1, a másikban $1 + 1$, és semmilyen T testben nem igaz, hogy $1 + 1 = 1$, hiszen akkor az egységelem nulla lenne, ami testben lehetetlen (lásd 2.2.20. Feladat).

4.1.11. Ha $ag = bg$, akkor g inverzével jobbról szorozva, és az asszociativitást felhasználva

$$a = a(gg^{-1}) = (ag)g^{-1} = (bg)g^{-1} = b(gg^{-1}) = b\,.$$

Hasonlóan látható be az is, hogy balról szabad egyszerűsíteni.

4.1.12. Legyen $x \in S$, ekkor van balinverze, vagyis olyan y, hogy $yx = e$. Az y elemnek is van balinverze, azaz olyan z, hogy $zy = e$. Ekkor $x = ex = (zy)x = z(yx) = ze$, de innen $xe = (ze)e = z(ee) = ze = x$. Mivel ez minden x-re igaz, beláttuk, hogy e jobb oldali egységelem is. Speciálisan $x = ze = z$, tehát az x elemnek y kétoldali inverze.

4.2. Permutációk előjele és ciklusfelbontása.

4.2.3. Mindkét oldal könnyen kiszámolhatóan az

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

permutáció.

4.2.4. Miben különböznek a $P(x_1, x_2, x_3, \ldots, x_n)$ és $P(x_2, x_1, x_3, \ldots, x_n)$ polinomok? Át kell tekintenünk, hogy az x_i és x_j változók különbsége a két polinomban $x_i - x_j$, vagy $x_j - x_i$ formában jelentkezik-e.

Tegyük fel először, hogy $2 < i < j$. Ekkor mindkét polinomban az $x_i - x_j$ különbség fordul elő: ez az i-edik és a j-edik argumentumok különbsége.

Legyen most $2 < i$ tetszőleges. Az $x_1 - x_i$ szintén mindkét polinomban szerepel: az első polinomban ez az első és az i-edik argumentum különbsége, a másodikban pedig a második és az i-edik argumentum különbsége. Ugyanígy láthatjuk be, hogy az $x_2 - x_i$ különbség is mindkét polinomban szerepel.

Most már csak x_1 és x_2 különbségét kell megkeresnünk a két polinomban. Látjuk, hogy az elsőben $x_1 - x_2$, a másodikban pedig $x_2 - x_1$ szerepel. Ezért e két polinom egymás ellentettje, és így az (12) előjele -1.

4.2.6. Az igaz, hogy $f \circ g$ és $g \circ f$ általában különbözők, viszont $\mathrm{sg}(f)$ és $\mathrm{sg}(g)$ egész számok, és ezért felcserélhetők. Így persze $f \circ g$ és $g \circ f$ előjele mindig ugyanaz lesz.

4.2.14. Mindkét ciklus az a permutáció, amely az x_j elemet x_{j+1}-be viszi ($1 \leq j < k$), az x_k-t x_1-be, az X összes többi elemét pedig saját magába.

4.2.16. Legyenek f és g diszjunkt ciklusok. Az f-ben szereplő elemeket fessük pirosra, a g-ben szereplőket zöldre. Ekkor $f \circ g$ és $g \circ f$ is úgy kapható meg, hogy f-fel megcsináljuk azt, amit a piros elemeken kell, g-vel pedig azt, amit a zöld elemeken kell. Hiszen f a zöld elemeket fixen hagyja (önmagába viszi), ezért a zöld elemek szempontjából mindegy, hogy f-et g előtt, vagy g után alkalmazzuk rájuk. Ugyanígy a piros elemeket g hagyja fixen, ezért az ő szempontjukból is mindegy, hogy f-et vagy g-t alkalmazzuk-e előbb.

Egy fokkal formálisabban: ha p piros elem, akkor $f(p)$ is piros, hiszen az is az f ciklusban van. Ezért $g(p) = p$ és $g\big(f(p)\big) = f(p)$. Így pedig $f \circ g$ és $g \circ f$ is p-t $f(p)$-be viszi. Ugyanez a gondolatmenet működik a zöld elemekre is. Ha pedig egy elem se nem piros, se nem zöld, akkor $f \circ g$ és $g \circ f$ is fixen hagyja.

4.2.18. Az egyelemű ciklusokat akár kiírjuk, akár nem, a permutáció nyilván nem változik (hiszen minden egyelemű ciklus az identitás). Hasonlóképpen egy-egy ciklus felírását akármelyik eleménél elkezdhetjük. A diszjunkt ciklusokra bontás ezektől a változtatásoktól és a sorrendtől eltekintve lesz egyértelmű. Ez látszik a 4.2.17. Tétel bizonyításában alkalmazott rajzból: minden $x \in X$ abban az egyetlen ciklusban van benne, amely őt megmozdítja, és ha $f(x) = y$, akkor ebben a ciklusban x után csakis y következhet.

4.2.19. Képzeljük azt, hogy az $x_1, \ldots x_k$ elemek egy sorban ülnek egy színház nézőterén. A bal oldali permutáció azt jelenti, hogy az x_1-től kezdve mindenki eggyel arrébb ül, és a sor végén ülő x_k átül a sor legelejére. A jobb oldali permutáció során pedig a sor legvégén ülő x_k sorban helyet cserél a mellette ülőkkel, és így jut el a sor legelejére, miközben mindenki eggyel arrébb csúszik.

Ez a hasonlat érzékelteti, miről is van szó, de a feladatot rutinszerűen meg tudjuk oldani, ha sorra vesszük, hogy az egyes x_i elemekkel mi történik a bal, illetve a jobb oldalon.

Például az x_2 elem a bal oldali ciklusnál x_3-ba megy, a transzpozícióknál pedig az (x_2x_3) hat rá először (hiszen jobbról balra szorzunk), ez x_3-ba viszi, amit a többi transzpozíció már fixen hagy. Ugyanez a többi elemre is elmondható, kivéve az x_k-t, amely mindegyik transzpozíciónál eggyel előbbre jut, és végül x_1-be megy.

4.2.21. Az első permutáció ciklusfelbontását rajzolás nélkül a következőképpen számíthatjuk ki. Vesszük az 1-et, melynek képe 2, tehát leírunk ennyit: (12. A 2 képe 5, tehát így folytatjuk: (125. Az 5 képe 4, tehát leírjuk a 4-est is. A 4 képe már nem egy újabb elem, hanem 1, ami már szerepelt. Ezért ezt nem írjuk le, hanem becsukjuk a zárójelet, tehát itt tartunk: (1254). Most megkeressük az első elemet, ami ebben a ciklusban nem szerepel. Ez a 3, ami 6-ba megy, tehát folytatjuk a felírást így: (1254)(36. Mivel a 6 visszamegy a 3-ba, a második zárójelet is bezárjuk. Folytatjuk a 7-tel, a végeredmény (1254)(36)(78). Ebben három darab, azaz páratlan sok páros hosszú ciklus van, ezért ez egy páratlan permutáció (4.2.20. Következmény).

Ugyanígy kapjuk, hogy a második permutáció (158)(27)(36), ami páros permutáció, ebben nem írtuk ki az egy hosszúságú (4) ciklust (ami az identitás). A harmadik permutáció $(acedb)$, azaz páros.

Az (1234)(35)(1432)(35) permutációt a következőképpen számíthatjuk ki, rögtön diszjunkt ciklusok szorzatává alakítva. Vesszük az 1-et, és nyomon követjük, jobbról balra haladva, hogy mi történik vele. A (35) fixen hagyja, az (1432) elviszi 4-be, ezután a 4-et a (35) fixen hagyja, és az (1234) a 4-et visszaviszi az 1-be. Tehát ez a permutáció az 1-et önmagába viszi. Ezt jelezhetjük úgy, hogy leírjuk ezt: (1), de azt is megtehetjük, hogy semmit nem írunk le. Folytatva a 2-vel, ugyanezt a négy lépést végrehajtva azt kapjuk, hogy a 2 is fixen marad. Végül a 3 képe 4 lesz, vagyis leírjuk ezt: (1)(2)(34. A 4 képét végigszámolva 5-öt kapunk, az 5 képe pedig 3, tehát bezárjuk a zárójelet. Végülis $(1234)(35)(1432)(35) = (345)$ adódik, ami páros permutáció. (Természetesen azt, hogy ez páros permutáció, az eredeti (1234)(35)(1432)(35) alakból is láthatjuk, hiszen abban négy páros hosszú ciklus szorzata, vagyis négy páratlan permutáció szerepel.)

Az $(12345)(234)(12345)^{-1}$ kiszámításában az az újdonság, hogy itt egy ciklus inverze szerepel. Világos, hogy általában

$$(x_1, x_2, \ldots, x_{k-1}, x_k)^{-1} = (x_k, x_{k-1}, \ldots, x_2, x_1)\,,$$

hiszen az inverz azt jelenti, hogy a körön a nyilak mentén visszafelé kell haladni. Így az (12345)(234)(54321) permutációt kell kiszámítani, ami az előbbi módszerrel (345), tehát páros.

Az $[(12)(23)(34)]^{1222}$ esetében először az alapot számítjuk ki: $(12)(23)(34) = (1234)$. Ezt kell 1222-szer önmagával összeszorozni. Az (1234)-et önmagával négyszer összeszorozva az identitást kapjuk, hiszen négy lépésben egy négy hosszú körön visszaérünk a kiindulópontba. Így az (1234) permutáció negyedik, nyolcadik, tizenkettedik, általában minden néggyel osztható kitevőjű hatványa az identitás. Speciálisan az 1220-adik hatványa is az identitás, és így $(1234)^{1222} = (1234)^2 = (13)(24)$, ez páros permutáció.

Végül a „hátulról előre” permutáció az $1, 2, \ldots, n-1, n$ számoknak az $n, n-1, \ldots, 2, 1$ sorrendje. Ez azt jelenti, hogy az első elem az utolsóval, a második az utolsó előttivel cserélődik, és így tovább, vagyis ez a permutáció diszjunkt transzpozíciók szorzata. Hogy hányé, az attól függ, hogy mi az n szám. Ha n páratlan, akkor a „középső” szám fixen marad, például $n = 5$-re $(15)(24)$ az eredmény. Ha n páros, akkor a két középső elem is helyet cserél. Az előjelet a kapott transzpozíciók számából olvashatjuk le. A végeredmény: ez a permutáció akkor páros, ha n néggyel osztva nullát vagy egyet ad maradékul.

4.2.22. Mivel (12) és (345) diszjunkt ciklusok, egymástól függetlenül, diszjunkt halmazokon operálnak (lásd a 4.2.16. Gyakorlat megoldását). Az (12) ciklust sokszor egymás után végrehajtva, minden második lépésnél az identitást kapjuk. A (345) esetében minden harmadik lépésben kapjuk az identitást. Így pedig az $f = (12)(345)$ permutáció hatványai minden hatodik lépésben adják az identitást, hatosával periodikusan ismétlődnek az alábbiak szerint:

$$[(12)(345)]^1 = (12)(345)$$
$$[(12)(345)]^2 = (354)$$
$$[(12)(345)]^3 = (12)$$
$$[(12)(345)]^4 = (345)$$
$$[(12)(345)]^5 = (12)(354)$$
$$[(12)(345)]^6 = id\,.$$

Tehát hat különböző hatvány van, és $f^k = f^\ell$ akkor és csak akkor, ha $6 \mid k - \ell$.

4.2.23. Lásd a 2.2.5. Feladat megoldását. A 4.2.19. Gyakorlat segítségével egy másik bizonyítást nyerhetünk arra, hogy szomszédos elemek cseréjével minden ciklus, és így minden permutáció előáll.

4.2.24. A kártyacsomag lapjainak egy sorrendjét az adja meg, hogy a csomagban fölülről számítva hányadik helyen milyen lap áll. Hogyan változtat ezen a sorrenden a megadott kétféle mozdulat? A legfelső két lap cseréje az (12) transzpozíció. Ha a legalsó lapot legfelülre tesszük, akkor az első lapból második lesz, a másodikból harmadik, és így tovább, tehát ez az átrendezés az $f = (1, 2, \ldots, n)$ ciklus. Ha egy kisebb csomagot teszünk alulról felülre, az ugyanaz, mint ha a kisebb csomag lapjait egyenként tennénk alulról felülre egymás után. Ezért a csomag elemelése nem egyéb, mint az f ciklus egy hatványa. Ha a legfelső lapot tesszük alulra, az az f permutáció $n-1$-edik hatványa (és egyúttal az inverze), vagyis $f^{n-1} = f^{-1} = (n, n-1, \ldots, 2, 1)$.

Hogyan cserélhetjük ki a kártyacsomag i-edik lapját az $i+1$-edikkel? Leemelünk a csomagról $i-1$ lapot és alulra tesszük őket (vagyis végrehajtjuk az f^{n-i+1} permutációt). Ezáltal az i-edik lap legfelülre kerül. Mivel a felső két lapot szabad cserélni, ezeket megcserélhetjük. Végül az első $i-1$ lapot tartalmazó kis csomagot visszatesszük a pakli tetejére

(ez is egy emelés). Ezekkel a mozdulatokkal tehát megcseréltük az i-edik és az $i+1$-edik lapot. Ugyanezt a gondolatmenetet a permutációk nyelvén leírva azt mutattuk meg, hogy

$$(i, i+1) = f^{i-1}(12)f^{n-i+1}\,.$$

Tehát mozdulatainkkal bármely két szomszédos lap megcserélhető. A 4.2.23. Gyakorlatban beláttuk (bár nem a kártyalapok, hanem a könyvespolc példáján), hogy szomszédos cserékkel minden permutáció megkapható, és így a megadott mozdulatokkal is.

Azt bizonyítottuk tehát be, hogy S_n minden permutációja előáll az (12) és $(1, 2, \ldots, n)$ ciklusokból a kompozíció véges sokszori alkalmazásával. Persze egy-egy ilyen szorzatban mindkét ciklust rengetegszer felhasználtuk.

4.2.25. Most az (13) és az (1234) permutációkról van szó, és nem kapjuk meg S_4 minden elemét. Egy ilyesfajta bizonyításban kellemetlenséget jelent az, hogy ebből a két ciklusból végtelen sok szorzatot készíthetünk (hiszen akárhány tényező lehet), és nyilván nem tudjuk ellenőrizni minden ilyen szorzat esetében, hogy az soha nem lesz mondjuk (12)-vel egyenlő. E dilemma feloldására két út is kínálkozik.

Az első út az, hogy felírjuk az összes lehetséges permutációt, ami egyáltalán kijöhet. Induljunk ki az 1234 alapsorrendből. Emelést alkalmazva a 2341, 3412, 4123 sorrendek adódnak. Az első és harmadik lapot megcserélve az eredmény rendre 3214, 4321, 1432, 2143. Eddig nyolc lehetséges sorrend jött ki. De tovább már nem kell csinálni a dolgot, mert könnyű végigszámolni, hogy semelyik mozdulat nem ad már új sorrendet. Tehát az adott két mozdulattal csak nyolc sorrend valósítható meg, nem az összes.

Azon túl, hogy ez a bizonyítás nem elegáns, probléma lehet, hogy nagyobb kártyacsomag és több mozdulat esetén a kapott rengeteg sorrend felsorolása esetleg már számítógéppel sem lehetséges. Jobb lenne egy *elvet* találni, ami szintén megmutatja, hogy nem jöhet ki minden sorrend.

Rakjuk a négy kártyalapot körben rá egy négyzet négy csúcsára. Az első és a harmadik lap tehát az egyik átló két végpontjára kerül. Ha ezeket megcseréljük, miközben a másik két lap a helyén marad, akkor a négyzetet a másik átlójára tükröztük. Az emelések nyilván a négyzet forgatásainak felelnek meg. Ha tehát ezeket a mozdulatokat többször elvégezzük, akkor is mindig a négyzet egy egybevágósági transzformációját kapjuk (átló átlóba, oldal oldalba megy). Tehát olyan sorrendet, mint például 2134, soha nem kaphatunk, hiszen ennél az 13 átlóból a 23 oldal keletkezne.

4.2.26. Az A_n minden eleme előáll transzpozíciók szorzataként, és mivel ezek páros permutációk, a szereplő transzpozíciók száma is páros. Így elegendő megmutatni, hogy két transzpozíció szorzata felírható hármasciklusok szorzataként.

Tekintsük tehát az (ab) és (cd) transzpozíciók szorzatát. Ha ez a kettő ugyanaz, akkor a szorzatuk az identitás (ami nulla darab hármasciklus szorzata). Ha egy közös elemük van, akkor a szorzatuk maga hármasciklus: $(ab)(bd) = (abd)$. Végül ha diszjunktak, akkor

$$(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)\,.$$

4.2.27. Tegyük fel, hogy $f \circ (1, 2, \dots, n) = (1, 2, \dots, n) \circ f$, és jelölje i az $f(1)$ elemet. Tudjuk, hogy j-t az $(1, 2, \dots, n)$ ciklus $j+1$-be viszi, ha $j < n$, és 1-be, ha $j = n$. Vagyis a mod n összeadás jelét felhasználva tömören azt mondhatjuk, hogy j képe $j +_n 1$ lesz. Ezért

$$f(2) = \big(f \circ (1, 2, \dots, n)\big)(1) = \big((1, 2, \dots, n) \circ f\big)(1) = i +_n 1\,.$$

Az 1 helyett 2-t helyettesítve $f(3) = i +_n 1 +_n 1 = i +_n 2$, és így tovább, általában $f(j) = i + n(j-1) = j +_n (i-1)$. Vagyis f nem egyéb, mint az $(1, 2, \dots, n)$ ciklus $i-1$-edik hatványa. Összesen tehát n darab f permutáció felel meg a feltételeknek.

4.2.28. Egy permutáció akkor és csak akkor hatványa egy ciklusnak, ha egyforma hosszú diszjunkt ciklusok szorzata. Ennek igazolásához emeljük az $(1, 2, \dots, n)$ ciklust k-adik hatványra. Például $(123456)^4 = (153)(264)$. Általában, amikor az 1-ből elindulunk, akkor k-asával lépegetünk az n hosszú körön. Ezért a „bolhás” 1.5.8. Feladat szerint $n/(n, k)$ lépésben érünk vissza a kiindulópontra. Vagyis az 1 (és ugyanígy bármelyik másik elem is) egy $n/(n, k)$ hosszú ciklusba kerül. Tehát ez a hatvány egyforma hosszú diszjunkt ciklusok szorzata.

Megfordítva, tegyük fel, hogy adva van tetszőlegesen k darab m hosszú diszjunkt ciklus szorzata. Vegyük az $(1, 2, \dots, km)^k$ permutációt, ez a fentiek szerint szintén k darab m hosszú diszjunkt ciklus szorzata (csak más számok vannak a ciklusokban). Tehát át tudjuk számozni az $(1, 2, \dots, km)$ elemeit úgy, hogy a k-adik hatvány pont a mi előre adott permutációnk legyen. (Például ha az $(12)(34)$ van előre megadva, de az $(1234)^2$ eredménye $(13)(24)$, akkor a $2 \leftrightarrow 3$ átszámozást kell végrehajtani, és így $(1324)^2 = (12)(34)$.)

4.2.29. Tegyük fel, hogy G összefüggő. A könyvespolcon a könyveket most úgy kell rendbe rakni, hogy az élek által kijelölt helyeken cserélhetünk. Ez is lehetséges, a következőképpen. Keressük meg azt a könyvet, ami a legbaloldali helyre való. Azt a helyet, ahol ez a könyv van, egy G-beli út összeköti a legbaloldali hellyel. Az út éleinek megfelelő cseréket sorban alkalmazva ez a könyv a helyére kerül. Ezután folytathatjuk a balról második helyre való könyvvel, és így tovább.

Most tegyük fel, hogy a G gráfban nincs út i és j között. Ha egy transzpozíciót alkalmazunk, akkor minden pont vagy helyben marad, vagy a gráf egy éle mentén mozdul el. Ezért akárhogyan is szorzunk össze transzpozíciókat, az i pont soha nem tud j-be eljutni.

4.2.30. Minden k hosszú ciklus $k-1$ transzpozíció szorzata (lásd 4.2.19. Gyakorlat). Ha S_n egy permutációját diszjunkt ciklusok szorzatára bontjuk, akkor ezek összhossza legfeljebb n, és így összesen legfeljebb $n-1$ transzpozíció fog szerepelni.

Az $(1, 2, \dots, n)$ ciklus előállításához legalább $n-1$ transzpozícióra van szükség. Vegyünk ugyanis egy előállítást, és készítsük el az ebben szereplő transzpozíciókból az előző feladatban leírt G gráfot. Az $(1, 2, \dots, n)$ ciklus többszöri alkalmazásával bármelyik pontból bármelyik pontba el lehet jutni. Így az előző feladat (2) állítása miatt a G gráf összefüggő, és az A.2.5. Tétel miatt legalább $n-1$ éle van.

4.2.31. Az Útmutatóban leírtakat folytatva tegyük fel, hogy $k + t - 1 \leq n$, és hogy az állítás n-nél kisebb elemszámú halmazon igaz. A gráf triviálisan összefüggő, ha $k = 1$. Ha $k > 1$, akkor $k \neq t$ (mert k és t relatív prímek), a k és t esetleges cseréjével feltehető, hogy $k < t$. Tekintsük $1 \leq a \leq n - t$ esetén az $a < a + t - k < a + t$ hármast. Itt a és $a + t$ valamint $a + t - k$ és $a + t$ között megy él, és így a és $a + t - k$ úttal összeköthető. Húzzuk be az a és $a + t - k$ közötti élt is, elég belátni, hogy az így kapott gráf összefüggő. Most már az $[1, n-k]$ intervallumban a $t-k$ különbségűek össze vannak kötve. Az indukciós feltevést k, t, n helyett $k, t-k, n-k$-ra alkalmazva kapjuk, hogy 1-től $n-k$-ig bármely két pont összeköthető. Szimmetriaokokból ($x \leftrightarrow n+1-x$) a $[k+1, n]$ intervallumban is bármely két pont összeköthető. E két intervallum lefedi $[1, n]$-et, mert $n-k+1 \geq (k+t-1)-k+1 = t > k$ (azaz legalább $k+1$). Mivel van él a két intervallum között is (például $n - k$ és n között), ezért a gráf összefüggő.

4.3. Elemrend, ciklikus csoportok.

4.3.2. Ha az Olvasónak gondot jelent az alábbiak követése, akkor próbálja meg a 1.5. Szakaszban leírt bizonyításokat átvinni az általános esetre. Mi a 3.2.23. Feladatban javasolt módon fogunk eljárni, mert ez rövidebb, elegánsabb, és előkészíti a gyűrűelméletben használt *ideál* fogalmát. Legyen tehát g egy eleme a G csoportnak, és tekintsük az

$$I = \{k \in \mathbb{Z} : g^k = 1\}$$

halmazt, vagyis a g elem jó kitevőinek halmazát. A hatványozás azonosságai miatt I zárt az összeadásra és a $\mathbb{Z}$ elemeivel való szorzásra. Valóban, tegyük fel, hogy $g^k = g^\ell = 1$. Ekkor $g^{k+\ell} = g^k g^\ell = 1$ és $g^{kn} = (g^k)^n = 1^n = 1$. Ezért a 3.2.23. Feladat miatt van olyan d egész szám, hogy I a d többszöröseiből áll, vagyis a jó kitevők pontosan a d többszörösei. Ekkor pedig $g^k = g^\ell$ akkor és csak akkor igaz, ha $g^{k-\ell} = 1$, vagyis ha $d \mid k - \ell$.

Nyilván d helyett $-d$-re is teljesül ugyanez, vagyis feltehető, hogy $d \geq 0$. Ha $d = 0$, akkor csak a nulla lesz jó kitevő, és g minden hatványa különböző. Ekkor lesz g hatványainak száma, azaz rendje végtelen. Ha $d > 0$, akkor d a legkisebb pozitív jó kitevő, hiszen minden jó kitevő d-nek többszöröse. Ebben az esetben a g elemnek pontosan d különböző hatványa van: $g^0 = 1, g, g^2, \ldots g^{d-1}$. A hatvány rendjének képletét a „bolhás" feladat segítségével ugyanígy kapjuk, mint az 1.5.9. Tétel bizonyításában. Végül ha $o(g) = 1$ akkor $g = g^1 = 1$, vagyis g az egységelem (aminek tényleg már az első hatványa is 1).

4.3.7. Egy g egész szám többszöröseiként minden egész akkor áll elő, ha g minden egésznek osztója, azaz egység. Így $\mathbb{Z}^+$ generátorelemei az 1 és a -1. A $\mathbb{Z}_{12}^+$ csoportot pontosan azok az elemek generálják, amelyeknek 12 különböző többszöröse van, vagyis amelyek rendje 12. A hatvány rendjének képletét alkalmazzuk az 1 elemre. Eszerint az $1 \cdot k$ elem rendje $12/(k, 12)$. Ez akkor lesz 12, ha $(k, 12) = 1$, vagyis ha $k = 1, 5, 7, 11$.

4.3.9. Ha $\varphi : G \to H$ és $\psi : H \to K$ homomorfizmusok, akkor $\psi \circ \varphi : G \to K$ is szorzattartó, hiszen

$$(\psi \circ \varphi)(xy) = \psi\big(\varphi(xy)\big) = \psi\big(\varphi(x)\varphi(y)\big) = \psi\big(\varphi(x)\big)\psi\big(\varphi(y)\big) = (\psi \circ \varphi)(x)(\psi \circ \varphi)(y)\,.$$

Tegyük fel, hogy $\psi : G \to H$ izomorfizmus, és legyen φ az inverze. Be kell látni, hogy $\varphi(xy) = \varphi(x)\varphi(y)$. Mivel ψ injektív, elég azt megmutatni, hogy a bal és jobb oldal ψ-nél vett képe megegyezik. De $\varphi(xy)$ képe xy, $\varphi(x)\varphi(y)$ képe pedig ψ művelettartása miatt $\psi\big(\varphi(x)\big)\psi\big(\varphi(y)\big) = xy$. Ezért izomorfizmus inverze tényleg izomorfizmus.

4.3.10. Az identikus leképezés izomorfizmus, ezért minden csoport izomorf önmagával. Ha $\varphi : G \to H$ izomorfizmus, akkor az inverze, $\varphi^{-1} : H \to G$ is az, tehát az izomorfia szimmetrikus. Ha $\varphi : G \to H$ és $\psi : H \to K$ izomorfizmusok, akkor $\psi \circ \varphi : G \to K$ is az, tehát az izomorfia tranzitív.

4.3.11. Ha n pozitív, akkor $g^n = g \cdot g \cdot \ldots \cdot g$, összesen n tényezővel. Mivel ψ szorzattartó,

$$\psi(g^n) = \psi(g \cdot g \cdot \ldots \cdot g) = \psi(g) \cdot \psi(g) \cdot \ldots \cdot \psi(g) = \psi(g)^n\,.$$

Ha $n = 0$, akkor $g^0 = 1_G$, és mivel $\psi(1_G) = 1_H$, ezért $\psi(g^0) = \psi(g)^0$ tényleg teljesül. Végül tegyük fel, hogy n negatív, vagyis $n = -k$, ahol k pozitív. Tudjuk, hogy ψ tartja az inverzet, és hogy $g^n = (g^{-1})^k$. Ezért a már bizonyítottak miatt

$$\psi(g^n) = \psi\big((g^{-1})^k\big) = \big(\psi(g^{-1})\big)^k = \big(\psi(g)^{-1}\big)^k = \psi(g)^n\,.$$

4.3.12. Ha $g^k = 1_G$, akkor $1_H = \psi(g^k) = \psi(g)^k$, tehát k jó kitevője $\psi(g)$-nek is. Speciálisan $k = o(g)$ esetén azt kapjuk, hogy $\psi(g)$ rendje osztója g rendjének. Ha izomorfizmusról van szó, akkor az oszthatóság fordítva is fennáll (mert ψ inverzére alkalmazhatjuk az előző észrevételt). Tehát ilyenkor a két elem rendje megegyezik.

4.3.13. Tegyük fel, hogy G kommutatív, és legyen $h_1, h_2 \in H$. Mivel ψ szürjektív, van olyan $g_1, g_2 \in G$, hogy $\psi(g_1) = h_1$ és $\psi(g_2) = h_2$. Így

$$h_1h_2 = \psi(g_1)\psi(g_2) = \psi(g_1g_2) = \psi(g_2g_1) = \psi(g_2)\psi(g_1) = h_2h_1\,.$$

Most azt tegyük fel, hogy G a b elem hatványaiból áll. Megmutatjuk, hogy H a $\psi(b)$ elem hatványaiból áll. Valóban, ha $h \in H$, akkor ψ szürjektivitása miatt van olyan $g \in G$, hogy $\psi(g) = h$. Ekkor $g = b^n$ alkalmas n egészre, és innen $h = \psi(g) = \psi(b^n) = \psi(b)^n$.

4.3.19. Egy Abel-csoportban mindig részcsoportot alkotnak azok a g elemek, amelyekre $g^n = 1$ teljesül. Speciálisan az n-edik egységgyökök az $\varepsilon = \cos(2\pi/n) + i\sin(2\pi/n)$ hatványai, tehát ciklikus csoportot alkotnak. Ennek rendje n, tehát tényleg $\varphi(n)$ generátora van. Ezek a generátorok a primitív n-edik egységgyökök (azok a számok, amelyek hatványai pontosan az n-edik egységgyökök).

4.3.22. A $\mathbb{Z}_m^+$ csoport ciklikus, az 1 generálja. A hatvány rendjének képlete miatt $k = 1 \cdot k$ rendje $m/(m, k)$. Ennek alapján $\mathbb{Z}_7^+$, $\mathbb{Z}_8^+$ és $\mathbb{Z}_{12}^+$ elemeinek rendjei kiszámíthatók.

Most számítsuk ki $\mathbb{Z}_7^\times$-ben a 3 rendjét. A 3 számot addig kell hatványozni modulo 7, amíg 1-et nem kapunk. Nyilván $3^1 = 3$ és $3^2 = 3 *_7 3 = 2$. A 3^3 kiszámításakor felhasználhatjuk, hogy 3^2 értéke 2 mod 7, így $3^3 = 2 *_7 3 = 6$. A hatványozást tovább folytatva $3^4 = 4$, innen $3^5 = 5$, végül $3^6 = 1$ adódik. Tehát a 6 a legkisebb olyan pozitív szám, amire 3-at emelve 1-et kapunk mod 7, és így a 3 rendje ebben a csoportban 6.

Most mutatunk egy olyan lehetőséget, amivel a fenti számolás egy részét megspórolhatjuk. A számelméletből ismerjük (de be is fogjuk látni a 4.4.17. Gyakorlatban) az Euler–Fermat-tételt, miszerint ha az a és n pozitív egészek relatív prímek, akkor $a^{\varphi(n)} \equiv 1\ (n)$. Ez azt jelenti, hogy $\varphi(n)$ jó kitevője a-nak, és így minden elem rendje csak a $\varphi(n)$ osztói közül kerülhet ki. A fenti példában $\varphi(7) = 6$, hiszen a 7 prímszám. Ezért a 3 rendje csak 6-nak osztója lehet. Amikor tehát elérkezünk arra pontra, hogy 3^3 értéke sem 1 mod 7, akkor a negyedik, ötödik, hatodik hatványt már fölösleges kiszámolni, hiszen a 6-nak 3-nál nagyobb osztója csakis a 6 lehet.

Ezek szerint a hatelemű $\mathbb{Z}_7^\times$ csoport a 3 hatványaiból áll, vagyis ciklikus. Így a többi elem rendjét megkapjuk, ha a hatvány rendjének a képletét alkalmazzuk a 3 hatványaira. Az eredmény:

$$o(2) = o(3^2) = 6/(6, 2) = 3\,,$$
$$o(6) = o(3^3) = 6/(6, 3) = 2\,,$$
$$o(4) = o(3^4) = 6/(6, 4) = 3\,,$$
$$o(5) = o(3^5) = 6/(6, 5) = 6\,,$$

végül az egységelem rendje természetesen 1.

Az 1.1.13. Gyakorlatban már beláttuk, hogy $\mathbb{Z}_8^\times$ mind a négy elemének a négyzete az egységelem. Ezért az egységelem rendje 1, a 3, 5, 7 elemek rendje 2. Ugyanígy a $\mathbb{Z}_{12}^\times$ csoportban is minden elem négyzete az egységelem, tehát itt 5, 7, 11 rendje szintén 2.

4.3.23. A keresett elemrendek a következők.

(1) Végtelen, a -1 többesei az egész számok.
(2) 2, mert $-1 \neq 1$, de $(-1)^2 = 1$.
(3) A hatvány rendjének képlete miatt $19/(19, 17) = 19$.
(4) A 17-nek az Euler–Fermat-tétel miatt $\varphi(19) = 18$ jó kitevője, így a keresett rend osztója 18-nak. A hatványozást a 17 helyett kényelmesebb a vele mod 19 kongruens -2-vel végezni. Az eredmény $o(17) = 9$ lesz.
(5) A hatvány rendjének képlete miatt $32/(32, 3) = 32$.
(6) A 3 rendje $\varphi(32) = 16$-nak osztója. Hatványozással látható, hogy ez a rend 8.
(7) Az $x + 1$ polinom többszörösei az $nx + n$ alakú polinomok, ahol $n \in \mathbb{Z}_{11}$. Ezek mind különbözők, és így a keresett rend 11.

(8) Mivel a 11 prímszám, a $\mathbb{Z}_{11}$ test. Így a $\mathbb{Z}_{11}[x]$ polinomgyűrű invertálható elemei (egységei) a 3.1.11. Gyakorlat szerint a nem nulla konstans polinomok. Vagyis a $\mathbb{Z}_{11}[x]^\times$ csoport ugyanaz, mint a $\mathbb{Z}_{11}^\times$ csoport. Ebben az 5 rendje csakis $\varphi(11) = 10$ osztója lehet. A hatványozást elvégezve 5 adódik eredményül.

4.3.24. A 4.3.3. Állítást alkalmazva a 4.2.21. Gyakorlat eredményére a keresett rendek a következők:

$$o\big((1254)(36)(78)\big) = 4\,, \qquad o\big((1234)(35)(1432)(35)\big) = o\big((345)\big) = 3\,,$$
$$o\big((158)(27)(36)\big) = 6\,, \qquad o\big((12345)(234)(12345)^{-1}\big) = o\big((345)\big) = 3\,,$$
$$o\big((acedb)\big) = 5\,, \qquad o\big([(12)(23)(34)]^{1222}\big) = o\big((13)(24)\big) = 2\,,$$

végül a „hátulról előre” permutáció rendje 2 (ha $n > 1$).

4.3.25. Összesen $(n-1)!$ ilyen ciklus van. Valóban, mivel a ciklust bármelyik elemével kezdhetjük, az első helyre 1-et írhatunk. Tehát a ciklus így néz ki: $(1, x_1, \ldots, x_{n-1})$. Ilyen ciklust nyilván $(n-1)!$-féleképpen írhatunk fel, azt kell megmutatni, hogy ezek mind különböző permutációk.

Tegyük fel, hogy $(1, x_1, \ldots, x_{n-1}) = (1, y_1, \ldots, y_{n-1})$. Az 1 képe az első ciklusnál x_1, a másodiknál y_1. Mivel egyenlő permutációkról van szó, $x_1 = y_1$. Ennek az elemnek a képe az első permutációnál x_2, a másodiknál y_2, így $x_2 = y_2$. Tovább haladva sorra látjuk, hogy $x_i = y_i$ minden i-re.

4.3.26. A 4.3.3. Állítás szerint az elemrend a ciklushosszak legkisebb közös többszöröse. Egy másodrendű elem tehát csak diszjunkt transzpozíciók szorzata lehet, és mivel A_7 elemei páros permutációk, ebben a szorzatban páros számú transzpozíciónak kell szerepelnie. Így a szereplő transzpozíciók száma csakis 2 lehet (mert nulla transzpozíció az identitást adná, ami nem másodrendű, négy diszjunkt transzpozíció pedig nem fér el egy hételemű halmazon). Az $(ab)(cd)$ alakú elemek száma

$$\binom{7}{4} \cdot 3 = 105\,,$$

hiszen ha kiválasztottuk a négyelemű $\{a, b, c, d\}$ halmazt, akkor ezekből három ilyen permutációt készíthetünk: $(ab)(cd)$ mellett még $(ac)(bd)$-t és $(ad)(bc)$-t is.

Harmadrendű elem vagy hármasciklus, vagy két hármasciklus szorzata lehet. A hármasciklusok száma

$$\binom{7}{3} \cdot 2 = 70\,,$$

hiszen ha kiválasztottuk az $\{a, b, c\}$ halmazt, akkor ezekből két hármasciklust csinálhatunk: (abc)-t és (acb)-t. Két diszjunkt hármasciklust

$$\frac{1}{2} \cdot \binom{7}{3} \cdot 2 \cdot \binom{4}{3} \cdot 2 = 280$$

módon választhatunk ki (az elsőt, mint láttuk 70-féleképpen, a másodikat a megmaradó négyelemű halmazon 8-féleképpen, de így minden permutációt kétszer számoltunk, hiszen a két hármasciklus megcserélhető). Összesen tehát 350 darab harmadrendű elem van.

Negyedrendű elemet úgy kaphatunk, ha a ciklusok hosszának legkisebb közös többszöröse 4. Tehát a permutáció diszjunkt négyesciklusok és transzpozíciók szorzata, de egy négyesciklusnak mindenképpen szerepelnie kell. Mivel ez páratlan permutáció, kell mellé még egy transzpozíció is (más már nem fér el a 7 elemen). Tehát az $(abcd)(ef)$ alakú elemek lesznek negyedrendűek. Ezek száma

$$\binom{7}{4} \cdot (4-1)! \cdot \binom{3}{2} = 630\,.$$

Ugyanis ha $\{a, b, c, d\}$ megvan, akkor ezekből az előző feladat szerint $(4-1)!$-féleképpen készíthetünk négyesciklust, a megmaradó háromelemű halmazon pedig háromféleképpen vehetünk egy transzpozíciót.

Ötödrendű elem csak egy ötösciklus lehet, ezek száma

$$\binom{7}{5} \cdot (5-1)! = 504\,.$$

Hatodrendű elem csak $(abc)(de)(fg)$ alakú lehet (mert minden hatosciklus páratlan permutáció), ezek száma

$$\binom{7}{4} \cdot 2 \cdot 3 = 210$$

(nyilván kétszer annyi van, mint másodrendű elem, hiszen minden másodrendű elem mellé kétféle hármasciklust írhatunk). Végül tizenkettedrendű elem nincs A_7-ben, mert egy ilyenben négyes- és hármasciklusnak is lennie kellene, de mindkettőből csak egy fér el, $(abcd)(efg)$ pedig páratlan permutáció.

4.3.27. Ha G véges, és $1 \neq g \in G$, akkor $1 < o(g)$ véges, hiszen g-nek csak véges sok hatványa lehet. Így $o(g)$-nek van egy p prímosztója. Ha $n = o(g)/p$, akkor a hatvány rendjének képlete szerint $o(g^n) = o(g)/n = p$.

4.3.28. A hatvány rendjének képlete szerint $\big(o(g), k\big) = 1$ akkor és csak akkor, ha g^k rendje és g rendje ugyanaz. Mivel g^k hatványai egyben a g hatványai is, e két elemnek akkor és csak akkor van ugyanannyi hatványa, ha a hatványaik halmaza megegyezik. Ha ez a két halmaz megegyezik, akkor persze g is hatványa g^k-nak. Megfordítva, ha g hatványa g^k-nak, akkor g minden hatványa is hatványa g^k-nak, tehát a két halmaz megegyezik.

4.3.29. A hatvány rendjének képletét (4.3.2. Gyakorlat) alkalmazva

$$n = o(g) = \frac{o(h)}{\big(o(h), m\big)}$$

adódik. Ezért $m \mid n \mid o(h)$, és így $\big(o(h), m\big) = m$, vagyis $o(h) = mn$.

4.3.30. Az első állítás igaz a 4.3.17. Lemma miatt. A második állítás nem igaz. Például a 4.3.22. Gyakorlat szerint a $\mathbb{Z}_8^\times$ csoportban három másodrendű elem van, holott $\varphi(2) = 1$.

4.3.31. Nem ciklikus. Ha ε egy 3^n-edik egységgyök, akkor a rendje véges (és 3^n-nek osztója). Ezért csak véges sok hatványa van, nem kaphatjuk meg az egész csoportot, amelynek végtelen sok eleme van.

4.3.32. Legyen $o(g) = n$ és $o(h) = m$. Ekkor $(gh)^{nm} = (g^n)^m(h^m)^n = 1^m 1^n = 1$, vagyis $k = o(gh)$ osztója nm-nek. A $(gh)^k = 1$ összefüggést n-edik hatványra emelve $1 = (gh)^{kn} = (g^n)^k h^{kn} = 1^k h^{kn} = h^{kn}$ adódik, vagyis $m = o(h)$ osztója kn-nek. De $(m, n) = 1$, így $m \mid k$. Szerepcserével kapjuk, hogy $n \mid k$. Mivel $(n, m) = 1$, ezért $nm \mid k$.

A feltételek egyike sem hagyható el. Ha $g = h^{-1}$, akkor rendjeik egyenlők (tehát $g \neq 1$ esetén nem relatív prímek), a gh rendje viszont 1 (és nem a két egyenlő rend szorzata). Ha pedig az S_3 csoportban a $g = (12)$ és $h = (123)$ elemeket vesszük, akkor ezek nem felcserélhetők, a g rendje 2, a h rendje 3, de a $gh = (23)$ szorzat rendje 2, és nem 6.

4.3.33. Az $(ab)^2 = 1$ összefüggést balról a-val, jobbról b-vel szorozva $aababb = ab$ adódik. De $a^2 = 1 = b^2$, és így $aababb = ba$. Tehát G Abel-csoport. Negyedik hatványra a négyzet szimmetriacsoportja lesz ellenpélda. Ebben négy forgatás és négy tükrözés van, valamennyinek a negyedik hatványa az identitás. Ugyanakkor egyik tengelyes tükrözés sem cserélhető fel egy 90 fokos forgatással. Ez közvetlen geometriai megfontolásokkal, vagy a 4.1.8. Állítás segítségével látható be.

4.3.34. Legyen $d = (a^n - 1, a^m - 1)$. Az $a^{(n,m)} - 1 \mid d$ oszthatóságot elemi számelméleti úton látjuk be. Az $x^n - 1 = (x - 1)(1 + x + \ldots + x^{n-1})$ azonosság miatt $x - 1$ osztója $x^n - 1$-nek minden x egészre. Speciálisan ha $k \mid n$, akkor a^n hatványa a^k-nak, és így $a^k - 1 \mid a^n - 1$. Ezért $a^{(n,m)} - 1$ osztója $a^n - 1$-nek is és $a^m - 1$-nek is, vagyis a legnagyobb közös osztójuknak is

A fordított oszthatóság bizonyításához vegyük észre, hogy $d \mid a^n - 1$, vagyis az a szám mod d vett n-edik hatványa 1. Ezért n jó kitevője az $a \in \mathbb{Z}_d^\times$ csoportelemnek, vagyis $o(a) \mid n$. Ugyanígy kapjuk, hogy $o(a) \mid m$. Tehát $o(a)$ osztója az n és m legnagyobb közös osztójának is, és így ez is jó kitevője a-nak, vagyis $d \mid a^{(n,m)} - 1$. Ezzel az állítást beláttuk.

A most elmondott bizonyításban van egy apró pontatlanság. Benne van-e az a szám a $\mathbb{Z}_d^\times$ csoportban? Az a nyilván relatív prím d-hez, hiszen $d \mid a^n - 1$. Az azonban előfordulhat, hogy a nem esik a $[0, d-1]$ intervallumba. Ezért ekkor a helyett a mod d vett $\overline{a}$ maradékával kell elmondani a fenti gondolatmenetet. Ez működik, hiszen a és $\overline{a}$ kongruensek mod d, és így tetszőleges k-ra $d \mid \overline{a}^k - 1$ akkor és csak akkor, ha $d \mid a^k - 1$. Az ilyen problémák kiküszöbölésére a számelméletben szokás tetszőleges d-hez relatív prím a szám rendjéről beszélni mod d, ami alatt az $\overline{a}$ maradéknak a rendjét értik. Erre az általánosabb rendfogalomra is nyilván érvényben marad, hogy $a^k \equiv 1\ (d)$ akkor és csak akkor, ha $o(a) \mid k$.

4.3.35. Jelölje $\overline{\Phi_n}$ a mod p vett Φ_n polinomot. Tegyük fel, hogy $\varepsilon \in \mathbb{Z}_p$ gyöke $\overline{\Phi_n}$-nak, és legyen ℓ az ε rendje $\mathbb{Z}_p$ multiplikatív csoportjában. Mivel $\Phi_n(x) \mid x^n - 1$, ezért $\varepsilon^n - 1 = 0$. Tehát n jó kitevője ε-nak, és így $\ell \mid n$.

Tegyük fel indirekte, hogy $\ell < n$. Ekkor ε gyöke már az $x^\ell - 1 \in \mathbb{Z}_p[x]$-nek is. De $x^\ell - 1 = \prod_{d\mid\ell} \Phi_d(x)$, vagyis van olyan $m \mid \ell$, hogy $\overline{\Phi_m}(\varepsilon) = 0$. Tehát az $x - \varepsilon$ gyöktényező kiemelhető a $\overline{\Phi_n}$ és a $\overline{\Phi_m}$ polinomokból. Persze $m \mid n$ és $m \neq n$, azaz ekkor ε legalább kétszeres gyöke $\overline{\Phi_m(x)}\,\overline{\Phi_n(x)} \mid x^n - 1$-nek. Az $x^n - 1$ polinomnak azonban nincs többszörös gyöke $\mathbb{Z}_p$-ben a 3.6.12. Gyakorlat miatt. Ez az ellentmondás bizonyítja, hogy ε rendje tényleg n.

Legyen most ε egy n-edrendű eleme $\mathbb{Z}_p^\times$-nek. Ekkor ε gyöke $x^n - 1 = \prod_{d\mid n} \overline{\Phi_d}(x)$-nek, tehát valamelyik $\overline{\Phi_d}$-nak is. Ha $d \neq n$ lenne, akkor $\Phi_d(x) \mid x^d - 1$ miatt $\varepsilon^d = 1$ teljesülne, ami ellentmond annak, hogy ε rendje n.

4.3.36. Tegyük fel, hogy a p prím osztja a $\Phi_n(nN)$ kifejezést (ahol N egész). Tudjuk, hogy $\Phi_n(nN) \mid (nN)^n - 1$, tehát p nem osztója n-nek. Az nN szám gyöke $\Phi_n(x)$-nek mod p, mert $p \mid \Phi_n(nN)$. Így az előző feladat miatt nN rendje n lesz mod p. Az Euler–Fermat-tétel miatt tudjuk, hogy $\mathbb{Z}_p^\times$ minden elemének rendje osztója $\varphi(p) = p - 1$-nek. Ezért $n \mid p - 1$, vagyis a p prím $nk + 1$ alakú.

Meg kell még mutatni, hogy $\Phi_n(nN)$-nek van prímosztója alkalmas N esetén. Ez nyilvánvaló, hiszen a nem konstans $\Phi_n(nx)$ polinom minden értéket csak véges sok helyen vehet fel (2.4.9. Gyakorlat), és így van olyan N, amikor a $\Phi_n(nN)$ érték 1-től és -1-től is különbözik.

4.4. Részcsoportok.

4.4.1. Ha H részcsoport, akkor $a, b \in H$ esetén $b^{-1} \in H$, és így $ab^{-1} \in H$. Megfordítva, tegyük fel, hogy tetszőleges $a, b \in H$ esetén $ab^{-1} \in H$. Mivel H nem üres, van egy c eleme. Ekkor $a = b = c$ választással $1 = cc^{-1} \in H$. Ezután $a = 1$ választással látjuk, hogy H zárt az inverzképzésre. Így zárt a szorzásra is, mert ha $a, d \in H$, akkor $b = d^{-1} \in H$, és a feltétel szerint $ad = ab^{-1} \in H$.

4.4.3. Azt kell megmutatni, hogy $(XY)Z = X(YZ)$. Ez igaz, mert mindkét halmaz az $(xy)z = x(yz)$ alakú elemekből áll, ahol $x \in X$, $y \in Y$, $z \in Z$. A második állítás hasonlóan következik az $(xy)^{-1} = y^{-1}x^{-1}$ azonosságból.

4.4.4. (1) $\Longrightarrow$ (2). Ha H részcsoport, akkor zárt a szorzásra és az inverzképzésre, tehát $HH \subseteq H$ és $H^{-1} \subseteq H$. De $H\{1\} = H$, tehát HH az egész H. Továbbá $H^{-1} = H$, hiszen H minden eleme a saját inverzének az inverze.

(2) $\Longrightarrow$ (3). Ha (2) igaz, akkor nyilván $HH^{-1} = HH = H \subseteq H$.

(3) $\Longrightarrow$ (1). Ez pontosan a 4.4.1. Gyakorlat állítása, a komplexusok nyelvén kifejezve.

Végül tegyük fel, hogy H részcsoport, és $h \in H$. Nyilván $hH \subseteq H$. Ugyanakkor $k \in H$ esetén $k = h(h^{-1}k)$, és mivel $h^{-1}k \in H$, ezért $k \in hH$. Vagyis $H \subseteq hH$. Beláttuk tehát, hogy $hH = H$. Ugyanígy igazolható az is, hogy $Hh = H$.

4.4.11. Nyilván $a = a1 \in aH$. Ha $a \in bH$, akkor az aH és bH mellékosztályoknak van közös eleme (az a elem), és így megegyeznek.

Ha az Olvasó számára ez túlságosan misztikus bizonyítás, akkor az állítást az eddigiekre való hivatkozás nélkül is könnyen ellenőrizheti. Ha $a \in bH$, akkor $a = bh$ alkalmas $h \in H$ elemre. Ekkor $aH = bhH = bH$, mert $hH = H$.

4.4.12. A keresett mellékosztályok a következők.

$$\begin{array}{rcl} idH = \{id, (12)\} & = & \{id, (12)\} = Hid \\ (12)H = \{(12), id\} & = & \{(12), id\} = H(12) \\ (123)H = \{(123), (13)\} & \neq & \{(123), (23)\} = H(123) \\ (132)H = \{(132), (23)\} & \neq & \{(132), (13)\} = H(132) \\ (13)H = \{(13), (123)\} & \neq & \{(13), (132)\} = H(13) \\ (23)H = \{(23), (132)\} & \neq & \{(23), (123)\} = H(23)\,. \end{array}$$

Látjuk, hogy három különböző bal oldali mellékosztály van, amelyek S_3 egy partícióját alkotják (hiszen $idH = (12)H$, $(123)H = (13)H$ és $(132)H = (23)H$). Ugyanígy három különböző jobb oldali mellékosztály van, amelyek S_3-nak egy másik partícióját alkotják.

4.4.13. Az $a + n\,\mathbb{Z}^+$ és $b + n\,\mathbb{Z}^+$ mellékosztályok akkor és csak akkor egyeznek meg, ha $a - b \in n\,\mathbb{Z}^+$, azaz ha $a \equiv b\ (n)$. Tehát minden szám mellékosztálya ugyanaz, mint az n-nel való osztási maradékának a mellékosztálya. A lehetséges osztási maradékok, azaz $0, 1, \ldots, n-1$ viszont csupa különböző mellékosztályban vannak, és így a mellékosztályok száma ugyanannyi, mint ezeknek a maradékoknak a száma, vagyis n.

4.4.14. Ha aH bal oldali mellékosztály, akkor $(aH)^{-1} = H^{-1}a^{-1} = Ha^{-1}$, ami egy jobb oldali mellékosztály. Ugyanígy egy jobb oldali mellékosztály komplexus-inverze bal oldali mellékosztály lesz. Mivel inverz inverze az eredeti mellékosztály, egy kölcsönösen egyértelmű megfeleltetést kaptunk a bal és jobb oldali mellékosztályok halmaza között.

4.4.17. Legyen $\overline{a}$ az a-nak n-nel való osztási maradéka. Ez is relatív prím n-hez, és így eleme a $\mathbb{Z}_n^\times$ csoportnak. E csoport rendje $\varphi(n)$, és ezért a 4.4.16. Következmény miatt az $\overline{a}$ elemet $\varphi(n)$-edik hatványra emelve az egységelemet, vagyis az 1-et kapjuk. Kongruenciával ezt így írhatjuk: $\overline{a}^{\varphi(n)} \equiv 1\ (n)$. De akkor $a^{\varphi(n)} \equiv 1\ (n)$ is teljesül.

Mint láthatjuk, egyre több kényelmetlenséget okoz, hogy a $\mathbb{Z}_n^\times$ csoport kapcsán csak a 0 és $n-1$ közötti elemek számelméletéről beszélhetünk közvetlenül. Már említettük korábban is, hogy ezen a problémán a maradékosztályok fogalmának bevezetése segít. Ezek nem mások, mint az $n\,\mathbb{Z}^+$ részcsoport szerinti mellékosztályok $\mathbb{Z}^+$-ban. A faktorcsoport és a faktorgyűrű bevezetésekor meglátjuk majd, hogyan lehet ezekkel műveleteket végezni, és akkor a $\mathbb{Z}_n^\times$ csoport szerepét is átértékeljük majd.

4.4.18. A hatványozás azonosságai (2.2.18. Gyakorlat) szerint $g^n g^m = g^{n+m}$, továbbá g^n inverze g^{-n}. Ezért a g hatványainak (nem üres) halmaza zárt a szorzásra és az inverzképzésre, vagyis részcsoport.

4.4.21. A 4.4.20. Állítás bizonyítása most is működik, csak egy apró módosítást kell tennünk. Amikor azt igazoljuk, hogy a megadott elemek részcsoportot alkotnak, problémát okozhat, hogy az $a = m_1 g_1 + \ldots + m_n g_n$ elemhez egy $b = k_1 g'_1 + \ldots + k_\ell g'_\ell$ típusú összeget kell hozzáadni, ahol $g_i, g'_j \in X$. Ezt úgy oldhatjuk meg, hogy mindkét összeget kibővítjük nulla együtthatójú tagokkal. Ha g'_j nem szerepel a $g_1, \ldots, g_n$ között, akkor bevesszük a-ba nulla együtthatóval. Ugyanígy kibővítjük b-t is a g_i elemekkel. Így (új jelölést alkalmazva) már ugyanazok az X-beli elemek szerepelnek mindkét kombinációban, és ezért el tudjuk végezni az összevonást.

4.4.24. Ha H és K is legszűkebb az adott halmazrendszerben, akkor $H \subseteq K$ (hiszen H legszűkebb), és $K \subseteq H$ (hiszen K is legszűkebb). Ezért $H = K$.

Ha H legszűkebb elem, akkor minimális is. Valóban, ha nem volna az, akkor létezne a rendszerben egy K elem, amely H-nak valódi része. Mivel H legszűkebb, $H \subseteq K$, ami nyilvánvalóan lehetetlen.

Aki most találkozik először a „legszűkebb” és „minimális” kifejezésekkel, annak érdemes megoldania a 4.4.32. Gyakorlatot is, ahol konkrét példákat láthat legszűkebb és minimális elemekre.

4.4.25. Legyen H a H_i részcsoportok metszete. Ez nem üres, mert az egységelem mindegyik H_i részcsoportnak eleme, és így a metszetben is benne lesz. Ha a és b elemei H-nak, akkor elemei mindegyik H_i-nek is. Mivel H_i részcsoport, tartalmazza az ab és az a^{-1} elemeket. Ez minden i-re igaz, és így $ab, a^{-1} \in H$. Ezért H zárt a szorzásra és az inverzképzésre, tehát részcsoport.

4.4.28. Tegyük fel, hogy ψ és φ is G-ből H-ba vezető homomorfizmusok, melyekre $\psi(g_i) = \varphi(g_i)$ mindegyik i-re. Meg kell mutatni, hogy akkor $\psi(g) = \varphi(g)$ tetszőleges $g \in G$ elemre. Ezt a 4.4.27. Tétel alkalmazásával is könnyen kihozhatnánk: a g elemet fel lehet írni a g_i és g_i^{-1} elemek alkalmas szorzataként, és a művelettartás miatt látnánk, hogy ψ és φ a g elemen is megegyezik. Elegánsabb azonban a következő gondolatmenet, rögtön végtelen X generátorrendszerre.

Tegyük fel, hogy $\psi(x) = \varphi(x)$ minden $x \in X$-re. Jelölje K azon $k \in G$ elemek halmazát, amelyekre $\psi(k) = \varphi(k)$. Ez részcsoportja G-nek, hiszen az egységelemet tartalmazza, és zárt a műveletekre. Valóban, ha $k_1, k_2 \in K$, akkor $\psi(k_1) = \varphi(k_1)$ és $\psi(k_2) = \varphi(k_2)$, ezért

$$\psi(k_1 k_2) = \psi(k_1)\psi(k_2) = \varphi(k_1)\varphi(k_2) = \varphi(k_1 k_2)\,,$$

vagyis $k_1 k_2 \in K$. Hasonlóan látható be az is, hogy K zárt az inverzképzésre.

A K részcsoport tartalmazza az X elemeit. De X generálja G-t, vagyis G a legszűkebb X-et tartalmazó részcsoport. Mivel K egy X-et tartalmazó részcsoport, ezért $G \subseteq K$ (valójában $K = G$), vagyis ψ és φ tényleg megegyezik G minden elemén.

4.4.29. A komplexusokkal való számolás (a 4.4.3. Gyakorlat) lehetővé teszi ennek az állításnak az egészen gyors igazolását. Ha $H = AB$ részcsoport, akkor $H^{-1} = H$, és így

$$AB = H = H^{-1} = (AB)^{-1} = B^{-1}A^{-1} = BA\,.$$

Megfordítva, ha $H = AB = BA$, akkor

$$HH = ABAB = AABB = AB = H\,,$$

és

$$H^{-1} = (AB)^{-1} = B^{-1}A^{-1} = BA = AB = H\,,$$

tehát a 4.4.4. Gyakorlat miatt H részcsoport.

Jelölje K az A és B által generált részcsoportot. Mivel K részcsoport, AB, $BA \subseteq K$. Ha viszont $AB = BA$ részcsoport, akkor ez tartalmazza az A és B részcsoportokat ($A\{1\}$ és $\{1\}B$ formában). Ezért a legszűkebb A-t és B-t tartalmazó részcsoport (vagyis K) része $AB = BA$-nak. Tehát $K = AB = BA$.

4.4.31.

(1) Igen, az osztályok a $\mathbb{Z}^+$ csoport $1848\,\mathbb{Z}^+$ részcsoportja szerinti mellékosztályok (a számelmélet nyelvén fogalmazva a modulo 1848 maradékosztályok).
(2) Nem, mert nem tranzitív. Az 1 relációban áll a 2-vel, a 2 a hárommal, de az 1 nem áll relációban a 3-mal.
(3) Igen az osztályok az origó középpontú körök, továbbá maga az origó, mint egyelemű halmaz.
(4) Igen, és az osztályok ugyanazok, mint az előző pontban.
(5) Igen, annyi osztály van, mint f értékkészletének az elemszáma. Ha u eleme az f értékkészletének, akkor a hozzá tartozó osztály az u ősképeinek a halmaza, vagyis azokból az $a \in X$ elemekből áll, melyekre $f(a) = u$.

4.4.32.

(1) Nincs se legszűkebb, se legbővebb elem, de mindegyik elem minimális is és maximális is.
(2) Nincs legszűkebb, sőt minimális elem sem, az egyetlen maximális elem egyben legbővebb is: maga $\mathbb{Z}$.
(3) Legszűkebb és minimális nincs. Legbővebb sincs, a maximális részhalmazok azok, amelyek komplementere egyelemű.
(4) A $\{7\}$ és $\{13\}$ minimális, legszűkebb nincs. A $\mathbb{Z}$ az egyetlen maximális, és egyben legbővebb is.
(5) A $\{7, 13\}$ legszűkebb, és az egyetlen minimális. A $\mathbb{Z}$ az egyetlen maximális, és egyben legbővebb is.

4.4.33. Az S_3 részcsoportjai 1, 2, 3 és 6 rendűek lehetnek ($|S_3| = 6$ osztói). Nyilván csak $\{id\}$ lesz 1 rendű és csak az egész S_3 lesz 6 rendű. Egy másodrendű részcsoportban csak első és másodrendű elemek lehetnek Lagrange tétele miatt, vagyis egy darab első, és egy darab másodrendű elem fér el. Ezért a kételemű részcsoportok $\{id, (12)\}$, $\{id, (13)\}$, $\{id, (23)\}$. Harmadrendű részcsoportban csak harmad- és elsőrendű elem lehet. Elsőrendű elem csak az id. Ha van egy f harmadrendű, akkor f, f^2, $f^3 = id$ kiadják az egész részcsoportot. Csak két harmadrendű elem, és így csak egy harmadrendű részcsoport van, az $\{id, (123), (132)\} = A_3$.

A $\mathbb{Z}_{12}^+$ ciklikus, így a 4.3.21. Állítás miatt minden $d \mid 12$-re egyetlen részcsoport van: $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$, $\mathbb{Z}_{12}$.

A $\mathbb{Z}_{12}^\times$ csoport elemei $\{1, 5, 7, 11\}$, az 1 kivételével mindegyik másodrendű (4.3.22. Gyakorlat). A két triviális részcsoporton kívül tehát három másodrendű részcsoport van, amit egy-egy másodrendű elem az egységelemmel együtt alkot.

Végül legyen H negyedrendű részcsoportja A_4-nek. Negyedrendű csoportban az elemek rendje 1, 2 és 4 lehet. Ha van negyedrendű elem, ennek hatványai négyen vannak, tehát kiadják a részcsoportot. De az A_4 csoportban nincs negyedrendű elem, mert a négyesciklus páratlan permutáció. Ezért H-ban három másodrendű elemnek kell szerepelnie. Az A_4 másodrendű elemei $(12)(34)$, $(13)(24)$ és $(14)(32)$, tehát az egyetlen lehetőség, hogy ezek alkotnak az egységelemmel negyedrendű részcsoportot. A szorzásokat elvégezve látjuk, hogy e három elem közül bármely kettő szorzata a harmadik, és mindegyiknek az inverze önmaga. Ezért ezek tényleg részcsoportot alkotnak.

4.4.34. Ha $H, K \leq G$, és van olyan $h \in H$, ami nincs K-ban, és van olyan $k \in K$ is, ami nincs H-ban, akkor $hk \notin H \cup K$ (és így ez az unió nem részcsoport). Valóban, tegyük föl, hogy $hk \in H \cup K$. Ekkor vagy $hk \in H$, vagy $hk \in K$. Az első esetben $h \in H$ miatt $k = h^{-1}(hk) \in H$, ami ellentmondás. A második esetben hasonlóan jutunk ellentmondásra.

Három részcsoport egyesítése már lehet nemtriviálisan is részcsoport. Például a $\mathbb{Z}_8^\times$ csoport a három kételemű részcsoportjának egyesítése, amelyek közül egyik sem tartalmazza egyik másikat sem.

4.4.35. Ha van másodrendű elem, akkor $|G|$ páros Lagrange tétele miatt. Megfordítva, párosítsunk minden elemet az inverzével. Az egységelem párja önmaga. Ha $|G|$ páros, akkor kell lennie még egy g elemnek, aminek a párja önmaga. Ekkor $g = g^{-1}$, azaz $g^2 = 1$. De $g \neq 1$, és ezért $o(g) = 2$.

4.4.36. Legyen G véges részcsoportja a T test multiplikatív csoportjának. Megmutatjuk, hogy a d rendű elemek száma legfeljebb $\varphi(d)$ lehet. Valóban, az állítás igaz, ha egyáltalán nincs d rendű elem. Tegyük fel, hogy g rendje d. Ekkor g-nek d különböző hatványa van, és mindegyiknek a d-edik hatványa 1. Az Útmutatóban láttuk, hogy T-ben nincs is több olyan elem, aminek d-edik hatványa 1. Speciálisan a d rendű elemek mind g hatványai. Ezek között viszont $\varphi(d)$ darab d rendű elem van a 4.3.17. Lemma miatt.

Jelölje n a G csoport rendjét. Ha d nem osztója n-nek, akkor G-ben Lagrange tétele miatt nincs d rendű elem. Ha $d \mid n$, akkor a d rendű elemek száma az eddigiek szerint legfeljebb $\varphi(d)$. Ezért G elemeinek száma legfeljebb

$$n = |G| \leq \sum_{d|n} \varphi(d)\,.$$

Azonban a 3.9.6. Gyakorlat miatt ez az összeg összeg n, vagyis G rendje. Ez csak úgy lehetséges, ha minden $d \mid n$ esetén tényleg $\varphi(d)$ darab d rendű elem van G-ben (és nem kevesebb). Speciálisan van n rendű elem, tehát G ciklikus.

4.4.37.

(1) A páros számok halmaza nyilván a 28 és 34 számokat tartalmazó részcsoport. Belátjuk, hogy ez a legszűkebb ilyen részcsoport, vagyis ha H részcsoport G-ben, amelyre $28, 34 \in H$, akkor H minden páros számot tartalmaz. Ez világos, hiszen $34 - 28 = 6 \in H$, innen $6 \cdot 6 = 36 \in H$, tehát $36 - 34 = 2 \in H$.

Az Olvasó bizonyára észrevette, hogy valójában az euklideszi algoritmust végeztük el a 28 és a 34 számokra. Ezért okoskodhattunk volna a következőképpen is. A 28 és 34 számok legnagyobb közös osztója 2, ami (az euklideszi algoritmusnál tanultak miatt) felírható $28x + 34y$ alakban alkalmas x, y egészekre, és ezért $2 \in H$. Tehát H tényleg minden páros számot tartalmaz.

Általában az egész számok között $\langle u, v\rangle = \langle (u, v)\rangle$. Ezt az észrevételt általánosítjuk majd a 4.4.42. Feladatban. Megjegyezzük, hogy az állítást a 3.2.23. Feladat segítségével is megmutathattuk volna, erről később a gyűrűelméleti részben még beszélni fogunk.

(2) A $2^n 3^m$ alakú valós számok, ahol n és m egészek.

(3) S_n (lásd 4.2.24. Gyakorlat).

(4) A 4.2.25. Gyakorlatban ezt a részcsoportot határoztuk meg. Az ott leírt nyolc lehetséges sorrend, vagyis a négyzet szimmetriáinak a halmaza pontosan a keresett részcsoport.

(5) Az eredmény A_4. Ebben az adott elemek benne vannak. Tegyük fel, hogy H az adott elemeket tartalmazó részcsoport, meg kell mutatni, hogy A_4 minden eleme H-beli. Ezt meg lehetne úgy mutatni, hogy A_4 minden elemét kifejezzük (123) és (12)(34) segítségével. De Lagrange tétele miatt $|H|$ osztója $|A_4| = 12$-nek, tehát elég 7 elemet kifejezni. Az (12)(34), *id*, (123), $(132) = (123)^2$ elemeken kívül $(243) = (12)(34)(123)$, $(234) = (243)^2$, $(124) = (123)(243) \in H$.

(6) Azok a mátrixok, melyek determinánsa 2-hatvány. Ezek a determinánsok szorzástétele miatt részcsoportot alkotnak, ami minden 2 determinánsú mátrixot tartalmaz. Tehát elég belátni, hogy minden ilyen mátrix kifejezhető 2 determinánsúakkal. Ha $\det(M) = 2^n$ ($n \in \mathbb{Z}$), akkor legyen N tetszőleges 2 determinánsú mátrix és $K = MN^{-n+1}$. Ekkor nyilván $\det K = 2$ és $M = KN^{n-1}$.

4.4.38. A 4.1.8. Állítás szerint D_n minden eleme felírható az F és T elemekből és inverzeikből készített szorzatként.

A D_5 csoportban $\langle F^2, T\rangle$ az egész csoport lesz. Valóban, $(F^2)^3 = F^6 = F$ (mert $F^5 = 1$). De F és T már az egész csoportot generálja.

A D_6 csoportban $\langle F^2, T\rangle$ egy hatelemű részcsoport lesz, amelynek elemei F^i és TF^i minden páros i-re. Az világos, hogy az összes ilyen elemet ki lehet fejezni F^2 és T segítségével, meg kell mutatni, hogy ezek részcsoportot alkotnak. Ezt megtehetnénk úgy, hogy elvégezzük mind a $6 \cdot 6 = 36$ szorzást és a 6 inverzképzést. Sokkal elegánsabb és gyorsabb azonban a következő gondolatmenet.

Ha T átlóra való tükrözés, akkor vegyük észre, hogy a szabályos hatszög csúcsai két szabályos háromszöget alkotnak, legyen az egyik ABC. Könnyen látható, hogy a felsorolt hat elem pontosan az ABC háromszöget önmagába vivő egybevágóságok halmaza lesz. Ezek pedig nyilván részcsoportot alkotnak.

Ha T nem átlóra, hanem oldalfelező merőlegesre való tükrözés, akkor a hat oldalfelező pont által alkotott két szabályos háromszöget tekintsük. A felsorolt hat elem ezek bármelyikének az összes egybevágósága lesz.

Eszerint a D_6 csoportban két különböző hatelemű részcsoportot is találtunk. Egy harmadik az összes forgatásokból áll, és meg lehet mutatni, hogy nincs több hatelemű (azaz kettő indexű) részcsoport.

4.4.39. Legyen $K = gHg^{-1}$. Ekkor

$$KK = gHg^{-1}gHg^{-1} = gHHg^{-1} = gHg^{-1} = K\,, \text{ és}$$

$$K^{-1} = (gHg^{-1})^{-1} = (g^{-1})^{-1}H^{-1}g^{-1} = gHg^{-1} = K\,.$$

Tehát K részcsoport. A $h \mapsto ghg^{-1}$ megfeleltetés kölcsönösen egyértelmű H és K között, hiszen van inverze, a $k \mapsto g^{-1}kg$ leképezés. Ezért H és K rendje ugyanaz. Végül nyilván $gH = gHg^{-1}g = Kg$, tehát az utolsó állítás is igaz.

Könnyen meg lehet mutatni, hogy a $h \mapsto ghg^{-1}$ megfeleltetés művelettartó, és ezért a G csoportot önmagára képző izomorfizmus (4.7.13. Gyakorlat). Ebből számolás nélkül is következett volna, hogy részcsoportot részcsoportba visz.

4.4.40. Ha G véges, akkor a $|G : H| = |G|/|H|$ összefüggés felhasználásával azonnal adódik az állítás, az alábbi bizonyítás azonban végtelen G csoportra is működik.

Mivel $H \leq K$, a K csoport bizonyos H szerinti bal oldali mellékosztályok egyesítése, és akár azt tudjuk, hogy $|G : H|$ véges, akár azt, hogy $|H : K|$ véges, mindenképpen csak véges sok ilyen mellékosztály van. Legyenek ezek $a_1H, \ldots, a_kH$, ahol tehát $k = |K : H|$. Ekkor a bK mellékosztály a (szintén páronként diszjunkt) $ba_1H, \ldots, ba_kH$ mellékosztályok egyesítése. A G csoport K szerinti mellékosztályokra bomlik, és mindegyiket k darab H szerinti mellékosztályra bonthatjuk, ezért $|G : H| = k|G : K|$.

4.4.41. Megmutatjuk, hogy ha H és K részcsoportok G-ben, akkor $a(H \cap K) = aH \cap aK$. A bal oldal elemei ag alakúak, ahol $g \in H \cap K$. A jobb oldal elemei $ah = ak$ alakúak, ahol $h \in H$ és $k \in K$. De ha $ah = ak$, akkor $h = k \in H \cap K$ az egyszerűsítési szabály miatt. Tehát $a(H \cap K) = aH \cap aK$ tényleg teljesül. Ezért minden $H \cap K$ szerinti bal mellékosztály előáll egy H szerinti és egy K szerinti bal mellékosztály metszeteként. Így $|G : (H \cap K)| \leq |G : H| \cdot |G : K|$.

4.4.42. A $\langle a/c, b/d \rangle$ részcsoport elemei az $x(a/b)+y(c/d)$ alakú számok. Közös nevezőre hozva ez $(ux + vy)(a, c)/[b, d]$, ahol

$$u = \frac{a}{(a,c)}\frac{[b,d]}{b} = \frac{a}{(a,c)}\frac{d}{(b,d)}$$

és

$$v = \frac{c}{(a,c)}\frac{[b,d]}{d} = \frac{c}{(a,c)}\frac{b}{(b,d)}$$

a 3.1.29. Gyakorlat miatt. Könnyen láthatóan u és v relatív prímek, és így $ux + vy$ alakban minden egész szám előáll. Ezért $\langle a/c, b/d \rangle = \langle (a, c)/[b, d] \rangle$.

4.4.43. Belátjuk, hogy $\mathbb{Q}^+$ egy X részhalmaza akkor és csak akkor generátorrendszer, ha minden q prímhatványhoz van olyan egyszerűsíthetetlen tört X-ben, melynek nevezője osztható q-val.

Tegyük fel először, hogy X generátorrendszer. Legyen $q = p^n$ ahol p prím, és írjuk fel az $1/q$ törtet az X véges sok elemének egész együtthatós lineáris kombinációjaként. Az ebben szereplő X-beli elemek valamelyikének nevezője osztható kell, hogy legyen q-val, mert különben a közös nevezőben p kitevője n-nél kisebb lesz, és akkor nem lehet $1/q$ az eredmény. Ezért X a kívánt tulajdonságú.

Megfordítva, tegyük fel, hogy az X halmaz rendelkezik a fenti tulajdonsággal. Ha a/b és c/d két egyszerűsíthetetlen tört X-ben, akkor az előző 4.4.42. Feladat miatt a szintén egyszerűsíthetetlen $(a, c)/[b, d]$ tört kifejezhető ezek segítségével. Így akármilyen egésszel osztható nevezőjű egyszerűsíthetetlen törteket gyárthatunk az X elemeinek lineáris kombinációjaként, az ilyenek többszöröseként pedig minden tört előáll. Vagyis X tényleg generátorrendszer.

De akkor minden generátorrendszerből bármelyik elem elhagyható úgy, hogy generátorrendszer maradjon, hiszen egy elem elhagyásával a fenti feltétel nem romlik el. Valóban, hagyjuk el az a/b elemet, és legyen $q = p^n$ prímhatvány. Válasszuk $m \geq n$-et olyan nagyra, hogy p^m már ne legyen osztója b-nek. Ekkor van olyan tört X-ben, aminek a nevezője p^m-mel osztható, de ez biztosan nem az a/b. Ezért az a/b elhagyása után is van olyan tört, aminek a nevezője q-val osztható. Így a feltétel a/b elhagyása után is teljesül.

Beláttuk tehát, hogy $\mathbb{Q}^+$-nak nincs véges, sőt minimális generátorrendszere sem.

4.4.44. Az Útmutatóban elkezdett megoldást folytatjuk, azaz belátjuk, hogy az ott definiált Y halmaz generálja H-t. Legyen $h \in H$. Ekkor $h = x_1 \dots x_N$, ahol $x_1, \dots, x_N \in X$. Mivel $x_N \in X$ és $1 \in R$ reprezentáns, $x_N 1 = r'h'$ alkalmas $r' \in R$ és $h' \in Y$ elemekre. De $x_{N-1} \in X$, ezért $x_{N-1} r' = r''h''$ alkalmas $r'' \in R$ és $h'' \in Y$ elemekre. Ezután $x_{N-2} r''$-t írjuk fel $r'''h'''$ alakban, és így tovább. Végeredményben azt kapjuk, hogy $h = r^* h^*$, ahol $r^* \in R$, és a h^* elem Y-beli elemek szorzata. Mivel $h, h^* \in H$, ezért $r^* \in H$, azaz $r^* = 1$.

4.4.45. Az Útmutatóban definiált gráfra alkalmazható a König–Hall–Ore-tétel feltétele. Valóban, ha kiveszünk k darab bal mellékosztályt, akkor ezek U uniója $k|H|$ elemű. Mivel minden jobb mellékosztály elemszáma $|H|$, és a jobb mellékosztályok együttesen lefedik az U halmazt, legalább k darab jobb mellékosztálynak részt kell vennie ebben a lefedésben (különben $k|H|$-nál kevesebb elemet tudnának csak lefedni). Így a tétel feltétele teljesül, és ezért minden bal mellékosztályhoz hozzá tudunk rendelni egy jobb mellékosztályt, mindegyikhez különbözőt, amellyel van közös eleme. Válasszunk ki minden bal mellékosztályból egy ilyen közös elemet. A kapott halmaz kétoldali reprezentánsrendszert lesz, hiszen minden jobb és minden bal mellékosztályban van eleme.

4.5. Homomorfizmusok és normálosztók.

4.5.3. Ha $h_1, h_2 \in \mathrm{Im}(\varphi)$, akkor van olyan $g_i \in G$, melyre $\varphi(g_i) = h_i$ (ahol $i = 1, 2$). Ekkor φ művelettartása miatt $\varphi(g_1 g_2) = h_1 h_2$ és $\varphi(g_1^{-1}) = h_1^{-1}$, ezért $h_1 h_2$ és h_1^{-1} is benne van $\mathrm{Im}(\varphi)$-ben. Benne van továbbá az egységelem is, mert $\varphi(1_G) = 1_H$, és ezért $\mathrm{Im}(\varphi)$ részcsoport. A φ értékkészlete $\mathrm{Im}(\varphi)$, és ezért φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi)$ az egész H.

4.5.4. Legyen $K \leq H$, és tekintsük a K identikus leképezését. Ez nyilván homomorfizmus, melynek képe K.

4.5.6. Ha $g_1, g_2 \in \mathrm{Ker}(\varphi)$, akkor $\varphi(g_1) = \varphi(g_2) = 1$, és így φ művelettartása miatt $\varphi(g_1 g_2) = \varphi(g_1^{-1}) = 1$. Ezért $g_1 g_2$ és g_1^{-1} is benne van $\mathrm{Ker}(\varphi)$-ben. Benne van továbbá az egységelem is, és ezért részcsoport.

Tegyük fel, hogy $\mathrm{Ker}(\varphi) = \{1\}$. Ha $\varphi(g_1) = \varphi(g_2)$ valamilyen $g_1, g_2 \in G$ elemekre, akkor $1 = \varphi(g_1)^{-1} \varphi(g_2) = \varphi(g_1^{-1} g_2)$, vagyis $g_1^{-1} g_2 \in \mathrm{Ker}(\varphi)$. Tehát $g_1^{-1} g_2 = 1$, ahonnan $g_1 = g_2$. Így beláttuk, hogy φ injektív.

Megfordítva, tegyük fel, hogy φ injektív, és legyen $g \in \mathrm{Ker}(\varphi)$. Ekkor $\varphi(g) = 1 = \varphi(1)$, ahonnan φ injektivitása miatt $g = 1$. Tehát $\mathrm{Ker}(\varphi) = \{1\}$.

4.5.7. Ha $h \in \mathbb{Z}_n$, akkor $\varphi(g) = h$ akkor és csak akkor, ha g felírható $nq + h$ alakban, vagyis ha $g \in h + n\,\mathbb{Z}$. Speciálisan $h = 0$ esetén $\mathrm{Ker}(\varphi) = n\,\mathbb{Z}$.

4.5.8. $(12)N = N(12) = \{(12), (13), (23)\}$. Szó sincs azonban arról, hogy az (12) felcserélhető lenne az N elemeivel: $(12)(123) = (23)$ és $(12)(132) = (13)$, míg a jobbról való szorzásnál pont fordítva van, $(123)(12) = (13)$ és $(132)(12) = (23)$.

4.5.9. Ha $gN = Ng'$, akkor $g = g1 \in gN = Ng'$. Tehát az Ng és Ng' jobb oldali mellékosztályoknak g közös eleme, és így ez a két mellékosztály megegyezik. Vagyis $gN = Ng' = Ng$.

4.5.13. Elsőnek azt mutatjuk meg, hogy ψ homomorfizmus. Valóban,

$$\psi(g_1)\psi(g_2) = (g_1N)(g_2N) = (g_1g_2)N = \psi(g_1g_2)\,,$$

hiszen a szorzást a g_1 és g_2 reprezentánsokkal is el szabad végezni. A ψ szürjektív is, hiszen a K csoportot a mellékosztályok halmazának definiáltuk.

Ebből már a másik két állítás is következik. Valóban, homomorfizmusnál az egységelem képe az egységelem lesz, és ezért $\psi(1) = 1N = N$ a K csoport egységeleme. Az asszociativitás is könnyen láthatóan öröklődik szürjektív homomorfizmusnál, de közvetlenül is világos, hiszen

$$(g_1Ng_2N)g_3N = \big((g_1g_2)g_3\big)N = \big(g_1(g_2g_3)\big)N = g_1N(g_2Ng_3N)\,.$$

4.5.18. Legyen $\varphi : G \to H$ homomorfizmus, L részcsoport H-ban, és K az L teljes inverz képe G-ben. Ha $k_1, k_2 \in K$, akkor $\varphi(k_1), \varphi(k_2) \in L$. A φ művelettartása miatt $\varphi(k_1k_2) = \varphi(k_1)\varphi(k_2) \in L$, és $\varphi(k_1^{-1}) = \varphi(k_1)^{-1} \in L$, hiszen L részcsoport. Ezért k_1k_2 és k_1^{-1} is benne van K-ban. Benne van továbbá az egységelem is, és ezért K részcsoport. Ha $g \in \mathrm{Ker}(\varphi)$, akkor $\varphi(g) = 1 \in L$, és ezért $g \in K$. Tehát $\mathrm{Ker}(\varphi) \subseteq K$.

4.5.22. Érdekes, hogy több korábbi, nevezetesnek számító tétel is azt mondja ki, hogy egy-egy leképezés homomorfizmus.

(1) Igen, ez a determinánsok szorzástétele (lásd A.5.3. Tétel). Kép: az egész $T^\times$, mag: 1 determinánsú mátrixok, vagyis $\mathrm{SL}(n, T)$.
(2) Igen, ez a permutációk előjelének szorzástétele (4.2.10. Tétel). Kép: $\mathbb{Z}^\times = \{1, -1\}$, mag: A_n.
(3) Igen, ez leolvasható a 4.1.8. Állításból, vagy abból, hogy forgatások szorzata forgatás, tengelyes tükrözések szorzata is forgatás, egy forgatás és egy tengelyes tükrözés szorzata pedig tengelyes tükrözés. Kép: $\mathbb{Z}_2^+$, mag: forgatások.
(4) Igen, mert $|zw| = |z||w|$ (1.3.10. Állítás, ez a példa már szerepelt a 2.2.40. Gyakorlatban). Kép: pozitív valós számok, mag: az egységkörvonal, vagyis az 1 abszolút értékű komplex számok halmaza.
(5) Igen, lásd 2.4.2. Gyakorlat. A kép az összes komplex számok halmaza, mert az $f(x) = a + bx$ polinomba i-t helyettesítve $a + bi$ adódik. A mag azokból az $f \in \mathbb{R}[x]$ polinomokból áll, melyeknek az i gyöke. De akkor az i konjugáltja, vagyis a $-i$ is gyök, és ezért a polinomból kiemelhető $(x + i)(x - i) = x^2 + 1$ (3.3.6. Lemma). Tehát úgy is fogalmazhatunk, hogy a mag az $x^2 + 1$ polinom többszöröseiből áll.

4.5.23. A homomorfizmus-tételt az alábbi φ homomorfizmusokra kell alkalmazni.

(1) Az előző gyakorlat (3) pontjában szereplő homomorfizmus. A faktorcsoport elemei az origó körüli körök.
(2) $\varphi(x) = \cos(2\pi x) + i \sin(2\pi x)$ (vö. 2.2.40. Gyakorlat). A mag pontosan az egész számokból, a kép az 1 abszolút értékű komplex számokból áll.
(3) Az előző gyakorlat (2) pontjában szereplő homomorfizmus azt mutatja, hogy az S_n/A_n faktorcsoport izomorf a kételemű ciklikus csoporttal (nevezetesen $\mathbb{Z}^\times$-tel). Ez azonban izomorf bármelyik másik kételemű ciklikus csoporttal, így $\mathbb{Z}_2^+$-szal is.
(4) A 4.5.7. Gyakorlatban szereplő homomorfizmus.

4.5.24. Minden $\{1\}$ szerinti mellékosztály egyelemű, és $g \mapsto \{g\}$ izomorfizmus G és $G/\{1\}$ között. A G/G az egyelemű csoporttal izomorf.

4.5.25. A $\mathbb{Z}_{16}^\times$ csoport rendje 8, elemeit kényelmesebb lesz ±1, ±3, ±5 és ±7 alakban írni. Láthatjuk, hogy (mod 16 számolva) $(\pm1)^2 = 1 = (\pm7)^2$, tehát ezek az 1 kivételével másodrendű elemek. Ugyanakkor $(\pm3)^2 = (\pm5)^2 = 9 \equiv -7$, melynek négyzete már 1. Ebből következik, hogy ez a négy elem negyedrendű. (Valóban, a negyedik hatványuk $(-7)^2 = 1$, tehát a rendjük négynek osztója, de nem lehet 2 vagy 1, mert a négyzetük nem az egységelem.) Így a csoportban nincs nyolcadrendű elem, tehát nem ciklikus.

A megadott két részhalmaz részcsoport, hiszen 15 és 9 is másodrendű elemek. Normálosztók is, hiszen Abel-csoportban minden részcsoport az. Legyen $N = \{1, 15\}$. A $\mathbb{Z}_{16}^\times/N$ csoport ciklikus, a $3N$ generálja. Valóban, a csoport negyedrendű, tehát minden elem rendje négynek osztója. Ugyanakkor $3N$ négyzete $9N$, ami nem N, azaz nem az egységelem, és így $3N$ negyedrendű.

A $\mathbb{Z}_{16}^\times/\{1, 9\}$ csoport viszont nem ciklikus, mert minden elemének a négyzete az egységelem (hiszen $\mathbb{Z}_{16}^\times$ minden elemének a négyzete az $\{1, 9\}$ normálosztóban van).

4.5.26. Ha $\psi = \alpha \circ \varphi$, és $g \in \mathrm{Ker}(\varphi)$, akkor $\varphi(g) = 1$, és ezért $\psi(g) = \alpha\varphi(g) = \alpha(1) = 1$. Megfordítva, tegyük fel, hogy $\mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\psi)$. Próbáljuk meg az α leképezést a

$$\varphi(g) = h \implies \alpha(h) = \psi(g)$$

képlettel definiálni. Mivel φ szürjektív, ez minden $h \in H$-ra értelmezi α-t (csak esetleg többértelműen). Ha $h = \varphi(g_1) = \varphi(g_2)$, akkor $g_1 g_2^{-1} \in \mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\psi)$, és így $\psi(g_1) = \psi(g_2)$. Tehát α jóldefiniált. A definícióból nyilvánvaló, hogy $\psi = \alpha \circ \varphi$.

Végül belátjuk, hogy α művelettartó. Ha $h_1, h_2 \in H$, akkor legyen $\varphi(g_1) = h_1$ és $\varphi(g_2) = h_2$. Ezért $\varphi(g_1 g_2) = h_1 h_2$, és így

$$\alpha(h_1 h_2) = \psi(g_1 g_2) = \psi(g_1)\psi(g_2) = \alpha(h_1)\alpha(h_2)\,.$$

4.5.27. Tegyük fel, hogy X generátorrendszere a G csoportnak. A 4.4.28. Gyakorlat megoldásához hasonlóan most is kétféleképpen járhatunk el. Az első megoldásban a 4.4.27. Tételt alkalmazva megmutathatjuk, hogy H minden eleme előáll egy olyan szorzatként, melynek tényezői az X elemeinek és inverzeinek ψ-nél vett képei. Ehelyett most is az elegánsabb megoldást részletezzük.

Legyen $Y = \psi(X)$ és L az Y által generált részcsoport. Meg kell mutatni, hogy $L = H$. Jelölje K az L részcsoport teljes inverz képét G-ben. Ez részcsoport, és tartalmazza X-et. Ezért az X által generált részcsoport (ami G) része K-nak. Tehát $K = G$, és mivel ψ szürjektív, $L = H$.

4.5.28. A 4.4.29. Gyakorlat miatt elég belátni, hogy $HN = NH$. De ez világos, hiszen $N \triangleleft G$, ezért $hN = Nh$ minden $h \in H$-ra.

4.5.29. Nyilván $H(N \cap K) \subseteq HN \cap K$, hiszen a bal oldal egy tipikus eleme hg, ahol $h \in H$ és $g \in N \cap K$ benne van a jobb oldalban is (hiszen $h \in H \subseteq K$).

Megfordítva, tegyük fel, hogy $k \in HN \cap K$. Ekkor $k = hn$ alkalmas $h \in H$ és $n \in N$ elemekre. De $H \leq K$ miatt $h \in K$, tehát $n = h^{-1}k \in K$. Ezért $n \in N \cap K$, és így $k = hn \in H(N \cap K)$.

4.6. Permutációcsoportok.

4.6.8. Hasonlóan járunk el, mint a kocka esetében. Tekintsünk egy szabályos sokszöget, és legyen G ennek a szimmetriacsoportja (a csúcsok halmazán). Ez nyilván tranzitív, hiszen a csúcsok forgatással egymásba vihetők. Ha A egy csúcs, akkor tehát G rendje $n|H|$, ahol H az A csúcs stabilizátora. Legyenek B és C az A szomszédai. Ekkor a H csoport elemeinél B képe csakis B vagy C lehet, mert az összes további csúcs A-tól messzebb van, mint B illetve C. Tehát $\{B, C\}$ orbit H-nál. Ha A és B fixen marad, akkor C is, ezért C-nek az A-tól különböző szomszédja is, és körbe haladva látjuk, hogy minden további csúcs is. Ezért H kételemű, G rendje pedig $2n$.

4.6.9. Egy él felező merőleges síkjára való tükrözés kicseréli az él két végpontját, miközben a másik két csúcs fixen marad. Ezért a csúcsok halmazán minden transzpozíció megvalósítható egybevágósági transzformációval. De tudjuk, hogy a transzpozíciók generálják a szimmetrikus csoportot (azaz minden permutáció cserék szorzata), ezért S_4 mindegyik eleme megkapható egy alkalmas egybevágósági transzformációval.

4.6.10. Írjuk rá az $\{1, 2, 3\}$ számokat egy szabályos háromszög csúcsaira. Ekkor D_3 csoport egybevágósági transzformációi pontosan az S_3 permutációit valósítják meg a csúcsok halmazán.

4.6.11. Legyen $ABCD$ egy téglalap. Négy szimmetria biztosan van: az identitáson kívül a két oldalfelező merőlegesre való tükrözés, illetve a középpontos tükrözés. Ezek a csúcsok halmazán tranzitívak. Az A csúcstól a másik három csúcs csupa különböző távolságra van, hiszen ez a téglalap nem négyzet. Ezért ha A fixen marad, akkor a másik három is, vagyis az A stabilizátora egyelemű. Így a szimmetriák száma négy, nincs több, mint amit már felsoroltunk. Nyilván mindegyiknek a négyzete az identitás.

Az AB oldal felező merőlegesére való tükrözés a csúcsok halmazán az $(AB)(CD)$ permutáció. Ugyanígy látszik, hogy a másik tengelyes tükrözés az $(AD)(BC)$, a középpontos tükrözés pedig az $(AC)(BD)$ permutáció. Így annak bizonyítása, hogy bármely kettő szorzata a harmadik, e permutációk összeszorzásával történhet. Pontosan ezt a számolást már el is végeztük a 4.4.33. Gyakorlatban.

4.6.13. Íme D_4 szorzástáblája. A két 90 fokos forgatás a két (negyedrendű) négyesciklus. A középpontos tükrözés az (13)(24), az utolsó négy (másodrendű) elem tengelyes tükrözés.

D_4	id	(1234)	(13)(24)	(1432)	(12)(34)	(24)	(14)(23)	(13)
id	id	(1234)	(13)(24)	(1432)	(12)(34)	(24)	(14)(23)	(13)
(1234)	(1234)	(13)(24)	(1432)	id	(13)	(12)(34)	(24)	(14)(23)
(13)(24)	(13)(24)	(1432)	id	(1234)	(14)(23)	(13)	(12)(34)	(24)
(1432)	(1432)	id	(1234)	(13)(24)	(24)	(14)(23)	(13)	(12)(34)
(12)(34)	(12)(34)	(24)	(14)(23)	(13)	id	(1234)	(13)(24)	(1432)
(24)	(24)	(14)(23)	(13)	(12)(34)	(1432)	id	(1234)	(13)(24)
(14)(23)	(14)(23)	(13)	(12)(34)	(24)	(13)(24)	(1432)	id	(1234)
(13)	(13)	(12)(34)	(24)	(14)(23)	(1234)	(13)(24)	(1432)	id

4.6.14. Elegendő az I^2, J^2, K^2, illetve az IJ, JI, IK, KI, JK, KJ mátrix-szorzásokat elvégezni.

4.6.15. Izomorf csoportokban ugyanannyi másodrendű elem van, hiszen másodrendű elem képe izomorfizmusnál másodrendű. A D_4 csoportban 5, a kvaterniócsoportban viszont 1 a másodrendű elemek száma, ezért nem lehetnek izomorfak.

4.6.18. Ha $g*x = y$, akkor $g^{-1}*y = g^{-1}*(g*x) = (g^{-1}g)*x = 1*x = x$. Megfordítva, ha $g^{-1} * y = x$, akkor $g * x = (gg^{-1}) * y = 1 * y = y$. Az $x \mapsto g * x$ leképezésnek tehát van inverze, és így permutáció.

4.6.22. Azt kell belátni, hogy $\psi(gh) = \psi(g) \circ \psi(h)$. Ez a két függvény akkor egyenlő, ha minden elemen megegyeznek.

$$\big(\psi(gh)\big)(x) = (gh) * x\,,$$

és

$$\big(\psi(g) \circ \psi(h)\big)(x) = g * (h * x)\,.$$

De $(gh) * x = g * (h * x)$ a hatás definíciója miatt. Így ψ tényleg homomorfizmus.

A hatás magja azokból a $g \in G$ elemekből áll, melyekre $\psi(g)$ az identitás, vagyis melyekre $g * x = x$ minden x-re. Az ilyen g elemek tényleg azok, amelyek mindegyik stabilizátorban benne vannak.

A homomorfizmus-tétel szerint $\mathrm{Im}(\psi) \cong G/\mathrm{Ker}(\psi)$. Ha a hatás hű, akkor a magja csak az egységelemből áll, és ezért $\mathrm{Im}(\psi) \cong G$. Így G maga izomorf az S_X csoport $\mathrm{Im}(\psi)$ részcsoportjával, vagyis beágyazható S_X-be.

4.6.24. Hatások ekvivalenciáját ugyanúgy kezelhetjük, mint a csoportok közötti izomorfizmust. Ha úgy gondoljuk, hogy két hatás ekvivalens, akkor megadhatjuk azt a bijekciót, amely ezt megmutatja. Ha azt gondoljuk, hogy nem, akkor egy olyan tulajdonságot kereshetünk, ami az egyiknek megvan, a másiknak nincs, de hatásnál megőrződik.

Ilyen tulajdonság például a hatás magja, vagy az egyes $g \in G$ elemekhez tartozó permutációk ciklusszerkezete. Könnyű megmutatni, hogy ekvivalens hatásoknál tetszőleges g elemhez tartozó permutáció mindkét hatás esetében ugyanannyi ciklusból áll, és az egymásnak megfelelő ciklusok hosszai is ugyanazok. Hiszen ha az $x \mapsto g * x$ permutációnál $(x_1, \ldots, x_k)$ egy ciklus, akkor a vele ekvivalens hatásban $(\alpha(x_1), \ldots, \alpha(x_k))$ is ciklus lesz. Hasonlóan megmutatható, hogy ekvivalens hatásnál az egymásnak megfelelő elemek stabilizátora is ugyanaz.

Eszerint $*_1$, $*_2$ és $*_4$ páronként nem ekvivalensek, hiszen a g elemnek megfelelő permutáció ciklusszerkezete, mint láttuk, más és más a három esetben. Azt már igazoltuk, hogy $*_1$ és $*_5$ ekvivalensek. Ezekkel ekvivalens a $*_3$ is. Például

$$1 \leftrightarrow 2 \quad 2 \leftrightarrow 1 \quad 3 \leftrightarrow 4 \quad 4 \leftrightarrow 3$$

ekvivalenciát létesít $*_1$ és $*_3$ között.

4.6.26. A $g * (aH) = gaH$ szorzás jóldefiniált, mert ha $aH = bH$, akkor $gaH = gbH$. Hatást kaptunk, mert

$$g_1 * (g_2 * aH) = g_1 g_2 aH = (g_1 g_2) * aH\,, \quad \text{és} \quad 1 * (aH) = 1aH = aH\,.$$

Ez a hatás tranzitív, mert $a*(1H) = aH$, vagyis az $1H$ orbitja az összes bal mellékosztályt tartalmazza. Az aH stabilizátora azon g elemekből áll, melyekre $gaH = aH$. De

$$gaH = aH \iff a^{-1}ga \in H \iff g \in aHa^{-1}\,.$$

A 4.6.22. Gyakorlat szerint a hatás magja e stabilizátorok metszete, és G/N izomorf S_k egy részcsoportjával. Végül ha H egyelemű, akkor az aH mellékosztályt az a elemmel azonosíthatjuk. Így $g * a = ga$, a g-vel való balszorzás pedig a Cayley-tételben szereplő permutáció.

4.6.27. A G hatását X-en ugyanúgy $*$-gal fogjuk jelölni, mint G hatását a H szerinti bal mellékosztályokon.

Legyen $\alpha(aH) = a * x$. Megmutatjuk, hogy az α leképezés jóldefiniált. Tegyük fel, hogy $aH = bH$. Ekkor van olyan $h \in H$, hogy $b = ah$. Mivel H az x stabilizátora, $h * x = x$, és így $b * x = (ah) * x = a * x$. Ezért $\alpha(bH) = b * x = a * x = \alpha(aH)$, vagyis α tényleg jóldefiniált.

Mivel G tranzitív X-en, α szürjektív. Belátjuk, hogy injektív. Ha $\alpha(aH) = \alpha(bH)$, akkor $a * x = b * x$, azaz $(a^{-1}b) * x = x$, ahonnan $a^{-1}b \in H$. Ezért $aH = bH$, vagyis α tényleg injektív.

Végül be kell látni, hogy $\alpha(g * aH) = g * \alpha(aH)$. Ez világos, mert mindkét oldalon $(ga) * x$ szerepel.

4.6.28.

(1) Orbitok: origó középpontú körök, illetve maga az origó. Stabilizátorok: egyeleműek, kivéve az origót, melynek stabilizátora az egész csoport.
(2) Orbitok: az x-tengellyel párhuzamos egyenesek. Stabilizátorok: egyeleműek.
(3) Már láttuk a 4.6.8. Gyakorlatban, hogy ez a csoport kételemű. Orbitok: az adott csúcson átmenő tengelyre szimmetrikus csúcspárok, illetve a tengelyen levő csúcsok önmagukban (1, illetve 2 csúcs, attól függően, hogy n páratlan-e, vagy páros). Stabilizátorok: egyelemű orbitokhoz az egész (kételemű) csoport, kételemű orbithoz egyelemű stabilizátor tartozik.
(4) Legyen A a kiválasztott csúcs, és jelölje B, C, D a három szomszédját. Mivel a kocka szimmetriacsoportja 48 elemű (4.6.7. Állítás), amely a csúcsokon tranzitív, az A csúcs G stabilizátora $48/8 = 6$ elemű. Ezeknél a szimmetriáknál nemcsak A, hanem a vele átellenes csúcs is fixen marad. A BCD szabályos háromszög, és minden A-t fixáló egybevágóság ennek a háromszögnek szimmetriája. Ezért $G \cong D_3$, és B orbitja háromelemű.

    Azt, hogy $G \cong D_3$, a következőképpen láthatjuk be. Rendeljük hozzá G minden g eleméhez a g elemnek a BCD háromszögön való hatását. Így egy $\varphi : G \to D_3$ homomorfizmust kapunk. De φ magja csak az identitásból áll, hiszen ha B, C, D fix, akkor a kocka minden csúcsa is helyben marad. Ezért ez a homomorfizmus injektív (4.5.6. Gyakorlat). Mivel G is és D_3 is hatelemű csoport, φ izomorfizmus lesz.

    A B csúcs G-beli stabilizátora $6/3 = 2$ elemű, az identitáson kívüli eleme az AB élet és a kocka középpontját tartalmazó síkra való tükrözés. Összefoglalva: a G csoportnak két egyelemű és két háromelemű orbitja van, a stabilizátorok a D_3, illetve a $\mathbb{Z}_2^+$ csoportokkal izomorfak.
(5) Tranzitív, az x pont stabilizátora az x-et nem tartalmazó két hármasciklus és az identitás.

4.6.29. Ha pontosan két szimmetria van, akkor az, amelyik az identitástól különbözik, másodrendű, tehát ciklusfelbontása (a négyszög csúcsain) (ab), vagy $(ab)(cd)$. Az első esetben átlóra való tükrözésről van szó (hiszen két csúcs fixen marad), tehát a négyszög deltoid (ami nem rombusz, mert akkor több szimmetriája is lenne). A második esetben egyik csúcs sem marad helyben. Ha a szemközti csúcsok cserélődnek, akkor középpontos tükrözésről van szó, vagyis a négyszög paralelogramma, ami sem téglalap, sem rombusz nem lehet, mert akkor ismét lenne több szimmetria. Végül ha szomszédos csúcsok cserélődnek, akkor ez egy oldalfelező merőlegesre való tükrözés, a négyszög pedig szimmetrikus trapéz, ami nem lehet téglalap. Tehát két szimmetriája a felsorolt háromféle négyszögnek van (deltoid, paralelogramma, szimmetrikus trapéz).

A rombusznak négy szimmetriája van, az átlókra tükrözés, a középpontos tükrözés, és az identitás, ezek is Klein-csoportot alkotnak. A téglalapnak is négy szimmetriája van (4.6.11. Gyakorlat), a négyzetnek pedig nyolc, ez a D_4 diédercsoport.

4.6.30.

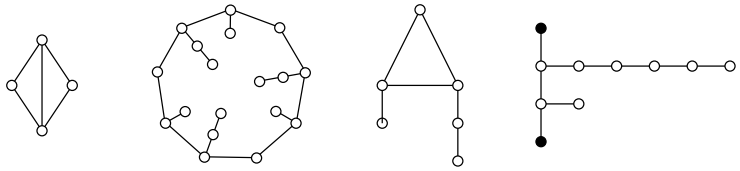
(1) 8, a csoport tranzitív, mert a síkra tükrözésekkel egy csúcs minden csúcsba elvihető, és a stabilizátorok egyeleműek.
(2) 16, tranzitív, egy csúcs stabilizátora pedig kételemű (a vele egy négyzetlapon lévő két szomszédja helyet cserélhet az átlósíkra való tükrözésnél).
(3) 12, tranzitív, és kételeműek a stabilizátorok.
(4) 6 (az alap helyben kell, hogy maradjon). Ezért a szimmetriacsoport D_3.
(5) Az oktaéder szimmetriacsoportja izomorf a kockáéval, mert a kocka lapközéppontjai oktaédert alkotnak, és így a kocka minden szimmetriája az oktaédernek is szimmetriája, és viszont. Így az oktaédernek is 48 szimmetriája van.

4.6.31. Az AB élet az AC élbe elviszi egy átlósíkra való tükrözés. Így sorban haladva minden él minden élbe elvihető. A stabilizátorok elemszáma $48/12 = 4$, és mindegyik a Klein-csoporttal izomorf.

Két szomszédos lap is egymásba vihető átlósíkra tükrözéssel, és így a lapok halmazán is tranzitív a hatás, a stabilizátor $48/6 = 8$ elemű. Az $ABCD$ lapot fixen hagyó egybevágóságok persze pontosan ennek a négyzetnek az egybevágóságai, vagyis a D_4-gyel izomorf csoportot alkotnak. (Meg kell gondolni, hogy a négyzet minden egybevágósága egyértelműen megadja a kocka egy egybevágóságát.)

Végül tekintsük a kocka szimmetriacsoportjának a hatását a szemköztes lappárok alkotta háromelemű halmazon. Ez értelmes, mert egy szemköztes lappár képe egybevágóságnál szintén szemköztes lappár lesz. Egy lappár stabilizátora $48/3 = 16$ elemű, és így van 16 elemű részcsoport. Az előbbi $ABCD$ lap szimmetriacsoportja, és a vele párhuzamos, a kocka középpontján átmenő síkra való tükrözés által generált réscsoport pontosan egy ilyen 16 elemű stabilizátor lesz.

4.6.32. Két szimmetria: tetszőleges út (ami legalább egy élből áll). Négy szimmetria: egy négy hosszú kör egy átlóval. Három szimmetria: egy 9 hosszú kör csúcsaira alkalmasan 1 és 2 hosszú utakat akasztunk. Egy szimmetria: egy háromszög csúcsaira alkalmasan 1 és 2 hosszú utakat akasztunk.



4.6.33. Az Útmutatóban rajzolt gráfban a színeket és az irányítást úgy szüntethetjük meg, hogy egy nyíl helyére berakjuk a következő gráfot: egy 3 hosszú út második csúcsáról lelógatunk egy élt, a harmadik csúcsáról pedig a nyíl színétől függő hosszúságú (de legalább két élből álló) utat.

4.6.34. Az n pont stabilizátora az $\{1, \ldots, n-1\}$ halmaz összes páros permutációiból áll, tehát A_{n-1}-gyel izomorf. Ugyanez a többi stabilizátorra is elmondható.

4.6.35. Mivel g permutáció és X véges, ezért $g(Y) \subseteq Y$ ugyanazt jelenti, mint hogy $g(Y) = Y$. Legyen $g * Y = g(Y)$. Ez könnyen láthatóan G-nek hatása az X összes részhalmazain, és itt Y stabilizátora pontosan az a részhalmaza G-nek, amelyről be kell látnunk, hogy részcsoport.

4.6.36. A $\langle g \rangle$ részcsoportnál az x és y elemek akkor és csak akkor vannak egy orbitban, ha van olyan i egész, hogy $g^i(x) = y$. Mivel X véges, a g rendje is véges, és így feltehető, hogy $i \geq 0$. Az x-et tartalmazó ciklusban viszont pont az x, $g(x)$, $g^2(x)$, ... elemek vannak.

4.6.37. Mivel $g * x = y$, ezért $f * y = y \iff (fg) * x = g * x \iff (g^{-1}fg) * x = x$. De az x stabilizátora H, ezért ez pontosan akkor igaz, ha $g^{-1}fg \in H$, azaz ha $f \in gHg^{-1}$.

4.6.38. A B mellékosztály orbitja az AB-beli mellékosztályok halmaza, ennek hossza tehát $|AB|/|B|$. A B stabilizátora azokból az $a \in A$ elemekből áll, melyekre $aB = B$, azaz $a \in B$, tehát a stabilizátor $A \cap B$. Így $|AB|/|B| = |A|/|A \cap B|$.

4.6.39. Jelölje P azoknak a (g, x) pároknak a halmazát, melyekre $g * x = x$. Ha g rögzített, akkor a P-beli (g, x) párok száma a g fixpontjainak a száma, és így P elemszáma a G-beli permutációk fixpontszámainak összege. Ha viszont x rögzített, akkor a P-beli (g, x) párok száma az x stabilizátorának elemszáma. Ha O jelöli x orbitját, akkor az x stabilizátorának az elemszáma $|G|/|O|$. Amikor az x az O orbitot befutja, akkor tehát a (g, x) párok száma $|O||G|/|O| = |G|$ lesz. Így P elemszáma az orbitok számának $|G|$-szerese.

4.6.40. Az Útmutatóban szereplő X halmaz elemszáma $\binom{9}{4} = 126$. Az identitásnak tehát ennyi fixpontja van. Könnyű meggondolni, hogy mindkét 90 fokos forgatásnak 2 fixpontja van, a középpontos tükrözésnek 6, a négy tengelyes tükrözésnek pedig 12. Ezek átlaga, vagyis az orbitok száma, és így a feladatban kérdezett szám a 23.

4.6.41. Alkalmazzuk az előző feladat állítását. Az orbitok száma 1, ezért a fixpontok átlagos száma is 1. De az egységelemnek ennél több fixpontja van, és így van olyan elem is, aminek 1-nél kevesebb fixpontja van, vagyis fixpontmentes.

Nem tranzitív csoportra az állítás nem igaz. Az egyelemű csoport triviális példájától eltekintve

$$G = \{id, (12)(34), (12)(56), (34)(45)\} \leq S_6$$

is ellenpélda.

4.6.42. Az izomorfia-osztályok:

$$\{\mathbb{Z}_2^+, \mathbb{Z}_3^\times, \mathbb{Z}_6^\times, S_2\}, \{\mathbb{Z}_3^+, A_3\}, \{\mathbb{Z}_4^+, \mathbb{Z}_5^\times\}, \{\mathbb{Z}_8^\times, \mathbb{Z}_{12}^\times\}, \{S_3, D_3, \mathrm{GL}(2, \mathbb{Z}_2)\}, \{D_4\}, \{Q\}, \{\mathbb{Z}_8^+\}\,.$$

Ez az eddig tanultakból következik, az alábbiak miatt. Tudjuk, hogy izomorf csoportok rendje egyenlő, és megfordítva, egyenlő rendű *ciklikus* csoportok izomorfak. Mivel a prímrendű csoportok ciklikusak, elintéztük a 2 és 3 rendű csoportokat. Negyedrendű csoport kétféle van, ezeket az különbözteti meg, hogy van-e bennük negyedrendű elem. A három hatodrendű csoport azért izomorf, mert mindegyik elemeit egy-egy háromelemű halmaz összes permutációi határozzák meg. Ez a háromelemű halmaz az S_3 esetén az $\{1, 2, 3\}$, a D_3 esetén egy szabályos háromszög három csúcsa, a $GL(2, \mathbb{Z}_2)$ esetén pedig a $\mathbb{Z}_2$ feletti kétdimenziós vektortér összesen három, nem nulla vektora. Az utolsó három (nyolcadrendű) csoport közül semelyik kettő sem izomorf: egyetlen kommutatív van, a másik kettőben pedig nem ugyanaz a negyedrendű elemek száma (lásd 4.6.15. Gyakorlat).

4.6.43. A Klein-csoport esetében $\{id, (12)(34), (13)(24), (14)(23)\}$, a D_3 diédercsoport esetében pedig $\{id, (123)(456), (132)(465), (14)(26)(35), (15)(24)(36), (16)(25)(34)\}$.

4.7. Hogyan keressünk normálosztót?

4.7.6. Minden elem konjugált önmagával, hiszen $1a1^{-1} = a$. A szimmetria azért teljesül, mert $b = gag^{-1}$ esetén $a = (g^{-1})b(g^{-1})^{-1}$ (vagyis ha a g elem „odakonjugál", akkor az inverze „visszakonjugál"). Végül a tranzitivitás abból következik, hogy ha g az a-t b-be konjugálja, h pedig a b-t c-be, akkor a hg elem a-t c-be konjugálja.

4.7.12. $Z(G)$ nyilván részcsoportja G-nek (ez közvetlen számolással is látható, vagy pedig abból következik, hogy a centrum nyilván az összes elem centralizátorainak a metszete). Nyilvánvalóan $Z(G) \triangleleft G$, hiszen $Z(G)$ (egyelemű) konjugált osztályok egyesítése. Hasonló okokból $Z(G)$ minden részcsoportja normálosztó G-ben.

4.7.13. Jelölje φ_g a g elemmel való konjugálást, azaz legyen $\varphi_g(x) = gxg^{-1}$. Ekkor $\varphi_g(x)\varphi_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \varphi_g(xy)$. A g-vel való konjugálás inverze a g^{-1}-gyel való konjugálás, hiszen $g^{-1}gxg^{-1}(g^{-1})^{-1} = x$ és $gg^{-1}x(g^{-1})^{-1}g^{-1} = x$. Ezért a konjugálás bijekció G-ből G-re.

4.7.15. Automorfizmusok kompozíciója és inverze is automorfizmus (4.3.10. Gyakorlat). A belső automorfizmusokról először azt mutatjuk meg, hogy részcsoportot alkotnak. Mint az előző feladatban is, jelölje φ_g a g elemmel való konjugálást. Ekkor $\varphi_{gh} = \varphi_g \circ \varphi_h$, hiszen tetszőleges $x \in G$-re

$$\varphi_g\varphi_h(x) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \varphi_{gh}(x)\,.$$

Már az előző feladatban igazoltuk, hogy a g-vel való konjugálás inverze is belső automorfizmus, nevezetesen a g inverzével való konjugálás. Így a belső automorfizmusok részcsoportot alkotnak.

Azt, hogy a belső automorfizmusok részcsoportot alkotnak, számolás nélkül is megkaphattuk volna a 4.6.22. Gyakorlatból. Hiszen a belső automorfizmusok csoportja éppen annak a homomorfizmusnak a képe, amely minden $g \in G$ elemhez a vele való konjugálást, mint a G egy permutációját rendeli. Ezt az észrevételt fel is használjuk majd a következő gyakorlat megoldásában.

Már csak azt kell belátni, hogy $\mathrm{Inn}(G)$ zárt a konjugálásra, és ehhez elég megmutatni, hogy $\alpha \in \mathrm{Aut}(G)$ esetén $\alpha \circ \varphi_g \circ \alpha^{-1} = \varphi_{\alpha(g)}$. Ez is egy tetszőleges $x \in G$ behelyettesítésével látszik, hiszen $\varphi_{\alpha(g)}(x) = \alpha(g)x\alpha(g)^{-1}$, ami ugyanaz, mint

$$(\alpha \circ \varphi_g \circ \alpha^{-1})(x) = \alpha\big(g\alpha^{-1}(x)g^{-1}\big)\,.$$

4.7.16. A hatás magja azokból a $g \in G$ elemekből áll, amelyekkel való konjugálás az identikus leképezés, vagyis amelyekre $gxg^{-1} = x$ minden $x \in G$-re. Ezek tehát pontosan a centrum elemei. A φ képe, vagyis a φ_g alakú leképezések halmaza pontosan a belső automorfizmusokból áll. A homomorfizmus-tételt φ-re alkalmazva kapjuk, hogy $G/Z(G) \cong \mathrm{Inn}(G)$.

4.7.17. Mivel a konjugálás szorzattartó, az állítást elég egy ciklusra megmutatni, vagyis azt, hogy $f \in S_n$ esetén $f\big(1, 2, \ldots, k\big)f^{-1} = \big(f(1), f(2), \ldots, f(k)\big)$. Ez közvetlenül kiszámolható az $f(i)$ elemek behelyettesítésével (a 4.2.8. Lemma bizonyításához hasonlóan).

4.7.18. Az A_n konjugált elemei konjugáltak S_n-ben is. Az azonban elképzelhető, hogy A_n két elemét az S_n-ben egymásba lehet konjugálni, de az A_n-ben egyik átkonjugáló elem sincs benne (mert mindegyik páratlan permutáció).

Például az $(123) \in S_4$ hármasciklusnak a konjugáltjai a hármasciklusok, összesen 8 darab. Emiatt (123) centralizátora $24/8 = 3$ elemű, vagyis csak a saját hatványaiból áll. Az A_4-ben ezek mind benne vannak, ezért az A_4-beli centralizátor ugyanez, viszont így A_4-ben csak $12/3 = 4$ darab konjugált lesz! Ezért az S_4-ben egy osztályt alkotó hármasciklusok A_4-ben két osztályra bomlanak. Ugyanakkor az $(12)(34)$ elemnek csak három konjugáltja

van S_4-ben, így centralizátora 8-elemű. E centralizátornak eleme például (12), ami nincs benne A_4-ben. Ezért A_4-ben az (12)(34) centralizátora csak négyelemű lesz, viszont a háromelemű konjugált osztálya ugyanaz marad, mint S_4-ben.

Így tehát az A_4 csoportnak négy konjugált osztálya van: az egységelem egyedül, a három $(ab)(cd)$ alakú permutáció egy osztály, és végül a hármasciklusok két négyelemű osztályt alkotnak. Ezekből kell összerakni normálosztót, azaz részcsoportot. Ennek a rendje osztója a 12-nek. Mivel $4+3$ már több, mint 12-nek a fele, ezért nemtriviális normálosztóban csak egyetlen nem egyelemű konjugált osztály lehet. De $4+1$ sem osztója 12-nek, ezért A_4 egyetlen nemtriviális normálosztója a másodrendű elemekből és az egységelemből álló, már az S_4-nél megismert Klein-féle részcsoport.

Be kell még látnunk, hogy ha $g \in A_n$, akkor g konjugáltjainak a száma S_n-ben vagy kétszer annyi, vagy ugyanannyi, mint az A_n-beli konjugáltjainak a száma. A konjugáltak száma a centralizátor indexe, azaz S_n-ben $|S_n|/|C_{S_n}(g)|$, A_n-ben pedig $|A_n|/|C_{A_n}(g)|$. Elég tehát megmutatni, hogy $|C_{S_n}(g)|/|C_{A_n}(g)|$ vagy 1, vagy 2. Ez nyilvánvaló az első izomorfizmus-tételből, mert

$$C_{A_n}(g) = C_{S_n}(g) \cap A_n\,,$$

és $|S_n : A_n| = 2$.

Ezek szerint megállapíthatjuk, hogy ha a g elem felcserélhető páratlan permutációval is, akkor ugyanazok a konjugáltjai S_n-ben, mint A_n-ben, ha viszont csak páros permutációkkal cserélhető fel, akkor feleannyi konjugáltja van A_n-ben, mint S_n-ben.

4.7.20. Az (1) állításban az a bizonyítandó, hogy ha K karakterisztikus részcsoport, akkor nemcsak $\alpha(K) \subseteq K$, hanem $\alpha(K) = K$ is teljesül minden α automorfizmusra. Ez azért igaz, mert az α automorfizmusnak az α^{-1} inverze is automorfizmus, és így $\alpha^{-1}(K) \subseteq K$, ahonnan α-t alkalmazva $K \subseteq \alpha(K)$ adódik.

A (2) bizonyításához tegyük fel, hogy K karakterisztikus részcsoport az N normálosztóban. Ekkor G minden φ_g belső automorfizmusa N-et önmagába viszi, hiszen $gNg^{-1} = N$. Ezért φ_g (pontosabban a φ_g-nek az N-re való leszűkítése) automorfizmusa az N csoportnak. Mivel K karakterisztikus részcsoport, $\varphi_g(K) = K$. Így K zárt minden konjugálásra, és ezért normálosztó G-ben.

A (3) állítás bizonyítása hasonló. Ha K karakterisztikus részcsoportja N-nek, N pedig G-nek, akkor G minden α automorfizmusa N-et N-be viszi, és így α leszűkíthető N-re. Ez a leszűkítés automorfizmusa N-nek, és ezért K-t önmagába viszi. Tehát $\alpha(K) = K$.

4.7.21. Legyen N az N_i normálosztók metszete. Ez részcsoport (4.4.25. Gyakorlat), meg kell mutatni, hogy zárt a konjugálásra. Tegyük fel, hogy $g \in G$ és $n \in N$. Ekkor n eleme mindegyik N_i-nek is, és mivel ezek normálosztók, $gng^{-1} \in N_i$ minden i-re. De akkor $gng^{-1} \in N$, és így N tényleg zárt a konjugálásra.

4.7.22. Azt kell belátni, hogy a legszűkebb X-et tartalmazó N normálosztó ugyanaz, mint a legszűkebb Y-t tartalmazó H részcsoport. Az N normálosztó tartalmazza X-et, és ezért X elemeinek konjugáltjait is, vagyis Y-t. Tehát N egy Y-t tartalmazó részcsoport, és mivel H a legszűkebb ilyen részcsoport, $H \subseteq N$.

A fordított irányú tartalmazáshoz elég megmutatni, hogy H normálosztó, hiszen az X elemeit H tartalmazza, és így N, mint a legszűkebb X-et tartalmazó normálosztó, része lesz H-nak. Mivel H részcsoport, azt kell belátni, hogy zárt a konjugálásra. Ezt könnyen igazolhatnánk annak felhasználásával, hogy H elemeit az Y elemeiből és ezek inverzeiből készített szorzatok alakjában írhatjuk fel. Elegánsabb azonban a következő gondolatmenet. Legyen φ_g belső automorfizmusa G-nek. Ekkor $\varphi_g(Y) = Y$, és így $\varphi_g(H)$ egy Y-t tartalmazó részcsoportja G-nek. Mivel H a legszűkebb ilyen részcsoport, $H \subseteq \varphi_g(H)$. A φ_g inverze is belső automorfizmus, és ezért ugyanezt a gondolatmenetet φ_g^{-1}-re elmondva $H \subseteq \varphi_g^{-1}(H)$ adódik, ami azt jelenti, hogy $\varphi_g(H) \subseteq H$.

4.7.27. Tegyük fel, hogy $n \in N$ és $k \in K$. Tekintsük az $[n,k] = nkn^{-1}k^{-1}$ elemet. Ezt kétféleképpen is átalakíthatjuk. Mivel K normálosztó,

$$[n,k] = (nkn^{-1})k^{-1} \in nKn^{-1}K = KK = K\,.$$

A másik átalakítás:

$$[n,k] = n(kn^{-1}k^{-1}) \in NkNk^{-1} = NN = N\,,$$

hiszen N is normálosztó. Így $[n,k] \in N \cap K$. Ha ez $\{1\}$, akkor átrendezéssel $nk = kn$.

4.7.31. A 4.4.4. Gyakorlat utolsó állítása miatt $H \subseteq N_G(H)$. Ha $H \subseteq K \leq G$, akkor H pontosan akkor normálosztó K-ban, ha minden $k \in K$-ra $kH = Hk$, azaz ha $K \subseteq N_G(H)$.

4.7.33.

(1) Nyilván egy g elem akkor és csak akkor cserélhető fel X minden elemével, ha minden $x \in X$-nek benne van a centralizátorában.
(2) Hasson G a G összes részhalmazainak a halmazán konjugálással: $g * X = gXg^{-1}$. Ez nyilván hatás, és X stabilizátora $N_G(X)$.
(3) Ha $g \in N_G(X)$, akkor a g-vel való φ_g konjugálás X-nek egy permutációja. Ezért a $\varphi : g \to \varphi_g$ leképezés homomorfizmus $N_G(X)$-ből S_X-be, melynek magja $C_G(X)$.
(4) Ha X részcsoport, akkor a (3) pontban szereplő φ_g automorfizmusa X-nek, és így φ az $\mathrm{Aut}(X)$ csoportba képez. A homomorfizmus-tétel miatt tehát az állítás igaz.

4.7.35.

(1) Igen, mert $\mathbb{Z}^+$ Abel-csoport.
(2) Igen, a 4.1.8. Állításból láthatjuk, hogy a D_6 csoportban csak F^2 és F^4 lesz harmadrendű elem. Ezért konjugálásnál ezek helyben maradnak, vagy helyet cserélnek (hiszen a konjugálás az elemrendet megőrzi). Így H zárt a konjugálásra, és részcsoport is, mert az F^2 hatványaiból áll.

(3) Nem, az F elemmel való konjugálás kivezet ebből a halmazból, hiszen a 4.1.8. Állítás miatt $FTF^{-1} = TF^5F^{-1} = TF^4$.
(4) Nem. Tekintsünk ugyanis egy egyenesre való tükrözést. Ennek a mátrixa diagonális, ha a bázist ügyesen választjuk, vagyis ha a b_1 bázisvektor a tengellyel párhuzamos, b_2 pedig rá merőleges. De például a $b_1 + b_2$ és $b_1 - b_2$ vektorokból álló bázisban ez a mátrix már nem diagonális (sőt nem is háromszögmátrix). Mivel a bázistranszformáció konjugálást jelent, a diagonális mátrixok közül a konjugálás kivezet. Ugyanezt a példát $n \times n$-es mátrixokra is elmondhatjuk $n \geq 2$ esetén, ha a $b_3, \ldots, b_n$ bázisvektorok képeit saját maguknak definiáljuk (vagyis ha egy „hipersíkra" tükrözünk).
(5) Igen, ez része $\mathrm{GL}(n, \mathbb{R})$ centrumának, hiszen az egységmátrix skalárszorosai minden mátrixszal felcserélhetők. Részcsoport is, ezért a 4.7.12. Gyakorlat miatt normálosztó. A 4.13.2. Gyakorlatban belátjuk majd, hogy ez a normálosztó a $\mathrm{GL}(n, \mathbb{R})$ csoport centruma.
(6) Nem, a (4)-beli ellenpélda ebben a szituációban is működik.

4.7.36. A D_3 és a $\mathrm{GL}(2, \mathbb{Z}_2)$ csoportok izomorfak az S_3 szimmetrikus csoporttal (lásd 4.6.42. Gyakorlat), amelynek már meghatároztuk a konjugált osztályait és normálosztóit. Az eredmények az izomorfizmus mentén átvihetőek. Így D_3 egyetlen nemtriviális normálosztója a forgatásokból áll, mert ezek felelnek meg az *id*, (123), (132) elemeknek. A $\mathrm{GL}(2, \mathbb{Z}_2)$ esetében a

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

mátrixokból álló normálosztót kapjuk.

A D_4 csoportban (miként minden más csoportban is) az egységelem centralizátora az egész csoport, így konjugált osztálya egyelemű. Ugyanez mondható el F^2-ről is (ez a középpontos tükrözés). Valóban, a 4.1.8. Állítás miatt $TF^2 = F^2T$, ezért F^2 centralizátora az F hatványain kívül T-t is tartalmazza. Ez már 5 elem, és mivel a centralizátor rendje a 8-nak osztója, F^2 centralizátora tényleg az egész csoport. Ugyanezért a T centralizátora tartalmazza az 1, T, F^2, TF^2 elemeket, tehát elemszáma 4 vagy 8. De 8 nem lehet, hiszen $TF \neq FT = TF^3$. Tehát T-nek $8/4 = 2$ két konjugáltja van. Az egyik önmaga, és így a másik csak $FTF^{-1} = FTF^3 = TF^2$ lehet. Hasonló érvelés mutatja, hogy TF-nek is két konjugáltja van: önmaga, és TF^3. Végül F centralizátora $\langle F \rangle$, hiszen F hatványai biztosan centralizálják F-et, de T nem. Ezért F konjugáltjai a kimaradó két elem, F és F^3. Tehát D_4 konjugált osztályai $\{1\}$, $\{F^2\}$, $\{F, F^3\}$, $\{T, TF^2\}$, $\{TF, TF^3\}$. A normálosztók azok a részcsoportok, amik konjugált osztályok egyesítései, elemszámuk 8-nak osztója. Kételemű normálosztó tehát csak $\{1, F^2\}$ lehet, és a négyelemű normálosztókban is benne kell, hogy legyen az egységelemen kívül F^2 is (mert a többi konjugált osztálynak páros sok eleme van). Könnyű látni, hogy az így kapott összes lehetőség, $\{1, F^2, F, F^3\}$, $\{1, F^2, T, TF^2\}$, $\{1, F^2, TF, TF^3\}$ mindegyike részcsoportot, és így normálosztót ad. A két triviálissal együtt tehát hat normálosztó van D_4-ben.

Hasonló meggondolások mutatják, hogy a Q kvaterniócsoport konjugált osztályai $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$, a centrum $\{1, -1\}$. Minden részcsoport normálosztó, ezek $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$, $\langle -1\rangle$, és a két triviális.

A D_5 diédercsoportban konjugált osztály az öt tengelyes tükrözés, és minden forgatás az inverzével egy-egy konjugált osztályt alkot. Az egyetlen nemtriviális normálosztó a forgatásokból áll.

Az S_5 konjugált osztályait a 4.7.17. Gyakorlatból kapjuk. Az eredmény a következő:

24 darab $(abcde)$ alakú permutáció,
30 darab $(abcd)$ alakú permutáció,
20 darab (abc) alakú permutáció,
20 darab $(abc)(de)$ alakú permutáció,
10 darab (ab) alakú permutáció,
15 darab $(ab)(cd)$ alakú permutáció,
1 darab egységelem.

Az S_5 egyetlen nemtriviális normálosztója A_5, ennek megmutatásához kényelmesebb először az A_5 normálosztóit meghatározni, majd hivatkozni a 4.11.29. Gyakorlat megoldására.

Az A_5 konjugált osztályait a 4.7.18. Gyakorlat segítségével kereshetjük meg. Könnyű látni, hogy A_5-ben az ötösciklusok két tizenkételemű osztályt, a hármasciklusok egy húszelemű osztályt, az $(ab)(cd)$ alakú permutációk egy tizenöt elemű osztályt alkotnak. A kapott 1, 12, 12, 15, 20 számokból nem lehet összeadással kikeverni 60 valódi osztóját úgy, hogy 1 is köztük legyen, és így A_5 egyszerű csoport.

4.7.37. Az $(1, 2, \dots, n)$ konjugáltjai az n hosszú ciklusok, vagyis $(n-1)!$ konjugáltja van. Ezért centralizátora n-elemű, és így az $(1, 2, \dots, n)$ hatványai a teljes centralizátort kiadják.

4.7.38. Ha A Abel-csoport, akkor centruma az egész A, kommutátor-részcsoportja pedig $\{1\}$. A Q kvaterniócsoportnak a 4.7.36. Gyakorlat szerint a centruma $Z(Q) = \{1, -1\}$. Ugyanez a kommutátor-részcsoportja is. Valóban a szerinte vett faktor négyelemű csoport, ezért kommutatív, és így $Q' \subseteq Z(Q)$. Ha Q' ennél kisebb lenne, akkor csak $\{1\}$ lehetne, ami azt jelentené, hogy Q kommutatív. Ez nem igaz, és így $Q' = Z(Q)$.

A D_n csoportban tudjuk, hogy ha T tengelyes tükrözés és R tetszőleges forgatás, akkor $TR = R^{-1}T$. Ezért T akkor és csak akkor cserélhető fel R-rel, ha $R^2 = 1$. Ha n páratlan, akkor innen $R = 1$, ilyenkor D_n centruma egyelemű. Ha n páros, akkor D_n centruma az identitásból és a középpontos tükrözésből áll.

A fenti egyenlőséget átrendezve $TRT^{-1}R^{-1} = R^{-2}$ adódik, vagyis minden forgatás négyzete kommutátor. Ha n páratlan, akkor ezek az összes forgatást kiadják, ilyenkor a

kommutátor-részcsoport a forgatásokból áll. (Ennél nagyobb nem lehet, hiszen a forgatások normálosztója szerinti faktor kételemű, vagyis Abel-féle.) Ha n páros, akkor a forgatások négyzetei egy $n/2$ elemű részcsoportot alkotnak, és ilyenkor ez lesz a kommutátor-részcsoport. (Ez könnyen láthatóan normálosztó, és a rá vett faktor négyelemű, tehát ismét csak kommutatív.)

Az S_n csoport $n = 2$ esetén Abel. Ha $n > 2$, akkor centruma $\{1\}$, kommutátor-részcsoportja A_n. Valóban, tegyük fel, hogy $f \in Z(S_n)$, akkor az előző feladat szerint f az $(1, 2, \ldots, n)$ ciklus i-edik hatványa alkalmas i-re. De $(1, 2, \ldots, n)^i$-nel (12)-t konjugálva $(i + 1, i + 2)$ adódik (az összeadást mod n értve). Ez $n > 2$ miatt csak akkor lehet $(12) = (21)$, ha $i = 0$. Ezért f az egységelem, és ezzel beláttuk, hogy $Z(S_n) = \{1\}$.

Mivel S_n/A_n kételemű csoport, amely ciklikus, és így Abel-féle, az S_n kommutátor-részcsoportja benne van A_n-ben. Az $[(ab), (ac)] = (abc)$ összefüggés miatt minden hármasciklus kommutátor. Mivel a hármasciklusok generálják A_n-et (4.2.26. Gyakorlat), $n > 2$ esetén $S_n' = A_n$.

Az A_4 csoportnak a 4.7.18. Gyakorlatban már meghatároztuk a konjugált osztályait, és így látjuk, hogy centruma egyelemű. Belátjuk, hogy A_4' a négyelemű Klein-féle normálosztó. Valóban, az erre vett faktor háromelemű, és így kommutatív, ennél szűkebb normálosztó azonban csak az $\{1\}$ van, ami nem lehet A_4', mert ez nem kommutatív csoport.

Megjegyezzük, hogy $n \geq 5$ esetén A_n centruma $\{1\}$, kommutátor-részcsoportja önmaga. Ez következik abból, hogy A_n ilyenkor nemkommutatív egyszerű csoport (4.11.22. Tétel).

4.7.39. Az $\{1, F^2\}$ normálosztó D_4-ben, sőt az előző gyakorlat szerint az D_4 centruma. A $D_4/\{1, F^2\}$ faktorcsoport rendje 4, és minden elemének a négyzete az egységelem. Valóban, D_4 minden elemének négyzete az egységelem, kivéve az F és F^3 elemeket, de ezeknek a négyzete is benne van az $\{1, F^2\}$ normálosztóban, és így az ezekből álló mellékosztály négyzete $\{1, F^2\}$. Ezért ez a faktorcsoport a Klein-csoporttal izomorf.

Legyen $K = \{id, (12)(34), (13)(24), (14)(23)\}$ Az S_4/K faktorcsoportban való számoláshoz tekintsük az S_4-ben a 4 pont H stabilizátorát. Megmutatjuk, hogy ennek elemei reprezentánsrendszert alkotnak K szerint. Valóban, ha h_1 és h_2 ugyanabban a mellékosztályban lenne K szerint, akkor $h_1^{-1}h_2 \in K \cap H = \{1\}$, és ezért $h_1 = h_2$. A H elemei tehát csupa különböző mellékosztályokban vannak, és mivel H elemszáma és a mellékosztályok száma is 6, ezért minden mellékosztályba jut is reprezentánselem. A faktorcsoportban ezek szerint számolhatunk a H elemeivel, mint reprezentánsokkal, és így a $h \mapsto hK$ izomorfizmus H és A_4/K között. A H viszont az $\{1, 2, 3\}$ összes permutációiból áll, és így S_3-mal izomorf. Ezért $A_4/K \cong S_3$. Megjegyezzük, hogy ez az izomorfia az első izomorfizmustételből (4.5.20. Következmény) is adódik, hiszen $HK = A_4$, és így $A_4/K \cong H/(H \cap K)$.

A $D_8/\{1, F^2, F^4, F^6\}$ faktorcsoport szintén négyelemű, és szintén a Klein-csoporttal izomorf, mert D_8 minden elemének négyzete benne van a $\{1, F^2, F^4, F^6\}$ normálosztóban.

4.7.40. Legyen G egy $2p$ rendű nemkommutatív csoport, ahol $p > 2$ prím. Ekkor G-ben nincs $2p$ rendű elem, különben ciklikus, és így kommutatív lenne. Ha egy p rendű elem felcserélhető lenne egy másodrendű elemmel, akkor a szorzatuk a 4.3.32. Gyakorlat miatt $2p$ rendű lenne, ami lehetetlen. Ezért minden egységtől különböző elem centralizátora csak az elem hatványaiból áll. A csoportban nem lehet minden elem másodrendű a 4.3.33. Feladat miatt, ugyanakkor van benne másodrendű elem a 4.4.35. Feladat miatt. Így az elemrendek 1, 2 és p. Egy másodrendű elemnek a centralizátora kételemű, és így $2p/2 = p$ konjugáltja van. Ez p darab másodrendű elemet jelent (legalább). Több azonban nem fér el, mert van p rendű elem is, és annak $p-1$ darab p rendű hatványa van (4.3.30. Gyakorlat). Legyen f egy p rendű, t egy másodrendű elem. Ekkor tf nem lehet hatványa f-nek, mert akkor t is hatványa lenne, és így f és t felcserélhetők lennének. Ezért tf másodrendű elem, azaz $tftf = 1$ ahonnan $tf = f^{-1}t$. Mivel f^i rendje is p, ha $1 \leq i < p$, ezért tf^i is másodrendű, és így egyrészt $tf^i = f^{-i}t$, másrészt $t = tf^0$-val együtt az összes másodrendű elemet megkapjuk. Ezért a G elemei kölcsönösen egyértelműen és művelettartóan megfelelnek a D_p diédercsoport elemeinek (lásd 4.1.8. Állítás).

4.7.41. Legyen $N = \{1, a\}$. Az $\{1\}$ mindig konjugált osztálya G-nek, és mivel N a G konjugált osztályainak egyesítése, $\{a\}$ is az. Tehát $a \in Z(G)$.

4.7.42. Az nyilvánvaló, hogy ha $H = \langle X \rangle$ kommutatív, akkor az $X \subseteq H$ elemei is egymással felcserélhetőek. A megfordítást bizonyíthatnánk a 4.4.27. Tételre való hivatkozással is, hiszen ha X elemei páronként felcserélhetők, akkor a belőlük és inverzeikből készített szorzatok is. Elegánsabb azonban a következő gondolatmenet.

Tegyük fel, hogy X elemei páronként felcserélhetők. Ekkor az X részhalmaz $C_G(X)$ centralizátora tartalmazza X összes elemét. Sőt, X része a $C_G(X)$ csoport Z centrumának is, hiszen X elemei a centralizátor definíciója szerint felcserélhetők $C_G(X)$ elemeivel. Tehát Z egy X-et tartalmazó részcsoport, és így tartalmazza a legszűkebb X-et tartalmazó részcsoportot, azaz H-t is. Mivel Z Abel-féle, H is az.

4.7.43. A $\mathbb{Z}^+$ végtelen ciklikus csoportnak két generátoreleme van, az 1 és a -1. Ezért egy automorfizmus az 1-et vagy 1-be, vagy -1-be viszi, és ez az automorfizmust már egyértelműen meghatározza. Az első esetben az identitást kapjuk, a másodikban az ellentettképzést. Ezért $\mathrm{Aut}(\mathbb{Z}^+)$ a kételemű (ciklikus) csoport.

A $\mathbb{Z}_n^+$ homomorfizmusait is egyértelműen meghatározza az 1 generátorelem képe. Ha automorfizmusról van szó, akkor az 1 képe is generátorelem kell, hogy legyen. A generátorelemek pontosan az n-hez relatív prím elemek, hiszen a hatvány rendjének képlete miatt ezek rendje lesz szintén n. Ha $\alpha(1) = k$, akkor α összegtartása miatt $\alpha(i) = ik$ (4.3.11. Gyakorlat). Megfordítva, az $\alpha_k(i) = ik$ képlet nyilván $\mathbb{Z}_n^+$ automorfizmusát definiálja, hiszen

$$\alpha_k(i+j) = (i+j)k = ik + jk = \alpha_k(i) + \alpha_k(j)$$

(az itt használt összeadás és szorzás a $\mathbb{Z}_n$ gyűrű műveletei). Meg kell még vizsgálnunk ezeknek az automorfizmusoknak a kompozícióját:

$$(\alpha_k \circ \alpha_\ell)(i) = k\ell i = \alpha_{k\ell}(i)$$

miatt a $k \mapsto \alpha_k$ leképezés izomorfizmus a $\mathbb{Z}_n^\times$ és az $\mathrm{Aut}(\mathbb{Z}_n^+)$ csoportok között.

A Klein-csoport szorzási szabálya szimmetrikus (bármely két nem egység elem szorzata a harmadik nem egység elem, bármely elem négyzete az egységelem). Így az egységtől különböző elemek bármely permutációja automorfizmus, tehát az automorfizmus-csoport S_3.

Az S_3 csoportot generálja a három transzpozíció, és ezeknek a képe is másodrendű elem kell, hogy legyen. Vagyis minden automorfizmus a három transzpozíció egy permutációjából származik, és így legfeljebb hat automorfizmus lehet. Azonban a belső automorfizmusok száma pontosan hat, hiszen az S_3 csoport centruma egyelemű, és így a 4.7.16. Gyakorlat miatt $\mathrm{Inn}(S_3) \cong S_3/Z(S_3) \cong S_3$. Tehát minden automorfizmus belső, és $\mathrm{Aut}(S_3) \cong S_3$.

4.7.44. Legyen α másodrendű, fixpontmentes automorfizmus. Ha $g^{-1}\alpha(g) = h^{-1}\alpha(h)$, akkor átrendezéssel $hg^{-1} = \alpha(hg^{-1})$, és így $hg^{-1} = 1$, vagyis $g = h$. A $g^{-1}\alpha(g)$ elemek tehát páronként különbözők, és mivel G véges, az összes elemét kiadják. Az $\alpha^2 = id$ feltétel miatt

$$\alpha\big(g^{-1}\alpha(g)\big) = \alpha(g^{-1})g = \big(g^{-1}\alpha(g)\big)^{-1}.$$

Ez azt jelenti, hogy α a G minden elemét az inverzébe viszi. Így

$$h^{-1}g^{-1} = (gh)^{-1} = \alpha(gh) = \alpha(g)\alpha(h) = g^{-1}h^{-1},$$

vagyis G kommutatív. Az inverzképzés akkor és csak akkor lesz fixpontmentes, ha az egységelemen kívül egyetlen elem sem egyenlő az inverzével, vagyis ha nincs másodrendű elem. Ez úgy is átfogalmazható, hogy G rendje páratlan (4.4.35. Feladat). Megfordítva, páratlan rendű kommutatív csoportban az inverzképzés mindig szorzattartó, bijektív, és fixpontmentes.

4.7.45. Az S_3 csoportban az (12) által generált részcsoport nem normálosztó, és indexe három, így nem hagyható el az a feltétel, hogy a csoport rendje páratlan legyen. Tegyük fel, hogy $|G : H| = 3$, és hogy $|G|$ páratlan.

Tekintsük G hatását a H szerinti bal mellékosztályok halmazán. A 4.6.26. Gyakorlat állításait alkalmazzuk. A célunk annak megmutatása, hogy a hatás magja H, mert akkor H normálosztó lesz G-ben.

Jelölje a hatás magját N, ez H konjugáltjainak a metszete, és így $N \subseteq H$. Tudjuk, hogy G/N izomorf S_3 egy részcsoportjával. Mivel G rendje páratlan, ez a részcsoport nem lehet az egész S_3, és így rendje legfeljebb 3. Így $|G : N|$ legfeljebb 3, tehát $H = N$.

4.7.46. Az n rendű elemek halmaza zárt minden automorfizmusra. Ezért az általa generált részcsoportot minden automorfizmus önmagába viszi (a 4.5.27. Gyakorlat miatt).

4.7.47. Az alábbiakban α a G csoport egy automorfizmusát jelöli.

(1) A végtelen ciklikus csoportnak két automorfizmusa van (az identitás és az inverzképzés, lásd 4.7.43. Feladat), és ezek minden részcsoportot megőriznek. Ha H részcsoportja a G véges ciklikus csoportnak, akkor G-nek csak egyetlen $|H|$ elemszámú részcsoportja van (4.3.21. Állítás). Ezért ezt minden automorfizmus csak önmagába viheti.

(2) Mivel $g \in Z(G)$ felcserélhető minden $h \in G$-vel, $\alpha(g)$ is felcserélhető minden $\alpha(h)$-val, vagyis a csoport összes elemével. Ezért $\alpha\big(Z(G)\big) \subseteq Z(G)$. Ugyanezt α^{-1}-re alkalmazva a fordított tartalmazást kapjuk.

(3) Ha $n \in N$, $k \in K$, akkor nyilván $[\alpha(n), \alpha(k)] = \alpha([n, k])$. Így ha N és K karakterisztikus, akkor minden $[n, k]$ kommutátor képe $[N, K]$-ban van, és így $\alpha([N, K]) \subseteq [N, K]$. A fordított tartalmazást most is az α^{-1} szolgáltatja. Ha ugyanezt a gondolatmenetet a belső automorfizmusokra mondjuk el, akkor azt kapjuk, hogy $N, K \triangleleft G$ esetén $[N, K] \triangleleft G$.

(4) Könnyű ellenőrizni, hogy (A kommutativitása miatt) részcsoportokról van szó. Mivel α összegtartó, $\alpha(na) = n\alpha(a)$ teljesül tetszőleges n egészre (4.3.11. Gyakorlat). Ezért a megadott részcsoportokat minden automorfizmus önmagába képzi.

4.7.48. Az Útmutatóban szereplő két azonosságot a kommutátorok közvetlen kifejtésével igazolhatjuk. Az első azonosság szerint $[N, K]$ generátorai a $[K, N]$ generátorainak inverzei, és így a két részcsoport megegyezik, hiszen mindegyik tartalmazza a másik generátorelemeit.

Mivel $L \subseteq LN$, ezért $[K, L] \subseteq [K, LN]$. Ugyanígy kapjuk, hogy $[K, N] \subseteq [K, LN]$, és így $[K, L][K, N] \subseteq [K, LN]$. A fordított tartalmazáshoz elég azt megmutatni, hogy $[K, LN]$ minden generátoreleme benne van $[K, L][K, N]$-ben. Ezt mutatja az Útmutatóban szereplő második azonosság (hiszen azt már az előző gyakorlatban beláttuk, hogy $[K, N]$ normálosztó, vagyis zárt a konjugálásra).

4.8. A direkt szorzat.

4.8.1. Az asszociativitást komponensenként lehet ellenőrizni. Legyen $g = (\dots, g_i, \dots)$, $h = (\dots, h_i, \dots)$ és $k = (\dots, k_i, \dots)$. Ekkor $(gh)k$-nak az i-edik komponense $(g_ih_i)k_i$, és $g(hk)$-nak az i-edik komponense $g_i(h_ik_i)$. Ezek egyenlők, hiszen az i-edik komponensben a szorzás asszociatív. Így $(gh)k = g(hk)$, mert minden komponensük egyenlő. Ugyanígy mutathatjuk meg az egységelemről és az inverzről szóló állítást.

4.8.3. A $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ csoportban számítsuk ki az $(1, 1)$ elem rendjét. A hatványok (azaz többszörösök) a következők:

$$1 \cdot (1, 1) = (1, 1)\,, \quad 2 \cdot (1, 1) = (0, 2)\,, \quad 3 \cdot (1, 1) = (1, 0)\,,$$
$$4 \cdot (1, 1) = (0, 1)\,, \quad 5 \cdot (1, 1) = (1, 2)\,, \quad 6 \cdot (1, 1) = (0, 0)\,,$$

hiszen az első komponensben mod 2, a második komponensben mod 3 kell összeadni. Láthatjuk, hogy ennek az elemnek a rendje 6 (és mellesleg fel is soroltuk a $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ csoport mind a hat elemét). Így ez ciklikus csoport, tehát $\mathbb{Z}_6^+$-szal izomorf (és az izomorfizmust megadja a fenti táblázat).

Ugyanilyen számolás mutatja, hogy a $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$ csoportban minden elem kétszerese az egységelem (hiszen ez mindkét komponensben minden elemre igaz). Ez a négyelemű csoport tehát nem a ciklikus, hanem a Klein-csoporttal izomorf.

4.8.10. Tegyük fel, hogy $\mathbb{Z}_k^\times$ ciklikus, és legyen $k = nm$, ahol n és m relatív prímek. Ekkor a 4.8.7. és a 4.8.9. Következmények miatt a $\mathbb{Z}_n^\times$ és a $\mathbb{Z}_m^\times$ csoportoknak is ciklikusaknak, és relatív prím rendűeknek kell lenniük. E csoportok rendjei $\varphi(n)$ és $\varphi(m)$. De ha $n > 2$, akkor $\varphi(n)$ páros. Ezért m és n valamelyike 1 vagy 2 kell, hogy legyen. Beláttuk, hogy a k szám csak úgy bontható két relatív prím szám szorzatára, hogy az egyik tényező 1 vagy 2 lehet csak. A számelmélet alaptételéből azonnal látszik, hogy ekkor k prímhatvány, vagy annak kétszerese.

4.8.13. Az egyszerűbb jelölés végett az állítást $n = 3$ esetére mutatjuk meg, az általános esetben ehhez képest már nincsen újdonság. Nyilvánvaló, hogy G_i^* a G_i-vel izomorf részcsoport, megmutatjuk, hogy G_2^* normálosztó. Valóban,

$$(g_1, g_2, g_3)(1_{G_1}, g, 1_{G_3})(g_1, g_2, g_3)^{-1} = (1_{G_1}, g_2 g g_2^{-1}, 1_{G_3}) \in G_2^*,$$

hiszen $g_1 \cdot 1_{G_1} \cdot g_1^{-1} = 1_{G_1}$ (és ugyanez történik a harmadik komponensben is). Mivel

$$(g_1, g_2, g_3) = (g_1, 1_{G_2}, 1_{G_3})(1_{G_1}, g_2, 1_{G_3})(1_{G_1}, 1_{G_2}, g_3),$$

ezért $G = G_1^* G_2^* G_3^*$. Belátjuk, hogy $G_1^* \cap G_2^* G_3^*$ csak az egységelemből áll. Valóban, G_1^* elemeinek minden komponense az egységelem, esetleg az elsőt kivéve. A $G_2^* G_3^*$ elemeinek első komponense viszont 1_{G_1}, hiszen ez igaz a G_2^* és a G_3^* elemeire, és így a szorzataikra is. Ezért $G_1^* \cap G_2^* G_3^*$ elemeinek mindegyik komponense az egységelem.

A megfordításhoz tegyük föl, hogy $G = G_1 G_2 G_3$, ahol G_i normálosztó G-ben, és mindegyik G_i csak az egységelemben metszi a másik kettő szorzatát. Ekkor a 4.8.12. Tétel miatt $G \cong G_1 \times (G_2 G_3)$. Ezért elegendő azt megmutatni, hogy $G_2 G_3 \cong G_2 \times G_3$. Ez ismét a 4.8.12. Tételből következik, azt kell csak belátni, hogy $G_2 \cap G_3 = \{1\}$. Ez következik a $G_2 \cap G_1 G_3 = \{1\}$ feltételből, hiszen $G_3 \subseteq G_1 G_3$.

Igazából azt láttuk be, hogy $G \cong G_1 \times (G_2 \times G_3)$. Ez persze izomorf a $G_1 \times G_2 \times G_3$ direkt szorzattal, mert $(g_1, (g_2, g_3)) \leftrightarrow (g_1, g_2, g_3)$ nyilván kölcsönösen egyértelmű, művelettartó megfeleltetés. Ezt úgy is fogalmazhatjuk, hogy a direkt szorzat képzése *asszociatív*.

Általános n esetében a fenti gondolatmenet második felét könnyű általánosítani úgy, hogy az n-ről $n + 1$-re lépés bizonyítását adja, vagyis n szerinti indukciót alkalmazhatunk. A bizonyítást indukció nélkül is végig lehet vinni a 7.2.2. Gyakorlat megoldásának ötlete alapján.

4.8.16. Ez következik az első izomorfizmus-tételből (4.5.20. Következmény), amely azt állítja, hogy $NH/N \cong H/H \cap N$. Most $NH = G$ és $H \cap N = \{1\}$, tehát $G/N \cong H$ adódik.

4.8.17. A 4.7.15. Gyakorlat megoldásában már beláttuk, hogy $\varphi_{gh} = \varphi_g \circ \varphi_h$, azaz hogy φ homomorfizmus.

4.8.19.

(1) A szorzás asszociativitásának megmutatásához az $\big((n_1, h_1)(n_2, h_2)\big)(n_3, h_3)$ és az $(n_1, h_1)\big((n_2, h_2)(n_3, h_3)\big)$ szorzatokról kell belátni, hogy egyenlőek. A második komponensre ez nyilvánvaló, az első komponensek esetében pedig mindkétszer

$$n_1\big(\psi(h_1)\big)(n_2)\big(\psi(h_1h_2)\big)(n_3)$$

adódik. Az (1, 1) egységelem, az (n, h) inverze $\big(\big(\psi(h^{-1})\big)n^{-1}, h^{-1}\big)$ lesz.

(2) Az $(n, 1) \leftrightarrow n$ leképezés izomorfizmus N^* és N között, emiatt N^* részcsoport. Az N^* normalizátora N^*-ot tartalmazza, de tartalmazza H^*-ot is az (5)-beli egyenlőség miatt. Így tartalmazza N^*H^*-ot is, ami (4) szerint az egész csoport. Ezért N^* tényleg normálosztó.

(3) Az $(1, h) \leftrightarrow h$ leképezés izomorfizmus H^* és H között, emiatt H^* is részcsoport.

(4) Nyilván $(n, h) = (n, 1)(1, h)$.

(5) Ez a szorzás képletének közvetlen alkalmazásával adódik.

4.8.20. (0, 1), (0, 3), (1, 1), (1, 3).

4.8.21. A másodrendű elemek száma az első csoportban 7, a másodikban csak 3.

4.8.22. Hányféleképpen bontható fel például a 48 prímhatványok szorzatára? A 3 mindig szerepel. A 16 felbontásait a legnagyobb benne szereplő szám szerint csoportosíthatjuk. Ha ez 16, akkor a felbontás egytényezős. Ha 8, akkor csak $8 \cdot 2$ lehet. Ha 4, akkor $4 \cdot 4$ és $4 \cdot 2 \cdot 2$ adódik. Ha 2, akkor csak $2 \cdot 2 \cdot 2 \cdot 2$ lehetséges. Összesen tehát 5 lehetőség van. A kapott öt csoport az alaptétel egyértelműségi állítása miatt egymással páronként nem izomorf. Például $\mathbb{Z}_3^+ \times \mathbb{Z}_4^+ \times \mathbb{Z}_4^+$ és $\mathbb{Z}_3^+ \times \mathbb{Z}_4^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$ nem izomorfak, mert a negyedrendű tényezők száma az egyik felbontásban kettő, a másikban egy. Az eredmény 6-ra 1, 8-ra 3, 16-ra 5 és 32-re 7.

4.8.23. Olyan A és B normálosztókat keresünk, melyekre $A \cap B = \{e\}$ és $AB = G$. Abelcsoportban elég részcsoportokat keresni, hiszen minden részcsoport normálosztó. A $\mathbb{Z}_6^+$ a $\{0, 2, 4\}$ és $\{0, 3\}$ normálosztók direkt szorzata. A $\mathbb{Z}_8^+$ csoportnak is négy részcsoportja van, hiszen a részcsoportok a 8 osztóinak felelnek meg a 4.3.21. Állítás miatt, de nincs nemtriviális direkt felbontása, mert mindegyik nem egyelemű részcsoport tartalmazza a 4 elemet. A $\mathbb{Z}^+$ csoportnak sincsen, mert ha A és B nemtriviális részcsoportok, és $a \in A$ valamint $b \in B$ nem nulla elemek, akkor ab nem nulla elem $A \cap B$-ben. Ugyanígy $\mathbb{Q}^+$ is direkt felbonthatatlan: ha $p/q \in A$ és $r/s \in B$, akkor $pr \in A \cap B$. A $\mathbb{C}^+$ csoportnak

viszont sok direkt felbontása van, például két különböző, origón átmenő egyenesnek a direkt összege.

A 4.8.9. Következmény miatt $\mathbb{Z}_{15}^{\times}$ felbontható, és valóban $\mathbb{Z}_{15}^{\times}$ az $\{1, 2, 4, 8\}$ és $\{1, 14\}$ ciklikus normálosztók direkt szorzata. A $\mathbb{Z}_{16}^{\times}$ csoport az $\{1, 15\}$ és $\{1, 3, 9, 11\}$ normálosztók direkt szorzata (amelyek szintén ciklikusak, és így $\mathbb{Z}_{15}^{\times} \cong \mathbb{Z}_{16}^{\times} \cong \mathbb{Z}_2^+ \times \mathbb{Z}_4^+$).

A D_3, D_4, Q, A_4, S_5 csoportoknak már kiszámoltuk a normálosztóit a 4.7.18. és a 4.7.36. Gyakorlatokban, és ebből látszik, hogy mindegyik direkt felbonthatatlan. Végül legyen $A = \{1, F^2, F^4, T, TF^2, TF^4\} \triangleleft D_6$ és $B = \{1, F^3\} \triangleleft D_6$. Ezek a normálosztók mutatják, hogy $D_6 \cong D_3 \times \mathbb{Z}_2^+$.

4.8.24. Olyan A és B ötelemű részcsoportokat keresünk, amelyek különbözők. Ekkor ugyanis metszetük Lagrange tétele miatt nulla, szorzatuk pedig 25 elemű, tehát az egész csoport. Ezek normálosztók is, mert $G = \mathbb{Z}_5^+ \times \mathbb{Z}_5^+$ Abel. Nyilván A ciklikus, sőt mind a négy nem nulla eleme generálja. A G csoportban minden nem nulla elem ötödrendű, tehát $25 - 1 = 24$ darab ötödrendű elem van. Ezek mindegyike egy ötelemű részcsoportot generál, de minden ilyen részcsoportot mind a négy nem nulla elemével generálhatjuk, és így mindegyiket négyszer számoltuk. Az ötelemű részcsoportok száma tehát $24/4 = 6$. Ezekből két különbözőt $6 \cdot 5 = 30$-féleképpen választhatunk ki (illetve ha az AB és a BA direkt felbontásokat azonosnak tekintjük, akkor 15-féleképpen).

4.8.25. Tekintsük azt a $\psi : A \times B \to (A/C) \times (B/D)$ leképezést, melyre

$$\psi : (a, b) \mapsto (a + C, b + D) .$$

Ez nyilván homomorfizmus, melynek képe az egész $(A/C) \times (B/D)$, magja pedig $A \times C$. Ezért a homomorfizmus-tétel miatt készen vagyunk.

4.8.26. Mivel $(g, h)(x, y) = (x, y)(g, h)$ pontosan akkor, ha $gx = xg$ és $hy = yh$, ezért $(g, h) \in Z(G \times H)$ akkor és csak akkor, ha g minden G-beli x-szel, h pedig minden H-beli y-nal felcserélhető, azaz ha $(g, h) \in Z(G) \times Z(H)$.

A kommutátor-részcsoportra vonatkozó állítás bizonyításához vegyük észre, hogy ha $x, y \in G$, akkor $[(x, 1), (y, 1)] = ([x, y], 1)$, és ezért $G' \times \{1\} \subseteq (G \times H)'$. Ugyanígy $\{1\} \times H' \subseteq (G \times H)'$, és így e két normálosztó szorzata, vagyis $G' \times H' \subseteq (G \times H)'$. A fordított irányú tartalmazás a

$$[(g, h), (x, y)] = (gxg^{-1}x^{-1}, hyh^{-1}y^{-1}) = ([g, x], [h, y])$$

összefüggésből következik, hiszen eszerint a $G' \times H'$ részcsoport tartalmazza $(G \times H)'$ generátorelemeit.

Megjegyezzük, hogy a bizonyítás második felét kommutátorelemekre való hivatkozás nélkül is elmondhatjuk. Ugyanis $(G \times H)/(G' \times H') \cong (G/G') \times (H/H')$ az előző gyakorlat miatt. A $G' \times H'$ normálosztó szerinti faktor tehát $(G/G') \times (H/H')$, azaz Abel-csoport, és így $G' \times H'$ tartalmazza $G \times H$ kommutátor-részcsoportját.

4.8.27. Mivel $(45)(34)(45)^{-1} = (35) \notin G$, ezért G nem normálosztó. Álljon A azokból a G-beli permutációkból, amelyek az 5, 6, 7, 8 mindegyikét fixálják, B pedig azokból, amelyek az 1, 2, 3, 4 mindegyikét fixálják. Ekkor G az A és B normálosztóinak direkt szorzata, melyek nyilván S_4-gyel izomorfak.

4.8.28. A kocka bármelyik szimmetriája az Útmutatóban leírt két szabályos tetraéder mindegyikét vagy önmagába, vagy a másik ilyen tetraéderbe viszi. Tekintsük a kocka G szimmetriacsoportjának a hatását ezen a két tetraéderből álló halmazon. Ez tranzitív hatás, hiszen a középpontos tükrözés az egyik tetraédert a másikba viszi. Így az első tetraéder N stabilizátora egy kettő indexű részcsoport (és így normálosztó) G-ben. A 4.6.7. Állítás miatt G rendje 48, tehát N elemszáma 24. Ez a 24-elemű részcsoport egy szabályos tetraéder csúcsait permutálja. Más permutációnak más szimmetria felel meg, hiszen ha egy szimmetria a tetraéder minden csúcsát fixálja, akkor a kockán is az identitás. Mivel $4! = 24$, a tetraéder négy csúcsának összes permutációját megkapjuk. Az N tehát S_4-gyel izomorf (és megmutattuk azt is, hogy a tetraéder csúcsainak minden permutációját megvalósítja a kocka valamelyik egybevágósága). Legyen K az identitásból és a középpontos tükrözésből álló részcsoport. Mivel a középpontos tükrözés G minden elemével felcserélhető, K normálosztó, és így $G \cong N \times K$.

4.8.29. Az Útmutatóban megadott szorzásra nem teljesülnek a vektortér-axiómák, hiszen $(1 +_2 1) * 1 = 0 * 1 = 0$, ugyanakkor $1 * 1 + 1 * 1 = 1 + 1 = 2$, és így $\mathbb{Z}_4^+$ nem válik vektortérré $\mathbb{Z}_2$ fölött. A problémát az okozza, hogy $2a = 0$ nem teljesül minden $a \in \mathbb{Z}_4^+$-re.

Tegyük most fel, hogy $pa = 0$ minden $a \in A$ esetén. Ha $\lambda \in \mathbb{Z}_p$, akkor ez egész szám, és így értelmes a $\lambda a \in A$ elem, ez a-nak többszöröse. A hatványozás azonosságai (lásd 2.2.18. Gyakorlat) miatt teljesülnek az alábbiak tetszőleges $\lambda, \mu \in \mathbb{Z}_p$ és $a, b \in A$ esetén:

$$(\lambda + \mu)a = \lambda a + \mu a\,, \quad \lambda(a + b) = \lambda a + \lambda b\,, \quad (\lambda\mu)a = \lambda(\mu a)\,, \quad 1a = a\,.$$

Ezek azonban nem a $\mathbb{Z}_p$ fölötti vektortér-axiómák! Azokban ugyanis a λ és μ skalárok között nem az egész számok összeadását és szorzását, hanem a $\mathbb{Z}_p$ műveleteit, tehát a mod p összeadást és szorzást kell alkalmazni. Ha be akarjuk bizonyítani a

$$(\lambda +_p \mu)a = \lambda a + \mu a \quad \text{és} \quad (\lambda *_p \mu)a = \lambda(\mu a)$$

vektortér-axiómákat is, akkor fel kell használnunk, hogy A minden elemének p-szerese nulla. Ugyanis $(\lambda + \mu) - (\lambda +_p \mu)$ és $(\lambda\mu) - (\lambda *_p \mu)$ is p-vel osztható számok, ezekkel az a elemet szorozva nullát kapunk, és *ezért* következnek a hatványozás fenti azonosságaiból a $\mathbb{Z}_p$ fölötti vektortér-axiómák.

Az Olvasó figyelmét fölhívjuk arra, hogy a mostani feladat állítását a 7.3.15. Feladatban általánosítjuk, Abel-csoportok helyett modulusokra.

4.8.30. A $\mathbb{Z}_p^n$ vektortér invertálható lineáris leképezéseinek csoportja $\mathrm{GL}(n, \mathbb{Z}_p)$-vel izomorf. Belátjuk, hogy ezek ugyanazok, mint a $(\mathbb{Z}_p^+)^n$ direkt hatvány összegtartó invertálható leképezései, vagyis hogy minden összegtartó α leképezés skalárszoros-tartó is. Ez általános vektortérben nem igaz, $\mathbb{Z}_p$ fölött azonban igen, mert itt minden λ skalár az 1 néhány példányban vett összege. Így ha α összegtartó, akkor $\alpha(\lambda g) = \lambda\big(\alpha(g)\big)$, hiszen minden homomorfizmus tartja a hatványozást (4.3.11. Gyakorlat).

4.8.31. Állítsuk elő az A csoportot prímhatványrendű ciklikus csoportok direkt szorzataként. Jelölje e az A exponensét, ez a szereplő tényezők exponenseinek, azaz rendjeinek legkisebb közös többszöröse. Egy p prím néhány hatványának legkisebb közös többszöröse ezek közül a legnagyobb. Ezért ha $e = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, akkor a tényezők között van legalább egy $p_i^{\alpha_i}$ rendű A_i ciklikus csoport mindegyik i-re. Válasszunk ki egy-egy ilyet, ezeknek a tényezőknek a direkt szorzata ciklikus (a 4.8.8. Következmény miatt), és rendje e. Ezért van A-ban olyan elem, amelynek a rendje e. Ha tehát A rendje ugyanaz, mint az exponense, akkor A ciklikus. Megfordítva, egy véges ciklikus csoport exponense nyilván megegyezik a rendjével.

Tegyük fel, hogy G véges részcsoportja a T test multiplikatív csoportjának, és legyen G exponense e. Lagrange tétele miatt e osztója G rendjének, és az $x^e - 1$ polinomnak G minden eleme gyöke. Ennek a polinomnak legfeljebb annyi gyöke lehet, mint a foka (a 2.4.7. Tétel miatt), ezért G rendje legfeljebb e. Így G rendje ugyanaz, mint az exponense, és ezért ciklikus.

4.8.32.

(1) Ez a D_n diédercsoport lesz, az N-ben a forgatások vannak.

(2) Ez egy 21 elemű nemkommutatív csoport. Meg kell mutatni, hogy *létezik* olyan $\psi : \mathbb{Z}_3^+ \to \mathrm{Aut}(\mathbb{Z}_7^+)$ homomorfizmus, melyre $\big(\psi(1)\big)(x) = 2x$ minden $x \in \mathbb{Z}_7^+$ esetén. A $\mathbb{Z}_7^+$ csoport automorfizmus-csoportja a 4.7.43. Feladat szerint izomorf $\mathbb{Z}_7^\times$-tel, ez pedig a 4.3.16. Tétel szerint a hatodrendű ciklikus csoporttal izomorf. Ebben a csoportban az $\alpha : x \mapsto 2x$ leképezés (illetve a neki megfelelő $2 \in \mathbb{Z}_7^\times$) harmadrendű lesz (ezt is kiszámoltuk már a 4.3.22. Gyakorlatban). Ezért az α által generált ciklikus csoport izomorf $\mathbb{Z}_3^+$-szal, és így a tényleg létezik olyan ψ homomorfizmus, melyre $\psi(1) = \alpha$.

(3) Ez a D_4, ahol $N = \{1, T, F^2, TF^2\}$, $a = T$, $b = TF^2$, $H = \{1, TF\}$.

(4) Ez az A_4 alternáló csoport, N a Klein-féle négyelemű normálosztó, $H = \langle(123)\rangle$.

(5) Ez az S_4 szimmetrikus csoport, N a Klein-féle négyelemű normálosztó, H a 4 pont stabilizátora.

(6) Ez egy 12 elemű nemkommutatív csoport, amelynek van negyedrendű eleme, és ezért nem A_4, és nem $D_6 \cong D_3 \times \mathbb{Z}_2^+$ (amiknek nincs negyedrendű eleme). Most is meg kell gondolni, hogy az invertálás (azaz ellentettképzés) másodrendű automorfizmusa a $\mathbb{Z}_3^+$ csoportnak, és ezért van olyan ψ homomorfizmus, amely az $1 \in \mathbb{Z}_4^+$ elemhez ezt rendeli hozzá.

4.8.33. Legyen az a elem rendje p^n, és M maximális azon részcsoportok között, amelyekre $M \cap \langle a \rangle = \{0\}$ teljesül. Megmutatjuk, hogy $\langle a \rangle + M = A$. Kényelmesebb lesz az M szerinti faktorcsoportban dolgozni, ezért most lefordítjuk a feltételeinket e faktorcsoport nyelvére.

Legyen tehát $B = A/M$ és $b = a + M$. A b elem rendje p^n a 4.5.16. Állítás miatt. Mivel faktorizálásnál az elemrend nem nőhet, a b maximális rendű a B csoport p-hatványrendű elemei között is. A 4.5.19. Tétel szerint az $\langle a \rangle + M = A$ feltétel azzal ekvivalens, hogy $\langle b \rangle = B$. Végül a B csoportnak nincs olyan nem egyelemű K részcsoportja, melyre $K \cap \langle b \rangle = \{0\}$, mert ennek teljes inverz képe A-ban egy olyan M-et valódi módon tartalmazó részcsoport lenne, amely $\langle a \rangle$-t csak nullában metszi, és ez ellentmondana M maximalitásának.

Mindezzel felvértezve tegyük fel indirekt, hogy $\langle b \rangle \neq B$. Megmutatjuk, hogy B minden elemének a rendje p-hatvány. Valóban, ha $g \in B$, akkor g rendje felírható $p^m t$ alakban, ahol t már nem osztható p-vel. Ekkor a hatvány rendjének képlete miatt $p^m g$ rendje t. De akkor a $\langle b \rangle$ és a $\langle p^m g \rangle$ részcsoportok rendje relatív prím, és így a metszetük rendje (ami mindkét rendnek osztója) csakis 1 lehet. A feltételünk szerint tehát $\langle p^m g \rangle$ maga is az egyelemű részcsoport, vagyis a t rendű $p^m g$ elem a nulla. Ezért $t = 1$, és így g rendje tényleg p-hatvány.

Legyen c egy lehető legkisebb rendű olyan elem B-ben, ami nincsen benne $\langle b \rangle$-ben. Ekkor c rendje p^k alakú, és mivel b rendje maximális volt, $k \leq n$. A pc rendje $p^{k-1} < p^k$, és ezért $o(c)$ minimalitása miatt a pc elem benne van $\langle b \rangle$-ben, vagyis felírható ub alakban, ahol u egész. Innen p^{k-1}-gyel szorozva $0 = p^{k-1}pc = p^{k-1}ub$ adódik. Így b rendje, vagyis p^n osztója $p^{k-1}u$-nak, és mivel $k \leq n$, azt kapjuk, hogy $p \mid u$. Tehát $u = pv$ alkalmas v egészre, és $pc = pvb$.

Átrendezéssel $p(c - vb) = 0$. A $K = \langle c - vb \rangle$ részcsoport rendje tehát vagy 1, vagy p, és így nincs nemtriviális részcsoportja. Ezért $K \cap \langle b \rangle$ vagy szintén triviális, vagy pedig az egész K. Mivel nem egyelemű részcsoport nem metszheti $\{0\}$-ban $\langle b \rangle$-t, ezért vagy $K = \{0\}$, vagy $K \subseteq \langle b \rangle$. Mindkét esetben azt kapjuk, hogy $c - vb \in \langle b \rangle$, de akkor $vb \in \langle b \rangle$ miatt $c \in \langle b \rangle$ is igaz, holott abból indultunk ki, hogy ez nem így van. Ezzel az ellentmondással a bizonyítást befejeztük.

A most bizonyított állításból persze látszik, hogy minden véges Abel-csoport felbomlik prímhatványrendű ciklikus csoportok direkt szorzatára, hiszen sorban leválaszthatunk ilyen direkt tényezőket, amíg el nem fogy a csoport.

4.9. Szabad csoportok és definiáló relációk.

4.9.6. Az Útmutatóban definiált F/N csoport nyilván kommutatív, hiszen N tartalmazza az összes kommutátort, továbbá minden elemének a négyzete az egységelem, hiszen N tartalmazza a w^2 alakú szavakat. Elég megmutatni, hogy X és Y képe is bázis lesz az F/N vektortérben, mert a bázis elemszáma egyértelműen meghatározott. Mindkét kép nyilván generátorrendszer, a függetlenséget kell igazolni.

A $\mathbb{Z}_2$ fölött csak a 0 és az 1 skalárok, tehát egy vektorrendszer akkor lesz lineárisan összefüggő, ha néhány elemének az összege nulla. A faktorcsoportban szorzással jelöljük

a műveletet, és így X függetlenségéhez azt kell megmutatni, hogy bárhogyan szorzunk össze generátorokat, az eredmény soha nem lesz benne az N normálosztóban.

Tegyük fel, hogy $x_1, \ldots, x_k \in X$, és $x_1 \ldots x_k \in N$. Tekintsük azt a $\varphi : X \to \mathbb{Z}_2^+$ leképezést, amely x_1-hez 1-et, az X többi eleméhez nullát rendel. Mivel X szabad generátorrendszer, ez kiterjeszthető egy $\varphi : F \to \mathbb{Z}_2^+$ homomorfizmussá. Ennél a homomorfizmusnál minden $[u, v]$ kommutátor képe a nullelem lesz, hiszen $\mathbb{Z}_2^+$ kommutatív. Ugyanígy minden w^2 szó képe a nullelem lesz, hiszen $\mathbb{Z}_2^+$ minden elemének a kétszerese nulla. Ezért φ magja tartalmazza az N normálosztó generátorelemeit, és így az egész N-et is. Speciálisan $x_1 \ldots x_k \in N$ képe is nulla lesz. Ez azonban ellentmondás, hiszen $\varphi(x_1 x_2 \ldots x_k) = 1 + 0 + \ldots + 0 = 1$. Ez az ellentmondás bizonyítja az állítást.

Azt, hogy X és Y elemszáma megegyezik, arra a lineáris algebrai tételre vezettük vissza, hogy egy vektortér bármely két bázisának ugyanaz az elemszáma (ezt hívjuk a tér dimenziójának). Ez a tétel közismert, ha X és Y egyike véges. Ha mindkettő végtelen, akkor a tétel abban az általánosabb formában igaz, hogy az X és Y halmazok számossága egyenlő. Ennek bizonyításához nem elég önmagában a kicserélési tétel, hanem további megfontolások kellenek. Szerencsére $\mathbb{Z}_2$ fölött (ahol használtuk) az állítás könnyű, mert ha egy végtelen X halmaz bázisa egy $\mathbb{Z}_2$ fölötti vektortérnek, akkor a vektortér elemszáma ugyanaz, mint X elemszáma. Azonban az Olvasó eltűnődhet azon, hogy egy $\mathbb{R}$ feletti végtelen dimenziós vektortérnek miért nem lehet egy megszámlálható és egy ennél nagyobb elemszámú bázisa is egyszerre.

4.9.7. Legyen $F = F(x_1, x_2, \ldots)$ szabad csoport, és $\varphi : F \to F(u, v)$ az a homomorfizmus, amelyre $F(x_i) = u^i v u^{-i}$ minden pozitív i-re. Meg kell mutatnunk, hogy a φ leképezés injektív (mert akkor F izomorf lesz $\mathrm{Im}(\varphi)$-vel, ami $F(u, v)$ egy részcsoportja).

Tegyük fel, hogy egy w egyszerűsíthetetlen szó benne van φ magjában. Ha a w szóban egymás mellett áll x_i^n és x_j^m, akkor az egyszerűsíthetetlenség miatt $i \neq j$ és $n, m \neq 0$. A $\varphi(w)$ megfelelő darabja

$$u^i v^n u^{-i} u^j v^m u^{-j} = u^i v^n u^{j-i} v^m u^{-j}$$

lesz. Hajtsuk végre ezt az egyszerűsítést bármely két szomszédos v-hatvány között. Ekkor további egyszerűsítés már nem lehetséges, mert $i \neq j$ miatt bármely két v-hatvány között megmarad egy u-hatvány, és $n, m \neq 0$ miatt bármely két u-hatvány között megmarad egy v-hatvány. Így ha az eredeti w szó nem volt üres, akkor $\varphi(w)$ sem az.

4.9.11. Az $ft = tf^k$ összefüggés lehetővé teszi, hogy a t betűket a szavak elejére (vagy a végére) vigyük. A későbbiek megértéséhez azonban hasznosabb egy kicsit másképp nézni erre a csoportra. Legyen N az f által generált részcsoport. Az $ft = tf^k$ összefüggést átalakítva $t^{-1} f t = f^k$, vagyis t^{-1} az f elemet a k-adik hatványába konjugálja. Mivel a konjugálás automorfizmus, a t^{-1} az f minden hatványát is a k-adik hatványába konjugálja, ami N-beli. Ezért az N normalizátorában benne van a t^{-1} (és így t is), de benne van az $f \in N$ is. Az f és t generálja G-t, tehát $N_G(N) = G$, azaz N normálosztó G-ben. A G/N faktorcsoportot generálják f és t mellékosztályai (a 4.5.27. Gyakorlat miatt), de fN az egységelem, vagyis a G/N faktorcsoportot tN is generálja. Az $f^n = 1 = t^m$ összefüggések miatt N elemszáma legfeljebb n, a G/N ciklikus csoport elemszáma pedig

legfeljebb m. Ezért G rendje legfeljebb nm (sőt, ennek osztója). Ha $H = \langle t \rangle$, akkor $NH = HN = G$, hiszen NH és HN is az f és t elemeket tartalmazó részcsoport. Ezért G minden eleme $t^i f^j$ és $f^k t^\ell$ alakban is felírható.

4.9.18. A 4.3.33. Feladat miatt $B(k, 2)$ kommutatív csoport. Ha a generátorait $g_1, \ldots, g_k$ jelöli, akkor ezeknek az elemeknek a kétszerese nulla, és így minden $m_1 g_1 + \ldots + m_k g_k$ alakú kombinációban feltehető, hogy mindegyik m_i értéke 0 vagy 1. Tehát mindegyik m_i számot kétféleképpen választhatjuk, és így ilyen összeget legfeljebb 2^k darabot lehet felírni. Ezért $|B(k, 2)| \leq 2^k$. Ugyanakkor $(\mathbb{Z}_2^+)^k$ elemszáma 2^k, minden elemének a kétszerese nulla, és k elemmel generálható (azokkal, amelyek egyetlen koordinátája 1, a többi nulla). Így $(\mathbb{Z}_2^+)^k$ homomorf képe $B(k, 2)$-nek, és mivel $|B(k, 2)| \leq 2^k$, ez a homomorfizmus izomorfizmus lesz.

4.9.19. Legyen G olyan csoport, amelyben minden elem köbe 1. Tetszőleges $s, t \in G$ esetén $(st^2)^3 = 1$, ezt jobbról ts^2t-vel beszorozva $(st)(ts) = (ts)(st)$ adódik. Speciálisan ha $s = h^{-1}$ és $t = hg$, akkor $st = g$ és $ts = hgh^{-1}$. Ezért g minden konjugáltjával felcserélhető.

Ez azt jelenti, hogy a g elem által generált N normálosztó kommutatív. Valóban, (a 4.7.22. Gyakorlat miatt) a g elem által generált normálosztó a g konjugáltjai által generált részcsoport, és mivel ezek páronként felcserélhetők, (a 4.7.42. Gyakorlat szerint) N Abel-csoport.

Belátjuk, hogy $B(3, k)$ véges, k szerinti indukcióval. Ez nyilvánvaló $k = 0$ esetén, mert akkor az egyelemű csoportot kapjuk. Ha már beláttuk, hogy $B(k-1, 3)$ véges, és elemszáma legfeljebb n, akkor legyenek $g_1, \ldots, g_k$ a $B(k, 3)$ csoport generátorai, $g = g_1$, és N a g által generált normálosztó. A $B(k, 3)/N$ faktorcsoportban generátorrendszert alkotnak a $g_1, \ldots, g_k$ elemek mellékosztályai (4.5.27. Gyakorlat), de a g_1 mellékosztálya az egységelem, ezért már a $g_2N, \ldots, g_kN$ elemek is generátorrendszert alkotnak. A $B(k, 3)/N$-ben is igaz, hogy minden elem köbe az egységelem, hiszen ez $B(k, 3)$-ban teljesül. Ezért $B(k, 3)/N$ homomorf képe $B(k-1, 3)$-nak, vagyis elemszáma legfeljebb n. Így $B(k, 3)$ elemszáma legfeljebb $n|N|$.

Az N része g centralizátorának, hiszen kommutatív. Ezért g centralizátorának indexe legfeljebb akkora lehet, mint N indexe, amiről már láttuk, hogy legfeljebb n. Ezért a g elemnek legfeljebb n darab konjugáltja lehet. Az N részcsoportot ezek a konjugáltak generálják. Mivel ez Abel-féle, és minden elemének a köbe az egységelem, az összes eleme egy n tagú lineáris kombináció, ahol az együtthatók a 0, 1, 2 számok. Így N elemszáma legfeljebb 3^n, és ezért $B(k, 3)$ rendje legfeljebb $n3^n$, vagyis véges. Ezzel az állítást beláttuk. Finomabb számolással az is kihozható lenne, hogy

$$|B(k, 3)| = 3^{k+\binom{k}{2}+\binom{k}{3}}.$$

4.9.20. Az alábbiak minden pontjában D a feladatbeli megfelelő, definiáló relációkkal megadott csoportot jelöli.

(1) $\langle a \mid a^2 = 1\rangle \cong \mathbb{Z}_2^+$. Valóban, minden szóból kihúzhatunk páros sok a betűt (és az inverzekkel sem kell törődni, mert $a^{-1} = a$), tehát két szó marad: a és 1 (az üres szó). Annak igazolásához, hogy ezek nem alakíthatók egymásba, megmutatjuk, hogy a $\mathbb{Z}_2^+$ csoportban az $a = 1$ elem teljesíti a definiáló relációkat. Valóban, a generálja a $\mathbb{Z}_2^+$ csoportot, és $1 +_2 1 = 0$ is igaz.

(2) $\langle a \mid a^3 = 1\rangle \cong \mathbb{Z}_3^+$.

(3) $\langle a \mid a^5 = 1,\ a^7 = 1\rangle$ az egyelemű csoport, mert $a^7 = 1 = a^5$-ből $a^2 = 1$, és innen $1 = a^5 = a^2a^2a = a$ következik.

(4) $\langle a, b \mid a^2 = 1,\ b^2 = 1,\ ab = ba\rangle$ a Klein-csoport. A lehetséges szavak a, b, ab és 1, ezért D elemszáma legfeljebb 4. A Klein-csoportban ezek a relációk teljesülnek, az a és b bármely két egymástól és az egységelemtől különböző elem lehet. Így a Klein-csoport homomorf képe D-nek, és mivel D elemszáma legfeljebb 4, ez izomorfizmus.

(5) $\langle a, b \mid a^2 = 1,\ b^3 = 1,\ ab = ba\rangle \cong \mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+$. Valóban, a szavak most $1, a, b, ab, b^2, ab^2$, és az $a = (1, 0)$, $b = (0, 1) \in \mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ generátorok kielégítik a relációkat.

(6) $\langle a, b \mid a^2 = 1,\ b^7 = 1,\ aba^{-1} = b^{-1}\rangle \cong D_7$ (4.9.10. Állítás).

(7) $\langle a, b \mid a^2 = 1,\ b^7 = 1,\ aba^{-1} = b^2\rangle \cong \mathbb{Z}_2^+$, mert a relációkból levezethetjük, hogy $b = 1$. Valóban, az a elemmel való konjugálás a $\langle b\rangle$ részcsoporton a négyzetre emelés. Ezért az a^2-tel való konjugálás ennek négyzete, vagyis a negyedik hatványra emelés. Ugyanakkor $a^2 = 1$, tehát a vele való konjugálás az identitás, ami azt jelenti, hogy $b^4 = b$. Ezt $b^7 = 1$-gyel összevetve $b = 1$ adódik.

(8) $\langle a, b \mid a^3 = 1,\ b^7 = 1,\ aba^{-1} = b^2\rangle$ egy 21 elemű nemkommutatív csoport, amely a 4.8.32. Gyakorlat (2) pontjában megadott G csoporttal izomorf. Valóban, a 4.9.11. Gyakorlat szerint D elemszáma legfeljebb 21. A G csoportban van egy $\mathbb{Z}_7^+$-szal izomorf N normálosztó, és egy $\mathbb{Z}_3^+$-szal izomorf H részcsoport, amelynek egy alkalmas b eleme az N elemeit a négyzetükbe konjugálja. Így ez a b, és tetszőleges $1 \neq a \in N$ kielégíti a megadott definiáló relációkat.

(9) $\langle a, b \mid a^6 = 1,\ b^2 = a^3,\ bab^{-1} = a^{-1}\rangle$ egy 12 elemű nemkommutatív csoport, amely a 4.8.32. Gyakorlat (6) pontjában megadott G csoporttal izomorf. Valóban, a 4.9.11. Gyakorlat szerint D elemei a^ib^j alakban írhatók. Mivel b^2 helyettesíthető a^3-nel, feltehető, hogy $0 \leq i < 2$ és $0 \leq j < 5$. Ezért D elemszáma legfeljebb 12. Jelölje a G csoportban az N normálosztó elemeit $\{1, c, c^2\}$, a H részcsoport elemeit pedig $\{1, d, d^2, d^3\}$, tudjuk, hogy $dcd^{-1} = c^{-1}$. Könnyű kiszámolni, hogy az $a = cd^2$ és $b = d$ generátorelemek kielégítik a relációkat. (Használjuk fel, hogy d^2 a csoport centrumában van.)

(10) $\langle a, b \mid a^2 = 1,\ b^2 = 1,\ (ab)^3 = 1\rangle \cong D_3$. Legyen $f = ab$ és $t = a$. Ekkor t és f kielégíti D_3 definiáló relációit, hiszen $tft^{-1} = a(ab)a = ba = f^{-1}$. Tehát az

f és t által generált részcsoport homomorf képe D_3-nak. Ez a részcsoport az egész D, mert f és t segítségével a és b is kifejezhető, és így D maga is homomorf képe D_3-nak. Másfelől viszont D_3 két tükrözése nyilván kielégíti a fenti relációkat, és ezért D-nek is homomorf képe D_3.

(11) $\langle a, b \mid a^2 = 1,\ b^2 = 1,\ (ab)^n = 1\rangle \cong D_n$, ugyanúgy, mint az előző pontban. Érdemes megjegyezni, hogy ezek szerint egy véges csoportban két másodrendű elem mindig diédercsoportot generál (kivéve ha a szorzatuk rendje 1 illetve 2, amikor a $\mathbb{Z}_2^+$, illetve Klein-csoportot kapjuk).

(12) $\langle a, b \mid a^3 = b^2 = (ab)^3 = 1\rangle \cong A_4$. Legyen $c = aba^{-1}$ és $d = a^{-1}ba$. Ezek négyzete 1, és $cd = ababa = b$. Ezért $(cd)^2 = 1$, ahonnan $cd = dc$. Az a elem körbekonjugálja c, d, b-t, és ezért $\{1, c, d, b\}$ normálosztó D-ben, a szerinte vett faktort a generálja. Így $|D| \leq 4 \cdot 3 = 12$. Másrészt az A_4 csoport $a = (123)$, $b = (12)(34)$ generátorelemei nyilván teljesítik a relációkat.

(13) $\langle a, b \mid a^3 = b^2 = (ab)^4 = 1\rangle \cong S_4$. Legyen $v = (ab)^2$, ekkor $v^2 = 1$. Ha $u = a^2$, akkor persze $u^3 = 1$. Továbbá $(uv)^3 = (bab)^3 = 1$. Ezért u és v kielégíti az előző pontbeli definiáló relációkat, és így $N = \langle u, v\rangle$ elemszáma legfeljebb 12. Belátjuk, hogy N normálosztó. Persze $a = u^2 \in N$, tehát elég megmutatni, hogy N zárt a b-vel való konjugálásra. De $bub = (bab)^2$, viszont $bab = a^{-1}v \in N$. Így $bvb = (bab)a \in N$ is igaz. Az N indexe legfeljebb 2, hiszen a szerinte vett faktort b generálja. Ezért $|D| \leq 24$. Másrészt az S_4 csoport $a = (123)$ és $b = (14)$ generátorelemei kielégítik a relációkat.

(14) $\langle a, b, c \mid a^2 = b^2 = c^3 = 1,\ ab = ba,\ cac^{-1} = b\rangle \cong A_4 \times \mathbb{Z}_2^+$. Legyen N az a részcsoport, amit a, b és d generál, ahol $d = cbc^{-1}$. Belátjuk, hogy$N$ legfeljebb nyolcelemű kommutatív normálosztó. Valóban, c körbekonjugálja az a, b, d elemeket, hiszen $cdc^{-1} = c(cbc^{-1})c^{-1} = c(c(cac^{-1})c^{-1})c^{-1} = c^3ac^{-3} = 1a1 = a$. Nyilván $d^2 = 1$, továbbá az $ab = ba$ összefüggést c-vel konjugálva $bd = db$, még egyszer konjugálva $da = ad$ adódik. Tehát N-et három, páronként felcserélhető elem generálja, melyek legfeljebb másodrendűek, ezért N kommutatív (4.7.42. Gyakorlat), és legfeljebb $2^3 = 8$ elemű. Továbbá $a, b \in N$, és $c \in N_G(N)$, hiszen N zárt a c-vel való konjugálásra. Így N normálosztó, és a rá vett faktort c képe generálja, azaz legfeljebb 3 elemű. Így $|D| \leq 8 \cdot 3 = 24$. Másrészt az $A_4 \times \mathbb{Z}_2^+$ csoportban $a = ((12)(34), 1)$, $b = ((14)(23), 1)$, $c = ((123), 0)$ teljesíti a relációkat. Még azt kell belátni, hogy ez a három elem generálja $A_4 \times \mathbb{Z}_2^+$-t. Ez abból látszik, hogy $ab = ((13)(24), 0)$ és c generálja $A_4 \times \{0\}$-t.

4.9.21. Meg kell mutatni, hogy az Útmutatóban definiált $\psi : F \to G$ homomorfizmusra $\varphi = \alpha \circ \psi$. Ezt elegendő az X generátorrendszeren ellenőrizni (4.4.28. Gyakorlat). De ha $x \in X$, akkor $\alpha\big(\psi(x)\big) = \varphi(x)$, hiszen pontosan így választottuk a $\psi(x)$ ősképet.

4.9.22. Elsőnek vegyük észre, hogy a „nullösszegű" tulajdonság nem változik meg, ha egy szón elemi átalakítást végzünk: akár betoldunk, akár kihúzunk xx^{-1}-et, a kitevők összege egyik változóban sem változik meg. Ezért az alábbiakban nem kell ragaszkodnunk ahhoz, hogy a szavakat egyszerűsíthetetlen alakjukban írjuk fel.

Az $[u, v] = uvu^{-1}v^{-1}$ kommutátor biztosan nullösszegű szó, hiszen az u-beli bármely változóhoz tartozó kitevő-összeget kioltja a u^{-1}-beli kitevő-összeg, és ugyanez igaz v-re is. Mivel nullösszegű szavak szorzata és inverze is nyilván nullösszegű, ezért F kommutátorrészcsoportja csupa nullösszegű szavakból áll.

A megfordításhoz minden nullösszegű szót elő kell állítanunk kommutátorok szorzataként. Ezt a szó hosszára vonatkozó indukcióval tesszük. Legyen w nullösszegű szó, melynek első betűje x (ami vagy generátor, vagy annak inverze). Ekkor a szóban biztosan szerepel x^{-1} is, hiszen nullaösszegű. Vagyis $w = xux^{-1}v$ alkalmas u és v szavakra. Mivel w nullaösszegű, uv is az, de rövidebb w-nél, és így az indukciós feltevés miatt uv benne van F'-ben. De akkor

$$w = xux^{-1}v = xux^{-1}u^{-1}uv = [x, u](uv) \in F' ,$$

hiszen minden kommutátor F'-ben van, és F' részcsoport.

4.10. Prímhatványrendű csoportok, Sylow tételei.

4.10.4. Legyen $gZ(G)$ a $G/Z(G)$ generátoreleme. Ekkor a $g^nZ(G)$ halmazok kiadják a G csoport összes elemét (n egész). De ezek elemei felcserélhetők, hiszen ha $a, b \in Z(G)$, akkor $(g^na)(g^mb) = (g^mb)(g^na)$. Így G kommutatív.

4.10.7. Tegyük fel, hogy $H \leq G$ indexe a p prím. Legyen $H \leq K \leq G$. A 4.4.40. Gyakorlat miatt $p = |G : H| = |G : K| \cdot |K : H|$. Ezért vagy $|G : K| = 1$, és ekkor $K = G$, vagy $|K : H| = 1$, és akkor $K = H$.

4.10.10. Az $\mathrm{U}(3, \mathbb{Z}_p)$ csoport elemei $E + N$ alakúak, ahol E a (háromszor hármas) egységmátrix, N pedig szigorú felső háromszögmátrix (vagyis a főátlóban és az alatt is nulla áll). Mátrix-szorzással könnyű ellenőrizni, hogy $N^3 = 0$ (és így $p > 2$ miatt $N^p = 0$). Az E és az N felcserélhetők, hiszen $EN = NE = N$. Így alkalmazható a binomiális tétel az $(E + N)^p$ kiszámítására. A mátrixok elemei $\mathbb{Z}_p$-beliek, azaz p-szeresük nulla. Így (a 3.3.18. Feladatban látottak miatt) tagonként lehet p-edik hatványra emelni. Ekkor pedig $(E + N)^p = E^p + N^p = E$. Vagyis $\mathrm{U}(3, p)$ minden egységtől különböző eleme p rendű.

Szintén mátrix-szorzással igazolható, hogy $\mathrm{U}(3, p)$ nem kommutatív, sőt, hogy a centruma azokból a mátrixokból áll, melyekben a jobb felső sarokban tetszőleges elem állhat, a főátlóban 1-esek, másutt pedig nulla.

Az $\mathrm{U}(3, p)$ csoport két elemmel generálható, bármely két olyan eleme generálja, amelyek nem felcserélhetők. Ha ugyanis két ilyen elem valódi részcsoportot generálna, akkor annak rendje legfeljebb p^2 lehetne, és így kommutatív lenne.

Tegyük fel, hogy $p = 2$. Négyzetre emeléssel meggyőződhetünk róla, hogy a csoportban csak két negyedrendű elem van, és így a D_4 diédercsoportot kapjuk.

4.10.11. A 4.7.43. Feladat szerint $\mathbb{Z}^+_{p^2}$ automorfizmus-csoportja $\mathbb{Z}^\times_{p^2}$, és az $\alpha : x \mapsto (p+1)x$ automorfizmusnak a $p+1$ elem felel meg. A binomiális tétel szerint

$$(p+1)^p = 1 + p\binom{p}{1} + \binom{p}{2}p^2 + \dots .$$

Itt az első kivételével minden tag osztható p^2-tel, és ezért $p+1$-nek a p-edik hatványa 1 lesz modulo p^2. Ugyanakkor $p+1$ nem kongruens 1-gyel modulo p^2, és így rendje p. Vagyis α rendje is p. Ez azt jelenti, hogy létezik olyan $\psi : \mathbb{Z}^+_p \to \mathrm{Aut}(\mathbb{Z}^+_{p^2})$ homomorfizmus, melyre $\psi(1) = \alpha$. Az ehhez tartozó $\mathbb{Z}^+_{p^2} \rtimes \mathbb{Z}^+_p$ szemidirekt szorzat tehát egy nem kommutatív, p^3 rendű csoport, amelyben van egy p^2 rendű a elem és egy p rendű b elem úgy, hogy $bab^{-1} = \alpha(a) = a^{p+1}$. Így ez a csoport kielégíti a feladatban megadott definiáló relációkat. Ugyanakkor a 4.9.11. Gyakorlat miatt ennek a definiáló relációkkal megadott csoportnak a rendje legfeljebb p^3, tehát a most konstruált szemidirekt szorzattal izomorf.

4.10.19. Az N a P konjugált osztályainak egyesítése, amelyek elemszáma osztója P rendjének, azaz p-hatvány, és így vagy 1, vagy p-vel osztható. Az N-ben benne van az egységelem, ez egyelemű osztály. Az N rendje osztója P rendjének, ezért p-hatvány, és mivel $|N| > 1$, osztható p-vel. De akkor kell lennie még N-ben egyelemű konjugált osztálynak. Ez része P centrumának.

4.10.20. Mivel $H < P$, választhatunk olyan $H < K$ részcsoportot, amely tartalmazásra minimális. Ekkor H maximális részcsoportja K-nak, és így a 4.10.8. Tétel miatt $H \lhd K$.

4.10.21. Az első izomorfizmus-tétel miatt $(PN)/N \cong P/(P \cap N)$, így $(PN)/N$ egy olyan p-csoport, amely részcsoportja G/N-nek, és $|PN| = |P||N|/|P \cap N|$. A $(PN)/N$ indexe viszont nem osztható p-vel, mert

$$|G/N : (PN)/N| = \frac{|G|}{|PN|} = \frac{|G||P \cap N|}{|P||N|} = \frac{|G : P|}{|N : (N \cap P)|},$$

és ez osztója $|G : P|$-nek. Tehát $(PN)/N$ tényleg p-Sylow G/N-ben. Ez az átalakítás azt is mutatja, hogy $|N : (N \cap P)|$ sem osztható p-vel. Mivel $N \cap P$ viszont p-csoport, ez N-nek egy p-Sylowja.

4.10.22. Egy p^3 rendű G csoport minden valódi részcsoportja legfeljebb p^2 rendű, és így kommutatív (4.10.3. Tétel). Ha $G \cong A \times B$ nemtriviális direkt felbontás lenne, akkor tehát A és B is kommutatív, de akkor G is kommutatív lenne.

4.10.23. Tekintsük azt a ψ leképezést, amely egy felső háromszögmátrixhoz a főátlójában álló elem-n-est rendeli. Ez szorzattartó, hiszen könnyű ellenőrizni, hogy két felső háromszögmátrix szorzásakor a főátló megfelelő elemei szorzódnak össze. A képe a $T^\times$ csoport n-edik direkt hatványa, a magja pedig $\mathrm{U}(n, T)$. A homomorfizmus-tétel tehát pont az állítást adja.

4.10.24. Ezek a prímhatványrendű ciklikus csoportok. Tegyük fel, hogy a G véges csoportnak M az egyetlen maximális részcsoportja. Legyen $g \in G - M$, ekkor a $\langle g \rangle$ részcsoport csak G lehet, mert ha valódi részcsoport lenne, akkor része lenne G egy maximális részcsoportjának, ami nem lehet M. Tehát G ciklikus. Tudjuk, hogy egy ciklikus csoport részcsoportjai a rendje pozitív osztóinak felelnek meg kölcsönösen egyértelműen. Így $|G|$ minden p prímosztójához van p indexű részcsoport, ami persze maximális. Ezért G rendjének csak egy prímosztója lehet.

4.10.25. A D_4 diédercsoporttal. Valóban, $|S_4| = 2^3 \cdot 3$, tehát minden 2-Sylow részcsoport 8-elemű, és megfordítva, minden 8-elemű részcsoport 2-Sylow. A Sylow-tétel miatt ezek konjugáltak, tehát izomorfak is, vagyis elég egy 8-elemű részcsoportot találni. A D_4 csoport azonban izomorf S_4 egy részcsoportjával, hiszen egy négyzet csúcsainak permutációiból áll (és a csúcsok permutációja meghatározza az egybevágósági transzformációt).

4.10.26. Mindegyik p-Sylow részcsoport rendje p, és így Lagrange tétele miatt bármely kettő metszete csak az egységelem. Mindegyikben $p-1$ darab p rendű elem van, és minden p rendű elem benne van egy p-Sylow részcsoportban.

4.10.27. Ha egy p-Sylow részcsoport normálosztó, akkor minden konjugáltja önmaga. A Sylow-tétel miatt a többi p-Sylow ennek konjugáltja, és így egyetlen p-Sylow részcsoport van. De egy p-Sylow részcsoportot minden automorfizmus p-Sylow részcsoportba visz, hiszen automorfizmusnál a rend megőrződik. Ha csak egy p-Sylow részcsoport van, akkor tehát ez minden automorfizmusnál saját magába megy, és így karakterisztikus.

4.10.28. Az S_3 csoportnak az összes részcsoportját leírtuk a 4.4.33. Gyakorlatban. Eszerint három 2-Sylow és egy 3-Sylow részcsoport van.

Az S_4 csoport rendje $2^3 \cdot 3$. Nyolc hármasciklus van benne, tehát a 3-Sylowok száma a 4.10.26. Gyakorlat miatt $8/2 = 4$. A kimaradó 15 elem (a ciklusfelbontásból láthatóan) másod- és negyedrendű, tehát a 2-Sylowok unióját alkotja (hiszen minden 2-hatvány rendű elem benne van egy 2-Sylow részcsoportban). Ezért több, mint egy 2-Sylow van. Másrészt a 2-Sylowok száma egy 2-Sylow normalizátorának az indexe, azaz $24/8 = 3$-nak osztója. Tehát csak 3 darab 2-Sylow lehet. (Könnyű belátni, hogy ezek páronként ugyanabban a 4-elemű Klein-féle normálosztóban metszik egymást.)

Az A_5 csoportnak a 4.7.36. Gyakorlatban már feltérképeztük az elemeit. Az ötösciklusok száma 24, tehát az 5-Sylowok száma $24/(5-1) = 6$. A hármasciklusok száma 20, tehát a 3-Sylowoké $20/(3-1) = 10$. A fennmaradó 15 elem két-két transzpozíció szorzata. Ezek öt 2-Sylowot alkotnak, amelyek páronként csak $\{1\}$-ben metszik egymást. Ugyanis jelölje H valamelyik (mondjuk az 5) pont stabilizátorát. Ebben azok a páros permutációk vannak, amelyek 5-öt fixen hagyják, vagyis ez az A_4 csoport, aminek csak három másodrendű eleme van, és így egyetlen 2-Sylow fér el benne, a már ismert Klein-féle K normálosztó. A K egy 2-Sylow A_5-ben is, és a normalizátora tartalmazza H-t, aminek indexe 5. Tehát legfeljebb 5 darab 2-Sylow lehet, és ezeket már meg is találtuk: minden pont stabilizátorában egyet.

Könnyen kiszámíthatjuk a Sylowok normalizátorait is. Azt már láttuk, hogy egy 2-Sylow normalizátora A_4-gyel izomorf. Az 5-Sylowok normalizátorai $60/6 = 10$-eleműek, és D_5-tel izomorfak, hiszen az ötszög csúcsain való hatás alapján D_5 részcsoportja A_5-nek, és ebben az 5-Sylow normálosztó. A 3-Sylowok normalizátora S_3-mal izomorf.

A D_n diédercsoportban a forgatásokból álló normálosztó minden részcsoportja is normálosztó (hiszen minden forgatás csak az inverzével konjugált, lásd 4.7.36. Gyakorlat). Ezért $p > 2$ esetén csak egy p-Sylow van. Valóban, a forgatások részcsoportjában lehet megfelelő rendű részcsoportot találni, hiszen ez ciklikus, és az indexe 2. Így van olyan p-Sylow, ami normálosztó, de akkor minden konjugáltja önmaga, és a Sylow-tétel miatt ez az egyetlen p-Sylow részcsoport.

Legyen $n = 2^k m$, ahol m páratlan. Belátjuk, hogy a 2-Sylowok száma m. Jelölje K a forgatások normálosztójának egyetlen 2^k rendű részcsoportját. Ez minden 2-hatvány rendű forgatást tartalmaz, hiszen a forgatások csoportja ciklikus. Legyen P egy K-t tartalmazó 2-Sylow részcsoport. Mivel K normálosztó az egész csoportban, minden konjugáltja önmaga. Ezért K benne van P minden konjugáltjában is, vagyis mindegyik 2-Sylow részcsoportban. A P rendje 2^{k+1}, és mivel minden 2-hatvány rendű forgatást már K is tartalmaz, P fennmaradó 2^k elemének tükrözésnek kell lennie. Ez érvényes mindegyik 2-Sylowra. Bármely két 2-Sylow metszete K, hiszen K része mindegyiknek, és mindegyikben maximális részcsoport. Ezért minden tükrözés pontosan egy 2-Sylowban van benne. A tükrözések száma $n = 2^k m$, ezért a 2-Sylowok száma ennek 2^k-adrésze, vagyis m.

4.10.29. Egy $200 = 2^3 \cdot 5^2$ elemű csoportban az 5-Sylowok száma osztója 8-nak, és kongruens eggyel modulo 5, tehát csak egy lehet, vagyis az 5-Sylow normálosztó. Ugyanez a gondolatmenet működik minden $204 = 2^2 \cdot 3 \cdot 17$ elemű csoportban is, ahol a 17-Sylow, és minden $260 = 2^2 \cdot 5 \cdot 13$ rendű csoportban is, ahol a 13-Sylow lesz normálosztó.

Legyen most a G csoport rendje $56 = 2^3 \cdot 7$. A 7-Sylowok száma csak 1 vagy 8 lehet. Ha 1, akkor ez normálosztó. Ha 8, akkor a hetedrendű elemek száma a 4.10.28. Gyakorlat szerint $8(7-1) = 48$, és így csak $56 - 48 = 8$ további elem marad. Ezért csak egyetlen 2-Sylow fér el, és ez akkor normálosztó.

Ha $|G| = 616 = 2^3 \cdot 7 \cdot 11$, akkor a 11-Sylowok száma csak 56 lehet, a 7-Sylowok száma legalább 8, tehát csak egy 2-Sylow fér el.

4.10.30. Tegyük fel, hogy van pqr rendű egyszerű csoport. A prímek átjelölésével elérhető, hogy $p < q < r$ legyen. Ekkor az r-Sylowok száma osztója pq-nak, és kongruens 1-gyel mod r. Így sem p, sem q nem lehet, de 1 sem, mert akkor az r-Sylow normálosztó lenne. Ezért az r-Sylowok száma csak pq lehet. A 4.10.26. Gyakorlat szerint tehát $pq(r-1)$ darab r rendű elem van. A q-Sylowok száma sem lehet p, hiszen $p < q$, vagyis legalább r darab q-Sylow, és így legalább $r(q-1)$ darab q rendű elem van. A p-Sylowok száma legalább q, ez $q(p-1)$ darab p rendű elem. Összesen ez több, mint pqr, ami ellentmondás.

4.10.31. Ha csak egy p-Sylow részcsoport van G-ben, akkor ez normálosztó. Ha nem, akkor a p-Sylowok száma osztója egy p-Sylow indexének, ami a q prím. Így a p-Sylowok száma q. Tegyük fel, hogy bármely két p-Sylow metszete csak az egységelemből áll. Ekkor mindegyik p-Sylowban $p^2 - 1$ olyan elem van, melynek rendje p-hatvány. Ez összesen $q(p^2 - 1) = |G| - q$. Tehát csak q darab q-hatvány rendű elem lehet, azaz csak egy q-Sylow fér el, ami így normálosztó lesz.

Ha viszont léteznek olyan P_1 és P_2 különböző p-Sylow részcsoportok, amelyek D metszete nem az egységelem (hanem p elemű), akkor tekintsük a D normalizátorát. Mivel P_1 és P_2 Abel-csoportok (hiszen rendjük p^2), az $N_G(D)$ részcsoport tartalmazza P_1-et és P_2-t is, tehát nagyobb, mint P_1. De P_1 maximális részcsoport, hiszen az indexe a q prím. Ezért $N_G(D) = G$, vagyis D nemtriviális normálosztó.

4.10.32. Ha csak egy p-Sylow van G-ben, akkor ez normálosztó. Tegyük fel, hogy nem ez a helyzet, ekkor a p-Sylowok száma osztója egy p-Sylow indexének, ami a q prím. Így a p-Sylowok száma q. Legyenek P_1 és P_2 olyan p-Sylowok, melyek D metszete a lehető legnagyobb elemszámú. Ha $|D| = 1$, vagyis ha bármely két p-Sylow csak az egységelemben metszi egymást, akkor könnyen megszámolhatjuk a p-hatvány rendű elemeket. Mindegyik p-Sylowban $p^\alpha - 1$ ilyen elem van, ez összesen $q(p^\alpha - 1) = |G| - q$. Tehát csak q darab q-hatvány rendű elem lehet, azaz csak egy q-Sylow fér el, ami így normálosztó lesz.

Tegyük fel, hogy $|D| > 1$. Belátjuk, hogy D normálosztó G-ben (és így G nem egyszerű). A 4.10.20. Gyakorlat miatt van olyan $D < K \leq P_1$, amiben D normálosztó. Tehát $K \leq N_G(D)$. Ha $N_G(D)$ egy p-csoport lenne, akkor része lenne egy P_3 p-Sylow részcsoportnak. Ekkor $D < K \subseteq P_1 \cap P_3$, ami ellentmond annak, hogy D a lehető legnagyobb elemszámú két p-Sylow metszetei között. Ezért $N_G(D)$ nem p-csoport, vagyis tartalmazza G egy Q q-Sylow részcsoportját. Bármely P p-Sylow részcsoportra igaz, hogy $QP = G$, hiszen a 4.6.38. Gyakorlat miatt PQ rendje G rendjével egyenlő. Ha tehát $g \in G$ tetszőleges elem, akkor $g = hk$ alakban írható, ahol $h \in P$ és $k \in Q$. Tudjuk, hogy $k \in Q \leq N_G(D)$, és ezért $gDg^{-1} = hkDk^{-1}h^{-1} = hDh^{-1} \subseteq PDP$. Ha $P = P_1$ (vagy $P = P_2$), akkor $D \subseteq P$, ezért $gDg^{-1} \subseteq PDP = P$. Így $gDg^{-1} \subseteq P_1 \cap P_2 = D$. Tehát D zárt a konjugálásra, és így normálosztó.

4.10.33. Ha $g \in G$, akkor gPg^{-1} is p-Sylow N-ben (a rendje miatt, és mert a konjugálás nem vezet ki az N normálosztóból), ezért nPn^{-1} alakban írható alkalmas $n \in N$ elemre. Ekkor $n^{-1}gP = Pn^{-1}g$, ezért $n^{-1}g \in N_G(P)$, ahonnan $g \in NN_G(P)$.

A második állítás megmutatásához legyen P_1 egy P-t tartalmazó p-Sylow részcsoportja G-nek. Ekkor $P_1 \cap N$ nem lehet P-nél nagyobb, hiszen ez a metszet p-csoport, a P pedig p-Sylow N-ben. Ezért $P_1 \cap N = P$, vagyis $P \lhd P_1$ (hiszen N normálosztó). Ekkor pedig $P_1 \subseteq N_G(P)$.

4.10.34. A P részcsoport p-Sylowja K-nak is, ezért a Frattini-elvet a $K \lhd N_G(K)$ normálosztóra alkalmazva kapjuk, hogy $N_G(K) = KN_G(P)$, ami azonban K, hiszen feltettük, hogy $N_G(P) \subseteq K$.

A második állítás bizonyításához vegyük észre, hogy K-ban a p-Sylow részcsoportok száma $|K : N_K(P)|$ (és persze G-ben $|G : N_G(P)|$). Ezért mindkét index kongruens 1-gyel mod p. De $N_K(P) = K \cap N_G(P) = N_G(P)$, és így

$$|G : N_G(P)| = |G : K| \cdot |K : N_G(P)| = |G : K| \cdot |K : N_K(P)| .$$

Ezért $|G : K|$ is 1-gyel kongruens mod p.

4.10.35. Az Útmutatóban leírt gondolatmenetet folytatjuk. Mivel p prím, létezik primitív gyök mod p, azaz $\mathbb{Z}_p^\times$ ciklikus csoport. Így az egyforma rendű elemek egymás hatványai (4.3.18. Állítás), tehát $s = t^k$ alkalmas k egészre ($\mathbb{Z}_p$-ben). Legyen $c = b^k$. Ekkor a c elemmel való konjugálás a b-vel való konjugálás k-adik hatványa, vagyis $\langle a \rangle$ minden elemét a $t^k = s$-edik hatványába viszi.

Legyen most G és H két pq rendű nemkommutatív csoport, ahol a G-hez t, a H-hoz az s szám tartozik. Ekkor G-ben a b elemet c-re cserélve azt kapjuk, hogy igazából G-hez is az s szám tartozik. De akkor G és H izomorfak, mert ugyanazon csoportoknak ugyanazon ψ homomorfizmus segítségével készített szemidirekt szorzatai.

4.11. Primitív és többszörösen tranzitív csoportok.

4.11.2. Ha adottak a páronként különböző $x_1, \ldots, x_{n-2}$ és az ugyancsak páronként különböző $y_1, \ldots, y_{n-2}$ pontok, akkor jelölje a két kimaradó pontot x_{n-1} és x_n, illetve y_{n-1} és y_n. Az S_n-ben két olyan permutáció van, amely $i \leq n-2$ esetén mindegyik x_i pontot y_i-be viszi. Az egyiknél x_{n-1} az y_{n-1}-be megy, ezt jelölje f. A másiknál x_{n-1} az y_n-be megy, ezt jelölje g. Nyilván $f = g \circ (x_{n-1}, x_n)$. Ezért f és g közül pontosan az egyik lesz páros permutáció.

4.11.4. Ha a $G \leq S_X$ csoport szigorúan k-tranzitív, akkor minden $x \in X$ pont stabilizátora szigorúan $k-1$-tranzitív részcsoportja $S_{X-\{x\}}$-nek. Valóban, a 4.11.3. Állítás miatt ez a stabilizátor $k-1$-tranzitív. Ha lenne két eleme, amely az $x_2, \ldots, x_k \in X - \{x\}$ pontrendszert $y_2, \ldots, y_k \in X - \{x\}$-ba viszi, akkor ez a két elem az $x, x_2, \ldots, x_k$ pontrendszert $x, y_2, \ldots, y_k$-ba vinné, ami ellentmond annak, hogy G szigorúan k-tranzitív.

Megfordítva, ha $G \leq S_X$ tranzitív, és van olyan $x \in X$ pont, amelynek a stabilizátora szigorúan $k-1$-tranzitív $S_{X-\{x\}}$-ben, akkor G az S_X-nek szigorúan k-tranzitív részcsoportja. Valóban, a 4.11.3. Állítás miatt a G csoport k-tranzitív. Tegyük fel, hogy g_1 és g_2 is olyan elemek, amelyek x_i-t y_i-be viszik minden $1 \leq i \leq k$-ra. Ekkor $g = g_1 g_2^{-1}$ az összes x_i pontot fixálja. Mivel G tranzitív, van olyan $h \in G$, melyre $h(x_1) = x$, és így hgh^{-1} fixálja az $x = h(x_1), \ldots, h(x_k)$ elemeket. Ezért hgh^{-1} benne van az x pont stabilizátorában, és mivel ez szigorúan $k-1$-tranzitív, $hgh^{-1} = id$, vagyis $g = id$, és így $g_1 = g_2$.

4.11.6. A $G = \mathrm{Aff}(n, T)$ csoportban az eltolások, vagyis az $x \mapsto x + v$ transzformációk, ahol $v \in T^n$, egy $(T^+)^n$-nel izomorf N normálosztót, az $x \mapsto Mx$ alakú leképezések, ahol $M \in \mathrm{GL}(n, T)$, pedig egy $\mathrm{GL}(n, T)$-vel izomorf H részcsoportot alkotnak. Könnyű ellenőrizni, hogy N normálosztó, H részcsoport, $NH = G$ és $N \cap H = \{1\}$.

4.11.7. Legyen $G = \mathrm{Aff}(n, T)$. A $0 \in V = T^n$ stabilizátora pontosan a lineáris leképezésekből áll. A lineáris algebrából ismert előírhatósági tétel szerint minden $b_1, \ldots, b_k$ független vektorrendszer minden $c_1, \ldots, c_k$ független vektorrendszerbe elvihető alkalmas invertálható lineáris leképezéssel. Ezért a $\mathrm{GL}(n, T^n)$ csoport tranzitív a V nem nulla vektorainak halmazán. Mivel az $x \mapsto x + v$ eltolások csoportja tranzitív V-n, a 4.11.3. Állítás miatt G már 2-tranzitív a V halmazon.

Az $\mathrm{Aff}(n, T)$ pontosan akkor lesz szigorúan 2-tranzitív, ha $n = 1$. Valóban, ehhez a fentiek szerint az szükséges és elégséges, hogy az invertálható lineáris leképezések szigorúan 1-tranzitívan (más néven regulárisan) hassanak a $V - \{0\}$ halmazon, vagyis hogy egy rögzített $v \neq 0$ vektor stabilizátora egyelemű legyen. Ez tényleg akkor igaz, ha $n = 1$, hiszen ha v és w független vektorok, akkor amellett, hogy v képe v, a w képe w és $v + w$ is lehet egy invertálható lineáris leképezésnél. Ha viszont $n = 1$, akkor egy v-t fixáló lineáris leképezés csak az identitás lehet.

Az $\mathrm{Aff}(n, T)$ csoportok közül $\mathrm{Aff}(1, \mathbb{Z}_3) \cong S_3$ és $\mathrm{Aff}(n, \mathbb{Z}_2)$ lesz 3-tranzitív. Az első szigorúan 3-tranzitív is, a második akkor szigorúan 3-tranzitív (és egyben 4-tranzitív), ha $n = 2$ (ez az $\mathrm{Aff}(2, \mathbb{Z}_2) \cong S_4$ csoport szokásos hatása a négyelemű halmazon).

Valóban, tegyük fel, hogy az $\mathrm{Aff}(n, T)$ csoport 3-tranzitív. Ismét legyen $v \neq 0$ rögzített vektor, és tekintsük azokat a lineáris leképezéseket, amelyek v-t fixálják. Ezek tranzitívan kell, hogy hassanak a $V - \{0, v\}$ halmazon. Ha $\lambda \in T$, melyre $\lambda \neq 0, 1$, akkor λv fixen marad (hiszen v fixen marad). Ez csak úgy lehetséges, ha $V = \{0, v, \lambda v\}$ (azaz $n = 1$ és $|T| = 3$), vagy ha egyáltalán nincs ilyen λ, azaz $|T| = 2$. A Galois-elméletről szóló fejezetben látni fogjuk (de könnyű számolással is ellenőrizhető), hogy minden kételemű test izomorf $\mathbb{Z}_2$-vel, és minden háromelemű test izomorf $\mathbb{Z}_3$-mal. Ezért az első esetben az $\mathrm{Aff}(1, \mathbb{Z}_3) \cong S_3$ csoport szigorúan 3-tranzitív hatását kapjuk a háromelemű halmazon. A második esetben kapott $\mathrm{Aff}(n, \mathbb{Z}_2)$ csoport is 3-tranzitív, hiszen bármely $w \notin \{v, 0\}$ vektor független v-től, és így minden 0-tól és v-től különböző vektorba elvihető invertálható lineáris transzformációval. Ez utóbbi csoport csak $n = 2$ esetén lesz szigorúan 3-tranzitív (mert egy harmadik bázisvektor akkor is elmozdulhat, ha az első és a második fix).

4.11.10. Az állítás a 4.11.4. Gyakorlat gondolatmenetével adódik (amikor $k = 1$). Ha az x pont stabilizátora egyelemű, akkor az orbitjának a hossza G rendjével egyenlő. Ha G tranzitív is, akkor ez a pontok száma, vagyis a csoport foka.

4.11.12. A Cayley-tételben a g elemhez tartozó permutáció a g elemmel való balszorzás. Minden stabilizátor egyelemű, hiszen ha $gx = x$, akkor $g = 1$. A csoport tranzitív is, hiszen az $x \in G$ pontot $y \in G$-be elvihetjük a $g = yx^{-1}$ elemmel. Megjegyezzük, hogy megfordítva, minden reguláris permutációcsoport ekvivalens a Cayley-tételben megadott hatással a 4.6.27. Feladat miatt.

4.11.14. Az orbitokról tudjuk, hogy ekvivalencia-relációt alkotnak. Ha x és y egy orbitban van, akkor $g \in G$ esetén $g * x$ és $g * y$ is egy orbitban van, nevezetesen az x-et és y-t tartalmazó orbitban. Ezért kongruenciát kaptunk. A csoport akkor és csak akkor tranzitív, ha az egész X egyetlen orbit, vagyis ha ez az 1_X kongruencia.

4.11.15. Mivel átlót minden egybevágóság átlóba visz, a megadott partíció tényleg kongruencia. Ugyancsak nemtriviális kongruenciát kapunk, ha a csúcsokat két szabályos háromszögre bontjuk. Könnyű meggondolni, hogy nincs más nemtriviális kongruencia.

4.11.16. Ha A és B két osztálya a $\sim$ kongruenciának, $a \in A$ és $b \in B$, akkor a tranzitivitás miatt van olyan g eleme a csoportnak, melyre $g * a = b$. Mivel $\sim$ kongruencia, g az A minden elemét egy B-beli elembe viszi. De a g hatása permutáció, ezért injektív az A halmazon, és így A elemszáma legfeljebb akkora, mint B elemszáma. Az A és B szerepét megcserélve $|A| = |B|$ adódik.

4.11.17. Csak annyit kell végiggondolni, hogy a kongruenciák, illetve a részcsoportok között megadott két leképezés egymás inverze.

Ha $H \leq K \leq G$, akkor az ehhez tartozó $\sim$ kongruenciánál $g_1 * x \sim g_2 * x$ akkor és csak akkor, ha $g_1^{-1} g_2 \in K$. A $\sim$ kongruenciához azt a részcsoportot rendeltük, amelyben a g elem pontosan $g * x \sim x$ esetén van benne. Be kell látni, hogy ez K, vagyis hogy $g \in K$ pontosan akkor, ha $g * x \sim x$. De $g * x \sim x$ akkor és csak akkor, ha $g^{-1} 1 \in K$ a $\sim$ definíciója miatt, azaz ha $g \in K$.

Megfordítva, ha $\sim$ adott, akkor az ehhez tartozó K részcsoportban azok a g elemek vannak, melyekre $g * x \sim x$. A K-hoz tartozó relációnál $g_1 * x$ és $g_2 * x$ akkor és csak akkor vannak egy osztályban, ha $g_1^{-1} g_2 \in K$. Be kell tehát látni, hogy $g_1^{-1} g_2 \in K$ akkor és csak akkor, ha $g_1 * x \sim g_2 * x$. De $g_1 * x \sim g_2 * x$ akkor és csak akkor, ha $x \sim g_1^{-1} g_2 * x$, ezért ez az állítás is igaz.

4.11.23. Ha a bizonyításon végigmegyünk $n = 5$ esetén, akkor a következőkre jutunk. Az N normálosztó most sem tartalmazhatja a H stabilizátort. Ha $N \cap H = \{1\}$, akkor ebben az esetben is kiderül, hogy N ötelemű, és ennek nem nulla elemein H konjugálással úgy hat, amilyen A_4 szokásos hatása, vagyis 2-tranzitívan. Ez lehetetlen, hiszen N ötödrendű ciklikus csoport, amelynek az automorfizmus-csoportja $\mathbb{Z}_5^\times$ csak négyelemű. Azonban most $N \cap H$ még lehet a $H \cong A_4$ csoport egyetlen nemtriviális (Klein-féle) normálosztója is. Ezt az esetet némi számolással ki lehet zárni (kijön, hogy N csak 20-elemű lehet, de akkor az ötösciklusok nem férnek el benne).

4.11.26. A 4.6.37. Gyakorlat miatt gHg^{-1} a $g(x)$ pont stabilizátora. Mivel $g \notin H$, ezért $g(x) \neq x$. Tehát $H \cap gHg^{-1}$ elemei két pontot fixálnak, és Frobenius-csoportban ilyen elem csak az identitás lehet.

Megfordítva, a H szerinti mellékosztályokon való hatásban a stabilizátorok pontosan a H konjugáltjai (a 4.6.26. Gyakorlat miatt). Így ez a hatás hű, vagyis G az S_n részcsoportjának tekinthető, ahol $n = |G : H|$. A H bármely két konjugáltja csak az egységelemben metszi egymást, mert az $aHa^{-1} \cap bHb^{-1}$ metszetet a^{-1}-gyel konjugálva $H \cap gHg^{-1}$ adódik, ahol $g = a^{-1}b$, és erről tudjuk, hogy egyelemű. Ha tehát egy permutációnak két fixpontja van, akkor két pont stabilizátorában is benne van, tehát az identitás. A csoport tranzitív, hiszen a H mellékosztályain való hatás az, és nem reguláris, mert H nemtriviális részcsoport.

A kapott Frobenius-csoport N magjában pontosan azok az elemek vannak az egységelemen kívül, amelyeknek nincs fixpontja, tehát amelyek H egyetlen konjugáltjában sincsenek benne. Az N tehát konjugált osztályok egyesítése, és így ha részcsoport, akkor normálosztó is. A H-ra kirótt feltétel miatt $N_G(H) = H$, ezért H-nak n konjugáltja van. Ezek páronként diszjunktak (az egységelemet leszámítva), és így a mag elemszáma

$$|G| - n(|H| - 1) + 1 = n\,,$$

hiszen $n = |G : H|$. Nyilván $H \cap N = \{1\}$, és így $|NH| = |N||H| = n|H| = |G|$. Ezért $NH = G$.

4.11.27. Az S_3 az $\{1, 2, 3\}$ halmazon hat, a mag az $\{id, (123), (132)\}$, a komplementumok a 2-Sylow részcsoportok. A D_{2n+1} diédercsoport a szabályos $2n + 1$-szög csúcsain hat, a mag a forgatásokból áll, a kételemű komplementumokat egy-egy tükrözés generálja. Az S_3 előbbi hatása ennek speciális esete ha $n = 1$.

Az A_4 az $\{1, 2, 3, 4\}$ halmazon hat, a mag a négyelemű Klein-normálosztó, a komplementumok a stabilizátorok, azaz a 3-Sylow részcsoportok. Végül $\mathrm{Aff}(1, T)$ a T testen hat, a mag az $x + b$ alakú leképezésekből, vagyis az eltolásokból áll, a komplementumok a $T^\times$ csoporttal izomorfak.

4.11.28. Ha H egy prímrendű részcsoport, akkor H minden konjugáltja vagy maga H, vagy pedig H-t csak az egységelemben metszi. Ha minden $g \notin H$ esetén ez a második lehetőség áll fenn, vagyis ha $N_G(H) = H$ (és nem nagyobb), akkor tehát Frobenius-csoportot kapunk. A 4.10.18. Állítás szerint egy nemkommutatív pq rendű csoportban pontosan ez a helyzet, ahol H egy q-Sylow részcsoport. Így ez tényleg Frobenius-csoport, amelyben a mag a p-Sylow, a komplementumok a q-Sylowok (és $q \mid p - 1$).

4.11.29. Tegyük fel, hogy N nemtriviális normálosztó S_n-ben. Ekkor $N \cap A_n$ normálosztója A_n-nek, és mivel A_n egyszerű csoport, ez a metszet vagy $\{1\}$, vagy A_n.

A második esetben $A_n \subseteq N \subseteq S_n$. De $|S_n : A_n| = 2$, ezért A_n maximális részcsoport S_n-ben (4.10.7. Gyakorlat), tehát N csak A_n vagy S_n lehet.

Az első esetben $N \cap A_n = \{1\}$, és ezért N minden eleme felcserélhető A_n minden elemével (4.7.27. Gyakorlat). Legyen $1 \neq g \in N$, akkor g centralizátora tartalmazza A_n-et, és az azon kívüli g elemet is. Mivel A_n maximális részcsoport, a g centralizátora S_n. Ez azonban lehetetlen, mert $n > 2$ esetén S_n centruma egyelemű (4.7.38. Gyakorlat). Ezért S_n-nek a triviálisakon kívül csak A_n lehet normálosztója.

4.11.30. Legyen Y az olyan k elemű rendezett sorozatok halmaza, melyek komponensei páronként különböző X-beli elemek. Nyilván G (komponensenkénti) hatása akkor és csak akkor tranzitív Y-on, ha G hatása X-en k-tranzitív. Ilyenkor tehát Y egy orbit, és így elemszáma osztója G rendjének. De Y elemszáma pontosan $n(n-1)\dots(n-k+1)$. A szigorú k-tranzitivitás azt jelenti, hogy G regulárisan hat Y-on, azaz a stabilizátorok egyeleműek, tehát $|G| = |Y|$.

4.11.31. Elég belátni, hogy a stabilizátorok egyeleműek. Tranzitív csoportban a stabilizátorok egymás konjugáltjai (4.6.37. Gyakorlat), és mivel A Abel-féle, egyenlők. Tehát egy pont stabilizátorának elemei az összes pontot fixálják, és így minden stabilizátor egyelemű.

4.11.32. Minden kongruencia osztályai ugyanannyi elemből állnak (4.11.16. Gyakorlat), ez az elemszám tehát osztója a csoport fokának, ami prím. Így vagy minden osztály egyelemű, vagy csak egyetlen osztály van.

4.11.33. Az A_3 primitív, mert tranzitív és prímfokú. Az A_4 is, mert 2-tranzitív. Az A_4 Klein-normálosztója nem primitív. Valóban, ez reguláris permutációcsoport, hiszen minden stabilizátor egyelemű. Ugyanakkor a Klein-csoportban az egyelemű részcsoport nem maximális, hiszen három nemtriviális részcsoport is van.

A D_n pontosan akkor primitív az n-szög csúcsain, ha n prím. Valóban, prímfokú tranzitív csoport primitív, ha viszont n nem prím, hanem k valódi osztója, akkor az n-szöget k darab szabályos n/k-szögre bontva kongruenciát kapunk (vö. 4.11.15. Gyakorlat).

A kocka szimmetriacsoportja nem primitív a csúcsokon (a testátlók végpontjai kongruenciát adnak, melynek négy darab kételemű osztálya van), sem a lapokon (szemköztes lappárok), sem az éleken (párhuzamos élnégyesek).

4.11.34. Az $\mathrm{Aut}(G)$ pontosan akkor primitív a $G - \{1\}$ halmazon, ha $G \cong \mathbb{Z}_3^+$, vagy $G \cong (\mathbb{Z}_2^+)^n$. Valóban, már a tranzitivitásból is következik, hogy G minden 1-től különböző elemének a rendje ugyanaz. Mivel minden nemtriviális csoportban van prímrendű elem, ez a közös rend egy p prímszám. Így G a Cauchy-tétel miatt egy p-csoport. Ennek centruma nem egyelemű. Ha $1 \neq g \in Z(G)$, akkor g-t minden automorfizmus $Z(G)$-be viszi. Másrészt a tranzitivitás miatt bármely egységtől különböző elembe elviszik, és így $Z(G) = G$, vagyis G Abel-csoport. Az alaptétel miatt $G \cong (\mathbb{Z}_p^+)^n$.

Ezt a csoportot a 4.8.30. Gyakorlat szerint egy $\mathbb{Z}_p$ feletti V vektortérnek tekinthetjük, melynek automorfizmus-csoportja $\mathrm{GL}(n, \mathbb{Z}_p)$. Ha $\mathrm{Aut}(G)$ primitíven hat a $V - \{0\}$ halmazon, akkor minden $v \neq 0$ vektor stabilizátora maximális részcsoport. Ennél nagyobb lesz az a $K \leq \mathrm{Aut}(G)$, amelynek elemei a v vektort a v valamilyen skalárszorosába viszik, kivéve ha a test kételemű. Ha viszont $K = \mathrm{GL}(n, \mathbb{Z}_p)$, akkor $n = 1$, és ekkor a primitivitás azzal ekvivalens, hogy $\mathbb{Z}_p^\times$-nek nincs nemtriviális részcsoportja, azaz $p - 1$ prím, és mivel ez páros, csak 2 lehet, azaz $p = 3$. A $(\mathbb{Z}_2^+)^n$ megfelel a feltételeknek, mert 2-tranzitív is (4.11.7. Gyakorlat).

4.11.35. Az orbitok kongruenciát alkotnak, tehát ha a hatás primitív, akkor ez a kongruencia vagy 1_X (azaz a hatás tranzitív), vagy 0_X (amikor minden elem identikusan hat). Az utóbbi esetben minden partíció kongruencia, tehát ha csak triviális kongruencia van, akkor a pontok halmaza kételemű.

4.11.36. Az Útmutatóban megadott jelölésekkel legyen $g \in G$ és $n \in K$. Az N normálosztó tranzitív, ezért van olyan $m \in N$, hogy $m(x) = g^{-1}(x)$. Mivel N Abel-féle, $nm = mn$, tehát $ng^{-1}(x) = nm(x) = mn(x) \sim m(x) = g^{-1}(x)$, és innen $gng^{-1}(x) \sim x$, azaz $gng^{-1} \in K$. Az nyilvánvaló, hogy K részcsoport, és így normálosztó. Az N minimalitása miatt $K = \{1\}$ vagy $K = N$. Az első esetben $\sim$ a 0_X (hiszen az osztályai egyformák). A másodikban N tranzitivitása miatt x osztálya az egész X.

A feladatot talán könnyebb úgy megoldani, hogy „lefordítjuk" az állítást egy stabilizátor mellékosztályain való hatásra, és így „tiszta" csoportelméleti állítást kapunk. Azt kell megmutatni, hogy ha N Abel-féle minimális normálosztó G-ben, és H részcsoport (egy stabilizátor), melyre $NH = G$ (ez felel meg annak, hogy N tranzitív), akkor H maximális részcsoport. Ezt a következőképpen láthatjuk be. Ha $H \leq L \leq G$, akkor a $L \cap N$ normalizátora tartalmazza N-et, hiszen N Abel, de tartalmazza L-et is, hiszen $N \triangleleft G$ miatt $L \cap N \triangleleft L$. Így $N_G(L \cap N)$ tartalmazza $NL \geq NH = G$-t is, vagyis $L \cap N \triangleleft G$. Az N minimalitása miatt vagy $L \cap N = N$ (ebben az esetben $N \subseteq L$, vagyis $G = NH \subseteq L$ miatt $L = G$), vagy pedig $L \cap N = \{1\}$ (ebben az esetben pedig $L = H$ a moduláris szabály, vagyis a 4.5.29. Gyakorlat miatt). Könnyű meggondolni, hogy a fenti megoldás valójában a most mutatott gondolatmenetnek a „visszafordítása" a permutációcsoportok nyelvére.

4.11.37. Rajzoljuk le a 4.2.29. Feladatból már ismert gráfot az $X = \{1, 2, \ldots, p\}$ halmazon: b és c akkor legyen összekötve, ha $(bc) \in G$. Elég belátni, hogy ez összefüggő. Ha $g \in G$, akkor $g(bc)g^{-1} = (g(b), g(c))$, azaz G elemei éltartók, és így komponens képe komponens lesz. Ezért a gráf komponensei kongruenciát alkotnak X-en. Mivel G tranzitív és prímfokú, ezért primitív. Van benne transzpozíció, így a kapott kongruencia nem a 0_X, tehát csak 1_X lehet.

Második megoldás: Mivel van p hosszú orbit, $|G|$ osztható p-vel, így Cauchy tétele miatt van G-ben p rendű elem. Ez csak p hosszú ciklus lehet. Alkalmas hatványát véve a G-ben levő transzpozíció elemei a ciklusban szomszédosak lesznek, tehát a 4.2.24. Gyakorlat miatt készen vagyunk.

4.11.38. Ha $n \geq 8$, akkor a Cayley-tétel miatt van, különben nincs. A kvaterniócsoportban ugyanis minden 1-től különböző elemnek hatványa a -1. Ha tehát egy x pont nem fixpontja a -1-hez tartozó permutációnak, akkor nem fixpontja a többi hat nem identikus permutációnak sem. Ezért az x stabilizátora egyelemű, vagyis orbitja nyolcelemű.

4.11.39. Tekintsük G hatását a H szerinti bal mellékosztályokon. Ennek magja nem G (hiszen a mag a H konjugáltjainak a metszete a 4.6.26. Gyakorlat miatt, és $n > 1$ miatt $H < G$). Mivel G egyszerű, ez a mag csak az egységelemből áll, és így G beágyazható S_n-be.

4.11.40. A G véges csoport $\overline{G} \leq S_G$ Cayley-reprezentációjában a g elem balszorzással hat. Ezért az $x \in G$ ciklusa $(x, gx, \ldots, g^{k-1}x)$. Ez az első olyan k-nál ér véget, amikor $gg^{k-1}x = x$, vagyis ha $g^k = 1$. Ezért minden ciklus hossza $o(g)$, és így a ciklusok száma $|G|/o(g)$. Ez akkor páratlan permutáció, ha g rendje páros, de $|G|/o(g)$ páratlan, vagyis

ha $o(g)$ osztható egy 2-Sylow rendjével. Tehát akkor és csak akkor van a $\overline{G}$-ban páratlan permutáció, ha a G csoport 2-Sylowja ciklikus.

Ebben az esetben a $\overline{G}$ részcsoportot az $A_G \triangleleft S_G$ alternáló csoport egy valódi normálosztóban metszi, aminek az indexe az első izomorfizmus-tétel miatt 2 lesz. Ha G egyszerű, és van 2 indexű normálosztója, akkor G a kételemű ciklikus csoport.

4.11.41. Ha a G egyszerű csoport rendje $1960 = 2^3 \cdot 5 \cdot 7^2$ lenne, akkor a 7-Sylowok száma csak 8 lehetne a Sylow-tétel miatt, tehát a 4.11.39. Feladat miatt G beágyazható lenne S_8-ba, de annak rendje nem osztható 49-cel.

Ha G rendje $120 = 2^3 \cdot 3 \cdot 5$, akkor az 5-Sylowok száma csak 6 lehet, ezért a 4.11.39. Feladat miatt G beágyazható S_6-ba, sőt a 4.11.40. Feladat megoldásában használt gondolatmenet miatt A_6-ba is (különben lenne benne 2 indexű normálosztó). De akkor G indexe A_6-ban $360/120 = 3$ lenne, ami ismét a 4.11.39. Feladat miatt lehetetlen, hiszen A_6 is egyszerű.

Végül tegyük fel, hogy G rendje $180 = 2^2 \cdot 3^2 \cdot 5$. Az imént használt gondolatmenetből látszik, hogy G-nek nem lehet 7-nél kisebb indexű valódi részcsoportja (mert akkor G beágyazható lenne A_6-ba 2 indexű részcsoportként, ami lehetetlen). Az 5-Sylowok száma a Sylow-tétel szerint vagy 6, vagy 36. De 6 nem lehet, mert nincs 6 indexű részcsoport. Tehát az 5-Sylowok száma 36.

> Ha használhatnánk a 4.11.25. Frobenius-tételt, akkor készen lennénk. Ugyanis az 5-Sylow normalizátora önmaga, és így a 4.11.28. Gyakorlat miatt G Frobenius-csoport, vagyis a magja nemtriviális normálosztó. Érdemes azonban tovább dolgozni, hogy elemi bizonyítást kapjunk.

Az ötödrendű elemek száma $36(5-1) = 144$. A 3-Sylowok száma sem lehet 4 (mert nincs 4 indexű részcsoport), ezért ez 10. Ha a 3-Sylowok páronként diszjunktak lennének, akkor már nem férnének el a 3-hatványrendű elemek. Tehát alkalmas P_1 és P_2 3-Sylowokra a $H = P_1 \cap P_2$ elemszáma 3. Ekkor $N_G(H)$ tartalmazza P_1-et és P_2-t is. A Sylow-tételt $N_G(H)$-ra alkalmazva kapjuk, hogy a 3-Sylowok száma legalább 4 (nem lehet 1, mert ebben a csoportban P_1 és P_2 is benne van). Így $N_G(H)$ rendje legalább $9 \cdot 4 = 36$, de akkor indexe legfeljebb 5, ami ismét lehetetlen.

4.11.42. Mivel G tranzitív, az X elemszáma osztja G rendjét, azaz $|G|$ páros. Tegyük fel, hogy $|G| = 4k + 2$. Ekkor a 4.11.40. Feladat miatt G-ben van egy kettő indexű N normálosztó. Mivel G primitív, N tranzitív, és így X elemszáma osztja N rendjét, ami lehetetlen, mert $|N|$ páratlan.

4.11.43. Tranzitív hatásban a stabilizátorok konjugáltak (4.6.37. Gyakorlat), ekvivalens hatásokban a stabilizátorok ugyanazok a részcsoportok. Ha tehát a H szerinti mellékosztályokon való hatás ekvivalens a K szerinti mellékosztályokon való hatással, akkor (mivel H is és K is stabilizátorok a megfelelő hatásban), H és K konjugáltak.

Megfordítva, ha K konjugáltja H-nak, akkor (a 4.6.26. Gyakorlat miatt) K is stabilizátor a H mellékosztályain való hatásban. A 4.6.27. Feladat miatt minden tranzitív hatás ekvivalens egy tetszőleges stabilizátor szerinti mellékosztályokon való hatással. Tehát a H szerinti mellékosztályokon való hatás ekvivalens a K szerintivel.

4.11.44. A feltétel az, hogy minden $1 \neq h \in H$ esetén $\psi(h)$ fixpontmentes automorfizmusa legyen N-nek (abban az értelemben, hogy csak az egységelemet fixálja).

Valóban, tudjuk, hogy a $\psi(h)$ automorfizmus szemidirekt szorzatban a h-val való konjugálás az n-en. Ha $n \neq 1$ fixpontja a $\psi(h)$-nak, akkor $hnh^{-1} = n$, vagyis $hn = nh$. Ekkor azonban $h \in nHn^{-1} \cap H$, ami lehetetlen, ha azt akarjuk, hogy H a Frobenius-csoport komplementuma legyen (vö. 4.11.26. Gyakorlat).

Megfordítva, tegyük fel, hogy $h \neq 1$ esetén $\psi(h)$ fixpontmentes. Legyen $g \in G - H$, ekkor $g = nk$, ahol $1 \neq n \in N$ és $k \in H$. Nyilván $gHg^{-1} = nkHk^{-1}n^{-1} = nHn^{-1}$, és így elegendő belátni, hogy $n \neq 1$ esetén $H \cap nHn^{-1} = \{1\}$. Ha ez nem így van, hanem ez a metszet tartalmazza a $h \neq 1$ elemet, akkor $nhn^{-1}h^{-1} \in H \cap N$, mert N normálosztó. Ezért ez az egységelem, ahonnan $nh = hn$, tehát az n-nel való konjugálás fixálja a h elemet.

Könnyű megmutatni, hogy egy Frobenius-csoport „természetes” (vagy ami ezzel ekvivalens, a H komplementum mellékosztályain való) hatása mindig ekvivalens a csoportnak az N magon való azon hatásával, amelynél N elemei balszorzással, H elemei konjugálással hatnak. Ezt lényegében meg is mutattuk kicsit általánosabban a 4.11.22. Tétel bizonyításában. Ennek az észrevételnek a felhasználásával a fenti számolás némileg rövidebbé és természetesebbé tehető.

4.12. Feloldható csoportok.

4.12.6. Ha egy csoportnak van olyan kompozíciólánca, amelyben a faktorok prímrendű ciklikusak, akkor mivel ezek kommutatívak, a csoport feloldható. Megfordítva, tegyük fel, hogy a G véges csoportnak van olyan normállánca, amelyben a faktorok kommutatívak. Ha ezt elkezdjük finomítani, akkor ez azt jelenti, hogy az $N \lhd K$ közé betoldunk egy M-et, melyre $N \lhd M \lhd K$. A második izomorfizmus-tétel miatt $K/M \cong (K/N)/(M/N)$, tehát ha K/N Abel, akkor ennek minden faktorcsoportja, speciálisan K/M is Abel. Ugyanakkor M/N részcsoportja K/N-nek a 4.5.19. Tétel miatt, és így szintén kommutatív. Vagyis egy finomító lépés során megmaradt a lánc azon tulajdonsága, hogy minden faktora Abel. Mivel G véges, az eredeti normálláncot véges sok lépésben kompozícióláncca finomíthatjuk. Ebben szintén minden faktor kommutatív lesz, de egyúttal egyszerű csoport is. A kommutatív egyszerű csoportok azonban a prímrendű ciklikusak (4.7.4. Következmény).

Ha G egyszerű, akkor az egyetlen kompozíciófaktora maga G, ennek kell prímrendű ciklikusnak lennie ahhoz, hogy G feloldható legyen.

4.12.7. Az S_2 prímrendű ciklikus csoport. Az S_3 csoportban az $\{id\} \lhd \{id, (123), (132)\} \lhd S_3$ olyan kompozíciólánc, amelyben minden faktor Abel-féle. Az S_4 esetén

$$\{id\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$$

olyan normállánc, amelynek faktorai Abel-csoportok (hiszen a 4.7. szakaszban meghatároztuk S_4 összes normálosztóit, és láttuk, hogy a fenti négyelemű normálosztó a Klein-csoporttal izomorf).

4.12.15. Az $A \times B$ direkt szorzat egy normálláncát elkészíthetjük úgy, hogy vesszük A egy normálláncát, és a lánc mindegyik tagját direkt megszorozzuk $\{1_B\}$-vel (ekkor felérünk $A \times \{1_B\}$-ig), majd ezt folytatva vesszük B egy normálláncát, és ennek minden tagját direkt megszorozzuk A-val. A 4.8.25. Gyakorlatból adódik, hogy

$$(K \times \{1_B\})/(L \times \{1_B\}) \cong K/L \quad \text{és} \quad (A \times M)/(A \times N) \cong M/N\,.$$

Ezért a kapott láncnak a faktorai az eredeti két lánc faktorai lesznek együttvéve. Ezzel beláttuk, hogy két feloldható csoport direkt szorzata is feloldható. Ezt kétszer alkalmazva kapjuk, hogy $S_4 \times \mathbb{Z}_3^+ \times \mathbb{Z}_2^+$ is feloldható, és így kompozíciófaktorait a rendjéről leolvashatjuk: $24 \cdot 3 \cdot 2 = 2^4 3^2$, tehát négy $\mathbb{Z}_2^+$ és két $\mathbb{Z}_3^+$ szerepel.

4.12.16. Egy Abel-csoport minden kompozíciófaktora egyszerű Abel-csoport, azaz prímrendű ciklikus (lásd a 4.12.6. Gyakorlat megoldását). Ezért ha van kompozíciólánca, akkor minden faktor véges, és így a csoport is véges. Megfordítva, minden véges csoportnak van kompozíciólánca. Így példákat kaptunk olyan csoportra, amelynek nincs kompozíciólánca ($\mathbb{Z}^+$, $\mathbb{C}^\times$, és így tovább).

4.12.17. Ha a két prím egyenlő, akkor a csoport kommutatív (4.10.3. Tétel), és így feloldható. Ha a két prím különböző, akkor a 4.10.18. Tétel miatt a csoportban van prímrendű normálosztó. Ez kommutatív, és a rá vett faktor is prímrendű, tehát az is kommutatív.

4.12.18. Jelölje $G^{(i)}$ a G csoport kommutátorláncának felülről számított i-edik elemét (ahol tehát i darab vesszőt képzelünk G-re, precízen $G^{(0)} = G$ és $G^{(i+1)}$ a $G^{(i)}$ kommutátor-részcsoportja). A 4.7.25. Állítás szerint N/N' mindig Abel-csoport, és megfordítva, ha N/K Abel-csoport, akkor $N' \subseteq K$. Ha tehát a G csoportnak van olyan

$$\{1\} = N_n \lhd N_{n-1} \lhd \ldots \lhd N_2 \lhd N_1 \lhd N_0 = G\,.$$

normálláncа, amelyben a faktorok kommutatívak, akkor indukcióval azonnal láthatjuk, hogy $G^{(i)} \leq N_i$ minden i-re. Speciálisan $G^{(n)} = \{1\}$, vagyis a kommutátorlánc leér. Megfordítva, a kommutátorlánc faktorai kommutatívak, tehát ha ez a lánc leér, akkor a csoport feloldható.

A 4.7.47. Gyakorlat miatt a kommutátor-részcsoport karakterisztikus. De karakterisztikus részcsoport karakterisztikus részcsoportja is karakterisztikus (4.7.20. Gyakorlat), ezért a kommutátorlánc minden eleme karakterisztikus, speciálisan normálosztó.

4.12.19. Legyen H részcsoport a G feloldható csoportban. Indukcióval azonnal látjuk, hogy $H^{(i)} \subseteq G^{(i)}$ (a jelölést illetően lásd az előző feladat megoldását). Mivel G feloldható, van olyan n egész, hogy $G^{(n)} = \{1\}$. De akkor $H^{(n)} = \{1\}$, vagyis H is feloldható.

Most tegyük fel, hogy N normálosztó a G feloldható csoportban. A 4.7.48. Feladat miatt

$$\big(G^{(i)}N\big)' = [G^{(i)}N, G^{(i)}N] = [G^{(i)}, G^{(i)}][N, G^{(i)}][G^{(i)}, N][N, N] \subseteq G^{(i+1)}N\,,$$

hiszen $[G^{(i)}, G^{(i)}] = G^{(i+1)}$. Ez azt jelenti, hogy $\big(G^{(i)}N\big)\big/\big(G^{(i+1)}N\big)$ Abel-csoport. Ezért a második izomorfizmus-tétel miatt a $G^{(i)}N/N$ normálosztók olyan normálláncát képezik a G/N faktorcsoportnak, melynek faktorai kommutatívak.

4.12.20. Tekintsük G/N egy olyan normálláncát, amelynek faktorai kommutatívak, és vegyük a lánc mindegyik elemének teljes inverz képét G-ben. Ekkor egy olyan láncot kapunk, amely G-től N-ig halad le, és a második izomorfizmus-tétel miatt a faktorai kommutatívak. Fűzzük ehhez hozzá N egy olyan normálláncát, amelynek a faktorai szintén kommutatívak. A kapott lánc bizonyítja, hogy G feloldható.

Ha N és K feloldható normálosztók, akkor $NK/N \cong K/(K \cap N)$ feloldható az előző feladat miatt, hiszen K-nak homomorf képe. De akkor az NK csoportban az N normálosztó is, a szerinte vett faktor is feloldható, tehát a feladat első része miatt NK is az.

4.12.21. Legyen P egy p-Sylow részcsoport G-ben, ekkor $|G : P| = 4$. Tekintsük G hatását a P szerinti bal mellékosztályokon. Ha N jelöli a hatás magját, akkor a 4.6.22. Gyakorlat szerint G/N izomorf S_4 egy részcsoportjával, és így feloldható. Ugyanakkor $N \subseteq P$, ami P-csoport, és így N szintén feloldható. A 4.12.20. Feladat miatt tehát G is feloldható.

4.12.22. Az Útmutatóban szereplő állítások egyszerű mátrix-szorzással igazolhatók, és következik belőlük, hogy $N = \mathrm{U}(n, T)$ feloldható. (Indukcióval világos ugyanis, hogy a 4.12.18. Feladat jelöléseivel $N^{(i)}$ elemei $E + M$ alakban írhatók, ahol $M \in U_{i+1}$, sőt ennél sokkal jobb becslést is kaphatnánk.) A 4.10.23. Gyakorlat miatt $\mathrm{T}(n, T)/N$ Abel, és így $\mathrm{T}(n, T)$ is feloldható.

4.12.23. Ha N minimális normálosztó G-ben, akkor (a 4.12.19. Feladat miatt) feloldható, és így (a 4.12.18. Feladat miatt) $N' < N$. De N' karakterisztikus részcsoport N-ben, ezért (a 4.7.20. Gyakorlat szerint) $N' \triangleleft G$. Az N minimalitása miatt $N' = \{1\}$, azaz N Abel. Az N csoportnak van prímrendű eleme, válasszunk ki egy ilyen p prímet. Tekintsük a 4.7.47. Gyakorlatban definiált $N[p]$ karakterisztikus részcsoportot, amely az N azon elemeiből áll, melyek p-edik hatványa az egységelem. Ekkor $\{1\} < N[p]$, de $N[p]$ is normálosztó G-ben, tehát N minimalitása miatt $N[p] = N$. Vagyis N minden egységtől különböző eleme p rendű, és így a véges Abel-csoportok alaptétele szerint $\mathbb{Z}_p^+$-nak direkt hatványa.

4.12.24. A G csoport rendje szerinti indukcióval bizonyítunk. Legyen M maximális részcsoport G-ben, és N tetszőleges minimális normálosztó. Ekkor NM egy M-et tartalmazó részcsoport, és így vagy M, vagy G. Az első esetben $N \subseteq M$, tehát (a 4.5.19. Tétel miatt) $|G/N : M/N| = |G : M|$ és M/N maximális részcsoport G/N-ben. Az indukciós feltevést a G/N csoportban alkalmazva kapjuk, hogy M/N indexe prímhatvány, tehát készen vagyunk. A második esetben $|G| = |N||M|/|N \cap M|$ mutatja, hogy $|G : M|$ osztója $|N|$-nek, ami az előző feladat szerint prímhatvány.

Az Olvasó megkérdezheti, hogy mi a fenti esetben az indukció kezdő esete. Ezt a fajta indukciót már megismertük, amikor azt láttuk be, hogy a körosztási polinom egész együtthatós (3.9.7. Következmény), és akkor megtárgyaltuk a logikai vonatkozásokat is. A fentihez hasonló bizonyításoknál szokás úgy is fogalmazni, hogy feltesszük: G minimális elemszámú ellenpélda (vagyis minden kisebb elemszámú csoportra már igaz a bizonyítandó állítás), és ellentmondásra jutunk.

Ha G véges, feloldható, primitív permutációcsoport, akkor minden pont stabilizátora maximális részcsoport (4.11.19. Következmény), amelynek az indexe az előzőek szerint prímhatvány. Ennek a stabilizátornak az indexe a csoport foka, hiszen minden primitív csoport tranzitív.

4.13. Véges egyszerű csoportok.

4.13.1. Az egyetlen olyan 60-nál kisebb szám, aminek három különböző prímosztója is van, a 30. De egy 30 rendű csoport feloldható, a 4.10.30. Feladat miatt. A fennmaradó számok mindegyike $p^\alpha q$ vagy $4p^\alpha$ alakú, vagy prímhatvány. Így a 4.10.32, illetve a 4.12.21. Feladatok miatt készen vagyunk.

4.13.2. Elég belátni, hogy az $\mathrm{SL}(n, T)$ részcsoport centralizátora $\mathrm{GL}(n, T)$-ben éppen az egységmátrix nem nulla skalárszorosaiból áll. Jelölje E_{ij} $(i > j)$ azt a mátrixot, amelyben az i-edik sor j-edik eleme 1, és az összes többi elem nulla. Ekkor $E + E_{ij}$ invertálható, és a determinánsa 1, tehát $\mathrm{SL}(n, T)$-ben van (érdemes ezt összevetni a 4.12.22. Feladatra adott útmutatásban szereplő állításokkal). Könnyű számolás mutatja, hogy ha egy mátrix az $E + E_{ij}$ mátrixok mindegyikével felcserélhető, akkor az az egységmátrix skalárszorosa.

4.13.6. Legyen V egy n-dimenziós vektortér a q elemű T test felett, és $b_1, \ldots, b_n$ egy bázis. Az invertálható lineáris transzformációkat egyértelműen meghatározzák a bázisvektorok képei, amelyeknek függetleneknek kell lenniük. A b_1 képe tehát tetszőleges nem nulla vektor lehet, ez $q^n - 1$ módon választható. A b_2 bárhová képződhet a b_1 generálta altéren kívül, ez $q^n - q$-féleképp lehetséges, és így tovább. Ezért $\mathrm{GL}(n, q)$ rendje tényleg M.

A determináns a T multiplikatív csoportjára képez, ezért a homomorfizmus-tétel miatt $\mathrm{SL}(n, q)$ indexe $q - 1$, tehát rendje $M/(q - 1)$. Jelölje Z az egységelem nem nulla skalárszorosaiból álló normálosztót (azaz $\mathrm{GL}(n, q)$ centrumát) , ennek rendje is $q - 1$. A $\mathrm{PGL}(n, q)$ csoport a Z szerinti faktor, így rendje szintén $M/(q - 1)$.

Végül az utolsó állítás bizonyításához azt kell megmutatni, hogy a Z centrum 1 determinánsú elemeinek száma $d = (q - 1, n)$. Ehhez meg kell számolni T azon t elemeit, melyekre $t^n = 1$. Nyilván $t^n = 1$ akkor és csak akkor, ha t rendje a $T^\times$ csoportban osztója n-nek, és mivel t rendje osztója $T^\times$ rendjének (ami $q - 1$), ez azzal ekvivalens, hogy t rendje osztója $(q - 1, n) = d$-nek, azaz, hogy $t^d = 1$. A $T^\times$ csoport azonban ciklikus (4.3.16. Tétel), és így az ilyen elemek száma (a 4.3.18. Állítás szerint) éppen d.

4.13.9. Legyen G véges csoport, amelynek minden két elemmel generált részcsoportja feloldható. Tekintsük G egy kompozícióláncát, és ebben a K/N faktorcsoportot, amely tehát egyszerű, és így két elemmel generálható. Legyenek ezek gN és hN, és jelölje H a g és h által generált részcsoportot. Ekkor H képe a G/N faktorcsoportban az egész K lesz, hiszen mindkét generátorelemet tartalmazza. Vagyis $(K/N) = HN/N \cong H/(H \cap N)$. A H részcsoportól feltettük, hogy feloldható, és ezért minden homomorf képe, azaz K/N is az. Így K/N feloldható egyszerű csoport, tehát prímrendű ciklikus. Ezért G feloldható.

4.13.10. Legyen G egy 200 rendű csoport, és $F = N/K$ ennek egy kompozíciófaktora. Ekkor F egyszerű csoport, melynek rendje 200-nak osztója. Ilyen azonban a táblázat szerint nincs, mert a nemkommutatív véges egyszerű csoportok között csak két olyan van, amelynek rendje 200-nál nem nagyobb, de ezek a rendek (60 és 168) nem osztói 200-nak. Ezért F csak prímrendű ciklikus csoport lehet, és így G feloldható.

4.13.11. Könnyű kiszámolni, hogy

$$\varphi : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \frac{ax+b}{cx+d}$$

művelettartó, és magja a skalármátrixokból (vagyis az egységmátrix skalárszorosaiból) áll. A homomorfizmus-tétel szerint tehát $\mathrm{Im}(\varphi) = K(T) \cong \mathrm{GL}(2, T)/\mathrm{Ker}(\varphi) = \mathrm{PGL}(2, T)$.

4.13.12. A kételemű test felett minden nem nulla skalár 1, ezért a $\mathrm{GL}(n, 2)$, $\mathrm{SL}(n, 2)$ $\mathrm{PGL}(n, 2)$ és $\mathrm{PSL}(n, 2)$ csoportok mind izomorfak. A $\mathrm{GL}(2, 2)$ a $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$, azaz a Klein-csoport automorfizmus-csoportja (4.8.30. Gyakorlat), ami a 4.7.43. Feladat miatt S_3.

Az előző gyakorlat miatt $\mathrm{PGL}(2, 3) \cong L(3)$, ami egy négyelemű halmazon hat szigorúan 3-tranzitívan, vagyis ez a csoport izomorf S_4-gyel. Ebben $\mathrm{PSL}(2, 3)$ egy 2 indexű normálosztó, ami csak A_4 lehet (hiszen S_4 normálosztóit ismerjük).

4.13.13. Tegyük fel, hogy a G egyszerű csoport rendje 60. A 4.11.39. Feladat miatt minden valódi részcsoport indexe legalább 5, és ha találunk egy 5 indexű részcsoportot, akkor készen is vagyunk, mert akkor G beágyazható S_5-be, de mivel egyszerű, A_5-be is. A Sylow-tétel szokásos alkalmazásával kapjuk, hogy az 5-Sylowok száma 6, tehát az ötödrendű elemeké 24, a 3-Sylowok száma pedig 10 (mert 4 indexű részcsoport nincs), és így 20 harmadrendű elem van. Végül a 2-Sylowok száma csak 15 lehet. Ezek diszjunktan nem férnek el, tehát előfordul, hogy $H = P_1 \cap P_2$ kételemű, ahol P_1 és P_2 2-Sylowok. De akkor $N_G(H)$ tartalmazza (a kommutatív) P_1 és P_2 részcsoportokat, és így indexe legfeljebb 5.

4.13.14. Az $\mathrm{U}(n, p)$ egy $p^{n(n-1)/2}$ rendű részcsoportja $\mathrm{GL}(n, p)$-nek. De $\mathrm{GL}(n, p)$-nek ismerjük a rendjét (4.13.6. Feladat). Könnyű kiszámolni, hogy ebben a rendben a p prím kitevője $n(n-1)/2$.

4.13.15. A Cayley-tétel szerint G felfogható, mint egy n elemű halmazon ható permutációcsoport. Válasszuk ezt a halmazt egy vektortér bázisának, és rendeljük hozzá mindegyik permutációhoz azt a lineáris transzformációt, amely a bázison a permutációnak megfelelően hat. Ez beágyazza G-t $\mathrm{GL}(n, p)$-be. Ha G egy p-csoport, akkor G képe benne van $\mathrm{GL}(n, p)$ egy p-Sylowjában, ami az előző gyakorlat miatt izomorf $\mathrm{U}(n, p)$-vel.

11.5. Gyűrűk

5.1.19. 5.3.4. Lemma.

5.7.12. Ennek oka az, hogy az $x = y + w$ helyettesítéssel nem lehet eltüntetni az elsőfokú tagot (hiszen $(y + w)^2 = y^2 + w^2$). Így a gyökképlet nevezőjében nem véletlenül van ott a kettes (amivel 2 karakterisztikában nem tudunk osztani).

5.10.12. A kvaterniócsoportbeli i, j, k-t mint térbeli egységvektorokat képzelve láthatjuk, hogy $\mathrm{Aut}(Q)$ izomorf a kocka mozgáscsoportjával, azaz S_4-gyel. (vö. [**6**] 6/239).

A tetraéder csúcsai $i + j + k$, $i - j - k$, $-i + j - k$, $-i - j + k$.

11.6. Galois-elmélet

6.3.3. Az f egy gyökével bővítve a K testnek legfeljebb n-edfokú bővítését kapjuk (a bővítés foka valójában f egyik irreducibilis tényezőjének fokával egyezik meg). Ebben $f(x) = (x-\alpha)g(x)$, ahol $g \in K(\alpha)[x]$ legfeljebb $n-1$-edfokú polinom. A g egy gyökével bővítve az újabb bővítés legfeljebb $n-1$-edfokú lesz. És így tovább, a legrosszabb esetben a felbontási test egy $n!$ fokú bővítés.

6.3.12. A polinom gyökeit úgy kapjuk meg, hogy a $\sqrt[4]{2}$ számot végigszorozzuk a negyedik egységgyökökkel (1.5.4 Tétel), azaz ± 1-gyel és $\pm i$-vel. Így $x^4 - 2$ felbontási teste $\mathbb{Q}$ fölött

$$\mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)\,.$$

Látszik, hogy ez nyolcadfokú bővítése $\mathbb{Q}$-nak, hiszen $\mathbb{Q}(\sqrt[4]{2})$ negyedfokú $\mathbb{Q}$,

6.4.25. Legyen $K \leq L$ véges bővítés, ahol K tökéletes test. Mivel a nulla karakterisztikájú testek tökéletesek, csak az az eset érdekes, amikor K karakterisztikája $p > 0$. Az állítást $|L : K|$ szerinti indukcióval bizonyítjuk, azaz feltehetjük, hogy $K \leq T \leq L$ esetén T tökéletes. A 6.4.24. Feladat szerint ez azt jelenti, hogy a $\varphi(x) = x^p$ leképezésnél (azaz a Frobenius-endomorfizmusnál) $\varphi(T) = T$. Legyen $T = \varphi(L)$. Ez is résztest, hiszen φ homomorfizmus, és K-t tartalmazza, mert $K = \varphi(K) \subseteq \varphi(L) = T$. Megmutatjuk, hogy $T = L$. Ebből már következik az állítás, hiszen akkor $\varphi(L) = L$, vagyis L is tökéletes.

Tegyük fel, hogy $T < L$. Legyen $\alpha \in L$, ekkor $\beta = \varphi(\alpha) \in T$. De $\beta = \varphi(\gamma)$ alkalmas $\gamma \in T$-re, hiszen az indukciós föltevés miatt T tökéletes. Mivel φ injektív (5.7.6. Gyakorlat), ezért $\alpha = \gamma \in T$.

6.5.11. A számolások és az eredmények is ugyanazok, csak a gyökjelek alatt 2 helyett 5-öt kell írni. Apró különbség, hogy ha $\gamma = \sqrt[4]{5} + i\sqrt[4]{5}$, akkor $\gamma^4 = -20$, azaz γ az $x^4 + 20$ polinomnak lesz gyöke, ami irreducibilis a Schönemann–Eisenstein-kritérium miatt (ha a prímszámot a kritériumban 5-nek vesszük). Így a $T_4 = \mathbb{Q}\left(\sqrt[4]{5} + i\sqrt[4]{5}\right)$ test szintén negyedfokú bővítése $\mathbb{Q}$-nak.

6.5.12. Mivel $x^8 - 4 = (x^4 - 2)(x^4 + 2)$, azt kell megmutatni, hogy $x^4 - 2$ és $x^4 + 2$ gyökei egymást generálják. Legyen $\eta = (1 + i)/\sqrt{2}$, ez primitív nyolcadik egységgyök, és benne van $x^4 - 2$ felbontási testében, azaz a $\mathbb{Q}(i, \sqrt[4]{2})$ testben, mert ez tartalmazza az i és $\sqrt{2}$ számokat. De $x^4 + 2$ gyökei pontosan $\eta\sqrt[4]{2}$ negyedik egységgyökszörösei, és így ezek is benne vannak $x^4 - 2$ felbontási testében. Megfordítva, $x^4 + 2$ felbontási testében is benne vannak a negyedik egységgyökök, és mivel $\eta\sqrt[4]{2}$ négyzete $i\sqrt{2}$, ezért benne van $\sqrt{2}$, azaz η is, ahonnan $\sqrt[4]{2}$ is megkapható. Így az első állítást beláttuk.

Legyen $\gamma = \sqrt[4]{2} + i\sqrt[4]{2}$, ekkor $\gamma^2 = 2i\sqrt{2}$ és $\gamma^4 = -8$. Ezért $(2/\gamma)^4 = -2$, vagyis $2/\gamma$ gyöke az $x^4 + 2$ polinomnak. Ez a Schönemann–Eisenstein-kritérium miatt irreducibilis, és így $2/\gamma$ is generálja a T_4 testet.

Az eddigi állítások sikere azon múlt, hogy az η fölírásához a negyedik egységgyökökön kívül még $\sqrt{2}$-re van szükség, ezt pedig $\sqrt[4]{2}$-ből megkaptuk. Ugyanezt nem tudjuk megtenni $x^4 - 5$ esetében. Az most is világos, hogy $x^8 - 25 = (x^4 - 5)(x^4 + 5)$, és így ha $x^4 - 5$-nek és $x^4 + 5$-nek ugyanaz lenne a felbontási teste, akkor ebben benne lenne a fenti η nyolcadik primítív egységgyök is, és mivel i (mint negyedik egységgyök) benne van, benne lenne $\sqrt{2}$ is.

Legyen K az $x^4 - 5$ polinom felbontási teste. Azt, hogy $\sqrt{2}$ nincs benne K-ban, legegyszerűbben a Galois-elmélet később bizonyítandó főtétele (6.6.7. Tétel) segítségével láthatjuk be. Ez a tétel azt mondja, hogy a fenti ábrán lerajzolt, az előző 6.5.11. Gyakorlatban megadott résztesteken kívül K-nak nincs más részteste. A felsorolt résztestek között csak három olyan van, amely $\mathbb{Q}$ fölött másodfokú: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{5})$ és $\mathbb{Q}(i\sqrt{5})$. Ezek egyike sem egyenlő $\mathbb{Q}(\sqrt{2})$-vel a 6.1.23. Gyakorlat miatt.

6.8.20.

6.10.6. Az Útmutatóban leírtak szerint járunk el. Elsőként az S_4 tranzitív G részcsoportjait keressük, ezek rendje néggyel osztható, tehát Lagrange tétele miatt 4, 8, 12 és 24 lehet. Nyilván 24 rendű csak az S_4, ha pedig G rendje 12, akkor G indexe 2, tehát normálosztó, ami csak A_4 lehet (4.11.29. Gyakorlat). Ha G rendje 8, akkor 2-Sylow, és így D_4-gyel izomorf (4.10.25. Gyakorlat). Végül ha G rendje 4, akkor vagy ciklikus, vagy a Klein-csoporttal izomorf (4.6.12. Tétel). Ezért más Galois-csoport nem fordulhat elő, mint amit a feladatban felsoroltunk.

Az 3.8.7. Feladat miatt f harmadfokú g rezolvensének gyökei benne vannak az f polinom K fölötti L felbontási testében. Ha g irreducibilis, akkor ezek foka 3, és így G rendje hárommal osztható, vagyis G csak A_4 vagy S_4 lehet. Ezek között az tesz különbséget, hogy f diszkriminánsa négyzetelem-e K-ban (6.10.3. Lemma). Ezért az (1) állítást beláttuk.

Tegyük most föl, hogy g-nek az u_1 gyöke K-ban van, ekkor G elemei az u_1-et önmagába viszik. Jelölje $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ az f gyökeit L-ben, és legyen $u_1 = (\alpha_1\alpha_2 + \alpha_3\alpha_4)/2$ (3.8.7. Feladat). Írjuk föl az f gyökeit az $\alpha_1, \alpha_3, \alpha_2, \alpha_4$ sorrendben egy négyzet csúcsaira.

Könnyű meggondolni, hogy egy permutáció akkor és csak akkor viszi az u_1 kifejezést saját magába, ha ennek a négyzetnek szimmetriája. Ezért $u_1 \in K$ esetén G részcsoportja e négyzet szimmetriacsoportjának, vagyis D_4-nek.

Ha a harmadfokú rezolvens $u_2 = (\alpha_1\alpha_3 + \alpha_2\alpha_4)/4$ gyöke is K-ban van, akkor G elemei ezt is önmagukba viszik. Könnyű látni, hogy ilyen permutáció már csak négy van:

$$\{id, (\alpha_1\alpha_2)(\alpha_3\alpha_4), (\alpha_1\alpha_3)(\alpha_2\alpha_4), (\alpha_1\alpha_4)(\alpha_2\alpha_3)\},$$

amelyek az S_4 csoport szokásos, a Klein-csoporttal izomorf V normálosztóját alkotják (185. oldal). Tehát G részcsoportja V-nek, és mivel legalább négyelemű, $G = V$. Ezzel (2)-t is beláttuk.

Ha u_2 (és így u_3) nincs K-ban, akkor G nem részcsoportja V-nek, de $u_1 \in K$ miatt részcsoportja a fent megadott D_4-nek. Így G vagy maga D_4, vagy D_4-nek egy V-től különböző, de tranzitív részcsoportja. Egy ilyen részcsoport négyelemű, és így a stabilizátorok triviálisak az orbit-stabilizátor tétel miatt, vagyis csak a fixpontmentes permutációkból válogathatunk. Így V-n kívül csak a négyesciklus által generált részcsoport megfelelő, ami (3)-at igazolja.

Mivel $V \leq A_4$, de a négyesciklus páratlan permutáció, a (2) esetben az f diszkriminánsa négyzetelem K-ban, a (3) esetben pedig nem az.

6.10.7. A 3.8.10. Gyakorlat szerint a harmadfokú g rezolvens gyökei $b/2$ és $\pm\sqrt{d}$. Előbbi K-beli, a másik kettő pedig pontosan akkor K-beli, ha d négyzetelem K-ban. Ebben az esetben a 6.10.6. Feladat (2) esete érvényes, és így a Galois-csoport a Klein-csoport, amivel az (1) állítást beláttuk.

Az f polinom gyökei

$$\alpha_{1,2} = \pm\sqrt{\frac{-b + \sqrt{b^2 - 4d}}{2}} \quad \text{és} \quad \alpha_{3,4} = \pm\sqrt{\frac{-b - \sqrt{b^2 - 4d}}{2}}.$$

Az $y^2 + by + d$ gyökei α_1^2 és α_3^2, ezért a gyökök és együtthatók összefüggése szerint $d = (\alpha_1\alpha_3)^2$. Mivel $b^2 - 4d$ e polinom diszkriminánsa, $b^2 - 4d = (\alpha_1^2 - \alpha_3^2)^2$. Innen

$$d(b^2 - 4d) = \left(\alpha_1\alpha_3(\alpha_1^2 - \alpha_3^2)\right)^2.$$

Vegyük még észre, hogy $2u_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4 = -\alpha_1^2 - \alpha_3^2 = b$, vagyis $u_1 \in K$.

Így $\sqrt{d} \notin K$ esetén a 6.10.6. Feladat (2) esete áll fönn, azaz G tranzitív részcsoportja az $\alpha_1, \alpha_3, \alpha_2, \alpha_4$ négyzet szimmetriacsoportjának (vagy $G = D_4$, vagy $G = \mathbb{Z}_4^+$). Jelölje φ a G csoportnak azt az elemét, amely a gyökökön az $(\alpha_1\alpha_3\alpha_2\alpha_4)$ ciklus (ez mindkét esetben benne van G-ben). A φ az $e = \alpha_1\alpha_3(\alpha_1^2 - \alpha_3^2)$ elemet önmagába viszi (hiszen $\varphi(\alpha_3) = \alpha_2 = -\alpha_1$). Ha a Galois-csoport $\mathbb{Z}_4^+$, akkor ezt φ generálja, és így G minden eleme fixálja e-t, vagyis $e \in K$, és így $d(b^2 - 4d)$ négyzetelem K-ban.

Tegyük most föl, hogy a Galois-csoport D_4. Ekkor benne van az a ψ elem is, amely a gyökökön az $(\alpha_1\alpha_2)$ transzpozíció. Ennél $\psi(e) = -e$. Az e nem lehet nulla, mert f

irreducibilitása miatt egyik gyöke sem nulla, és minden gyöke különböző. Ezért $\psi(e) \neq e$, és így $e \notin K$, vagyis $d(b^2 - 4d)$ nem négyzetelem K-ban.

6.10.8. A 3.8.7. Feladatban bizonyított összefüggéseket és az Útmutatóban bevezetett jelöléseket is állandóan használni fogjuk. Legyen $e = (\alpha_1+\alpha_2-\alpha_3-\alpha_4)/2$, ekkor $e^2 = 2u-b$ és $c = e(\alpha_1\alpha_2 - \alpha_3\alpha_4)$. Mivel $c \neq 0$, ezért e sem nulla.

Az Útmutatóban szereplő egyenlőség kiszámolásához egy vázlatot adunk. A 3.8.7. Feladatból tudjuk, hogy ha az u gyök segítségével bontjuk fel f-et két másodfokú tényezőre, akkor ezek a tényezők $(x - \alpha_1)(x - \alpha_2)$ és $(x - \alpha_3)(x - \alpha_4)$ lesznek. Végezzük is el a számolást: $L(x) = e^2x^2 - cx + (u^2 - d)$, és itt a főegyüttható nem nulla. Ezért L egyetlen gyöke $c/2e^2$, és így

$$f(x) = (x^2 + u)^2 - (ex - c/2e)^2 = (x^2 - ex + u - c/2e)(x^2 + ex + u + c/2e)\,.$$

A $x^2 - ex + u - c/2e$ diszkriminánsát felírva $(\alpha_1 - \alpha_2)^2 = e^2 - 4u - 2c/e$ és hasonlóan $(\alpha_3 - \alpha_4)^2 = e^2 - 4u + 2c/e$. Felhasználva, hogy $e^2 = 2u - b = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2/4$ az Útmutatóban felírt összefüggés adódik.

Legyen G az f Galois-csoportja. A 6.10.6. Feladat szerint G vagy $\mathbb{Z}_4^+$, vagy D_4. Az előző feladat megoldásához hasonlóan van G-ben olyan φ automorfizmus, amely az f gyökein az $(\alpha_1\alpha_3\alpha_2\alpha_4)$ ciklus. Legyen

$$t = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)\,.$$

Ezt az elemet φ fixen hagyja. Ha $G = \mathbb{Z}_4^+$, akkor G minden eleme fixen hagyja t-t, vagyis $t \in K$ és ezért $t^2 = (2u - b)(2u + b)^2 - 4c^2$ négyzetelem K-ban. Ha viszont $G = D_4$, akkor van olyan $\psi \in G$, amely a gyökökön az $(\alpha_1\alpha_2)$ transzpozíció. Ez a t elemet az ellentettjébe viszi, és mivel $t \neq 0$, a t elem nincsen K-ban, vagyis $(2u - b)(2u + b)^2 - 4c^2$ nem négyzetelem.

6.10.9. Az, hogy $\mathbb{Z}_3$ karakterisztikája három, mindent elront. Mivel $(x + c)^3 = x^3 + c^3$, az $x \mapsto x + c$ helyettesítés nem változtatja meg az x^2 együtthatóját, tehát az x^2-es tagot nem lehet így kiejteni.

A Cardano-képletbe nem lehet behelyettesíteni a nevezőben található 3 miatt, de a képlet levezetésének a módszere sem működik. Valóban, a 13. oldalon található (1.3) egyenletrendszer $uv = -3p$ egyenlete három karakterisztikában azt adja, hogy u és v egyike, mondjuk $v = 0$, az $u^3 + v^3 = -q$ egyenlet miatt tehát $u^3 = -q$, ahonnan $u = -q$, hiszen $\mathbb{Z}_3$-ban minden elem köbe önmaga. Így az egyenlet gyökére $-q$ adódik, ami csak $p = 0$ esetén lesz gyök, általában nem.

Végül ha veszünk egy harmadfokú irreducibilis polinomot, mondjuk $x^3 - x + 1$-et $\mathbb{Z}_3$ fölött, akkor ennek egyetlen β gyöke a GF(27) testet generálja, amiben a polinom többi gyöke is benne van, hiszen véges test minden véges bővítése normális. E test minden nem nulla eleme gyöke az $x^{26} - 1$ polinomnak, tehát $x^3 - x + 1$ gyökei mind 26-odik egységgyökök. Ezek azonban nem gyökkifejezések $\mathbb{Z}_3$ fölött a 6.9.8. Definíció értelmében! Ha ugyanis β az lenne, akkor létezne egy $\mathbb{Z}_3 = K_0 < K_1 < \ldots < K_n$ testlánc úgy, hogy $\beta \in K_n$, és mindegyik K_{i+1} egy $x^p - \alpha$ alakú irreducibilis polinom gyökével való bővítéssel kapható

K_i-ből, ahol p prím és $\alpha \in K_i$. Mivel β harmadfokú, e bővítések valamelyikének foka 3. De ez lehetetlen: az $x^3 - \alpha$ polinom egy véges, 3 karakterisztikájú test fölött nem lehet irreducibilis, mert véges testben a köbre emelés automorfizmus (a Frobenius-automorfizmus), és ezért minden elem a test egy elemének a köbe (vagyis a köbgyökvonás egyértelműen elvégezhető). Ha $\alpha = \gamma^3$, akkor $x^3 - \alpha = (x - \gamma)^3$.

6.10.10. A 6.8.17. Tétel szerint ha f valamelyik gyöke szerkeszthető, akkor f felbontási testének foka 2-hatvány, és megfordítva is, ha e felbontási test foka 2-hatvány, akkor f mindegyik gyöke szerkeszthető. A 6.10.6. Feladat szerint viszont az f felbontási testének foka akkor és csak akkor 2-hatvány, ha a harmadfokú rezolvensnek van gyöke K-ban.

11.7. Modulusok

7.1. Részmodulusok, homomorfizmusok.

7.1.2. Lásd 2.2.18. Gyakorlat (ide kapcsolódik a 2.2.36. Gyakorlat is).

7.1.5. A 4.4.20. Állítás bizonyítása lényegében szó szerint átvihető.

7.1.7. A mag részmodulus, mert ha $\varphi(m) = 0$, akkor $\varphi(rm) = r\varphi(m) = r0 = 0$. A faktormodulus szorzásának jóldefiniáltsága a következőképpen igazolható. Tegyük föl, hogy $a+N = b+N$, meg kell mutatni, hogy $ra+N = rb+N$. Ez azért igaz, mert $a-b \in N$-ből $ra - rb = r(a - b) \in N$ következik (hiszen N részmodulus). Az $m \mapsto m + N$ leképezés azért tartja az r-rel szorzást, mert $r(m + N) = rm + N$ a faktormodulus szorzásának definíciója miatt.

7.1.8. Az állításokat megfogalmazzuk, de bizonyításukat az Olvasóra hagyjuk (csak hivatkozunk az analóg csoport- és gyűrűelméleti tételekre). Ugyanezek a tételek még általánosabban is beláthatók (lásd 8.2.20. Feladat).

A csoportelméleti 4.5.19. Tétel és a gyűrűelméleti 5.2.11. Tétel moduluselméleti változata a következő. Tegyük föl, hogy $\varphi : M \to K$ szürjektív modulus-homomorfizmus, melynek magja N. Ekkor a következő állítások teljesülnek.

(1) Ha U tetszőleges részmodulusa M-nek, akkor $\varphi(U)$ részmodulusa K-nak, melynek teljes inverz képe M-ben az $U + N = N + U$ részmodulus.
(2) A K részmodulusai kölcsönösen egyértelmű megfeleltetésben állnak az M azon részmodulusaival, amelyek N-et tartalmazzák. Egy $V \leq K$ részmodulushoz az $U = \varphi^{-1}(V)$ teljes inverz kép tartozik. Ebben az esetben az M/U és a K/V faktormodulusok izomorfak.

Az első izomorfizmus-tétel szerint ha N és K részmodulusok az M modulusban, akkor az $N+K$ részcsoport is részmodulus (vö. 7.1.13. Gyakorlat), és $(N+K)/N \cong K/(K \cap N)$. A második izomorfizmus-tétel azt mondja ki, hogy ha $K \leq N \leq M$ részmodulusok, akkor

$(M/K)/(N/K) \cong M/N$. Végül a homomorfizmus-tétel állítása az, hogy ha $\varphi : M \to K$ modulus-homomorfizmus, akkor $\mathrm{Im}(\varphi) \cong M/\mathrm{Ker}(\varphi)$.

7.1.9. A modulus-axiómák mindegyik esetben könnyen ellenőrizhetők (arra is oda kell figyelni, hogy a műveletek jóldefiniáltak-e). Csak néhány példabizonyítást mutatunk.

A (3) pont $M(A, V)$ modulusában igazoljuk az $(fg)v = f(gv)$ szabályt. Ehhez meg kell mutatni, hogy $\big((fg)(A)\big)(v) = f(A)\big(g(A)(v)\big)$. Ez azért igaz, mert lineáris algebrából tudjuk, hogy $(fg)(A) = f(A)g(A)$ (ami azon múlik, hogy az A hatványai egymással felcserélhetők). Természetesen $f(A)g(A)$ kompozíciót jelöl.

A (4)-beli példa abban különbözik a 7.1.2. Gyakorlattól, hogy a $\mathbb{Z}_m$ alapgyűrűben modulo m kell végezni a műveleteket. Ez azonban nem okoz gondot, mert A exponense m, és így minden elemének m-szerese nulla. Így ha k és n olyan egész számok, amelyek kongruensek mod m, akkor $ka = na$ minden $a \in A$-ra. Ezt a példát a 7.3.15. Gyakorlatban általánosítjuk.

Végül a (6) példában az R elemeivel való szorzás azért értelmes a J halmazon, mert J balideál, és így $r \in R$ és $a \in J$ esetén $ra \in J$.

7.1.10. Tegyük föl, hogy N részmodulusa T^n-nek, és létezik egy $v \in N$ nem nulla vektor. Meg kell mutatni, hogy N minden T^n-beli vektort tartalmaz. Ez azért igaz, mert minden $w \in T^n$-hez létezik egy olyan A mátrix, amire $Av = w$ (például a lineáris algebra előírhatósági tétele miatt).

7.1.11. Ha a $t \in T$ elemet konstans polinomnak értjük, akkor $t(A) = tI$ (ahol I az identikus transzformáció). Ezért $tv = t(I)(v)$ (mint konstans polinommal való szorzás). De $t(I)(v) = tv$ (mint skalárral való szorzás). Ebből az észrevételből látszik, hogy minden részmodulus altér is egyben.

Ha $W \leq V$ egy részmodulus, akkor minden $w \in W$ esetén $xw \in W$. De $xw = A(w)$, és így W egy A-invariáns altér. Megfordítva, tegyük föl, hogy $W \leq V$ egy A-invariáns altér. Legyen $f(x) = t_0 + t_1x + \ldots + t_kx^k \in T[x]$ és $w \in W$. Ekkor

$$fw = (t_0I + t_1A + \ldots + t_kA^k)(w) = t_0w + t_1A(w) + \ldots + t_kA^k(w)\,.$$

Ez az elem W-ben van, hiszen W altér, és $A^i(w) \in W$ minden i-re. Valóban, $A(w) \in W$, innen $A^2(w) = A(A(w)) \in W$, és így tovább.

7.1.12. Nem izomorfak. Ha ugyanis létezne egy $\varphi : \mathbb{R} \to \mathbb{R}$ modulus-izomorfizmus e két modulus között, akkor minden $f \in \mathbb{R}[x]$ polinomra

$$\varphi(f(1)r) = \varphi(fr) = f\varphi(r) = f(2)\varphi(r)$$

teljesülne. Speciálisan az $f(x) = x - 2$ polinomra alkalmazva $\varphi(-r) = 0$ adódik, vagyis φ azonosan nulla (és így nem bijekció).

Valójában itt az $M(A, \mathbb{R})$ modulusokról van szó, ahol az A az első esetben az $frm[o]--\times$ 1-es (1) mátrix, a másodikban pedig a (2) mátrix. Ha az Olvasó előrelapoz, akkor egyszerűbb bizonyítást is találhat arra, hogy e két modulus nem izomorf. Ugyanis az első modulus exponense $x - 1$, a másodiké $x - 2$ (vö. 7.3.6. Definíció, 7.3.18. Gyakorlat).

7.1.13. Legyenek N és K részmodulusai az M modulusnak. Az általuk generált részmodulusban benne vannak az $n+k$ alakú elemek, ahol $n \in N$ és $k \in K$. Ezek már részmodulust alkotnak: a csoportelméletből tudjuk, hogy $N+K$ részcsoport, ha pedig $r \in R$, akkor $r(n+k) = rn + rk \in N+K$, hiszen $rn \in N$ és $rk \in K$. Vagyis $N+K$ a legszűkebb N-et és K-t tartalmazó részmodulus. Több összeadandó esetén a bizonyítás hasonló (de hivatkozhatunk a 7.1.5. Gyakorlatra is: a lineáris kombinációk egy M_i-be eső darabjai az M_i egyetlen elemévé vonhatók össze).

7.1.14. A φ leképezés jóldefiniáltságához azt kell ellenőrizni, hogy ha $f_1 + E = f_2 + E$, akkor $\varphi_0(f_1) = \varphi_0(f_2)$. Ez világos, hiszen ilyenkor $f_1 - f_2 \in E \subseteq \mathrm{Ker}(\varphi_0)$. A kapott φ összegtartó és skalárszoros-tartó, ez utóbbit látjuk be. A faktormodulusban a műveletet a reprezentánsokkal végezzük, és ezért $r \in R$ esetén

$$\varphi\big(r(f+E)\big) = \varphi(rf+E) = \varphi_0(rf) = r\varphi_0(f) = r\varphi(f+E)\,.$$

Az összegtartás hasonlóan igazolható.

7.2. Direkt összeg és függetlenség.

7.2.2. Csak a különbségeket mutatjuk meg a 4.8.13. Gyakorlat megoldásához képest. Az újdonság egyrészt az, hogy normálosztók helyett most részmodulusokról beszélünk, másrészt az, hogy végtelen sok tényező van. Az M_i^* nyilván részmodulus, és e részmodulusok összege azért az egész M, mert az M minden elemének csak véges sok komponense nem nulla. Ha tehát az $m = (\ldots, r_i, \ldots) \in M$ elemnek csak az első, hatodik és tizedik komponense nem nulla, akkor

$$m = (r_1, 0, \ldots) + (\ldots, 0, r_6, 0, \ldots) + (\ldots, 0, r_{10}, 0, \ldots)\,.$$

Vagyis $m \in M_1^* + M_6^* + M_{10}^*$. Az is világos, hogy M_i^* csak a nullában metszi a többi M_i^* összegét, hiszen ebben az összegben minden elem i-edik koordinátája nulla.

Most tegyük föl, hogy az M_i^* részmodulusokra teljesül az (1) és a (2). Tekintsük a

$$\varphi : (\ldots, r_i, \ldots) \mapsto \sum_{i \in I} r_i$$

leképezést az M_i^* modulusok direkt összegéből az M modulusba. Ez a definíció értelmes, mert az összegnek csak véges sok nem nulla tagja van. Megmutatjuk, hogy a φ leképezés R-izomorfizmus. A művelettartás nyilvánvaló. Mivel M minden eleme előáll véges sok M_i^*-beli elem összegeként, a φ szürjektív. Az injektivitáshoz azt kell belátni, hogy ha $\varphi(m) = 0$, akkor $m = 0$. Legyenek m nem nulla komponensei $r_{i_1}, \ldots, r_{i_n}$, ekkor

$$\varphi(m) = r_{i_1} + \ldots + r_{i_n} = 0\,, \quad \text{azaz} \quad r_{i_1} = -r_{i_2} - \ldots - r_{i_n}\,.$$

Ez azonban azt jelentené, hogy a $0 \neq r_{i_1}$ elem benne van $M_{i_1}^*$-ban is, és a többi M_j^* összegében is. Ez az ellentmondás bizonyítja az állítást.

7.2.3. A 7.2.2. Gyakorlat (2) feltétele (a megoldásból láthatóan) úgy fogalmazható, hogy ha $m_1, \ldots, m_k$ csupa különböző indexű M_i részmodulusnak az elemei, és $m_1 + \ldots + m_k = 0$, akkor $m_1 = \ldots = m_k = 0$. Ezért (1) és (2) ekvivalens. A (3) lényegében ugyanaz, mint a (2), csak azt az m_i helyett az $r_i m_i \in M_i$ elemre kell alkalmazni.

7.2.5. Vektortérben az $rm = 0$-ból $r = 0$ vagy $m = 0$ következik (sőt még ferdetest fölötti modulusban is, sőt általános modulusban is igaz, hogy ha r invertálható és $rm = 0$, akkor $m = 0$, lásd a 2.2.27. Tétel bizonyítását). Ezért egy nem nulla vektorokból álló gyengén független rendszer független lesz.

7.2.6. Az 1 generátorrendszer, és (mint minden egyelemű rendszer) gyengén független. A 3 és 4 generátorrendszer, mert $4 - 3 = 1$ kifejezhető vele. A gyenge függetlenség igazolásához tegyük föl, hogy $n \cdot 3 +_6 k \cdot 4 = 0$, azaz egészekre áttérve $6 \mid 3n + 4k$. Mivel $3n$ osztható hárommal, $4k$ is osztható 3-mal, de 3 és 4 relatív prímek, ezért $3 \mid k$. De ekkor $k \cdot 4 = 0$ a $\mathbb{Z}_6^+$ csoportban, és így $n \cdot 3$ is nulla. A $\mathbb{Z}_6^+$-nak nemhogy bázisa, de egyetlen független eleme sincs, hiszen minden b elemre $6b = 0$, de $6 \neq 0$.

7.2.7. A 6 nem tehető be $\mathbb{Z}_{12}^+$ gyenge bázisába. Ha ugyanis $6 = b_1, b_2, \ldots, b_n$ gyenge bázis lenne, akkor $3 = r_1 b_1 + \ldots + r_n b_n$, ahonnan 2-vel szorozva $-b_1 + 2r_2 b_2 + \ldots + 2r_n b_n = 0$ (hiszen $b_1 = 6$ miatt $2r_1 b_1 = 0$, és $-b_1 = 2 \cdot (-3)$). Ez ellentmond a gyenge függetlenségnek, hiszen $-b_1 = 6$ nem nulla.

7.2.8. A 7.2.2. Gyakorlat (1) feltétele azzal ekvivalens, hogy m_i $(i \in I)$ generátorrendszer, a (2) feltétel pedig azzal, hogy m_i gyengén független (vö. 7.2.3. Gyakorlat).

7.2.10. Ha m_i $(i \in I)$ független, akkor nyilván gyengén független. Ha $rm_i = 0$, akkor ebből a függetlenség miatt $r = 0$, vagyis m_i rendje nulla. Megfordítva, ha m_i gyengén független, és minden elemének rendje nulla, akkor az $r_1 m_1 + \ldots + r_k m_k = 0$ összefüggésből a gyenge függetlenség miatt $r_i m_i = 0$ következik minden i-re. Mivel m_i rendje nulla, innen $r_i = 0$.

7.2.11. A $J \subseteq R$ pontosan akkor részmodulus, ha részcsoport, és $r \in R$, $a \in J$ esetén $ra \in J$. Itt az ra modulus-szorzat ugyanaz, mint az R gyűrűbeli ra szorzat, mert így definiáltuk az ${}_R R$ modulust. Így pontosan a balideál fogalmát kaptuk (5.1.6. Definíció).

7.2.12. Az összegtartás a 7.1.1. Definíció (2) axiómájából következik. Ha $r, s \in R$ és $m \in M$, akkor az, hogy φ tartja az s-sel szorzást, azt jelenti, hogy $s\varphi(r) = \varphi(sr)$, vagyis hogy $s(rm) = (sr)m$, ez pedig a (3) modulus-axióma.

7.2.14. Nyilván $r_1 e_1 + \ldots + r_n e_n = (r_1, \ldots, r_n)$, ahonnan könnyen látszik, hogy $e_1, \ldots, e_n$ generátorrendszer és független is. Végtelen sok tagú összeg esetén az e_i azt az elemet jelenti, amelynek az i-edik komponense 1, a többi nulla. Ezek (véges) lineáris kombinációi pont a $\bigoplus_{i \in I} {}_R R$ direkt összeg elemei. A függetlenség közvetlenül is triviális, és következik a 7.2.8. Gyakorlatból is.

7.2.16. Igen, ha $(0, 0) = k(1, 2) + n(1, 1) = (k + n, 2k + n)$, akkor az első komponensből $2 \mid k + n$, a másodikból $4 \mid 2k + n$. Így n páros, ezért k is, de akkor $4 \mid 2k$, azaz $4 \mid n$. Tehát $k(1, 2) = n(1, 1) = (0, 0)$.

7.2.17. Igen, sőt $\{(1, 0), (k, 1)\}$ is bázis minden k egészre (vö. 7.4.3. Gyakorlat).

7.2.18. Tegyük föl, hogy M az M_i részmodulusok direkt összege, és legyen $\mathbf{b}$ a $\mathbf{b}_i$ vektorrendszerek uniója. A 7.2.2. Gyakorlat miatt $\mathbf{b}$ generátorrendszer M-ben. Vegyük a $\mathbf{b}$ elemeinek egy (véges) lineáris kombinációját, ami nulla, és az összeg tagjait csoportosítsuk aszerint, hogy az egyes tagok melyik M_i modulusból valók. A 7.2.3. Gyakorlat miatt ezek a rész-összegek is nullával egyenlőek, és így a $\mathbf{b}_i$ (gyenge) függetlenségét tagonként alkalmazhatjuk.

Megfordítva, tegyük föl, hogy $\mathbf{b}$ gyenge bázis. Ekkor generátorrendszer is, és ezért az M_i modulusok generálják M-et. A 7.2.3. Gyakorlat feltétele könnyen adódik a $\mathbf{b}$ gyenge függetlenségéből.

7.2.19. A kicserélési tételt elsősorban annak megmutatására használjuk, hogy az F elemszáma legfeljebb akkora, mint a G elemszáma. Ehhez az kell, hogy egy-egy kicserélés során F elemszáma ne csökkenjen. Ha F-et halmaznak tekintjük, akkor a kicseréléskor csökkenhet az elemszáma abban az esetben, ha a g elem már benne volt az $F - \{f\}$-ben. Ha rendszerekkel fogalmazzuk az állítást, akkor ez nem okoz bajt, mert egy független rendszernek nem lehet két egyforma eleme, és így ilyen g-t nem választhatunk. Ha halmazokkal fogalmazunk, akkor azt kell megkövetelni, hogy minden $f \in F$-hez létezzen olyan $g \in G$, amely *nincs benne* $F - \{f\}$*-ben*, és $(F - \{f\}) \cup \{g\}$ független.

7.2.20. Ferdetest fölött igaz, hogy ha $r_1 b_1 + \ldots + r_n b_n = 0$, akkor mindegyik olyan b_i kifejezhető a többiek lineáris kombinációjaként, amelynek az r_i együtthatója nem nulla (mert szorozhatunk balról r_i inverzével). Az pedig tetszőleges modulusban teljesül, hogy ha Y lineárisan függ X-től (azaz $Y \subseteq \langle X \rangle$), és Z függ Y-tól, akkor Z függ X-től is (hiszen $Z \subseteq \langle Y \rangle \subseteq \langle X \rangle$). Ebből a két tulajdonságból következik, hogy minden minimális generátorrendszer független (azaz bázis), és a kicserélési tétel (lásd 7.2.19. Gyakorlat) is.

7.2.21. Az Útmutatóban megadott u és v vektorok egy-egy A-invariáns alteret (valójában sajátalteret) generálnak, hiszen $A(v) = v \in \langle v \rangle$ és $A(w) = -w \in \langle w \rangle$. Így ez a két altér részmodulus (7.1.11. Gyakorlat), és a direkt összegük a sík, ez adja a kívánt felbontást. Ha a tükrözés helyett a $+90$ fokos forgatást vesszük, akkor ennek nincs nemtriviális invariáns altere (mert minden nem nulla vektor független az elforgatottjától, és így ezek ketten az egész síkot generálják). Ezért csak triviális részmodulusok vannak (vagyis ez egy egyszerű modulus).

7.3. Elem rendje modulusban.

7.3.2. Nyilván $rm = 0$ pontosan akkor, ha $0 = \varphi(rm) = r\varphi(m)$. Ezért $O(m) = O\big(\varphi(m)\big)$.

7.3.3. A „bolhás” feladat (1.5.8. Feladat) megoldását követjük. Az $O(rm)$ elemei azok a $t \in R$ elemek, melyekre $trm = 0$, vagyis $tr \in O(m)$. De

$$trm = 0 \iff o(m) \mid tr \iff \frac{o(m)}{(o(m), r)} \,\Big|\, t$$

(ugyanúgy, mint egész számokra.)

7.3.5. Ugyanaz a számolás, mint az 5.3.7. Lemma bizonyítása (most X részhalmaza a modulusnak, a és r pedig gyűrűelemek).

7.3.7. Ha az exponens e, akkor $em = 0$ minden m moduluselemre. Tehát e minden modulus-elemnek „jó együtthatója”, és így minden elem rendjének többszöröse. Megfordítva, az elemrendek f legkisebb közös többszöröse minden elemet nullába szoroz, ezért az exponensnek többszöröse. Így e és f egymás osztói. A legkisebb közös többszörös „nem létezése” csak annyit jelent, hogy nincs olyan nullától különböző gyűrűelem, amely mindegyik elemrendnek osztója volna, és ilyenkor a modulus annullátora csak a $\{0\}$, vagyis az exponense is nulla.

7.3.8. Ha m generálja az M modulust, akkor m képe generálja M homomorf képeit, tehát (3) igaz. Az ${}_RR$ ciklikus, mert az 1 generálja. Így minden faktormodulus is ciklikus. Megfordítva, ha $\langle m \rangle$ ciklikus, akkor a $\varphi : r \mapsto rm$ modulus-homomorfizmus szürjektív ${}_RR$-ből $\langle m \rangle$-re, és így a homomorfizmus-tétel miatt $\langle m \rangle$ izomorf ${}_RR$ egy faktorával. Ennek a homomorfizmusnak a magja pontosan $O(m)$. Ezért ha két ciklikus modulust egyenlő (vagy asszociált) rendű elemek generálnak, akkor ezek egymással izomorfak (mert mindkettő az ${}_RR$ ugyanazon faktorával izomorf).

Legyen m_1 és m_2 az M modulus két generátoreleme. Ekkor $sm_1 = m_2$ alkalmas $s \in R$ elemre. Ha $rm_1 = 0$, akkor R kommutativitása miatt $rm_2 = rsm_1 = srm_1 = s0 = 0$. Ezért $O(m_1) \subseteq O(m_2)$. Hasonlóan adódik az $O(m_2) \subseteq O(m_1)$ tartalmazás is, vagyis m_1 és m_2 rendje egyenlő.

> Ebben a gondolatmenetben csak R kommutativitását használtuk föl. Egy másik bizonyítást nyerhetünk, ha alkalmazzuk a hatvány (pontosabban a többszörös) rendjének képletét (7.3.3. Gyakorlat), amiből következik, hogy m_1 és m_2 rendjei osztják egymást. Ez azonban csak főideálgyűrű fölött működik (mert itt az elem rendjéről mint gyűrűelemről, és nem mint ideálról beszélünk). Az előző gondolatmenetből látszik általában, hogy $O(sm) \supseteq O(m)$ minden kommutatív gyűrű fölötti modulusban.

Beláttuk tehát, hogy ugyanannak a ciklikus modulusnak bármely két generátora egyenlő rendű. Tegyük föl, hogy φ izomorfizmus az $\langle m_1 \rangle$ és $\langle m_2 \rangle$ modulusok között. Ekkor $\varphi(m_1)$ generálja $\langle m_2 \rangle$-t, és mivel az elemrend izomorfizmusnál megőrződik, a rendjük ugyanaz. De m_2 és $\varphi(m_1)$ rendje is ugyanaz (mert ezek ugyanannak a ciklikus modulusnak a generátorai). Ezzel az (1) állítást igazoltuk.

Az ${}_RR/(r)$ modulusban az $1 + (r)$ rendje (r), hiszen $s\big(1 + (r)\big) = s + (r)$ akkor és csak akkor nulla, ha $s \in (r)$. Így (2) is igaz. Végül a (4) bizonyításához az Útmutatóban használt ötlettel látjuk, hogy $\langle m \rangle$ minden részmodulusa ciklikus. A 7.1.8. Gyakorlatot a

$\varphi : r \mapsto rm$ homomorfizmusra alkalmazva azt kapjuk, hogy $\langle m \rangle$ részmodulusai kölcsönösen egyértelmű megfeleltetésben állnak az ${}_R R$ modulusnak az $O(m) = (o(m))$ ideált tartalmazó részmodulusaival. Mivel R (kommutatív) főideálgyűrű, ezek ideálok, és így $o(m)$ osztóinak felelnek meg (5.5.4. Lemma). Megjegyezzük, hogy ebből a második állításból is következik, hogy minden részmodulus ciklikus (hiszen főideálnak, azaz ciklikus modulusnak homomorf képe).

Végül ciklikus modulusban minden elem rendje osztója a generátorelem rendjének a hatvány rendjének képlete miatt, ezért (5) is igaz (hiszen a 7.3.7. Gyakorlat miatt az exponens az elemrendek legkisebb közös többszöröse).

7.3.9. Az alábbiak elolvasása előtt érdemes átismételni a felsorolt állítások csoportelméleti megfelelőinek bizonyítását. Az (1) azért igaz, mert $r(\ldots, m_i, \ldots)$ akkor és csak akkor nulla, ha $rm_i = 0$ mindegyik i-re. A (2) az (1)-ből következik, hiszen az exponens az elemrendek legkisebb közös többszöröse (és a direkt összeg elemeinek komponensei között mindegyik modulus mindegyik eleme előfordul). Most belátjuk a (4) állítást (amelynek (3) persze speciális esete).

Tudjuk, hogy R alaptételes. A $v_1, \ldots, v_k$ együttvéve relatív prímek. Valóban, ha egy p prím mindegyik v_i-nek osztója, akkor $p \mid u$, vagyis $p \mid u_i$ valamelyik i-re. De $p \mid v_i$ miatt p osztója valamelyik i-től különböző indexű u_j-nek is (hiszen v_i ezek szorzata), ami lehetetlen, mert u_i és u_j relatív prímek. Ezért a $(v_1, \ldots, v_k)$ ideál az egész R, vagyis (az 5.1.9. Állítás miatt) vannak olyan $r_i \in R$ elemek, hogy $r_1 v_1 + \ldots + r_k v_k = 1$. Ekkor

$$m = (r_1 v_1 + \ldots + r_k v_k)m = r_1(v_1 m) + \ldots + r_k(v_k m)\,.$$

Ez azt jelenti, hogy $\langle m \rangle \subseteq \langle v_1 m \rangle + \ldots + \langle v_k m \rangle$. A fordított tartalmazás nyilvánvaló, hiszen $v_i m \in \langle m \rangle$. Ezért már csak azt kell megmutatni, hogy a $v_1 m, \ldots, v_k m$ elemek gyengén függetlenek (a 7.2.8. Gyakorlat miatt). Tegyük föl, hogy $s_1 v_1 m + \ldots + s_k v_k m = 0$. Ekkor $o(m) = u$ osztója $s_1 v_1 + \ldots + s_k v_k$-nak. Mivel $u_i \mid v_j$ ha $j \neq i$, innen kapjuk, hogy $u_i \mid s_i v_i$. De u_i és v_i relatív prímek, ezért $u_i \mid s_i$. Ekkor viszont $u = u_i v_i \mid s_i v_i$, ahonnan $s_i v_i m = 0$ (hiszen az m rendje u). Tehát a $v_i m$ elemek tényleg gyengén függetlenek. A hatvány rendjének képlete miatt $o(v_i m) = u/v_i = u_i$, és ezzel a (4) állítást beláttuk.

Hátra van még az (5) bizonyítása. Ha r és s relatív prímek, akkor a (3) állítás miatt az rs rendű ciklikus modulus tényleg izomorf az r rendű és az s rendű ciklikus modulusok direkt szorzatával. Sőt általában ha $u = u_1 \ldots u_k$, ahol $u_1, \ldots, u_k$ páronként relatív prímek, akkor az u rendű ciklikus modulus is izomorf az $u_1, \ldots, u_k$ rendű modulusok direkt szorzatával a (4) miatt. Ezt úgy is fogalmazhatjuk, hogy páronként relatív prím rendű ciklikus modulusok direkt szorzata is ciklikus.

Megfordítva, tegyük föl, hogy M az r rendű, N pedig az s rendű ciklikus modulus, és az $M \times N$ modulus ciklikus, generálja az (m, n) elem. Persze akkor $M = \langle m \rangle$ és $N = \langle n \rangle$, mert a projekció-homomorfizmusoknál generátorelem képe generátorelem lesz. Ezért m rendje r és n rendje s. Mivel $\langle (m, n) \rangle = M \times N$, van olyan $u \in R$, hogy $u(m, n) = (m, 0)$. Innen $(u - 1)m = 0$ és $un = 0$, vagyis $r \mid u - 1$ és $s \mid u$. De akkor (r, s) osztója $u - 1$-nek is és u-nak is, ezért r és s relatív prímek.

Tegyük föl végül, hogy $M_1 \times \ldots \times M_k$ ciklikus modulus. Ekkor ezt M_1 és $N = M_2 \times \ldots \times M_k$ direkt szorzatának is felfoghatjuk. Mivel ciklikus modulus homomorf képe ciklikus, a projekciókra alkalmazva látjuk, hogy M_1 és N is az. Az előző bekezdésben látottak miatt a rendjeik relatív prímek. Így k szerinti indukcióval beláttuk, hogy az M_i páronként relatív prím rendű ciklikus modulusok.

7.3.11. Legyen T az M torzió-részmodulusa. Ha $a, b \in T$, akkor $ra = 0$ és $sb = 0$ alkalmas r, s nem nulla gyűrűelemekre. De akkor rs sem nulla, és $(rs)(a \pm b) = 0$. Ezért $a \pm b \in T$. Ugyanígy látható be, hogy T zárt az R elemeivel való szorzásra is.

Ha $c + T$ az M/T tetszőleges eleme, és $r(c + T)$ nulla, akkor $rc \in T$, azaz van olyan $s \neq 0$, hogy $s(rc) = 0$. Ezért $c \in T$, vagyis $c+T$ is nulla. Ezzel igazoltuk, hogy M/T-ben csak a nulla elem rendje lehet nem nulla.

7.3.13. A $\mathbb{Z}_n^+[m]$ részcsoportban azok a k elemek vannak, amelyek rendje osztója m-nek. Mivel $k \in \mathbb{Z}_n^+$, a k rendje osztója n-nek is, ezért osztója az (m, n) legnagyobb közös osztónak. Az ilyen elemek egy (m, n) rendű ciklikus részcsoportot alkotnak a 4.3.18. Állítás miatt. Ezért $\mathbb{Z}_n^+[m] \cong \mathbb{Z}_{(m,n)}^+$.

Tekintsük a $\varphi : x \mapsto mx$ homomorfizmust $\mathbb{Z}_n^+$-ből $\mathbb{Z}_n^+$-ba. Ennek magja $\mathbb{Z}_n^+[m]$, a képe $m\,\mathbb{Z}_n^+$. A homomorfizmus-tétel miatt így $m\,\mathbb{Z}_n^+$ elemszáma ugyanaz, mint $\mathbb{Z}_n^+ / \mathbb{Z}_n^+[m]$ elemszáma, vagyis $n/(n, m)$. De akkor $\mathbb{Z}_n^+ / m\,\mathbb{Z}_n^+$ elemszáma (n, m). Ez ciklikus csoport, tehát $\mathbb{Z}_n^+ / m\,\mathbb{Z}_n^+ \cong \mathbb{Z}_{(m,n)}^+$.

7.3.14. A számolások nyilvánvalóak, az R kommutativitása ahhoz kell, hogy részmodulust kapjunk (és ne csak részcsoportot).

7.3.15. Az $\big(s + (r)\big)m = sm$ jóldefiniáltsága azt jelenti, hogy ha $s_1 + (r) = s_2 + (r)$, akkor $s_1 m = s_2 m$. Ez azért igaz, mert ilyenkor $r \mid s_1 - s_2$, és $rm = 0$. A modulus-axiómák triviálisan teljesülnek. Ugyanezt a gondolatot speciális esetben már láttuk a 4.8.29. Feladatban.

Legyen $\overline{s_i} = s_i + (r)$. Ekkor $\overline{s_1}m_1 + \ldots + \overline{s_k}m_k = s_1 m_1 + \ldots + s_k m_k$. Speciálisan az R és az $R/(r)$ fölött „ugyanazok” a lineáris kombinációk egyenlők nullával, és így a gyenge függetlenség is ugyanazt jelenti.

> Vigyázzunk, a függetlenség nem ugyanaz R és $R/(r)$ fölött! Ez utóbbi ugyanis már nem csak lineáris kombinációkról szóló állítás, mint a gyenge függetlenség. Az $s_i m_i = 0$ ekvivalens azzal, hogy $\overline{s_i} m_i = 0$, de természetesen az $s_i = 0$ nem ekvivalens azzal, hogy $\overline{s_i} = 0$. Például a $\mathbb{Z}_6^+$ csoportban $\{3, 4\}$ gyengén független $\mathbb{Z}$ és $\mathbb{Z}_6$ fölött is. Ez a rendszer független is $\mathbb{Z}_6$ fölött, de nem független $\mathbb{Z}$ fölött (vö. 7.2.6. Gyakorlat).

Végül N akkor és csak akkor részmodulusa M-nek $R/(r)$ fölött, ha minden $s \in R$ és $n \in N$ esetén $\big(s + (r)\big)n \in N$. De ez a szorzat pont sn, tehát ez a feltétel azzal ekvivalens, hogy N részmodulus R fölött.

7.3.16. Mivel $A^2 = I$, minden $v \in V$ vektorra $(x^2 - 1)v = 0$. Ezért v rendje az $x^2 - 1$ polinomnak osztója. A normált osztók $1, x-1, x+1, x^2-1$. Az 1 pontosan a nullvektornak a rendje. A v rendje akkor és csak akkor $x - 1$, ha $v \neq 0$, de $(x - 1)v = 0$, vagyis ha $Av = v$. Ezek az $y = x$ egyenes vektorai (vö. 7.2.21. Feladat). Ugyanígy pontosan az $y = x$-re merőleges egyenes nem nulla vektorainak lesz $x+1$ a rendje, a többi vektor rendje tehát csak $x^2 - 1$ lehet. A modulus exponense így $x^2 - 1$ (ami az A minimálpolinomja). A modulus ciklikus, hiszen mindegyik $x^2 - 1$ rendű v eleme generálja, ilyenkor v és $Av = xv$ például bázist alkot.

Általában $M(A, V)$ akkor lesz ciklikus, ha van olyan v vektor, hogy fv alakban V minden eleme fölírható (ahol $f \in \mathbb{R}[x]$). Mivel V kétdimenziós, ehhez elegendő, hogy v és $xv = Av$ független legyen (mert akkor ez bázis is, és $(\lambda x + \mu)v$ alakban minden vektort megkapunk). Ha tehát $M(A, V)$ nem ciklikus, akkor A-nak V minden vektora sajátvektora kell, hogy legyen, vagyis a sajátalterek uniója az egész V. Mivel A-nak csak legfeljebb két sajátaltere lehet (hiszen V kétdimenziós, és így A karakterisztikus polinomja másodfokú), e két altér uniója csak akkor lehet az egész V, ha valamelyik V-vel egyenlő (4.4.34. Gyakorlat). Vagyis van olyan $\lambda \in \mathbb{R}$, hogy $Av = \lambda v$ minden v-re (tehát A nyújtás). Megfordítva, egy nyújtáshoz tartozó modulus nem ciklikus, mert minden vektor benne van egy egydimenziós invariáns altérben, vagyis részmodulusban (7.1.11. Gyakorlat). Összefoglalva: ha V kétdimenziós, akkor $M(A, V)$ akkor és csak akkor ciklikus, ha A nem nyújtás.

7.3.17. Egyszerű számolás mutatja, hogy az u, $xu = Au \in \langle u \rangle$, és $x^2u = A^2u \in \langle u \rangle$ vektorok lineárisan függetlenek, tehát vektortér-bázist alkotnak V-ben. Ezért u generálja az M modulust. (A 7.1.11. Gyakorlat szerint ugyanis az M által generált részmodulus altér is, vagyis a fenti három vektor lineáris kombinációit is tartalmazza). Nyilván

$$\lambda_1 u + \lambda_2 Au + \lambda_3 A^2 u = (\lambda_1 + \lambda_2 x + \lambda_3 x^2)u$$

(ezért elég a legfeljebb másodfokú polinomokat használni). Most meghatározzuk, hogy az u rendje (vagyis az M ciklikus modulus rendje, vö. 7.3.8. Feladat) melyik polinom.

Az A karakterisztikus polinomja $f(x) = -x(1 - x)^2$ (hiszen ez egy felső háromszögmátrix). Így $f(A) = 0$ (ez közvetlen számolással látható, vagy a Cayley-Hamilton tétel segítségével). De akkor $fu = f(A)(u) = 0$, és így u rendje osztója f-nek. Valódi osztó azonban nem lehet, mert ez legfeljebb másodfokú lenne, és ha

$$gu = (\lambda_1 + \lambda_2 x + \lambda_3 x^2)u = 0\,,$$

akkor $\lambda_1 u + \lambda_2 Au + \lambda_3 A^2 u = 0$, ahonnan az u, Au és A^2u függetlensége miatt mindegyik λ_i nulla, azaz $g = 0$. Tehát u rendje f. Szokás a rendet normált polinomnak venni, ekkor $x(x - 1)^2$ adódik.

Az eddigiekből következik, hogy $x(x - 1)^2$ egyúttal az A minimálpolinomja is. Valóban, ha ez a minimálpolinom m_A, akkor $m_A(A) = 0$ miatt $m_A u = 0$, és így $f = o(u) \mid m_A$. Másrészt láttuk, hogy $f(A) = 0$, és így $m_A \mid f$. Természetesen $x(x - 1)^2$ egyúttal az M exponense is, a 7.3.8. Gyakorlat (5) pontja miatt.

A 7.3.8. Feladat (4) pontja miatt az M részmodulusai kölcsönösen egyértelmű megfeleltetésben állnak az u rendjének, vagyis az $x(x-1)^2$ polinomnak a normált osztóival. Ezek száma a (3.1.20. Gyakorlat (2) pontja miatt) hat. Ha $g \mid x(x-1)^2$, akkor a hozzá tartozó részmodulus $\langle gu \rangle$ lesz, ez leolvasható a 7.3.8. Feladat megoldásából.

7.3.18. Tegyük fel, hogy $v \in M(A, V)$ rendje nulla. Ekkor az $1v, xv, x^2v, \ldots$ elemek lineárisan függetlenek, hiszen ha lenne közöttük egy lineáris összefüggés, mondjuk

$$0 = t_0(1v) + t_1(xv) + \ldots + t_k(x^k v) = (t_0 + t_1 x + \ldots + t_k x^k)v\,,$$

akkor, mivel v rendje nulla, $t_0 + t_1 x + \ldots + t_k x^k = 0$, de egy polinom csak akkor nulla, ha minden együtthatója nulla, vagyis a fenti lineáris kombináció triviális. Egy véges dimenziós vektortérben azonban nem lehet végtelen sok független vektor. Ezért v rendje nem lehet nulla.

Annak megmutatásához, hogy $M = M(A, V)$ exponense az A minimálpolinomjának asszociáltja, azt kell észrevenni, hogy ezek ugyanannak az ideálnak a generátorelemei. Hiszen az A minimálpolinomja esetében

$$(m_A) = \{f \in T[x] \,:\, f(A) = 0\}\,,$$

az e exponens esetében pedig

$$(e) = \operatorname{ann}(M) = \{f \in T[x] \,:\, fv = 0 \text{ minden } v \in V\text{-re}\}\,.$$

De $0 = fv = f(A)(v)$ minden v-re pontosan akkor teljesül, ha $f(A) = 0$. Tehát a fenti két ideál tényleg ugyanaz.

7.3.19. A faktormodulus definíciója miatt $r(b + M[p]) = rb + M[p]$ akkor és csak akkor nulla az $M/M[p]$ faktormodulusban, ha $rb \in M[p]$. Ez azzal ekvivalens, hogy $prb = 0$, vagyis hogy $o(b) \mid pr$.

Ha b rendje nulla, akkor innen $r = 0$, vagyis ekkor $b + M[p]$ rendje is nulla. Ha $o(b)$ nem nulla, de nem osztható p-vel, akkor $o(b) \mid r$ (hiszen ekkor $o(b)$ és p relatív prímek). Ezért ilyenkor a $b + M[p]$ „jó" együtthatói pontosan az $o(b)$ többszörösei, vagyis $b + M[p]$ rendje $o(b)$. Végül ha $p \mid o(b)$, akkor $o(b) \mid pr$ azzal ekvivalens, hogy $o(b)/p$ osztója r-nek, és így $b + M[p]$ rendje $o(b)/p$.

7.3.20. Az M_p azért zárt az összeadásra, mert két p-hatvány legkisebb közös többszöröse is p-hatvány. Az, hogy M az M_p részmodulusok összege, abból következik, hogy M minden elemét föl lehet bontani prímhatványrendű elemek összegére. Ez a 7.3.9. Gyakorlat (4) állításának speciális esete, amikor az u_i elemek az u elemnek a prímhatvány-osztói.

Végül annak bizonyításához, hogy az M_p modulusok összege direkt összeg, a 7.2.3. Gyakorlatot használjuk. Tegyük föl, hogy $m_i \in M_{p_i}$ és $m_1 + \ldots + m_k = 0$. Az m_1 rendje legyen $p_1^{\alpha_1}$. Ezzel szorozva $p_1^{\alpha_1} m_2 + \ldots + p_1^{\alpha_1} m_k = 0$ adódik. Ez már egy rövidebb összeg, tehát (k szerinti indukcióval bizonyítva) azt kapjuk, hogy mindegyik tagja nulla. Ez azt jelenti, hogy $o(m_i) \mid p_1^{\alpha_1}$. De m_i rendje relatív prím $p_1^{\alpha_1}$-hez (mert $m_i \in M_{p_i}$, és p_i nem asszociáltja p_1-nek). Ezért $o(m_i) = 1$, azaz $m_i = 0$ minden $i \geq 2$-re. Persze akkor az eredeti összefüggésből $m_1 = 0$.

7.3.21. Az állításokat már beláttuk a 7.3.8. Gyakorlat megoldásában.

7.3.22. Álljon M_i azokból a mátrixokból, amelyeknek az i-edik oszlop kivételével mindegyik eleme nulla. Ezek balideálok, és a csoportelméleti direkt összegük $T^{n\times n}$. A lineáris transzformációk nyelvén ez a következőképpen mondható el. Legyen $e_1, \ldots, e_n$ a T^n szokásos bázisa, ekkor M_i azokból a transzformációkból áll, amelyek az e_i kivételével mindegyik e_j vektort a nullába viszik (ebből látszik, hogy M_i balideál). Az M_i egyszerű R-modulus (vagyis minimális balideál), mert ha $0 \neq A, C \in M_i$, akkor az előírhatósági tétel miatt könnyen konstruálhatunk egy olyan D lineáris transzformációt, melyre $DA = C$ (mert ehhez csak az kell, hogy $DA(e_i) = C(e_i)$ teljesüljön).

Az M_i modulusok páronként izomorfak lesznek. Legyen ugyanis A_{ij} az a (bijektív) lineáris transzformáció, amely kicseréli e_i-t e_j-vel, és a többi e_k bázisvektort önmagába viszi. Ekkor $A \in M_i$ akkor és csak akkor, ha $AA_{ij} \in M_j$, és könnyen ellenőrizhető, hogy $A \mapsto AA_{ij}$ modulus-izomorfizmus M_i-ről M_j-re. Megjegyezzük, hogy az M_i modulusok izomorfiája a 7.3.26. Feladatból is következik.

7.3.23. Tekintsük az $\{N\} \cup \{M_i \ : \ i \in I\}$ halmaz azon részhalmazait, amelyek függetlenek, és N-et tartalmazzák. A Zorn-lemma miatt ezek között van maximális, mondjuk $\{N\} \cup \{M_j \ : \ j \in I'\}$. Legyen $K = \sum\{M_j \ : \ j \in I'\}$, ez persze direkt összeg, miként $N + K$ is az. Ha $i \in I$, akkor M_i egyszerűsége miatt vagy $M_i \subseteq N + K$, vagy $M_i \cap (N + K) = \{0\}$. Az utóbbi eset ellentmond az $\{N\} \cup \{M_j \ : \ j \in I'\}$ halmaz maximalitásának. Ezért $N + K = M$.

7.3.24. Az (1) állítás faktorokra vonatkozó része igaz, mert egyszerű modulus homomorf képe egyszerű, vagy nulla. Ha N része M-nek, akkor az előző feladat miatt direkt összeadandó, és ha $M = N \oplus K$, akkor $N \cong M/K$, azaz teljesen reducibilis. A (2) bizonyításához legyen M/N egyszerű. Ekkor (1) miatt $M = N \oplus K$ alkalmas K-ra, azaz $M/N \cong K$. Így elég részmodulusra bizonyítani. Legyen $N \leq M$ egyszerű részmodulus. Az előző feladat miatt $M = N \oplus K$, ahol $K = \sum\{M_j \ : \ j \in I'\}$. Mivel $K < M$, van olyan $i \in I$, hogy $M_i \not\subseteq K$. Ekkor $M = K \oplus M_i$, hiszen $M/K \cong N$ egyszerű, és ezért $N \cong M/K \cong M_i$.

7.3.25. A szabad R-modulusok teljesen reducibilisek, hiszen ezek ${}_RR$ diszkrét direkt hatványai. De minden R-modulus egy szabadnak homomorf képe, ezért az előző gyakorlat miatt teljesen reducibilis.

7.3.26. Legyen $r \in R$, ekkor az r elemmel való jobbszorzás, vagyis az $s \mapsto sr$ leképezés egy ${}_RR \to {}_RR$ modulus-homomorfizmus. Így ${}_R(Jr)$ vagy nulla, vagy izomorf ${}_RJ$-vel. Másrészt $I = \sum\{Jr \ : \ r \in R\}$ kétoldali ideál, és így R egyszerűsége miatt $I = R$, azaz ${}_RR$ teljesen reducibilis. Legyen M egyszerű R-modulus, és $0 \neq m \in M$. Ekkor $\langle m \rangle = M$, ezért az $r \mapsto rm$ homomorfizmus szürjektív, azaz M faktora ${}_RR$-nek. Így az előző gyakorlat (2) pontja miatt M izomorf ${}_RJ$-vel.

7.3.27. Legyen $R = A_1 \times \cdots \times A_k$ a teljes mátrixgyűrűk direkt szorzatára való felbontás, és J_i az A_i egy minimális balideálja (7.3.22. Feladat). Mivel $j \neq i$ esetén $A_j J_i = 0$, ezért ${}_R J_i$ is egyszerű modulus, az A_i minimális balideáljai mint R-modulusok is izomorfak, és ${}_R J_i$ nem izomorf ${}_R J_j$-vel (hiszen A_i másképp hat rajtuk). Ezért ha ${}_R R$-et előállítjuk az összes A_i összes minimális balideáljainak összegeként, akkor éppen k-féle izomorfiatípus fog szerepelni. A 7.3.24. Gyakorlat (2) pontja és a 7.3.26. Feladat miatt R felett pontosan k-féle egyszerű modulus van.

7.3.28. Jelölje J az ${}_R R$ minimális balideáljainak összegét (ha nincs ilyen, akkor $J = 0$). A Krull-tétel bizonyításához (260. oldal) hasonlóan látjuk, hogy ha $J \neq R$, akkor J része egy K maximális balideálnak. Ez direkt összeadandó, vagyis ${}_R R = K \oplus N$ alkalmas N balideálra. Mivel K maximális, ${}_R R/K \cong N$ egyszerű modulus, vagyis minimális balideál. Ezért $N \subseteq J \subseteq K$, ami ellentmondás, azt mutatja, hogy $J = R$, vagyis hogy ${}_R R$ teljesen reducibilis.

7.4. Végesen generált modulusok.

7.4.3. Helyettesítsük b_1-et $b_1' = b_1 + rb_2$-vel. Nyilván

$$r_1(b_1 + rb_2) + r_2b_2 + r_3b_3 + \ldots + r_kb_k = r_1b_1 + (r_2 + r_1r)b_2 + r_3b_3 + \ldots + r_kb_k\,.$$

Ezért $\langle b_1', b_2, \ldots, b_n\rangle \subseteq \langle b_1, \ldots, b_n\rangle$. De megfordítva, $b_1 = b_1' - rb_2$, vagyis b_1 is kifejezhető b_1'-vel és b_2-vel, tehát a fordított tartalmazás is teljesül. Így a régi és az új rendszer ugyanakkor lesz generátorrendszer. Ha $b_1, \ldots, b_n$ független, akkor az új is, mert ha a fenti lineáris kombináció nulla, akkor $r_1 = r_3 = \ldots = r_k = 0$ és $r_2 + r_1r = 0$. Így viszont r_2 is nulla, és így az új rendszer is független.

Gyenge függetlenségre ez a gondolatmenet nem működik. Ekkor ugyanis csak azt kapjuk, hogy $r_1b_1 = 0 = (r_2 + r_1r)b_2$, és innen nem tudunk továbblépni. Ha például $M = \mathbb{Z}_6^+$, $b_1 = 3$ és $b_2 = 4$, akkor ez gyenge bázis (7.2.6. Gyakorlat). Legyen $r = 1$, így $b_1' = 1$. De az 1 és a 3 nem gyengén függetlenek, hiszen $3 \cdot 1 - 1 \cdot 3 = 0$, és egyik tag sem nulla.

7.4.4. Csak az (1) állítást bizonyítjuk abban az esetben, amikor $i = 1$ és $j = 2$, a többi számolás hasonló. Tegyük föl, hogy $b_1' = b_1 + rb_2$, és

$$g = r_1b_1 + r_2b_2 + \ldots + r_kb_k\,,$$

vagyis a „régi" mátrix valamelyik sora $(r_1, r_2, r_3, \ldots, r_k)$. Ekkor

$$g = r_1b_1' + (r_2 - r_1r)b_2 + \ldots + r_kb_k\,,$$

vagyis az „új" mátrixban ez a sor $(r_1, r_2 - r_1r, r_3, \ldots, r_k)$ lesz.

7.4.10. Ha $s_1, \ldots, s_{k-1}$ egység, akkor a 7.4.8. Állítás miatt M egy s_k rendű ciklikus modulus, hiszen egy egység rendű ciklikus modulus csak a nullából áll, ami minden direkt felbontásból elhagyható. Megfordítva, ha M ciklikus, akkor a 7.3.9. Gyakorlat (5) pontja miatt minden direkt felbontásában a ciklikus tényezők rendjei páronként relatív prímek. Az $s_1 \mid s_2 \mid \ldots \mid s_k$ oszthatóság miatt ez csak akkor lehetséges, ha $s_1, \ldots, s_{k-1}$ egység.

7.4.11. A 7.4.8. Állítás miatt a mátrix sorai olyan (u, v) egész számok, melyekre a $\mathbb{Z}_6^+$ csoportban $u \cdot 2 + v \cdot 3 = 0$, azaz $6 \mid 2u + 3v$. Innen látszik, hogy $3 \mid u$ és $2 \mid v$, hiszen 2 és 3 relatív prímek.

A mátrix első sorába tegyük a $(3, 0)$, a másodikba a $(0, 2)$ számokat. Ennek a sornak a segítségével a többi (u, v) sort kinullázhatjuk. Valóban, mivel $3 \mid u$, kivonhatjuk az első sor $u/3$-szorosát, és ugyanígy a második sor $v/2$-szeresét. Ezeket a csupa nulla sorokat nem írjuk ki. A kapott mátrixot a következőképpen alakíthatjuk át.

$$\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \quad \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \quad \begin{bmatrix} 2 & 0 \\ 2 & 3 \end{bmatrix} \quad \begin{bmatrix} 2 & -2 \\ 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 \\ -2 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}.$$

Az első lépésben egy sor és oszlopcserével a legkisebb normájú (abszolút értékű) 2 elemet a bal felső sarokba vittük. Ezután az első sort hozzáadtuk a másodikhoz, a második oszlopból kivontuk az elsőt, és így a jobb alsó sarokban 1 keletkezett. Ezt két cserével a bal felső sarokba vittük, és segítségével kinulláztuk az első sort és oszlopot.

Így a szabad $\mathbb{Z}^+ \times \mathbb{Z}^+$ modulusban van egy olyan b_1, b_2 bázis, hogy $\mathbb{Z}_6^+ \cong (\mathbb{Z}^+ \times \mathbb{Z}^+)/K$, és a K részmodulust generálják az új mátrix sorainak megfelelő $1b_1 + 0b_2$ és $0b_1 + 6b_2$ elemek. (A mátrix többi sora, amit nem írtunk ki, csupa nulla, az ezekhez tartozó generátorelem is nulla.) Vagyis

$$\mathbb{Z}_6^+ \cong (\mathbb{Z}^+ \times \mathbb{Z}^+)/\langle b_1, 6b_2 \rangle .$$

Ez a 7.4.7. Lemma szerint azt jelenti, hogy $b_1 + K = 0$ és $6b_2 + K$ generátorrendszert alkot $\mathbb{Z}_6^+$-ban, és ez utóbbi elem rendje 6.

Természetesen $\mathbb{Z}_6^+$-ról már eleve tudtuk, hogy ciklikus, az előző számolás arra szolgál, hogy lássuk a tétel bizonyítását egy nagyon egyszerű speciális esetben. A fenti gondolatmenet nem adja meg, hogy $\mathbb{Z}_6^+$ melyik generátorelemét kaptuk. Általában fontos lenne, hogy a felbontandó modulusban konkrétan ki is tudjunk számítani egy gyenge bázist. Ehhez végig kell követni a mátrixok átalakítása során azt is, hogy hogyan változik a szabad modulus bázisa. Ennek semmi akadálya, de ezzel az eljárással ebben a könyvben nem foglalkozunk. (Ide kapcsolódik a 7.6.6. Tétel utáni megjegyzés is.)

A (2) esetben a mátrix (a csupa nulla sorok elhagyásával)

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} \quad \text{amelynek normálalakja} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{bmatrix}.$$

Ezért ez a csoport $\mathbb{Z}_2^+ \times \mathbb{Z}_6^+$-ként bomlik fel. A $\mathbb{Z}_6^+$ tényezőt tovább bonthatjuk $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ra a 7.3.9. Gyakorlat alapján.

A (3) esetben először azt ellenőrizzük, hogy $\{3, 5\}$ tényleg generátorrendszer-e. A 3 által generált részcsoport elemei $1, 3, 9, 11$. Ennek indexe 2, de az 5 nincs benne, ezért a 3 az 5-tel együtt már biztosan az egész csoportot generálja. Mellesleg a 3 és az 5 rendje is 4. Ez nem gyenge bázis, mert $3^2 \cdot 5^2 = 1$ (vigyázzunk, itt a művelet a szorzás, ezért együtthatóból kitevő lesz, és a lineáris kombinációban szorozni kell összeadás helyett).

A mátrix soraiban az olyan (u, v) egészek szerepelnek, amelyekre a $\mathbb{Z}_{16}^{\times}$ csoportban $3^u \cdot 5^v = 1$. A fentiekhez hasonlóan könnyű meggondolni, hogy a mátrixba elegendő az alábbi három sort beírni:

$$\begin{bmatrix} 4 & 0 \\ 0 & 4 \\ 2 & 2 \end{bmatrix} \quad \text{amelynek normálalakja} \quad \begin{bmatrix} 2 & 0 \\ 0 & -4 \\ 0 & 0 \end{bmatrix}.$$

Persze -4 helyett a vele asszociált 4 rendről beszélünk, tehát $\mathbb{Z}_{16}^{\times} \cong \mathbb{Z}_2^{+} \times \mathbb{Z}_4^{+}$.

7.4.12. A negyedik mátrix átalakítása a következő.

$$\begin{bmatrix} -x & 1 & 0 \\ 0 & -x & 0 \\ 0 & 0 & -x \end{bmatrix} \quad \begin{bmatrix} 1 & -x & 0 \\ -x & 0 & 0 \\ 0 & 0 & -x \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ -x & -x^2 & 0 \\ 0 & 0 & -x \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & -x & 0 \\ 0 & 0 & -x^2 \end{bmatrix}.$$

A többi mátrixnál az eredmény rendre az alábbi:

$$\begin{bmatrix} -x & 0 \\ 0 & -x \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1-x^2 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & -x & 0 \\ 0 & 0 & x^2-x \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & -x & 0 \\ 0 & 0 & -x^2 \end{bmatrix}.$$

7.4.13. Két oszlop (vagy sor) cseréjekor minden determináns előjelet vált. Ha egy aldeterminánsban egyik oszlop sincs benne, akkor ugyanannyi marad az értéke, ha mindkét megcserélt oszlop benne van, akkor előjelet vált. A harmadik eset az, amikor az aldeterminánsban a két megcserélt oszlop közül csak az egyik van benne. Jelölje ezt az aldeterminánst $(v_1, \ldots, v_i)$, és képzeljük azt, hogy az első oszlopot u-ra cseréljük. Természetesen az $u, v_2, \ldots, v_i$ oszlopvektorok valamilyen sorrendben szintén egy aldeterminánst alkotnak (a $v_2, \ldots, v_n$ ebben a sorrendben van, de az u közöttük bárhol lehet). Ebből a másik aldeterminánsból a csere után a $v_1, \ldots, v_i$ alkotta aldeterminánsz lesz az oszlopok valamelyik sorrendjében. Ezért ebben a harmadik esetben két $i \times i$ méretű aldeterminánsz „helyet cserél" (és még az előjelük is megváltozhat). De ekkor az összes ilyen aldeterminánsz kitüntetett közös osztója nem változik.

Ha az egyik oszlophoz egy másik r-szeresét adjuk, akkor a bizonyítás hasonló. Csak abban az esetben változhat meg egy $a = \det(v_1, v_2, \ldots, v_i)$ aldeterminánsz, ha ennek valamelyik, mondjuk az első oszlopához egy olyan u oszlop r-szeresét adtuk, ami ezen az aldeterminánson kívül van. Ekkor azonban szerepel a $\pm b = \det(u, v_2, \ldots, v_i)$ aldeterminánsz is (az oszlopok valamelyik sorrendjében). Az Útmutatóban írtak miatt a két régi aldeterminánsnak, és a két újnak ugyanaz lesz a kitüntetett közös osztója.

Ezzel beláttuk, hogy az eliminációs során a determinánsosztók (és így az elemi osztók) asszociáltság erejéig ugyanazok maradnak. Ha a mátrix már diagonális alakban van, és a főátlóban szereplő elemek $s_1 \mid s_2 \mid \ldots \mid s_k$, akkor $\Delta_i(L) = s_1 s_2 \ldots s_i$, és ezért az i-edik elemi osztó s_i (az Olvasóra bízzuk annak átgondolását, hogy ez utóbbi állítás akkor is igaz, ha az s_i sorozat elemei valamettől kezdve nullával egyenlőek). Valóban, a bal felső sarokban álló $i \times i$ méretű aldeterminánsz értéke $s_1 s_2 \ldots s_i$. Ugyanakkor ha egy $i \times i$ méretű

aldeterminánsnem nulla, akkor minden sorában és oszlopában pontosan egy s_j szerepel, és így az $s_1 \mid s_2 \mid \ldots \mid s_k$ oszthatóság miatt ez a determináns osztható $s_1 s_2 \ldots s_i$-vel.

7.4.14. Legyen T az R hányadosteste. A T fölött érvényes a determinánsok lineáris algebrából ismert szorzástétele, vagyis $\det(L)\det(L^{-1}) = 1$. Ha L^{-1} minden eleme R-beli, akkor persze $\det(L^{-1}) \in R$, és így $\det(L)$ invertálható (vagyis egység). Megfordítva, ha $\det(L)$ egység, akkor $1/\det(L) \in R$, és így az inverz mátrix képlete (lásd [**10**], 2.2.3. Lemma) miatt az L mátrix T fölött kiszámított inverzének minden eleme R-beli.

7.4.15. Az előző feladat miatt $L^{-1} = ((s_{ij})) \in R^{k\times k}$. Ekkor

$$b_j = s_{j1}c_1 + \ldots + s_{jk}c_k \quad (j = 1, \ldots, k)$$

közvetlen behelyettesítéssel igazolható. Erre a következőképpen is gondolhatunk. Írjuk a $b_1, \ldots, b_k$ vektorokat formálisan egy v oszlopvektorba. Ekkor az Lv oszlopvektorban pont $c_1, \ldots, c_k$ lesz. Ha ezt balról L^{-1}-gyel szorozzuk (ezt fejezi ki a fönti képlet), akkor persze az eredeti v vektort, tehát a b_i-ket kapjuk vissza.

Ha $t_1, \ldots, t_k \in R$ esetén $t_1c_1 + \ldots + t_kc_k = 0$, akkor visszahelyettesítve, és a b_i függetlenségét kihasználva azt kapjuk, hogy az L mátrix sorainak a $t_1, \ldots, t_k$ együtthatókkal vett lineáris kombinációja nulla. Tudjuk lineáris algebrából, hogy egy mátrix determinánsa akkor és csak akkor nulla, ha sorai lineárisan összefüggenek. Mivel L determinánsa nem nulla, azt kapjuk, hogy ez a lineáris kombináció triviális, vagyis $t_1 = \ldots = t_k = 0$. Ezért $c_1, \ldots, c_k$ független.

Az állítás második felét a következőképpen is megmutathattuk volna. Legyen T az R hányadosteste. Tudjuk, hogy M szabad modulus, izomorf ${}_RR^k$-val, és van olyan izomorfizmus is, ahol b_i az ${}_RR$ szokásos e_i bázisvektorának felel meg. Ezért R^k helyett T^k-ban is kiszámolhatjuk a c_i vektorokat, amelyek a fentiek szerint generátorrendszert alkotnak. De T^k már vektortér, tehát itt egy dimenziónyi elemszámú generátorrendszer biztosan bázis.

7.4.16. Az előző két feladat képleteivel számolva

$$b_1 = uc_1 - tc_2 \quad \text{és} \quad b_2 = vc_1 + sc_2\,.$$

A (2) állítás speciális esete az előző feladat második állításának (egy alkalmas mátrixot kell felírni, amelynek a determinánsa 1 lesz), de közvetlen számolással is igazolható.

7.4.17. Az (1) azért igaz, mert az előző gyakorlat jelöléseivel

$$r_{11}b_1 + r_{12}b_2 = d(sb_1 + tb_2) = dc_1 + 0c_2\,.$$

A (2) esetében legyen d az r_{11} és r_{21}) kitüntetett közös osztója, $d = r_{11}s + r_{21}t$, továbbá $u = r_{11}/d$ és $v = r_{21}/d$, végül

$$h_1 = sg_1 + tg_2 \quad \text{és} \quad h_2 = -vg_1 + ug_2\,.$$

Ekkor g_1, g_2-t h_1, h_2-re cserélve ismét generátorrendszert kapunk az előző feladat miatt, és az új mátrixban az első sor első eleme $sr_{11} + tr_{21} = d$, a második sor első eleme pedig

$$-vr_{11} + ur_{21} = -vud + uvd = 0\,.$$

Ezekkel a lépésekkel nyilván kiváltható a maradékos osztás a 7.4.5. Lemma bizonyításában (az persze kérdés marad, hogy ha nem euklideszi gyűrűben vagyunk, akkor milyen eljárással írjuk föl mondjuk r_{11} és r_{12} legnagyobb közös osztóját $r_{11}u + r_{12}v$ alakban).

Azt, hogy az eljárás véget ér, a következőképpen bizonyíthatjuk. Az R főideálgyűrű, így az 5.4.3. Tétel miatt érvényes benne ideálokra a maximum-feltétel. Tekintsük az eljárás során készített mátrixokban a bal felső sarokban található elem által generált főideált. A fenti lépések során ez csak növekedhet, és így az eljárás a maximum-feltétel miatt véget ér.

7.5. A felbontás egyértelműsége.

7.5.1. Az $m = r_1a_1 + \ldots + r_ka_k + s_1b_1 + \ldots + s_\ell b_\ell$ elemről kell belátni, hogy pontosan akkor nem nulla rendű, ha $r_1 = \ldots = r_k = 0$. Tegyük föl, hogy m rendje nem nulla. Ekkor van olyan $r \neq 0$, hogy $rm = 0$. Mivel $a_1, \ldots, a_k, b_1, \ldots, b_\ell$ gyengén független, $rm = 0$-ból $rr_ia_i = 0$ és $rs_jb_j = 0$ következik minden i-re és j-re. Mivel a_i rendje nulla, innen $rr_i = 0$, és $r \neq 0$ miatt $r_i = 0$ következik mindegyik i-re. Megfordítva, ha mindegyik $r_i = 0$, akkor nyilván $rm = 0$, ahol r a $b_1, \ldots, b_\ell$ elemek (nem nulla) rendjeinek a szorzata.

Mivel $b_j \in T$ minden j-re, az M/T modulust nyilván generálják az $a_1 + T, \ldots, a_k + T$ elemei, azt kell megmutatni, hogy függetlenek. Tegyük föl, hogy

$$r_1(a_1 + T) + \ldots + r_k(a_k + T) = (r_1a_1 + \ldots + r_ka_k) + T$$

értéke nulla (mármint az M/T nulleleme, vagyis T). Ekkor $r_1a_1 + \ldots + r_ka_k \in T$, vagyis véges rendű. Az előző bekezdésben ebből beláttuk, hogy mindegyik $r_i = 0$.

7.5.3. Mivel $o(c_i) = p^{\alpha_i}$, ezért a $c_i'' = p^{\alpha_i - 1}c_i$ elem p-szerese már nulla, és így $c_i'' \in M[p]$. Tegyük föl, hogy

$$0 = r_1c_1'' + \ldots + r_nc_n'' = r_1p^{\alpha_1 - 1}c_1 + \ldots + r_np^{\alpha_n - 1}c_n\,.$$

Mivel $c_1, \ldots, c_n$ gyengén független, innen $r_ip^{\alpha_i - 1}c_i = 0$, és így $r_ic_i'' = r_ip^{\alpha_i - 1}c_i$ is nulla minden i-re. Ezért $c_1'', \ldots, c_n''$ gyengén független.

Annak megmutatásához, hogy generátorrendszer is $M[p]$-ben, legyen $b \in M[p]$. Ekkor

$$b = r_1c_1 + \ldots + r_nc_n + s_1d_1 + \ldots + s_md_m\,.$$

Mivel $pb = 0$, a gyenge függetlenség miatt $pr_ic_i = 0$ minden i-re, és $ps_jd_j = 0$ minden j-re. A d_j rendje nulla, vagy relatív prím p-hez, és ezért $s_jd_j = 0$. Továbbá $pr_ic_i = 0$ miatt $o(c_i) = p^{\alpha_i} \mid pr_i$, ahonnan $r_i = t_ip^{\alpha_i - 1}$ alkalmas t_i-re. De akkor

$$b = t_1p^{\alpha_1 - 1}c_1 + \ldots + t_np^{\alpha_n - 1}c_n + 0 + \ldots + 0 = t_1c_1'' + \ldots + c_n''\,.$$

7.5.4. Nyilván

$$r_1c'_1 + \ldots + r_nc'_n + s_1d'_1 + \ldots + s_mc'_m$$

akkor és csak akkor nulla $M/M[p]$-ben, ha $r_1c_1 + \ldots + r_nc_n + s_1d_1 + \ldots + s_mc_m \in M[p]$, vagyis ha a p-szerese nulla. Innen $pr_ic_i = 0$ minden i-re és $ps_jd_j = 0$ minden j-re, de ez pontosan azt jelenti, hogy $r_ic_i, s_jd_j \in M[p]$, azaz $r_ic'_i = s_jd'_j = 0$. Ezzel a gyenge függetlenséget beláttuk. Az, hogy generátorrendszerről van szó, nyilvánvaló, hiszen egy generátorrendszer homomorf képe. Az elemrendekre vonatkozó állítás a 7.3.19. Gyakorlatból következik.

7.5.5. Mivel $pv = (x - \lambda)v = 0$ akkor és csak akkor, ha $A(v) = \lambda v$, az $M[p]$ a λ-hoz tartozó sajátaltér. A második állítás nyilvánvaló, hiszen a p-komponensben azok a v vektorok vannak, amelyekre $p^mv = 0$ alkalmas m egészre, és $p^mv = (A - \lambda I)^m(v)$.

7.5.6. Az $m \in M$ pontosan akkor van benne az $N[p]$ teljes inverz képében, ha $m + M[p]$ benne van $N[p]$-ben, azaz a p-szerese nulla. Ez azt jelenti, hogy $pm \in M[p]$, ami tényleg azzal ekvivalens, hogy $p^2m = 0$.

7.5.7. Nyilván

$$r_1(b_1 + pM) + \ldots + r_k(b_k + pM) = (r_1b_1 + \ldots + r_kb_k) + pM$$

akkor és csak akkor nulla M/pM-ben, ha $r_1b_1 + \ldots + r_kb_k \in pM$. Ez azt jelenti, hogy

$$p(s_1b_1 + \ldots + s_kb_k) = r_1b_1 + \ldots + r_kb_k$$

alkalmas $s_i \in R$ elemekre. Mivel $b_1, \ldots, b_n$ független, $ps_i = r_i$, azaz $r_i + (p)$ nulla az $R/(p)$ faktorgyűrűben. Ezért a $b_i + pM$ elemek függetlenek M/pM-ben $R/(p)$ fölött. Az nyilvánvaló, hogy generátorrendszert alkotnak, tehát a keresett dimenzió tényleg k.

Ebből az állításból valóban következik, hogy a bázis elemszáma egyértelmű, feltéve, hogy R-ben van prím. Előfordulhat, hogy nincs prím, például ha R már maga is test (persze ebben az esetben közvetlenül is igazolhatjuk az állítást). A 7.5.2. Lemmában leírt bizonyítás viszont minden kommutatív gyűrűben működik.

7.5.8. Az (1) és (2) állítások az eddigi számolásokhoz teljesen hasonló módon igazolhatók. A (3)-beli bizonyítás vázlata a következő. A torziómentes részt ugyanúgy kezeljük, mint a másik bizonyításban, a p-komponensekre bontást pedig a 7.3.20. Gyakorlat segítségével. Így elegendő a gyakorlatban megadott $\langle c_1\rangle \oplus \ldots \oplus \langle c_n\rangle$ modulussal foglalkozni. Az (1) állítás megadja a tényezők számát. Ezután áttérünk a pM részmodulusra, amelyben (2) miatt gyenge bázist alkotnak azok a pc_i elemek, amelyekre $\alpha_i \geq 2$. Itt megismételjük az eljárást, majd tovább haladunk p^2M-re (amelyben az $\alpha_i \geq 3$ feltételnek eleget tevő p^2c_i elemek alkotnak bázist), és így tovább. Természetesen a bizonyítás tényleges leírásakor egyszerűbb indukcióval bizonyítani (például a lehetséges legnagyobb α_i szerint), és az indukciós feltevést a pM modulusra alkalmazni.

7.6. A Jordan-féle normálalak.

7.6.3. Ha c rendje az f polinom (ami $p^m c = 0$ miatt p^m-nek valódi osztója), akkor a 2.4.16. Feladat szerint f fölírható $x - \lambda$ polinomjaként, azaz

$$f(x) = t_0 + t_1(x - \lambda) + \ldots + t_n(x - \lambda)^n$$

alakban, ahol $n < m$. Innen $fc = 0$ miatt $t_0c_1 + t_1c_2 + \ldots + t_{m-1}c_m = 0$ következik. De nem mindegyik t_i nulla, mert akkor f a nullapolinom lenne, ami nem osztója p^m-nek.

7.6.4. Legyen $B = A - \lambda I$. A mátrixból leolvasható, hogy $c_i = B^{i-1}(c)$, és $B^m(c) = 0$. Innen $p(A) = B$ miatt $c_i = p^{i-1}c$ ha $i < m$, és $p^m c = 0$. Mivel $c_1, \ldots, c_n$ bázis W-ben, a 7.6.2. Lemma szerint c generálja W-t mint $T[x]$-modulust, a 7.6.3. Gyakorlat miatt pedig c rendje p^m.

7.6.7. A 7.4.13. Feladat miatt elegendő megmutatni, hogy az $L - xI$ mátrixnak és a transzponáltjának ugyanazok a determinánsosztói, ami nyilvánvaló, hiszen transzponáláskor egy mátrix determinánsa nem változik.

7.6.8. A 7.6.6. Tétel miatt a minimálpolinomok leolvashatók a 7.4.12. Gyakorlat megoldásában megadott normálalakú mátrixokról, mint a jobb alsó sarokban álló polinom. A felsorolt mátrixok transzponáltjai közül az első, a harmadik és a negyedik már Jordan-alakban van, a fennmaradó két mátrixnak a Jordan-alakja

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{és} \quad \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Például az utolsó mátrix esetében azért, mert a karakterisztikus mátrix normálalakjában szereplő 1, $-x$ és $-x^2$ polinomok közül a másodiknak a 0 egyszeres, a harmadiknak pedig kétszeres gyöke, és így a 0 sajátértékhez egy 1×1-es és egy 2×2-es Jordan-blokk tartozik.

7.6.9. A 7.6.6. Tételt alkalmazzuk. A karakterisztikus mátrixok normálalakjai és a Jordan-alakok rendre a következők (1, ε_1, ε_2 a harmadik egységgyökök).

$$\begin{bmatrix} 1 & 0 \\ 0 & -(x-1)^2 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x(3-x) \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & (x^3 - x^2)/2 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 - x^3 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & \varepsilon_1 & 0 \\ 0 & 0 & \varepsilon_1 \end{bmatrix}$$

A minimálpolinomok a megfelelő mátrix jobb alsó sarkában vannak.

7.6.10. A 7.6.6. Tétel miatt a minimálpolinom mindegyik esetben a sorozat utolsó eleme, a Jordan-alakok pedig a következők.

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

7.6.11. Ha a blokk $n \times n$-es, és a sajátérték λ, akkor a főátlóban $n-1$ darab 1-es, és 1 darab $(x-\lambda)^n$ szerepel (előjeltől eltekintve). Ez nyilván következik a 7.6.6. Tételből, de az Olvasónak ajánljuk, hogy legalább egy 3×3-as, 0 sajátértékhez tartozó blokk esetében végezze el gyakorlásul a számolást.

7.6.12. Legyen A lineáris transzformációja a T végtelen test fölötti k-dimenziós V vektortérnek, és $M = M(A, V)$. Minden sajátaltér legfeljebb egydimenziós lehet, mert egy legalább kétdimenziós vektortérben végtelen test fölött végtelen sok altér van, amelyek mind A-invariánsak. (Végtelen sok különböző „iránytangensű" egyenest kell venni, pontosabban a $\langle b_1, b_2 + \lambda b_1 \rangle$ altereket, ahol b_1, b_2 független rendszer, és λ eleme az alaptestnek.) Most ezt általánosítjuk a következőképpen.

Legyen $p \in T[x]$ prím (azaz irreducibilis polinom). Mivel T most nem feltétlenül algebrailag zárt, nem tehetjük föl, hogy p elsőfokú. De most is tekinthetjük az $M[p]$ részmodulust (ami elsőfokú p esetén sajátaltér a 7.5.5. Gyakorlat miatt). A 7.5.3. Gyakorlat megoldásából tudjuk, hogy M felbontásában a p-hatvány rendű ciklikus tényezők száma ugyanaz, mint $M[p]$ dimenziója a $T[x]/(p)$ test fölött. Tegyük föl, hogy ez a dimenzió legalább kettő. A $T[x]/(p)$ test végtelen, hiszen T-nek bővítése (különböző T-beli skalárok nem lehetnek egy mellékosztályban (p) szerint). A fenti megjegyzés miatt így $M[p]$-nek végtelen sok altere van. Ezek részmodulusok $T[x]$ fölött is, azaz invariáns alterek.

Ha tehát véges sok invariáns altér van, akkor M prímhatványrendű ciklikusok direkt összegére való felbontásában minden prímhez legfeljebb egy tényező szerepelhet, vagyis a tényezők páronként relatív prímek. Ezért M ciklikus modulus (7.3.9. Gyakorlat).

Megfordítva, ha M ciklikus modulus, és egy u elem generálja, akkor a 7.3.8. Feladat miatt a részmodulusok kölcsönösen egyértelmű megfeleltetésben állnak az u rendjének osztóival (ahol az asszociált osztókat nem különböztetjük meg). Így véges sok invariáns altér van. Persze az u rendje a modulus exponense, vagyis az A minimálpolinomja. Egy konkrét ilyen példát elemeztünk a 7.3.17. Gyakorlatban.

Végül a 7.4.10. Gyakorlat miatt M akkor és csak akkor ciklikus, ha az A karakterisztikus mátrixának normálalakjában szereplő $s_1, \ldots, s_k$ közül az első $k-1$ polinom egység.

Mivel a szorzatuk a karakterisztikus polinom, ez pontosan akkor teljesül, ha A minimálpolinomja és karakterisztikus polinomja asszociáltak. De a karakterisztikus polinom foka a tér dimenziója (és a minimálpolinom osztója a karakterisztikus polinomnak), tehát ez úgy is fogalmazható, hogy m_A foka $\dim(V)$-vel egyenlő.

7.7. Homomorfizmusok csoportjai.

7.7.2. A számolások többsége triviális (és ugyanaz, mint lineáris algebrában), ezért csak néhány megjegyzést teszünk. Ha R kommutatív, $\varphi \in \mathrm{Hom}_R(M, N)$, akkor be kell látni, hogy $r\varphi \in \mathrm{Hom}_R(M, N)$ minden $r \in R$ esetén. Az összegtartás nyilvánvaló, a skalárral szorzást pedig azért tartja $r\varphi$, mert $m \in M$, $s \in R$ esetén

$$(r\varphi)(sm) = r\big(\varphi(sm)\big) = r\big(s\varphi(m)\big) = (rs)\big(\varphi(m)\big) = (sr)\big(\varphi(m)\big) = s\big((r\varphi)(m)\big)\,.$$

Az Olvasónak tanácsoljuk, hogy a fenti átalakítás-sorozat mindegyik lépésénél vizsgálja meg, hogy az miért megengedett. A $\mathrm{Hom}_R(M, N)$ nulleleme az azonosan nulla leképezés.

7.7.3. Az, hogy ψ_r összegtartó, nyilvánvaló. A skalárral szorzást azért tartja, mert R szorzása asszociatív:

$$\psi_r(sx) = (sx)r = s(xr) = s\psi_r(x)$$

tetszőleges $x, s \in R$ esetén. Ha $r\,id_R \in \mathrm{Hom}_R({}_RR, {}_RR)$, akkor

$$(r\,id_R)(sx) = s\big((r\,id_R)(x)\big)\,.$$

A bal oldal rsx, a jobb oldal srx, és ezek egyenlőek minden x és s esetén. Speciálisan $x = 1$-re azt kapjuk, hogy r felcserélhető R minden elemével.

7.7.5. Ha $\varphi \in \mathrm{Hom}(\mathbb{Z}_m^+, \mathbb{Z}_n^+)$, akkor $\varphi(1)$ rendje osztója n-nek, mert $\varphi(1) \in \mathbb{Z}_n^+$, és osztója m-nek, mert 1 rendje $\mathbb{Z}_m^+$-ban m. Ezért $\varphi(1) = 0$, de akkor $\varphi(k) = k\varphi(1) = 0$.

7.7.7. Lásd a 7.7.9. Gyakorlat megoldását.

7.7.9. A közvetlen számolás helyett megtehetjük, hogy megoldjuk a 7.7.26. Gyakorlatot, majd alkalmazzuk a 7.3.13. Gyakorlatot.

7.7.10. Feleltessük meg a $b \in M$ elemnek azt a $\varphi_b : R \to M$ leképezést, amelyre $\varphi(r) = rb$. A 7.2.12. Gyakorlatban már beláttuk, hogy ez R-homomorfizmus. Az is világos, hogy ha $\varphi \in \mathrm{Hom}_R({}_RR, M)$, és $\varphi(1) = b$, akkor $\varphi = \varphi_b$. Így a $b \leftrightarrow \varphi_b$ megfeleltetés kölcsönösen egyértelmű M és $\mathrm{Hom}_R({}_RR, M)$ között. Ez összegtartó, hiszen az $r(b_1 + b_2) = rb_1 + rb_2$ összefüggés következik a modulus-axiómákból. Ha R kommutatív, akkor ez a megfeleltetés skalárszoros-tartó is, mert

$$\varphi_{sb}(r) = r(sb) = s(rb) = s\varphi_b(r)\,.$$

7.7.11. Csak a megfeleltetéseket adjuk meg, annak egyszerű ellenőrzését, hogy izomorfizmusról van szó (tehát a művelettartást is), az Olvasóra hagyjuk. Annak igazolásához, hogy

$$\mathrm{Hom}_R\Big(\bigoplus_i M_i,\, K\Big) \cong \prod_i \mathrm{Hom}_R(M_i,\, K)\,,$$

rendeljük hozzá a $(\ldots, \varphi_i, \ldots) \in \prod_i \mathrm{Hom}_R(M_i, K)$ elemhez azt a $\varphi \in \mathrm{Hom}_R\left(\bigoplus_i M_i, K\right)$ homomorfizmust, amelyre

$$\varphi(\ldots, m_i, \ldots) = \sum_i \varphi_i(m_i)\,.$$

Ez az összeg értelmes, mert a direkt összeg egy elemének csak véges sok komponense nem nulla. Megadjuk ennek a megfeleltetésnek az inverzét is. Ha $\psi \in \mathrm{Hom}_R\left(\bigoplus_i M_i, K\right)$, akkor rendeljük ehhez hozzá a

$$(\ldots, \psi_i, \ldots) \in \prod_i \mathrm{Hom}_R(M_i, K)$$

elemet, amelyben a ψ_i definíciója $m_i \in M_i$ esetén

$$\psi_i(m_i) = \psi(\ldots, 0, m_i, 0, \ldots)$$

(vagyis ψ_i a ψ megszorítása az $M_i^* \leq \bigoplus_i M_i$ részmodulusra). Könnyű megmutatni, hogy a megadott két megfeleltetés egymás inverze.

Másodszor belátjuk, hogy

$$\mathrm{Hom}_R\Big(M, \prod_i K_i\Big) \cong \prod_i \mathrm{Hom}_R(M,\, K_i)\,.$$

Rendeljük hozzá a $(\ldots, \varphi_i, \ldots) \in \prod_i \mathrm{Hom}_R(M, K_i)$ elemhez azt a $\varphi \in \mathrm{Hom}_R\left(M, \prod_i K_i\right)$ homomorfizmust, amelyre

$$\varphi(m) = (\ldots, \varphi_i(m), \ldots)\,.$$

Ennek a megfeleltetésnek az inverze a következő. Ha $\psi \in \mathrm{Hom}_R\left(M, \prod_i K_i\right)$, akkor rendeljük ehhez hozzá a

$$(\ldots, \psi_i, \ldots) \in \prod_i \mathrm{Hom}_R(M, K_i)$$

elemet, amelyben a $\psi_i(m)$ a $\psi(m) \in \prod_i K_i$ elem i-edik komponense (vagyis $\psi_i = \pi_i \circ \psi$, ahol π_i az i-edik projekció.

Hasonló összefüggések nem érvényesek akkor, ha a Hom első argumentumában van direkt szorzat, vagy ha a második argumentumában van direkt összeg. Annyi látszik a fenti számolásból, hogy léteznek

$$\bigoplus_i \mathrm{Hom}_R(M, K_i) \hookrightarrow \mathrm{Hom}_R\Big(M, \bigoplus_i K_i\Big) \hookrightarrow \prod_i \mathrm{Hom}_R(M, K_i)$$

injektív homomorfizmusok (azaz beágyazások).

7.7.14. Osztható csoport homomorf képe osztható (mert ha $a = nb$, akkor $\varphi(a) = n\varphi(b)$). Ezért ha $\varphi : A \to B$ homomorfizmus, akkor $\varphi(A)$ osztható részcsoportja B-nek. Ez a feltétel miatt csak a nulla lehet, ezért $\varphi = 0$.

7.7.15. Tekintsük az a által generált A részcsoportot, ennek rendje n, és elég belátni, hogy ebben a osztható minden n-hez relatív prím m számmal. Ezt kongruenciákkal azonnal láthatjuk, sőt már igazoltuk is a 4.3.28. Gyakorlatban. Most egy másik, algebrai jellegű bizonyítást adunk. Tekintsük a $\varphi(x) = mx$ leképezést A-ból A-ba. Mivel $(m, n) = 1$, ennek magja csak a nulla, vagyis φ injektív. De A véges halmaz, és így φ szürjektív is.

7.7.17. Legyen $o(\varepsilon) = p^n$ és $o(\eta) = p^m$ két komplex egységgyök. Ha $n \leq m$, akkor ε hatványa η-nak (mert $\eta^{p^{m-n}}$ rendje p^n, és a primitív p^n-edik egységgyökök egymás hatványai az 1.5.12. Tétel miatt). Ha tehát $H \leq \mathbb{Z}_{p^\infty}$, és H-ban van akármilyen nagy rendű elem, akkor $H = \mathbb{Z}_{p^\infty}$, ha pedig H-ban a legnagyobb elemrend p^n, akkor H az összes p^n-edik egységgyökökből áll.

7.7.18. Ahhoz, hogy egy csoport osztható, nyilván elég megmutatni, hogy a csoport minden eleme minden prímszámmal osztható. A $\mathbb{Z}_{p^\infty}$ csoportban ez nyilvánvaló a p prímre (hiszen egy p-hatványadik egységgyök p-edik gyöke is p-hatványadik egységgyök), a többi prímre pedig a 7.7.15. Gyakorlatból következik.

7.7.19. Legyen A véges, osztható csoport, és $a \neq 0$ egy eleme, amelynek a rendje a lehető legnagyobb. Jelölje ezt a rendet n. Mivel A osztható, van olyan $b \in A$, melyre $nb = a$. A 4.3.29. Gyakorlat miatt b rendje n^2. Az n maximalitása miatt így $n^2 \leq n$, vagyis $n = 1$. Ez ellentmond annak, hogy $a \neq 0$.

7.7.21. Tegyük föl, hogy $((a_{ij})$ az A mátrixa a $(\mathbf{b}, \mathbf{c})$ bázispárban, ahol $\mathbf{b} = (b_1, \ldots, b_n)$ és $\mathbf{c} = (c_1, \ldots, c_m)$. Legyen $\mathbf{c}^* = (c_1^*, \ldots, c_m^*)$ és $\mathbf{b}^* = (b_1^*, \ldots, b_n^*)$ a duális bázis (lásd az Útmutatót). Ekkor A^* mátrixa a $(\mathbf{c}^*, \mathbf{b}^*)$ bázispárban az $((a_{ij}))$ transzponáltja lesz. Valóban,

$$A(b_j) = a_{1j}c_1 + \ldots + a_{mj}c_m\,,$$

azt kell belátni, hogy

$$A^*(c_i^*) = a_{i1}b_1^* + \ldots + a_{in}b_n^*\,.$$

Ez két lineáris függvény egyenlősége ezért elég a $\mathbf{b}$ bázison igazolni. Tudjuk, hogy

$$\big(A^*(c_i^*)\big)(b_j) = (c_i^* \circ A)(b_j) = c_i^*(a_{1j}c_1 + \ldots + a_{mj}c_m) = a_{ij}\,,$$

mert c_i^* lineáris, és $c_i^*(c_j)$ értéke 1 vagy 0 aszerint, hogy $i = j$-e vagy sem. A másik oldalba b_j-t helyettesítve ugyanez az érték adódik.

7.7.23. Az összegtartás azt jelenti, hogy

$$\psi \circ (f_1 + f_2) \circ \varphi = \psi \circ f_1 \circ \varphi + \psi \circ f_2 \circ \varphi \,.$$

Ez egy általános $n \in N$ elem behelyettesítésével igazolható. A skalárszoros-tartás azt jelenti, hogy

$$\psi \circ (rf) \circ \varphi = r(\psi \circ f \circ \varphi) \,.$$

Ez azért igaz, mert ψ tartja a skalárral szorzást. Láthatjuk, hogy R kommutativitását nem használtuk ki, az azért szükséges, mert általában az rf már R-homomorfizmus sem lesz.

7.7.24. Az első állításhoz azt kell megmutatni, hogy ha $f \in \mathrm{Hom}_R(L, K)$, akkor

$$f \circ (\psi \circ \varphi) = (f \circ \psi) \circ \varphi \,,$$

ami nyilvánvaló. A másik állítás hasonlóan igazolható.

7.7.25.

(1) $\mathrm{Hom}(\mathbb{Z}_n^+, \mathbb{Z}^+) = 0$, mert véges rendű elem képe véges rendű. Általában igaz, hogy $\mathrm{Hom}(A, B) = 0$, ha A torziócsoport, B pedig torziómentes.
(2) $\mathrm{Hom}(\mathbb{Q}^+, \mathbb{Z}_n^+) = 0$, mert $\mathbb{Q}^+$ osztható csoport, $\mathbb{Z}_n^+$-nak pedig csak a $\{0\}$ osztható részcsoportja (7.7.14. és 7.7.19. Gyakorlatok).
(3) $\mathrm{Hom}(\mathbb{Q}^+, \mathbb{Q}^+) \cong \mathbb{Q}^+$, mert a homomorfizmusok pontosan a $\varphi_r(x) = rx$ leképezések, ahol $r \in \mathbb{Q}$. Ehhez csak azt kell meggondolni, hogy ha $\varphi(1) = r$, akkor $\varphi(1/n)$ egy olyan elem, amelynek az n-szerese r, tehát csakis r/n lehet.
(4) $\mathrm{Hom}(\mathbb{Z}_{p^\infty}, \mathbb{Z}_n^+) = 0$ ugyanazért, mint a (2) pontban, hiszen $\mathbb{Z}_{p^\infty}$ is osztható csoport (7.7.18. Gyakorlat).

7.7.26. Ha $\varphi \in \mathrm{Hom}(\mathbb{Z}_m^+, B)$, akkor legyen $b = \varphi(1)$. Mivel $m \cdot 1 = 0$, ezért $mb = 0$ is teljesül, vagyis $b \in B[m]$. Persze $\varphi(x) = xb$ minden $x \in \mathbb{Z}_m^+$-ra (itt xb-t úgy értjük, mint a b csoportelem x egész számszorosát, vö. 2.2.36. Gyakorlat). Megfordítva, jelölje $b \in B[m]$ esetén φ_b azt a leképezést, amelyre $\varphi(x) = xb$ minden $x \in \mathbb{Z}_m^+$-ra. Megmutatjuk, hogy ez homomorfizmus. Ehhez azt kell belátni, hogy

$$\varphi_b(x +_m y) = \varphi(x) + \varphi(y) \,.$$

A bal oldalon $(x +_m y)b$, a jobb oldalon $xb + yb$ áll. Ez utóbbi $(x + y)b$-vel egyenlő a többszörös tulajdonságai miatt. Az, hogy $(x +_m y)b = (x + y)b$ azért teljesül, mert $(x + y) - (x +_m y)$ osztható m-mel, viszont $mb = 0$.

Ha az Olvasó nem érti, hogy miért szükséges ilyen részletesen indokolni a fentieket, akkor nézze meg a 2.2.40. Gyakorlat megoldását. Ide kapcsolódik a 7.3.15. Gyakorlat is, mert valójában arról van szó, hogy $B[m]$ modulus lesz a $\mathbb{Z}_m \cong \mathbb{Z}/(m)$ gyűrű fölött (sőt, az $mA = 0$ tulajdonságú Abel-csoportok között a $\mathbb{Z}_m^+$ az 1 elemmel generált szabad). Mivel $mB[m] = 0$, a fenti számolás helyett a 7.7.10. Gyakorlatot is alkalmazhattuk volna. Nagyon fontos pontosan látni, hogy a különböző jóldefiniáltságok milyen viszonyban állnak egymással.

Meg kell még mutatni, hogy a $b \leftrightarrow \varphi_b$ leképezés izomorfizmus lesz $\mathrm{Hom}(\mathbb{Z}_m^+, B)$ és $B[m]$ között. Ez azért igaz, mert az $x(b_1 + b_2) = xb_1 + xb_2$ összefüggés következik a többszörös tulajdonságaiból.

7.7.27.

7.7.28. Az összes állítás csak rutinszerű ellenőrzést kíván, amit az Olvasóra hagyunk.

7.8. A tenzorszorzat.

7.8.2. Az összegtartás az első, illetve a második változóban pontosan a két disztributív szabály, ez nemkommutatív gyűrűben is igaz. A skalárszoros-tartás az első változóban azt jelenti, hogy $(rx)y = r(xy)$, ez az R szorzásának az asszociativitásából következik. A skalárszoros-tartás a második változóban azt jelenti, hogy $x(ry) = r(xy)$. Ennek igazolásához R kommutativitását is fel kell használnunk.

7.8.3. Legyen $e_1, \ldots, e_k$, illetve $g_1, \ldots, g_\ell$ a T^k, illetve a T^ℓ vektortér szokásos bázisa, és $t_{ij} = f(e_i, g_j)$. Ekkor $u = x_1e_1 + \ldots + x_ke_k$, és $v = y_1g_1 + \ldots + y_\ell g_\ell$. Innen az állítás a bilinearitás miatt adódik.

7.8.4. Ha $f : N \times M \to K$ bihomomorfizmus, és $s \in R$, akkor sf is teljesíti a 7.8.1. Definícióban kirótt négy tulajdonságot. Például a (4)-et azért, mert $sr = rs$, és így

$$(sf)(m, rn) = s\big(f(m, rn)\big) = s\big(rf(m, n)\big) = (sr)f(m, n) = r\big((sf)(m, n)\big)\,.$$

Hasonlóan igazolható a másik három tulajdonság is. Meg kell mutatni, hogy két bilineáris függvény összege is bilineáris, továbbá, hogy a pontonkénti összeadásra és skalárral való szorzásra teljesül az összes modulus-axióma. A 7.7.2. Gyakorlat megoldásához hasonlóan ezt is az Olvasóra hagyjuk.

7.8.5. A bihomomorfizmus-tulajdonságokat úgy is fogalmazhatjuk, hogy az egyik változót rögzítve a másikban R-homomorfizmust kapunk. Így az állítás abból következik, hogy R-homomorfizmusok kompozíciója is R-homomorfizmus.

7.8.7. Természetesen a $\mathbb{Z}_3$ testen is bihomomorfizmus a szorzás (sőt, akkor is az, ha a $\mathbb{Z}_3^+$-t nem $\mathbb{Z}_3$, hanem $\mathbb{Z}$ fölött tekintjük modulusnak). Legyen $f(1, 1) = g$, akkor nyilván $f(m, n) = mng$. Tekintsük a $\varphi(n) = ng$ leképezést $\mathbb{Z}_3^+$-ból K-ba. Ha erről sikerül megmutatni, hogy homomorfizmus, akkor készen vagyunk. De ez igaz, mert $\varphi(n) = f(n, 1)$.

7.8.17.

(1) $\mathbb{Z}^+ \otimes \mathbb{Z}_n^+ \cong \mathbb{Z}_n^+$. A számolás nagyon hasonló a 7.8.6. Példa megoldásához, általánosságban a 7.8.18. Gyakorlat megoldásában szerepel.
(2) $\mathbb{Z}_m^+ \otimes \mathbb{Z}_n^+ \cong \mathbb{Z}_{(m,n)}^+$. A közvetlen számolás helyett megtehetjük, hogy megoldjuk a 7.8.19. Gyakorlatot, majd alkalmazzuk a 7.3.13. Gyakorlatot.
(3) $\mathbb{Q}^+ \otimes \mathbb{Z}_n^+ = 0$.
(4) $\mathbb{Z}_{p^\infty} \otimes \mathbb{Z}_n^+ = 0$.
(5) $\mathbb{Z}_{p^\infty} \otimes \mathbb{Z}_{p^\infty} = 0$.

Az utolsó három csoport a 7.8.20. Gyakorlat miatt nulla.

7.8.18. Legyen M egy bal R-modulus, $r_i, s_i \in R$ és $b_i \in M$, ekkor

$$\sum_i r_i(s_i \otimes b_i) = 1 \otimes (\sum_i r_i s_i b_i)\,.$$

Ezért ${}_RR \otimes M$ minden eleme $1 \otimes b$ alakban írható alkalmas $b \in M$-re. Tekintsük azt a $\varphi : M \to {}_RR \otimes M$ leképezést, amelyre $\varphi(b) = 1 \otimes b$, ez tehát szürjektív homomorfizmus.

A φ inverzének a megkonstruálásához legyen $f(r, b) = rb$. Ez nyilván bihomomorfizmus ${}_RR \times M$-ből M-be, így átvezethető a tenzorszorzaton (7.8.12. Tétel), vagyis létezik olyan $\psi : {}_RR \otimes M \to M$ homomorfizmus, hogy

$$\psi(r \otimes b) = f(r, b) = rb$$

minden $r \in R$-re és $b \in M$-re. Speciálisan ha $r = 1$, akkor azt kapjuk, hogy ψ az imént definiált φ-nek inverze.

7.8.19. Ha $n_i \in \mathbb{Z}$, $m_i \in \mathbb{Z}_m$ és $b_i \in B$, akkor

$$\sum_i n_i(m_i \otimes b_i) = 1 \otimes (\sum_i n_i m_i b_i)\,.$$

Ezért $\mathbb{Z}_m^+ \otimes B$ minden eleme $1 \otimes b$ alakban írható alkalmas $b \in B$-re. Tekintsük azt a $\varphi_0 : B \to \mathbb{Z}_m^+ \otimes B$ leképezést, amelyre $\varphi_0(b) = 1 \otimes b$, ez tehát szürjektív homomorfizmus. De $mB \subseteq \mathrm{Ker}(\varphi_0)$, mert

$$\varphi_0(mb) = (1 \otimes mb) = m(1 \otimes b) = (m \cdot 1 \otimes b) = 0 \otimes b = 0\,.$$

Ezért (a 7.1.14. Gyakorlat miatt) a $\varphi(b + mB) = 1 \otimes b$ leképezés jóldefiniált, és homomorfizmus B/mB-ből $\mathbb{Z}_m^+ \otimes B$-be.

A φ inverzének a megkonstruálásához tekintsük az $f(n, b) = nb + mB$ képlettel definiált leképezést. Ez nyilván bihomomorfizmus $\mathbb{Z}^+ \times B$-ből B/mB-be, mi azonban az első tényezőbe az $\mathbb{Z}$ helyett a $\mathbb{Z}_m$ elemeit szeretnénk írni. Ehhez azt kell megmutatni, hogy $n_1 \equiv n_2\ (m)$ esetén $f(n_1, b) = f(n_2, b)$. Ez azonban világos, mert ha $n_2 = n_1 + mk$, akkor

$$f(n_2, b) = n_2 b + mB = n_1 b + m(kb) + mB = n_1 b + mB = f(n_1, b)\,.$$

Ezért f-et tekinthetjük egy $\mathbb{Z}_m^+ \times B \to B/mB$ bihomomorfizmusnak is (igazából azt használtuk föl, hogy $\mathbb{Z}_m \cong \mathbb{Z}/(m)$, hasonló gondolatmenet szerepelt a 7.7.26. Gyakorlat megoldásában is). Így f átvezethető a tenzorszorzaton (7.8.12. Tétel), vagyis létezik olyan $\psi : \mathbb{Z}_m^+ \otimes B \to B/mB$ homomorfizmus, hogy

$$\psi(n \otimes b) = f(n, b) = nb + mB$$

minden $n \in \mathbb{Z}_m$-re és $b \in B$-re. Speciálisan ha $n = 1$, akkor azt kapjuk, hogy ψ az imént definiált φ-nek inverze.

7.8.20. Legyen A osztható, B torziócsoport. Ha $a \in A$ és $b \in B$, ahol $o(b) = n$ (ami véges, hiszen B torziócsoport), akkor mivel A osztható, van olyan $c \in A$, hogy $nc = a$. Így

$$a \otimes b = (nc) \otimes b = n(c \otimes b) = c \otimes (nb) = c \otimes 0 = 0\,.$$

7.8.21. Legyen $A = \mathbb{Z}^+$, $B = \mathbb{Q}^+$ és $C = \mathbb{Z}_2^+$. Ekkor $A \otimes C \cong \mathbb{Z}_2$ (7.8.18. Gyakorlat), és $B \otimes C = 0$ (7.8.20. Gyakorlat). Az $1 \otimes 1$ az első csoportban nem nulla, a másodikban nulla. Ha A direkt összeadandó B-ben, akkor ez a 7.8.23. Feladat (3) pontjának megoldása miatt nem fordulhat elő.

7.8.22. A 7.8.10. Tételben kirótt kívánalmakat f_0-ra és f_1-re is alkalmazhatjuk. Ezért olyan φ és ψ homomorfizmusokat nyerünk, melyekre tetszőleges $(m, n) \in M \times N$ esetén $f_1(m, n) = \varphi f_0(m, n)$ és $f_0(m, n) = \psi f_1(m, n)$. Azt kell megmutatni, hogy φ és ψ egymás inverzei. Ehhez az egyértelműséget használjuk. Tudjuk, hogy

$$(\psi \circ \varphi) f_0(m, n) = f_0(m, n) = id_{K_0} f_0(m, n)\,.$$

Az egyértelműség miatt tehát $\psi \circ \varphi = id_{K_0}$, és ugyanígy $\varphi \circ \psi = id_{K_1}$.

7.8.23. Az (1)-beli izomorfizmus igazolásához tekintsük az $f(m, n) = n \otimes m$ bihomomorfizmust. Ezt a tenzorszorzaton átvezetve egy $\varphi : M \otimes N \to N \otimes M$ homomorfizmust kapunk, melyre $\varphi(m \otimes n) = n \otimes m$. A φ inverzét az M és N megcserélésével konstruálhatjuk meg.

A (2) bizonyítása hasonló. Rögzített $m \in M$ esetén tekintsük az

$$f(m, n, k) = (m \otimes n) \otimes k$$

bihomomorfizmust $N \times K$-ból $(M \otimes N) \otimes K$-ba. Ez egy $\varphi_m : N \otimes K \to (M \otimes N) \otimes K$ homomorfizmust eredményez, amelyre $\varphi_m(n \otimes k) = (m \otimes n) \otimes k$. Most legyen

$$g(m, x) = \varphi_m(x)\,.$$

Ez egy bihomomorfizmus $M \times (N \otimes K)$-ból $(M \otimes N) \otimes K$-ba, amit a tenzorszorzaton keresztülvezetve egy

$$m \otimes (n \otimes k) \mapsto (m \otimes n) \otimes k$$

homomorfizmust kapunk. Ennek az inverzét is hasonlóan konstruálhatjuk meg.

A (3) állítás esetében az Útmutatóban megadott izomorfizmust bizonyítjuk. Tegyük föl, hogy $m = (\dots, m_i, \dots) \in \bigoplus_i M_i$ és $k \in K$. Ekkor

$$f(m,k) = (\dots, m_i \otimes k, \dots)$$

bihomomorfizmust definiál, amely egy olyan $\varphi : \big(\bigoplus_i M_i\big) \otimes K \to \bigoplus_i (M_i \otimes K)$ homomorfizmust eredményez, melyre

$$\varphi\big((\dots, m_i, \dots) \otimes k\big) = (\dots, m_i \otimes k, \dots)\,.$$

Ennek inverzét a következőképpen kapjuk meg. Legyen $m_i \in M_i$ esetén

$$f_i(m_i,k) = (\dots, 0, m_i, 0, \dots) \otimes k \in \Big(\bigoplus_i M_i\Big) \otimes K\,.$$

Ezt a tenzorszorzaton keresztülvezetve egy $\psi_i : M_i \otimes K \to \big(\bigoplus_i M_i\big) \otimes K$ homomorfizmust kapunk. Legyen

$$\psi(\dots, x_i, \dots) = \sum_i \varphi_i(x_i)$$

a $\bigoplus_i (M_i \otimes K)$ csoporton értelmezett homomorfizmus. Ez értelmes, mert az összegnek csak véges sok nem nulla tagja van, és nyilván a φ inverze.

Egy végtelen direkt szorzatnak egy M modulussal vett tenzorszorzatát általában nem lehet leírni a tényezőknek az M-mel vett tenzorszorzataival. Például megmutatható, hogy ha p prím, akkor

$$\Big(\prod_{i=1}^{\infty} \mathbb{Z}^+_{p^i}\Big) \otimes \mathbb{Q}^+$$

nem nulla (ez azon múlik, hogy ennek a direkt szorzatnak van végtelen rendű eleme is), de mindegyik $\mathbb{Z}^+_{p^i} \otimes \mathbb{Q}^+$ csoport nulla a 7.8.20. Gyakorlat miatt.

Végül a (4) bizonyításához legyen $\varphi : M \otimes N \to K$ egy homomorfizmus. Ehhez rendeljük hozzá azt az $\alpha : M \to \mathrm{Hom}(N,K)$ homomorfizmust, melyre

$$\big(\alpha(m)\big)(n) = \varphi(m \otimes n)\,.$$

Az inverz megkonstruálásához $\alpha : M \to \mathrm{Hom}(N,K)$ esetén tekintsük az

$$f(m,n) = \big(\alpha(m)\big)(n)$$

bihomomorfizmust. Ezt a tenzorszorzaton átvezetve egy ψ homomorfizmust kapunk, rendeljük hozzá ezt az α-hoz.

7.8.24. A $\mathrm{Hom}(\mathbb{Z}_2^+, \mathbb{Z}_4^+)$ csoport izomorf a $\mathbb{Z}_2^+$-szal (7.7.26. Gyakorlat), és ennél az izomorfizmusnál $\varphi \leftrightarrow 1$. Persze $1 \otimes 1$ nem nulla a $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \cong \mathbb{Z}_2^+$ csoportban (7.8.19. Gyakorlat). Az első értelmezés szerint viszont $\varphi \otimes \varphi = 0$, mert

$$(\varphi \otimes \varphi)(1 \otimes 1) = 2 \otimes 2 = 2(1 \otimes 2) = 1 \otimes (2 \cdot 2) = 1 \otimes 0 = 0\,.$$

7.8.25.

7.8.26. Legyen $s \in T$, és tekintsük azt az $f : T \times M \to T \otimes M$ bihomomorfizmust, amelyre $f(t, m) = (st) \otimes m$. Ez átvezethető a tenzorszorzaton, vagyis létezik egy olyan $\varphi_s : T \otimes M \to T \otimes M$ homomorfizmus, hogy $\varphi_s(t \otimes m) = (st) \otimes m$. Ezt az elemet nevezzük el $s(t \otimes m)$-nek. Könnyű belátni, hogy

$$\varphi_{s_1+s_2} = \varphi_{s_1} + \varphi_{s_2} \quad \text{és} \quad \varphi_{s_1 s_2} = \varphi_{s_1} \circ \varphi_{s_2} .$$

Ezért a most definiált szorzás modulussá teszi $T \otimes M$-et T fölött (ez lényegében következik a 7.7.28. Gyakorlatból). Megjegyezzük, hogy nem használtuk ki azt, hogy T az R hányadosteste, valójában minden olyan kommutatív T jó, amelynek az R részgyűrűje (és T egységeleme ugyanaz, mint R egységeleme).

Ha most M-et fölbontjuk az M_i ciklikus modulusok direkt összegére, akkor $T \otimes M$ is fölbomlik a $T \otimes M_i$ modulusok direkt összegére. Ez következik a 7.8.23. Feladat (3) pontjából, ha $T \otimes M$-et mint R-modulust tekintjük. Az $s \in T$-vel való szorzás definíciója miatt $T \otimes M_i$ részmodulusa lesz $T \otimes M$-nek T fölött is.

Mivel T az R hányadosteste, a T osztható R-modulus abban az értelemben, hogy R minden nem nulla elemével oszthatunk benne. Ezért a 7.8.20. Gyakorlathoz hasonlóan látjuk, hogy $T \otimes M_i = 0$ akkor, ha az M_i ciklikus modulus rendje nem nulla. Ha viszont M_i nulla rendű ciklikus, vagyis ${}_R R$-rel izomorf, akkor $T \otimes R_R$ izomorf T-vel a 7.8.18. Gyakorlat miatt. Könnyű megmutatni, hogy ez az izomorfizmus a T elemeivel szorzást is tartja. Ezért beláttuk, hogy a $T \otimes M$ vektortér T fölött, melynek dimenziója az M bármelyik ciklikusok direkt összegére való felbontásában a nulla rendű ciklikus összeadandók száma. Ez a 7.5.1. Gyakorlat második állítását, és a 7.5.2. Lemmát helyettesíti az egyértelműség bizonyításában.

11.8. Általános algebrák, hálók

8.1. Hálók.

8.1.2. Ha $M \subseteq H$ és $M \subseteq K$, akkor M minden eleme benne van K-ban és H-ban is, tehát $H \cap K$-ban is. Ezért $M \subseteq H \cap K$.

8.1.4. Ha m_1 és m_2 is legnagyobb eleme X-nek, akkor $m_1 \geq m_2$ (mert m_1 legnagyobb elem és $m_2 \in X$), továbbá $m_2 \geq m_1$ (mert m_2 legnagyobb elem és $m_1 \in X$). A rendezés antiszimmetriája miatt tehát $m_1 = m_2$. Így (1) igaz, és ebből (2) is világos, hiszen az X legnagyobb alsó korlátja az alsó korlátok halmazának legnagyobb eleme. Végül ha m legkisebb eleme X-nek, és m' alsó korlátja X-nek, akkor $m \in X$ miatt $m' \leq m$, tehát m tényleg legnagyobb alsó korlát.

8.1.6. A rendezés megfordítása is reflexív, antiszimmetrikus és tranzitív, vagyis rendezés. Ami az eredeti rendezésnél alsó korlát, az a megfordított rendezésnél felső korlát lesz, egy részhalmaz legnagyobb eleme a legkisebb elemmé, a maximális elemei minimális elemekké válnak.

8.1.8. Az egyetlen, amelyik nem háló, a felső sor jobboldali eleme, hiszen itt az a és b elemeknek nincs legkisebb felső korlátja. Azt, hogy a többi háló, vagy úgy igazolhatjuk, hogy az összes elempárnak megkeressük a legnagyobb alsó és legkisebb felső korlátját, vagy pedig úgy, hogy megmutatjuk, hogy egy ismert háló rajzáról van szó (lásd a 8.1.27. és a 8.1.10. Gyakorlatokat). Például M_3 a Klein-csoport összes részcsoportjainak a hálója (a 8.1.20. Tételben látjuk majd be, hogy a részcsoportok mindig hálót alkotnak).

8.1.10. Ha $h \leq k$, akkor $\{h, k\}$-nak h a legkisebb eleme, és így a legnagyobb alsó korlátja (8.1.4. Gyakorlat). Ugyanígy $h \vee k = k$ (ez a duális állítás). Ezért bármely két összehasonlítható elemnek van legnagyobb alsó és legkisebb felső korlátja, és így minden lánc tényleg háló. A racionális számok halmaza a szokásos rendezésre olyan lánc, amelyben nincs fedés, hiszen bármely két különböző racionális szám között van harmadik.

8.1.12. A C_2^2, a C_2^3 és az M_3 hálókban minden nem nulla elem atomok egyesítése és minden 1-től különböző elem koatomok metszete. A D_1-ben minden elem atomok egyesítése, de nem minden elem koatomok metszete, a duális D_2-ben pedig pont fordítva.

Egy darab atom természetesen önmagának az egytagú egyesítése. Kényelmesebb szóhasználatot eredményez, ha a nullelemet nulla darab atom egyesítésének, az egységelemet pedig nulla darab koatom metszetének tekintjük (vö. 8.1.19. Gyakorlat). A fenti utolsó mondatban már használtuk is ezt a konvenciót.

8.1.13. Mivel $u, v \leq u \vee v$, az $u \vee v$ felső korlátja x-nek és y-nak. Az $x \vee y$ legkisebb felső korlát, tehát $x \vee y \leq u \vee v$. A másik állítás az elsőnek a duálisa. Vigyázzunk azonban, az első állítás pontos duálisa a következő: $x \geq u$ és $y \geq v$ esetén $x \wedge y \geq u \wedge v$. Így ahhoz, hogy a második állítást megkapjuk, még változók cseréjére is szükség van.

8.1.14. Az asszociativitás azért teljesül, mert mind $(x \wedge y) \wedge z$, mind $x \wedge (y \wedge z)$ az $\{x, y, z\}$ halmaz legnagyobb alsó korlátja. Az elnyelési tulajdonság azért igaz, mert $x \geq x \wedge y$, és így a legkisebb felső korlátjuk x lesz.

8.1.15. Ha $h \leq k$, akkor $h \vee k = k$ és $h \wedge k = h$ (8.1.4. Gyakorlat). Megfordítva, ha h és k legnagyobb alsó korlátja h, akkor h alsó korlátja k-nak, vagyis $h \leq k$. Ugyanígy $h \vee k = k$-ból is következik, hogy $h \leq k$.

8.1.17. Legyen $y = x \wedge x$. Ekkor $x \vee y = x \vee (x \wedge x)$, ami (4) miatt x. Messük el ezt az egyenlőséget (balról) x-szel: $x \wedge x = x \wedge (x \vee y)$, és ez (4) miatt ismét x. A bizonyítás dualizálásával $x \vee x = x$ adódik.

8.1.19. Az üres halmaznak minden elem alsó (és felső) korlátja, hiszen minden $x \in L$ és $y \in \emptyset$ elemre tényleg teljesül, hogy $x \leq y$ (hiszen ilyen y nincs is). Az üres halmaz legnagyobb alsó korlátja tehát az L összes elemei közül a legnagyobb, ami 1_L.

Akit zavar az előző gondolatmenet, az gondolja végig a következőt. Tudna-e ellenpéldát adni arra az állításra, hogy az üres halmaznak minden elem alsó korlátja? Egy ilyen ellenpélda az x elem lenne akkor, ha x nem alsó korlátja az üres halmaznak. Csak attól lehetne nem alsó korlát, ha lenne az üres halmaznak egy y eleme, amelynél x nem lenne kisebb vagy egyenlő. De ilyen y nincs, hiszen az üres halmaznak nincs eleme. Hasonló jelenséggel már találkoztunk az üres feltétel vizsgálatakor, a 3.9.7. Következmény bizonyítása utáni megjegyzésben. Érdemes elolvasni ezzel kapcsolatban az A.1. Szakaszban található logikai összefoglalót is.

8.1.22. Tegyük föl, hogy $\theta_1 \leq \theta_2$ és $x \equiv_1 y$. Ez azt jelenti, hogy x és y a θ_1 partíciónak ugyanabban a V_1 osztályában vannak. Mivel $\theta_1 \leq \theta_2$, a V_1 része egy alkalmas θ_2-osztálynak, és így $x \equiv_2 y$ is teljesül. Megfordítva, tegyük föl, hogy $\equiv_1$ részhalmaza $\equiv_2$-nek, vagyis minden $x, y \in U$ esetén $x \equiv_1 y \implies x \equiv_2 y$. Legyen V_1 egy tetszőleges θ_1-osztály, meg kell mutatni, hogy van olyan V_2 osztálya θ_2-nek, hogy $V_1 \subseteq V_2$. Legyen $x \in V_1$ egy tetszőleges elem, és V_2 az x elem θ_2-osztálya. Annak belátásához, hogy $V_1 \subseteq V_2$, válasszunk egy tetszőleges $y \in V_1$ elemet. Ekkor $x \equiv_1 y$, és így a feltételünk szerint $x \equiv_2 y$ is igaz. Ezért y benne van az x elem θ_2-osztályában, vagyis V_2-ben.

8.1.24. Az eredmény 14589|23|67.

8.1.25. Először a feladat utolsó kérdésére válaszolunk. Tegyük föl, hogy x és y között van egy olyan sorozat, amit a feladat leír, azzal a különbséggel, hogy z_0 és z_1 között nem θ, hanem ρ szerepel, és azután következik θ és ρ váltakozva. Ekkor duplázzuk meg z_0-t, és a kapott elemek közé írjunk θ-t. Ez megtehető, mert a θ partíciónál z_0 egy osztályban van önmagával. A kapott, eggyel hosszabb sorozat már θ-val kezdődik. Hasonlóan javíthatjuk ki egy sorozat végét is úgy, hogy ρ-val végződjön.

Legyen $x \equiv y$ akkor és csak akkor, ha x és y között van a feladatban leírt sorozat, belátjuk, hogy $\equiv$ ekvivalencia-reláció. A reflexivitás nyilvánvaló, hiszen nulla hosszú sorozatokat is vehetünk. A tranzitivitás is világos, hiszen két megfelelő sorozatot egymás után fűzve ismét megfelelő sorozatot kapunk. A szimmetria igazolásához az x és y közötti sorozatot fordítsuk meg, majd egészítsük ki az előző bekezdésben leírt módon. Így $\equiv$ tényleg ekvivalencia-reláció, jelölje ψ a hozzá tartozó partíciót. Meg kell mutatnunk, hogy ψ a θ és ρ legkisebb felső korlátja.

Ha $x \; \theta \; y$, akkor az (x, y, y) sorozat mutatja, hogy $x \equiv y$, vagyis $\theta \leq \psi$. Hasonlóan $\rho \leq \psi$. Ezért ψ felső korlát. Ha $\theta \leq \psi'$ és $\rho \leq \psi'$ teljesül valamilyen ψ' partícióra, akkor be kell látni, hogy $\psi \leq \psi'$. De ez világos, mert ha $x \; \psi \; y$, akkor x és y között van a feladatban leírt sorozat, és ennek minden eleme ugyanabban a ψ'-osztályban kell, hogy legyen.

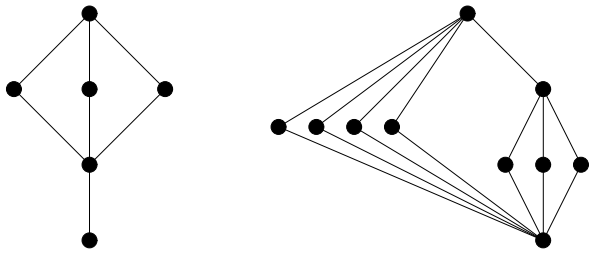
8.1.27. A kételemű és a háromelemű halmaz összes részhalmazainak hálója a 8.3. Ábrán a C_2^2 és a C_2^3 háló (ezt a jelölést a direkt szorzat fogalmának a bemutatása után magyarázzuk meg). A kételemű halmaz partícióhálója a kételemű lánc, a háromelemű halmaz partícióhálója pedig az ugyanezen az ábrán található M_3 háló.

8.1.29. C_2^2, C_2^3, M_3, N_5.

8.1.29. Legyen θ partíció az U halmazon, ehhez keresünk egy ρ komplementumot. Válasszunk ki a θ minden osztályából egyetlen elemet, ezek halmazát jelölje V. A ρ partíció osztályai legyenek V mellett csupa egyelemű halmazok. Nyilván $\theta \wedge \rho = 0_U$, és U bármely két x és y eleme között van a 8.1.25. Feladatban leírt sorozat: x-ből elmegyünk a vele egy θ-osztályban lévő V-beli elembe, innen pedig ρ mentén az y-nal egy θ-osztályban lévő V-beli elembe. Ezért $\theta \vee \rho = 1_U$.

8.1.30. A 4.4.33. Gyakorlat miatt az S_3 részcsoporthálója a 8.3. Ábrán látható M_3 hálóhoz hasonlít, csak a középső sorban nem három, hanem négy elem van. A Q kvaterniócsoportnak minden részcsoportja normálosztó (4.7.36. Gyakorlat), a normálosztóhálója izomorf a D_4 normálosztóhálójával (vö. 6.1. Ábra), és az alábbi 11.1. Ábrán látható.

Az A_4 alternáló csoportnak nincs hatelemű részcsoportja (mert az kettő indexű, és így normálosztó lenne, ami a 4.7.36. Gyakorlat szerint lehetetlen). Az egyetlen 2-Sylow részcsoport a Klein-csoporttal izomorf normálosztó, és így minden 2-hatvány rendű részcsoport ennek része. A fennmaradó nemtriviális részcsoportok a négy darab 3-Sylow. A rajz szintén a 11.1. Ábrán látható.



11.1. Ábra. A Q és az A_4 csoportok részcsoporthálója.

8.2. Algebrai struktúrák.

8.2.4. A részcsoport az, ami a szorzásra, és az inverzképzésre zárt, továbbá egy részcsoport egységeleme ugyanaz, mint az egész csoporté (lásd 2.2.16. Feladat). Ha az inverzképzést nem vesszük be műveletnek, akkor például az egész számok additív csoportjának a pozitív egészek részhalmaza részalgebrája lesz, de ez nem részcsoport. Az egységelemet viszont nem szükséges bevenni műveletnek, mert egy részalgebra nem lehet üres, és így az egységelem megkapható hh^{-1} alakban, vagyis minden részalgebrában benne lesz.

8.2.6. Igen, hálót alkotnak, (amely „ugyanúgy néz ki”, mint a C_2^2 háló), de nem alkotnak részhálót, mert a metszetképzés kivezet ebből a halmazból.

8.2.7. Pontosan a láncokban, hiszen $\{h, k\}$ akkor és csak akkor részháló, ha h és k összehasonlítható.

8.2.13. Mivel φ tartja az egyesítést, $\varphi(h \vee k) = \varphi(h) \vee \varphi(k)$. Ha $h \leq k$, akkor $h \vee k = k$, ezért $\varphi(k) = \varphi(h) \vee \varphi(k) \geq \varphi(h)$.

8.2.14. Tekintsük a 8.3. Ábrán látható C_2^2 hálót. Jelölje a C_4 négyelemű lánc elemeit $0 < c < d < 1$. Ha $\varphi(0) = 0$, $\varphi(a) = c$, $\varphi(b) = d$, $\varphi(1) = 1$, akkor $\varphi : C_2^2 \to C_4$ rendezéstartó bijekció, de nem tartja a és b metszetét.

8.2.20. Az állításokat megfogalmazzuk, az Útmutató jelöléseit használva, a bizonyításokat az Olvasóra hagyjuk. Legyen $\varphi : A \to C$ szürjektív homomorfizmus, melynek magja θ.

Ha B részalgebrája A-nak, akkor $\varphi(B)$ részalgebrája C-nek, és ennek teljes inverz képe φ-nél éppen a $B[\theta]$ részalgebra lesz. Speciálisan az A/θ részalgebrái kölcsönösen egyértelmű megfeleltetésben állnak az A azon részalgebráival, amelyek θ-osztályok egyesítései.

Ha ψ kongruenciája C-nek, akkor ψ osztályainak teljes inverz képei kongruenciát alkotnak az A algebrán. Ez a megfeleltetés kölcsönösen egyértelmű, rendezés-, metszet-, és egyesítéstartó a C összes kongruenciái és az A algebra θ-t tartalmazó kongruenciái között.

Első izomorfizmus-tétel: $B[\theta]/\theta \cong B/(B|_\theta)$.

Második izomorfizmus-tétel: $(A/\theta)/(\rho/\theta) \cong A/\rho$.

8.2.21. Legyenek θ_j kongruenciák ($j \in J$), és θ a metszetük. Ekkor a tetszőleges $a, b \in A$ elemek akkor és csak akkor akkor kongruensek θ-nál, ha mindegyik θ_j-nél kongruensek. Tegyük föl, hogy f egy n-változós művelet, és $a_i \equiv b_i\ (\theta)$ $(1 \leq i \leq n)$. Ekkor minden $j \in J$-re $a_i \equiv b_i\ (\theta_j)$. Mivel θ_j kongruencia, $f(a_1, \ldots, a_n) \equiv f(b_1, \ldots, b_n)\ (\theta_j)$. Ez minden j-re igaz, ezért $f(a_1, \ldots, a_n) \equiv f(b_1, \ldots, b_n)\ (\theta)$. Tehát θ kongruencia.

8.2.30. Az világos, hogy $\theta \circ \rho$ mindig részhalmaza $\theta \vee \rho$-nak. Ha θ és ρ felcserélhetők, akkor a 8.1.25. Feladat megoldásának mintájára csak azt kell megmutatni, hogy $\theta \circ \rho$ már maga is ekvivalencia-reláció. A reflexivitás nyilvánvaló, a szimmetria azonnal látszik θ és ρ felcserélhetőségéből. Végül a tranzitivitás azért igaz, mert a $\circ$ művelet asszociativitását felhasználva

$$(\theta \circ \rho) \circ (\theta \circ \rho) = \theta \circ (\rho \circ \theta) \circ \rho = \theta \circ (\theta \circ \rho) \circ \rho = (\theta \circ \theta) \circ (\rho \circ \rho) = \theta \circ \rho\,,$$

hiszen $\theta \circ \theta = \theta$ és $\rho \circ \rho = \rho$.

8.2.33. Egy kétváltozós művelet megadásához az összes $a * b$ szorzat értékét meg kell mondani, azaz $4 \cdot 4 = 16$-féle eredményt. Mindegyiket 4-féleképpen választhatjuk, a lehetőségek száma tehát $2^{16} = 65536$.

8.2.34. Csak az eredményeket adjuk meg, néhány mintabizonyítással és bizonyítási ötlettel. Az (1) és (2) izomorfak (a négyelemű ciklikus csoporttal). A (9) és (10) is izomorfak a dualitás elve miatt. Más izomorfia nincs a felsorolt struktúrák között. Ezt a szokásos módon, invariánsok megadásával bizonyíthatjuk. Például különválaszthatjuk azokat, amelyek minden eleme idempotens (vagyis minden elemre $x * x = x$), ezek: (6), (8), (9), (10), (11), (12). Kikereshetjük azokat, amelyekben van nullelem (azaz $0 * x = x * 0$ minden x-re). Hasonló választóvíz az egységelem létezése is. A (3) és (4) azért nem izomorf, mert a (4)-ben minden szorzat értéke a nullelem. Ezek egyike sem izomorf az (5)-tel, mert az utóbbiban van olyan elem, amelynek hatványaiként az összes elem előáll.

A megadott struktúrák között nincs egyszerű. Például (5)-ön kongruencia, ha a 27 és a 81 egy osztályban van, a 3 és a 9 két egyelemű osztályban. A (6)-ban $x * y = x$ teljesül minden x, y-ra, és ezért minden partíció kongruencia (és mellesleg minden részhalmaz részalgebra). A (7)-ben is összeejthetjük a két konstans függvényt, és kongruenciát kapunk.

Az egy elemmel generálható struktúrák az (1), (2), (5). Direkt szorzatra bontható a (4), a (6) (hiszen ezekben minden partíció kongruencia), a (8) (ez nemcsak félcsoportként, hanem gyűrűként is izomorf a kételemű test direkt négyzetével), a (9), a (10) és a (12). A bizonyításhoz a legegyszerűbb, ha a szereplő struktúráknak lerajzoljuk a kongruencia-hálóját, és komplementumokat keresünk.

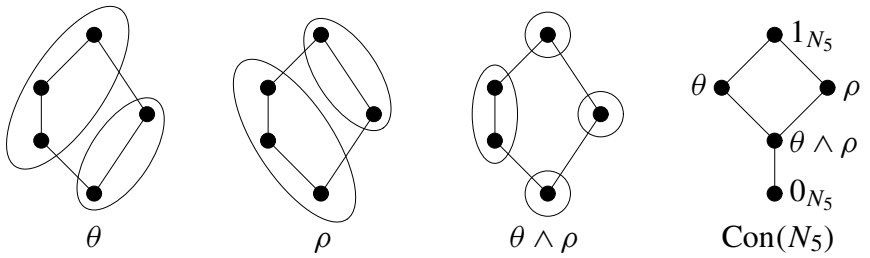
8.2.35. Ha $\equiv$ háló-kongruencia és $a \equiv b$, akkor ezt $c \equiv c$-vel egyesítve és metszve a kívánt tulajdonság adódik. Megfordítva, ha a gyakorlatban kirótt tulajdonság teljesül a $\equiv$ ekvivalencia-relációra, és $a \equiv b$, $c \equiv d$, akkor $a \equiv b$-ből $a \vee c \equiv b \vee c$ és $c \equiv d$-ből $b \vee c \equiv b \vee d$ következik, ahonnan a tranzitivitás miatt $a \vee c \equiv b \vee d$. A metszetről szóló állítás dualizálással adódik. Ezt a gondolatmenetet érdemes összevetni a 8.3.19. Gyakorlat megoldásával.

8.2.36. Legyen C egy $\equiv$ háló-kongruenciának osztálya. Ha $a, b \in C$, akkor $a \equiv b$, ahonnan $a \vee b \equiv a \vee a = a$, tehát $a \vee b$, és hasonlóan $a \wedge b$ is eleme C-nek. Tehát C részháló. Tegyük föl, hogy $h \leq a \leq k$ és $h, k \in C$. Ekkor $h \equiv k$, ahonnan a-val egyesítve $a = a \vee h \equiv a \vee k = k$. Ezért $a \in C$.

8.2.37. Először részletesen megmutatjuk, hogy M_3 egyszerű háló. Tegyük föl, hogy $\equiv$ egy nem nulla kongruencia, meg kell mutatnunk, hogy M_3 bármely két eleme kongruens. Mivel $\equiv$ nem nulla, van egy nem egyelemű C osztálya, amely a 8.2.36. Gyakorlat miatt konvex részháló. Mivel C véges, van egy legkisebb u és egy legnagyobb v eleme. Ha $u = 0$ és $v = 1$, akkor C konvexitása miatt készen vagyunk. Ha nem, akkor szimmetriaokokból (a dualitást is ide sorolva) föltehető, hogy $u = 0$ és $v = a$ (a 8.3. Ábra jelölése szerint). Tehát $a \equiv 0$, ahonnan $1 = b \vee a \equiv b \vee 0 = b$, és b helyett c-vel egyesítve $1 \equiv c$. De akkor $1 = 1 \wedge 1 \equiv b \wedge c = 0$. Ekkor pedig a konvexitás miatt $\equiv$-nek csak egy osztálya van.

Hasonló számolással (és megfelelő esetszétválasztással) kaphatjuk meg az N_5 háló kongruenciáit is. Az eredmény a 11.2. Ábrán látható.

Az $N_5/(\theta \wedge \rho)$ a négyelemű C_2^2 háló, a θ és ρ szerinti faktor pedig a kételemű lánc. A D_1 és D_2 hálók kongruencia-hálója is ugyanaz, mint az N_5 kongruencia-hálója, és a



11.2. Ábra. Az N_5 háló kongruenciái és kongruencia-hálója.

faktorhálók is ugyanazok lesznek. A D_1 esetében a legkisebb nem nulla kongruencia az, amelynél a 0 a b-vel, az a az egyetlen fedőjével, a c is az egyetlen fedőjével esik össze, az 1 pedig egyedül van.

A 8.3. Ábra hálói közül csak az M_3 egyszerű. Az ábrán a, b és c-vel jelölt elemek mindegyik hálóban egy minimális elemszámú generátorrendszert alkotnak (könnyű megmutatni ugyanis, hogy egy két elemmel generált hálónak maximum négy eleme lehet). Kivétel a D háló, ahol a, b, 0 lesz minimális generátorrendszer. Végül az ábrán szereplő hálók közül csak kettő bontható nemtriviálisan direkt szorzatra. A C_2^2 izomorf a kételemű lánc direkt négyzetével (ez indokolja a jelölését is). Ugyanígy a C_2^3 a kételemű háló direkt köbével izomorf.

8.2.38. A legfeljebb háromelemű hálók láncok (C_1, C_2, C_3). Négyelemű háló izomorfia erejéig kettő van, a láncon kívül a C_2^2 háló. Az ötelemű hálók száma öt, ezek, vagy a duálisuk a C_5 lánc kivételével mind szerepelnek a 8.3. Ábrán.

8.2.39. Az Útmutatóban megadott $*$ műveletre nézve nincs részalgebra, mert $x*x = x+_4 1$, és ezért minden elem generálja az algebrát már erre az egyváltozós műveletre nézve is. Ha $a < b$ kongruensek egy $\equiv$ kongruenciánál, akkor $a+1 = a*(a+1) \equiv b*(a+1) = a+_4 2$. Az $x*x$ unáris műveletet többször alkalmazva adódik, hogy bármely két szomszédos elem kongruens, és így a tranzitivitás miatt bármely két elem kongruens.

8.2.40. Legyenek $a_1, \ldots, a_N$ tetszőleges elemei a félcsoportnak, és $s_i = a_1 a_2 \ldots a_{i-1} a_i$ (az egymás mellé írás a félcsoport műveletét jelöli). Ha N nagyobb, mint a félcsoport elemszáma, akkor a kapott elemek között a skatulyaelv miatt van két egyenlő, mondjuk $s_i = s_j$, ahol $i < j$. Legyen $e = a_{i+1} a_{i+2} \ldots a_j$, ekkor $s_i e = s_j = s_i$, ahonnan $s_i e^k = s_i$ minden k-ra. A feltétel szerint $e^n = 0$ alkalmas n-re, de akkor $s_i = s_i e^n = 0$. Így pedig $a_1 a_2 \ldots a_N$ is nulla. Vagyis minden olyan szorzat nulla, amelyben a tényezők száma több, mint a félcsoport elemszáma.

8.2.41. Legyen $\equiv$ egy nullától különböző kongruencia egy véges U halmaz partícióhálóján. A 8.2.36. Gyakorlat szerint minden kongruenciaosztály konvex részháló, ezért vannak olyan $\theta \prec \rho$ partíciók az U-n, amelyek kongruensek. A fedés a partícióhálóban azt jelenti, hogy ρ a θ két osztályának egyesítésével kapható. Legyen a, illetve b eleme ennek a két

osztálynak, és ψ az a partíció, amelynek az egyetlen nem egyelemű osztálya $\{a, b\}$. Ekkor $\theta \vee \psi = \rho$ és $\theta \wedge \psi = 0_U$. Ezért $\theta \equiv \rho$-ból (ψ-vel metszve) $0_U \equiv \psi$ adódik.

Legyen most V tetszőleges részhalmaza U-nak, amely a és b közül pontosan egyet tartalmaz, és η az a partíció, amelynek az osztályai V és $U - V$. Ekkor η komplementuma ψ-nek, ezért $0_U \equiv \psi$-ből η-val egyesítve $\eta \equiv 1_U$ következik. Ez minden így gyártott η komplementumra igaz. Mivel minden $\equiv$-osztály részháló, ezeknek az η komplementumoknak a metszete is kongruens 1_U-val. De ez a metszet 0_U, hiszen U bármely két eleme elválasztható egy alkalmas V részhalmazzal.

8.3. Kifejezések, polinomok, szabad algebrák.

8.3.3. Nyilván $g_1(x_2, x_2) = g_1\big(\pi_2(x_1, x_2, x_3), \pi_2(x_1, x_2, x_3)\big)$, ezzel a technikával tehát változókat azonosíthatunk. Ugyanígy $g_3(x_3, x_1) = g_3\big(\pi_3(x_1, x_2, x_3), \pi_1(x_1, x_2, x_3)\big)$, ami változók cseréjét teszi lehetővé. Végül $g_2(x_3) = g_2\big(\pi_3(x_1, x_2, x_3)\big)$ bevezeti az extra x_1 és x_2 változókat. Így a gyakorlatban szereplő függvény minden argumentumát sikerült háromváltozóssá alakítanunk, vagyis a kompozíció immár a 8.3.1. Definícióban kívánt típusú.

8.3.6. Ha M egy (unitér) R-modulus, akkor a kifejezésfüggvényei az $r_1x_1 + \ldots + r_nx_n$ alakú függvények. Az nyilvánvaló, hogy ezek előállíthatók kompozíció segítségével az összeadásból, és az $x \mapsto rx$ alakú skalárral szorzásokból. Ahhoz, hogy nincs más kifejezésfüggvény, elég megmutatni, hogy a fenti alakú függvények halmaza zárt a kompozícióra, és tartalmazza a projekciókat. Utóbbi világos, hiszen az i-edik projekció az $1 \cdot x_i$ függvény. A kompozícióra zártság egyszerű számolással adódik: ha egy lineáris kombinációba lineáris kombinációt helyettesítünk, es felbontjuk a zárójeleket, akkor az eredmény is egy lineáris kombináció lesz.

8.3.9. Azt kell megmutatni, hogy egy $t \circ (g_1, \ldots, g_k)$ kompozíciót, ahol t is tetszőleges, már korábban megkapott kifejezésfüggvény, előállíthatunk több lépésben úgy, hogy az t-t alapműveletek kompozíciójára bontjuk. Ennek formális bizonyítása a t komplexitása szerinti indukcióval, a 8.3.8. Lemma bizonyításához hasonlóan történhet. Azon múlik igazából, hogy az általános kompozíció is asszociatív (a megfelelő értelemben).

8.3.10. A 8.2.16. Definícióban kiszabott kompatibilitási feltétel úgy fogalmazható, hogy ha mindegyik (a_i, b_i) pár eleme θ-nak, akkor $\big(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\big)$ is eleme. A direkt szorzatban komponensenként végezzük a műveleteket, ezért amikor az f (nevű) műveletet alkalmazzuk ezekre a párokra, akkor pont $\big(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\big)$ az eredmény. Vagyis a kompatibilitás feltétele azzal ekvivalens, hogy θ zárt az $A \times A$ alapműveleteire, azaz részalgebra.

8.3.11. Legyen f egy n-változós művelet, és $b_i = \varphi(a_i)$ (ha $1 \leq i \leq n$), ekkor mindegyik (a_i, b_i) pár eleme φ gráfjának. Az, hogy φ homomorfizmus, azt jelenti, hogy minden ilyen esetben $\big(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\big)$ is eleme a φ gráfjának. Ez pedig az előző gyakorlat megoldásában látott érvelés szerint azzal ekvivalens, hogy ez a gráf részalgebra $A \times B$-ben.

8.3.14. A 8.3.8. Lemma szerint minden részalgebra zárt az összes kifejezésfüggvényre. Ezért azt kell megmutatni, hogy ha t kifejezésfüggvény az A-n, akkor t-t komponensenként alkalmazva az A^n direkt hatvány egy kifejezésfüggvényét kapjuk. Ez nyilvánvaló, hiszen az alapműveleteket a direkt hatványban komponensenként alkalmazzuk (sőt az is világos, hogy az A^n-nek nincs is más kifejezésfüggvénye). (Ehhez hasonlóan írhatjuk le az $A \times B$ direkt szorzat kifejezésfüggvényeit is, lásd 8.3.23. Gyakorlat).

8.3.15. Adott $(a_1, \ldots, a_n) \in A^n$ esetén legyen $f(x_1, \ldots, x_n)$ egy n tagú ÉS, amelynek az i-edik tagja x_i ha $a_i = 1$, és $\neg x_i$ ha $a_i = 0$. Ekkor nyilván $f(a_1, \ldots, a_n) = 1$, és a többi A^n-beli helyen f értéke 0. Egy tetszőleges $g : A^n \to A$ függvényt úgy kaphatunk, hogy minden olyan A^n-beli helyhez, ahol a g értéke 1, legyártjuk az iménti f függvényt, és ezeket összeVAGYoljuk.

8.3.16. Legyen g tetszőleges monoton függvény. Minden olyan $(a_1, \ldots, a_n) \in A^n$ helyhez, ahol g értéke 1, készítünk egy $f(x_1, \ldots, x_n)$ függvényt, ami az ÉS-e azoknak az x_i változóknak, melyekre $a_i = 1$. Ezeknek az f függvényeknek az összeVAGYoltja jó lesz.

8.3.18. Ha a 8.3.6. Gyakorlat eredményében néhány x_i helyébe konstansokat írunk, akkor pont a kívánt eredmény jön ki, modulusok esetében $r_1x_1 + \ldots r_nx_n + c$, ahol c tetszőleges eleme a modulusnak.

8.3.19. Legyen $p(x_1, \ldots, x_n) = t(x_1, \ldots, x_n, a_1, \ldots, a_k)$ egy polinomfüggvénye az A algebrának, ahol t egy kifejezésfüggvény, $a_1, \ldots, a_n \in A$ pedig rögzített elemek. Mivel minden θ kongruencia reflexív reláció, az (a_i, a_i) párok elemei θ-nak. A 8.3.14. Gyakorlat miatt t megőrzi a θ részalgebrát, és így p is megőrzi azt.

Megfordítva, tegyük föl, hogy egy $\equiv$ ekvivalencia-relációt az A minden egyváltozós polinomfüggvénye megőriz, meg kell mutatni, hogy $\equiv$ kompatibilis. Az egyszerűbb jelölés érdekében háromváltozós f alapműveletre szorítkozunk (a kétváltozós eset a 8.2.35. Gyakorlat megoldásában szerepel). Ha $a_1 \equiv b_1$, $a_2 \equiv b_2$ és $a_3 \equiv b_3$, akkor

$$f(a_1, a_2, a_3) \equiv f(b_1, a_2, a_3)\,,$$

mert az $f(x, a_2, a_3)$ egyváltozós polinomfüggvény, és így megőrzi az $\equiv$ relációt. Szintén egyváltozós polinomfüggvény az $f(b_1, x, a_2)$ és az $f(b_1, b_2, x)$ is, és ezért

$$f(b_1, a_2, a_3) \equiv f(b_1, b_2, a_3) \equiv f(b_1, b_2, b_3)\,.$$

Ezzel a kompatibilitást igazoltuk. Láthatjuk, hogy elegendő lenne csak nagyon speciális polinomfüggvényekről föltenni, hogy tartják az $\equiv$ relációt: azokról, amelyek az alapműveletekből úgy keletkeznek, hogy egy kivételével az összes változójuk helyébe konstansokat írunk. Azt is láthatjuk, hogy $\equiv$ tranzitivitása fontos szerepet játszik.

A 8.2.23. Tétel pontosabb bizonyításában a most bizonyított észrevétel azért segít, mert ha tekintjük a bizonyításban szereplő $\theta - \rho$ sorozatot a és b között, és alkalmazunk rá egy tetszőleges egyváltozós polinomfüggvényt, akkor nyilvánvalóan ugyanilyen típusú sorozatot kapunk. Így pedig az olyan (a, b) párok halmaza, amelyek között van ilyen sorozat, kompatibilis reláció (és így kongruencia) lesz.

8.3.23. Az első állítás világos abból, hogy a direkt szorzatban a műveleteket komponensenként végezzük. A második állítás abból következik, hogy a homomorfizmusok pontosan azok, amelyeknek gráfja részalgebra (8.3.11. Gyakorlat), és hogy a részalgebrákat tartják a kifejezésfüggvények is (8.3.8. Lemma).

8.3.25. Mivel $G \in \mathcal{K}$ és F szabad, létezik egy olyan $\varphi : F \to G$ homomorfizmus, amely X-en az identikus leképezés. Hasonlóan létezik egy $\psi : G \to F$ homomorfizmus is, amely X-en az identitás. Ahhoz, hogy F és G izomorfak, elég belátni, hogy $\varphi \circ \psi = id_G$ és $\psi \circ \varphi = id_F$. Ez azért igaz, mert ezek a kompozíciók a G, illetve az F algebra X generátorrendszerén az identitással egyenlők (és egy generátorrendszeren felvett értékek a homomorfizmust már egyértelműen meghatározzák, lásd a 4.4.28. Gyakorlatra adott második megoldást).

8.3.28. Könnyű meggondolni, hogy egymásba helyettesítgetésekkel megkapjuk az összes olyan $x_1 + \ldots + x_k$ alakú függvényt, ahol k páratlan, továbbá hogy másmilyen függvényt már nem kapunk. Pontosabban: az összes olyan függvényt kapjuk, amely páratlan sok változó összege (mint például $x_3 + x_4 + x_7$).

Ez azonban nem jelenti azt, hogy a klónban például kétváltozós függvény egyáltalán nincs! Hiszen az x_2 eleme a klónnak, és ez kétváltozós függvénynek is tekinthető, ahol a változók x_1 és x_2 (csak éppen az első változójától nem függ; ez valójában a π_2^2 projekció). Ezért az összes olyan kifejezésfüggvényt, amelynek változói $x_1, \ldots, x_n$, úgy kaphatjuk meg, hogy kiválasztunk e változók közül páratlan sokat, és azokat összeadjuk. Így az n-változós függvények száma nem más, mint egy n elemű halmaz páratlan elemszámú részhalmazainak száma, vagyis 2^{n-1} (A.2.4. Tétel).

Ha a polinomokat akarjuk megszámolni, akkor vegyük észre, hogy $x + z$ is polinom, hiszen az alapműveletbe szabad y helyére nullát helyettesíteni. Vagyis az összeadás polinom, és persze a skalárral való szorzás is, hiszen az vagy konstans nulla, vagy pedig az $1 \cdot x = x$ függvény, vagyis az identitás (ami projekció). Tehát ennek az algebrának a polinomjai ugyanazok, mint a kételemű test fölötti egydimenziós vektortéré, és ezeket a 8.3.18. Gyakorlatban már leírtuk. A $\lambda_1 x_1 + \ldots + \lambda_n x_n + v$ képletben mindegyik λ_i skalár, és a v elem is kétféleképpen választható, vagyis az n-változós polinomok száma 2^{n+1}.

8.3.29. Az egy elemmel generált szabad háló egyelemű (mert minden egyelemű részhalmaz részháló). A két elemmel generált szabad háló négyelemű: a 8.3. Ábrán látható C_2^2 hálót az a és b elemei szabadon generálják. Ha ugyanis L tetszőleges háló, és $c, d \in L$, akkor az a $\varphi : C_2^2 \to L$ leképezés, amelyre $\varphi(a) = c$, $\varphi(b) = d$, $\varphi(0) = c \wedge d$, $\varphi(1) = c \vee d$, könnyen ellenőrizhetően háló-homomorfizmus.

8.3.30. Az Útmutatóban megadott gyűrűk azért szabadok, mert egy polinomba tetszőleges értékeket be szabad helyettesíteni, és ez a hozzárendelés homomorfizmus (lásd a 2.4.23. és a 2.6.9. Gyakorlatokat). Ezekben a gyakorlatokban csak az alaptest elemeit helyettesítettük, de ugyanúgy igazolható, hogy tetszőleges kommutatív gyűrű elemeit is helyettesíthetjük (az egyváltozós eset a5.1.25. Gyakorlat). Az egész együtthatókkal nincs probléma,

hiszen gyűrűelem egész számszorosát definiáltuk a 2.2.17. Definícióban. A konstans taggal csak egységelemes gyűrű esetében kell foglalkoznunk, ekkor az n konstans taghoz az egységelem n-szeresét rendelhetjük.

8.3.31. Az Útmutatóban megadott $*$ műveletre $x * x = x +_k 1$, ezt i-szer alkalmazva kapjuk, hogy $x +_k i$ kifejezésfüggvény minden i-re. Speciálisan $i = k - 1$ esetén az $x \mapsto x -_k 1$ függvény adódik, és így $\min(x, y) = x * y -_k 1$ is kifejezésfüggvény. Ezt többször önmagába helyettesítve a sokváltozós minimum-függvényt is megkapjuk. Mivel $x, x +_k 1, x +_k 2, \ldots, x +_k (k-1)$ minimuma tetszőleges x esetén 0, ezért a konstans nulla függvény is kifejezésfüggvény, és így $x +_k i$ alkalmazásával láthatjuk, hogy az összes konstans függvény is az.

Ha $0 \leq i \leq k-1$, akkor $f_i(x) = \min(1, x -_k i) -_k 1$ értéke i-nél $k-1$, másutt nulla. Legyen $(a_1, \ldots, a_n) \in A^n$ tetszőleges, akkor az $f_{a_i}(x_i)$ függvények minimuma $(a_1, \ldots, a_n)$-nél $k-1$, másutt nulla. Ezt a függvényt a min és a konstansok segítségével az $(a_1, \ldots, a_n) = \mathbf{a}$ helyen előre adott b magasságúra vághatjuk, jelölje a kapott kifejezésfüggvényt $f_{\mathbf{a},b}$.

Ha $g : A^n \to A$ tetszőleges függvény, akkor minden $\mathbf{a}$ helyhez készítsük el a fenti $f_{\mathbf{a},b}$ kifejezésfüggvényt, ahol $b = g(\mathbf{a})$. Az Útmutatóban megadott $v(x, y)$ kifejezésfüggvényre $v(0, x) = v(x, 0) = v(x, x) = x$ teljesül. Ezért a fenti $f_{\mathbf{a},b}$ függvényeket a v segítségével tetszőleges sorrendben „összeVAGYolva" végül g adódik (minden lépésben a g-t eggyel több helyen interpoláló, másutt azonosan nulla kifejezésfüggvényt kapunk).

8.4. Varietások.

8.4.3. A részalgebrákra vonatkozó állítás nyilvánvaló, hiszen csak kevesebb egyenlőséget kell ellenőrizni. A homomorf képre vonatkozó állítás abból következik, hogy a homomorfizmusok tartják a kifejezésfüggvényeket (8.3.23. Gyakorlat). Ugyanebben a gyakorlatban leírtuk az $A \times B$ direkt szorzat kifejezésfüggvényeit is, amiből világos a (kétténytezős) direkt szorzatra vonatkozó állítás is. Több (akár végtelen sok) tényező esetén a bizonyítás ugyanaz (hiszen a formális kifejezéseket itt is komponensenként kell kiértékelni, hogy a direkt szorzat kifejezésfüggvényeit megkapjuk).

8.4.4. A testek, illetve a nullosztómentes gyűrűk osztálya nem zárt a direkt szorzat képzésére, például $\mathbb{R} \times \mathbb{R}$ nem nullosztómentes (hiszen $(1, 0) \cdot (0, 1) = (0, 0)$), és így nem is test. Ha a csoportok definíciójában csak a szorzást tekintjük műveletnek, akkor nem kapunk varietást, például a $\mathbb{Z}^+$ csoportnak ekkor részalgebráját alkotják a pozitív egészek, ami nem csoport. Tehát a csoportok azonosságokkal való definíciójához az inverzképzésre, mint műveletre is szükség van.

8.4.6. Ha az azonosság mindenütt teljesül, akkor a szabad algebrák generátorain is. Megfordítva, tegyük föl, hogy $t_1^F(x_1, \ldots, x_n) = t_2^F(x_1, \ldots, x_n)$. Annak igazolásához, hogy a $t_1 \approx t_2$ azonosság az A algebra $a_1, \ldots, a_n$ elemein is teljesül, tekintsünk egy olyan $\varphi : F \to A$ homomorfizmust, amelyre $\varphi(x_i) = a_i$ minden i-re, és használjuk föl, hogy ez tartja a kifejezésfüggvényeket.

8.4.8. A (4) és (5) nyilvánvaló (például homomorf kép homomorf képe az eredeti algebrának is homomorf képe, mert két szürjektív homomorfizmus kompozíciója is szürjektív homomorfizmus). Az (1) állítás abból következik, hogy a homomorf kép egy részalgebrája a saját teljes inverz képének a képe (8.2.20. Feladat). Ha $\varphi : A_i \to B_i$ szürjektív homomorfizmusok, akkor definiáljuk a φ leképezést a $\prod A_i$ direkt szorzatról a $\prod B_i$ direkt szorzatba komponensenként, ez is nyilván szürjektív homomorfizmus lesz, így (2) is igaz. Ha $B_i \leq A_i$ részalgebrák, akkor $\prod B_i$ nyilván részalgebrája $\prod A_i$-nek, ami (3)-at bizonyítja. A (6) végiggondolását az Olvasóra hagyjuk, de megjegyezzük, hogy ez az állítás felfogható egy általános asszociativitási szabálynak is a direkt szorzatra nézve.

A $\mathsf{HSP}(\mathcal{K})$ azért zárt a direkt szorzatra, mert

$$\mathsf{PHSP}(\mathcal{K}) \subseteq \mathsf{HPSP}(\mathcal{K}) \subseteq \mathsf{HSPP}(\mathcal{K}) \subseteq \mathsf{HSP}(\mathcal{K})$$

a most bizonyított (2), (3) és (6) miatt. Hasonlóan láthatjuk, hogy $\mathsf{HSP}(\mathcal{K})$ zárt a részalgebraképzésre és a homomorf képre is.

8.4.10. Csak azt mutatjuk meg, hogy X szabad generátorrendszer $\mathsf{P}(\mathcal{K})$ fölött (a részalgebrára és homomorf képre vonatkozó állítás igazolása hasonló, de sokkal egyszerűbb). Legyen $A = \prod_{i \in I} A_i$ direkt szorzat, ahol $A \in \mathcal{K}$, és $\varphi : X \to A$ tetszőleges leképezés. Ekkor a feltétel szerint a $\pi_i \circ \varphi : X \to A_i$ leképezések (ahol π_i az i-edik projekció) kiterjeszthetők egy-egy $\varphi_i : F \to A_i$ homomorfizmussá. Legyen $t \in F$ esetén $\varphi^*(t) = (\ldots, \varphi_i(t), \ldots)$. Ekkor a $\varphi^* : F \to A$ homomorfizmus a φ keresett kiterjesztése.

8.4.11. A 8.3.27. Következmény miatt a $\mathcal{K}$ fölötti végesen generált szabad algebrák végesek. Ezek az algebrák szabadok a $\mathsf{V}(\mathcal{K})$ fölött is (8.4.10. Gyakorlat), és homomorf képükként a varietás minden végesen generált algebrája megkapható.

8.4.18. Az M_3, N_5, D_1 és D_2 hálók mind szubdirekt irreducibilisek (sőt M_3 egyszerű is) a 8.2.37. Gyakorlat miatt: a 11.2. Ábrán $\theta \wedge \rho$-val címkézett kongruencia lesz a monolit (8.4.14. Lemma).

8.4.19. A $\mathbb{C}[x]$ gyűrű $\mathbb{C}$ példányainak (tehát egyszerű gyűrűknek) a szubdirekt szorzatára is felbontható a következőképpen. Vegyük az $(x - c)$ alakú főideálok halmazát, ahol c befutja a komplex számokat. Az ezek szerinti faktor $\mathbb{C}$-vel izomorf, és így elég megmutatni, hogy ezeknek az ideáloknak (0) a metszete (8.4.15. Következmény). Ez azért igaz, mert tetszőleges nem nulla f polinomhoz van olyan c, hogy $f(c) \neq 0$ (hiszen f-nek csak véges sok gyöke van), és ekkor $f \notin (x - c)$.

Ha R a páratlan nevezőjű törtek gyűrűje, akkor álljon I_k azokból a törtekből, amelyek számlálója 2^k-nal osztható. Az I_k ideálok metszete (0), és így szubdirekt felbontást adnak.

Könnyű belátni, hogy $R/I_k \cong \mathbb{Z}_{2^k}$ (a $\mathbb{Z}^+_{2^k}$ csoportban ugyanis minden páratlan számmal korlátlanul oszthatunk, lásd 7.7.15. Gyakorlat). De $\mathbb{Z}_{2^k}$ szubdirekt irreducibilis gyűrű, hiszen a kongruencia-hálója lánc (az ideálok a 2^k osztóinak felelnek meg a 4.3.21. Állítás miatt).

8.4.20. Megmutatjuk, hogy ha A egy szubdirekt irreducibilis Abel-csoport, akkor A vagy p-hatványrendű ciklikus csoport, vagy a $\mathbb{Z}_{p^\infty}$ kváziciklikus csoporttal izomorf (7.7.16. Definíció), ahol p alkalmas prímszám. Ez „elemien" is bizonyítható (4.8.33. Feladat), gyorsabb azonban, ha felhasználjuk a véges Abel-csoportok alaptételét.

Legyen M az A monolitja. Mivel Abel-csoportban minden részcsoport normálosztó, az A minden nemtriviális B részcsoportja tartalmazza M-et, speciálisan mindegyik ilyen B részcsoport is szubdirekt irreducibilis. Innen egyrészt következik, hogy M-nek csak a két triviális részcsoportja van, és így p rendű ciklikus, ahol p prím, másrészt ha B véges, akkor a véges Abel-csoportok alaptétele miatt prímhatványrendű ciklikus csoportok direkt szorzata, és így a szubdirekt irreducibilitás miatt p-hatványrendű ciklikus.

Ha $g \in A$, akkor a g által generált ciklikus csoport tartalmazza M-et, így g rendje véges, és ezért az előző megjegyzés miatt p-nek hatványa. Ha h is eleme A-nak, akkor a $\langle g, h\rangle$ részcsoport is véges, így p-hatványrendű ciklikus, ezért g és h közül a kisebb vagy egyenlő rendű hatványa a másiknak. Így ha A végtelen, akkor van akármilyen nagy rendű eleme, és ezért felépíthetjük elemek egy végtelen $a_0, a_1, \ldots$ sorozatát, ahol a_k rendje p^k, és $pa_{k+1} = a_k$ minden k-ra (fel kell használni közben, hogy p-csoportban a p-hez relatív prím egészekkel szabad osztani). Könnyű meggondolni, hogy az ezek által generált C részcsoport kváziciklikus lesz. A C részcsoport tartalmazza A összes elemét, mert ha $g \in A - C$ lenne, amelynek rendje p^k, akkor a C-beli egyik p^k-rendű elemnek g hatványa az előző megjegyzések szerint.

8.4.21. Az Abel-csoportok között a szabadok pontosan a $\mathbb{Z}^+$ példányainak direkt összegei (7.2.15. Tétel), és ezek a $\mathbb{Z}^+$ direkt hatványainak részcsoportjai, tehát benne vannak a $\mathbb{Z}^+$ által generált varietásban. Ezért $\mathbb{Z}^+$ az Abel-csoportok varietását generálja.

A $\mathbb{Z}$, mint gyűrű, a kommutatív gyűrűk varietását generálja (ha az egységelemet művelettel jelöljük ki, akkor az egységelemesekét). Ehhez elég a szabad gyűrűket, vagyis a $\mathbb{Z}$ fölötti polinomgyűrűket generálni (ha az egységelem nem művelet, akkor a konstans tag nélküli polinomok gyűrűit). A 8.4.19. Gyakorlat megoldásához hasonlóan járunk el. Ha R egy ilyen polinomgyűrű, akkor a határozatlanok helyére tetszőleges egész számokat helyettesítve egy homomorfizmust kapunk $\mathbb{Z}$ egy részgyűrűjébe. Elég megmutatni, hogy ezek magjainak a metszete nulla, mert akkor R a $\mathbb{Z}$ részgyűrűinek szubdirekt szorzata lesz. Azt kell tehát belátni, hogy ha $p(x_1, \ldots, x_n)$ egész együtthatós polinom, akkor alkalmas (egész) helyettesítésre az értéke nem nulla. Ez következik többhatározatlanú polinomok azonossági tételéből (2.6.10. Feladat).

Valójában arról van szó, hogy ha $f \approx g$ egy azonosság kommutatív gyűrűk között, amely nem teljesül minden kommutatív gyűrűben (vagyis az f és g polinomok nem azonosak), akkor ez az azonosság már $\mathbb{Z}$-ben sem teljesül. Ezt pontosan az mutatja, hogy $f - g$ egészek alkalmas helyettesítésére nem lesz nulla.

8.4.22. Legyen a D_4 csoport az $\langle f, t \mid f^4 = t^2 = 1,\ ft = tf^{-1}\rangle$ definiáló relációkkal megadva, és $N = \{(1,1), (f^2, f^2)\}$. Ez normálosztó a $D_4 \times D_4$ csoportban, a szerinte vett faktorcsoportnak $i = (f,t)N$ és $j = (t,f)N$ elemei, és az általuk generált csoport könnyen láthatóan Q-val izomorf (a 4.9.15. Példa állítását is felhasználva).

Hasonlóan legyen a Q csoport az $\langle i, j \mid i^4 = j^4 = 1,\ i^2 = j^2,\ ij = ji^{-1}\rangle$ definiáló relációkkal megadva, és $K = \{(1,1), (-1,-1)\}$. Ez normálosztó a $Q \times Q$ csoportban, a szerinte vett faktorcsoportnak $f = (i,1)K$ és $t = (i,i)K$ elemei, és az általuk generált csoport könnyen láthatóan D_4-gyel izomorf.

8.4.23. A D_3 diédercsoportban Lagrange tétele miatt teljesül az $x^6 = 1$ azonosság. Így az x^2 elem biztosan forgatás, és mivel bármely két forgatás felcserélhető, igaz az $x^2y^2 = y^2x^2$ azonosság is. Megfordítva, belátjuk hogy ez a két azonosság olyan $\mathcal{V}$ csoportvarietást ad meg, amelyben csak $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$ és D_3 szubdirekt irreducibilis. Ebből persze következik, hogy a $\mathcal{V}$ varietást a D_3 generálja, hiszen $\mathbb{Z}_2^+, \mathbb{Z}_3^+ \in \mathsf{S}(D_3)$, és így készen leszünk. A 8.4.20. Feladat miatt minden szubdirekt irreducibilis Abel-csoport prímhatványrendű ciklikus, vagy kváziciklikus. Az $x^6 = 1$ azonosságot ezek közül csak $\mathbb{Z}_2^+$ és $\mathbb{Z}_3^+$ teljesíti. Tegyük föl, hogy $G \in \mathcal{V}$ szubdirekt irreducibilis, nemkommutatív csoport. Azt kell megmutatnunk, hogy $G \cong D_3$.

Legyen N az x^2 alakú elemek által generált részcsoport G-ben. Ez kommutatív, és minden elemének a köbe 1 a két azonosság miatt. Vagyis N egy elemi 3-csoport, ami normálosztó is, hiszen a generátorainak (a G négyzetelemeinek) a halmaza zárt a konjugálásra. Továbbá az $F = G/N$ csoportban minden elem négyzete az egységelem, így F kommutatív (4.3.33. Feladat), vagyis elemi Abel-féle 2-csoport.

Legyen t másodrendű eleme G-nek. Az N tekinthető $\mathbb{Z}_3$ fölötti vektortérnek, amelyen a t konjugálással hat, és ez a hatás egy A lineáris transzformáció N-en. Legyen N_+ azoknak az N-beli v elemeknek a halmaza, melyekre $A(v) = v$, és N_- azoké a v elemeké, amelyekre $A(v) = -v$ (additív írásmódban, vagyis amelyek a t-vel való konjugáláskor az inverzükbe mennek). Ezek tehát az 1-hez és a -1-hez tartozó sajátalterek. A direkt összegük az egész N, mert tetszőleges $v \in N$ esetén

$$v = \frac{v + A(v)}{2} + \frac{v - A(v)}{2} \in N_+ + N_-$$

(ne feledjük, hogy $\mathbb{Z}_3$ fölött szabad 2-vel osztani, és hogy $A^2(v) = v$). Belátjuk, hogy N_+ és N_- normálosztók G-ben.

Valóban, ha $g \in G$ és B a g-vel való konjugálás, mint lineáris transzformáció N-en, akkor elég megmutatni, hogy B és A felcserélhetők, mert lineáris algebrából tudjuk (és könnyű bizonyítani), hogy ilyenkor A minden sajátaltere, tehát N_+ és N_- is B-invariáns, vagyis zárt a g-vel való konjugálásra. Azt kell tehát megmutatni, hogy gt és tg ugyanúgy hat N-en, vagyis hogy $[g,t] = gt(tg)^{-1}$ triviálisan hat. De ez igaz, mert G/N és N is kommutatív (és így $[g,t] \in N$). Tehát N_+ és N_- tényleg normálosztók.

Mivel G szubdirekt irreducibilis, nem lehet két nemtriviális normálosztója, amik csak az egységelemben metszik egymást. Ezért N_+ és N_- egyike csak az egységelemből áll.

Beláttuk tehát, hogy egy tetszőleges t másodrendű elem vagy felcserélhető N minden elemével, vagy pedig N minden elemét az inverzébe konjugálja. Ez valójában G minden elemére igaz, hiszen ha $g \in G$, akkor $g = g^3 g^4$, itt g^3 másodrendű (vagy az egységelem), és $g^4 \in N$, vagyis N kommutativitása miatt g ugyanúgy hat N-en, mint g^3. Ekkor viszont N minden részcsoportja zárt a konjugálásra, vagyis normálosztó. De G szubdirekt irreducibilis, így N elemszáma legfeljebb 3. Másfelől viszont N nem lehet egyelemű, mert akkor $G \cong G/N$ kommutatív lenne. Így $|N| = 3$.

A következő lépésben megmutatjuk, hogy ha t olyan másodrendű elem, amely N-en triviálisan hat, akkor t benne van G centrumában. Legyen $g \in G$ tetszőleges és $s = g^3$, ekkor $s^2 = 1$. Mivel N tartalmazza G mindegyik elemének a négyzetét, t felcserélhető g^4-nel, és így $g = g^3 g^4$ miatt elég belátni, hogy $st = ts$. A t felcserélhető $(st)^4$-nel is, mert ez is négyzetelem, és mivel $(st)^6 = 1$, ezért

$$1 = (st)(st)(st)(st)(st)(st) = (sts)t(st)(st)(st)(st) = (sts)(st)(st)(st)(st)t = tsts\,,$$

hiszen $ss = tt = 1$. Innen balról t-vel, jobbról s-sel szorozva $ts = ttstss = st$. Tehát t tényleg a centrumban van.

Így viszont $\{1, t\}$ normálosztó, ami N-et csak az egységelemben metszi. Ez ellentmond annak, hogy G szubdirekt irreducibilis, tehát ilyen t elem nincs. Ez azonban azt jelenti, hogy N-en csak N elemei hathatnak triviálisan. Ha ugyanis a g elem triviálisan hat, akkor $g = g^3 g^4$ és $g^4 \in N$ miatt $t = g^3$ is triviálisan hat. Így t nem lehet másodrendű, de $t^2 = 1$, vagyis $t = 1$, és akkor $g = g^4 \in N$. Beláttuk tehát, hogy N centralizátora csak önmaga, és minden külső elem invertálásként hat N-en.

Mivel G nem kommutatív, $G \neq N$, vagyis létezik egy $g \in G - N$ elem. Legyen $t = g^3$. Ekkor $t \notin N$, hiszen $g = g^4 g^3$, és $g^4 \in N$. Így t másodrendű, és az eddigiek miatt invertálásként hat N-en. A bizonyítás befejezéséhez tehát elég megmutatni, hogy G hatelemű csoport, hiszen akkor $G = \langle t, N \rangle$, és G teljesíti a D_3 definiáló relációit (4.9.15. Példa). Legyen $h \notin N$, akkor h és t is invertálásként hat N-en. Így $h^{-1}t$ identikusan hat, vagyis az előzőek miatt $h^{-1}t \in N$, és így $h \in tN$. Ezért tN az egyetlen N-en kívüli mellékosztály.

A fenti bizonyítás elemi, amennyire lehet, komolyabb eszközökkel kicsit rövidíthető lenne. Például a fenti $(st)^6$-os számolás a következőképpen úszható meg. Legyen H az N, t és g által generált részcsoport, ez véges (mert H/N végesen generált Abel-csoport). Jelölje P a H csoportnak azt a 2-Sylow részcsoportját, ami a másodrendű t elemet tartalmazza. A P Abel, hiszen minden elem négyzete az egységelem. Továbbá P és N generálja H-t. A t viszont felcserélhető P elemeivel, és ha triviálisan hat N-en, akkor N elemeivel is, és így a H összes elemével, speciálisan g-vel is. Ez minden g-re elmondható, tehát t a centrumban van.

Az utolsó bekezdés számolása helyett mondhatnánk azt, hogy $F = G/N$ minden gN eleméhez rendeljük hozzá a g-vel való konjugálást, mint N automorfizmusát. Ez jóldefiniált, azaz gN elemei ugyanúgy hatnak N-en, hiszen N Abel. A kapott homomorfizmus magja triviális, hiszen külső elem nem hat identikusan N-en. A homomorfizmus-tétel miatt F izomorf N automorfizmus-csoportjával, ami kételemű.

8.4.24. Az Útmutatóban bevezetett jelöléseket használjuk.

Az alábbi bizonyítást sokkal könnyebb elképzelni abban az esetben, amikor az I indexhalmaz elemei a pozitív egészek, és az A_i részalgebrákra $A_1 \subseteq A_2 \subseteq \ldots$ teljesül. Ebben az esetben az olyan $\mathbf{c}$ sorozatokról van szó, amelyek valamettől kezdve konstansok, és φ ezt a konstans értéket rendeli a sorozathoz.

A φ jóldefiniáltságát a következőképpen igazoljuk. Tegyük föl, hogy a $\mathbf{c}$ sorozathoz i_1 és i_2 is megfelelő index, meg kell mutatni, hogy $c_{i_1} = c_{i_2}$. Az A_{i_1} és A_{i_2} is végesen generált, és ezért a generátorrendszereiket egyesítve egy olyan végesen generált A_j részalgebrát kapunk, amely A_{i_1}-et és A_{i_2}-t is tartalmazza. A feltétel szerint ekkor $c_{i_1} = c_j = c_{i_2}$. Most belátjuk, hogy φ szürjektív. Legyen c eleme A-nak, A_i a c által generált részalgebra, és $\mathbf{c}$ az a sorozat, amelyben $A_i \subseteq A_j$ esetén $c_j = c$, a többi helyen pedig a c_j értéke tetszőleges. Ez nyilván C-beli, és a φ-nél vett képe c. Végül megmutatjuk, hogy φ homomorfizmus. Legyen f az egyszerű jelölés kedvéért kétváltozós művelet, és $\mathbf{c}, \mathbf{d} \in C$. Ha a C definíciójában szereplő index e sorozatok esetében rendre i és k, akkor létezik olyan ℓ, hogy $A_i, A_k \subseteq A_\ell$. A φ definíciója szerint $\varphi(\mathbf{c}) = c_i = c_\ell$ és $\varphi(\mathbf{d}) = d_k = d_\ell$. Továbbá az $f(\mathbf{c}, \mathbf{d})$ sorozat is „majdnem konstans" ℓ-től kezdve, és e konstans értéke $f(c_\ell, d_\ell)$ (hiszen $A_\ell \subseteq A_j$ esetén $f(\mathbf{c}, \mathbf{d})$-nek a j-edik komponense $f(c_j, d_j) = f(c_\ell, d_\ell)$). Ezért

$$\varphi\big(f(\mathbf{c}, \mathbf{d})\big) = f(c_\ell, d_\ell) = f\big(\varphi(\mathbf{c}), \varphi(\mathbf{d})\big)\,,$$

azaz φ tartja az f műveletet.

8.4.25. Az nyilvánvaló, hogy a felsorolt azonosságok igazak $\mathcal{K}$-ban (8.4.6. Gyakorlat). Azt kell belátni, hogy ha egy A algebrában a felsorolt azonosságok igazak, akkor $A \in \mathcal{K}$. Ehhez elég igazolni, hogy az A végesen generált részalgebrái $\mathcal{K}$-ban vannak (8.4.24. Feladat). Legyen $B = \langle b_1, \ldots, b_n \rangle$ olyan algebra, amelyben a felsorolt azonosságok igazak. Az F szabad algebra elemei $t^F(x_1, \ldots, x_n)$ alakúak, ahol t egy formális kifejezés. Legyen $\varphi : F \to B$ az a leképezés, amely a $t^F(x_1, \ldots, x_n)$-hez a $t^B(b_1, \ldots b_n) \in B$ elemet rendeli. A φ jóldefiniált, mert ha $t_1^F(x_1, \ldots, x_n) = t_2^F(x_1, \ldots, x_n)$, akkor B-ben a feltevésünk szerint igaz a $t_1 \approx t_2$ azonosság, és ezért $t_1^B(b_1, \ldots, b_n) = t_2^B(b_1, \ldots, b_n)$. A φ igazándiból a $b_1, \ldots, b_n$ elemek behelyettesítése, tehát homomorfizmus (8.3.21. Állítás), és szürjektív is, mert generátorrendszert generátorrendszerbe visz. Így B homomorf képe F-nek, ezért benne van $\mathcal{K}$-ban.

8.5. Disztributív hálók és Boole-algebrák.

8.5.1. Az $(x \wedge y) \vee z \approx (x \vee z) \wedge (y \vee z)$ azonosság azt fejezi ki, hogy metszetbe tagonként lehet „be-egyesíteni". Ezt a második azonosság jobb oldalán található első metszetre alkalmazhatjuk:

$$(x \wedge z) \vee (y \wedge z) = \big(x \vee (y \wedge z)\big) \wedge \big(z \vee (y \wedge z)\big) = \big(x \vee (y \wedge z)\big) \wedge z$$

az elnyelési tulajdonság miatt. A nagy zárójel metszetébe be-egyesítve (vagyis az első azonosságot még egyszer alkalmazva) ez a következővel egyenlő:

$$\big((x \vee y) \wedge (x \vee z)\big) \wedge z = (x \vee y) \wedge \big((x \vee z) \wedge z\big) = (x \vee y) \wedge z$$

ismét az elnyelési tulajdonság miatt. Így a második azonosságot beláttuk az elsőből. A fordított irányú bizonyítás a most leírt gondolatmenet duálisa.

8.5.3. Az ábrán megadott elemekre az M_3 esetében

$$c = 0 \vee c = (a \wedge b) \vee c \neq (a \vee c) \wedge (b \vee c) = 1 \wedge 1 = 1\,.$$

Az N_5 esetében

$$a = 0 \vee a = (c \wedge b) \vee a \neq (c \vee a) \wedge (b \vee a) = c \wedge 1 = c\,.$$

Tehát egyik háló sem teljesíti az 8.5.1. Gyakorlatban felírt első azonosságot.

8.5.4. Ha $\mathbf{a} = (\ldots, a_i, \ldots) \in C_2^X$, akkor mindegyik a_i értéke 0 vagy 1. Rendeljük hozzá ehhez az elemhez azoknak az $i \in X$ indexeknek a halmazát, ahol $a_i = 1$. Ez a hozzárendelés bijektív: az $Y \subseteq X$ halmazhoz a C_2^X-nek az az eleme tartozik, amelynek az Y-beli helyekhez tartozó koordinátája 1, a többi nulla. De mindkét irányban rendezéstartó is, mert $\mathbf{a} \leq \mathbf{b}$ azt jelenti, hogy minden i-re $a_i \leq b_i$, és ez azzal ekvivalens, hogy ha $a_i = 1$, akkor b_i is 1, vagyis hogy az $\mathbf{a}$-hoz rendelt részhalmaz része a $\mathbf{b}$-hez rendelt részhalmaznak. Így háló-izomorfizmust kaptunk. Könnyű közvetlenül is ellenőrizni az egyesítés- és metszet-tartást.

8.5.5. Tegyük föl, hogy L lánc, és $a, b, c \in L$. Ha $a \leq b \leq c$, akkor $(a \wedge b) \vee c$ és $(a \vee c) \wedge (b \vee c)$ értéke is c. Hasonlóan ellenőrizhetjük a disztributivitást az a, b, c elemek többi lehetséges sorrendjére is.

Kis ügyeskedéssel redukálhatjuk az esetek számát, például szimmetriaokokból föltehető, hogy $a \leq b$. Az állítás következik a 8.6.16. Tételből is, hiszen láncban nem lehet M_3-mal, sem N_5-tel izomorf részháló.

8.5.6. Azt kell megmutatni, hogy $[(a, b), c] = [(a, c), (b, c)]$, ahol (a, b) legnagyobb közös osztót, $[a, b]$ legkisebb közös többszöröst jelöl. Ha a három szám között a nulla előfordul, akkor könnyű az azonosságot ellenőrizni. Ha nem, akkor az a, b, c számokat fölírhatjuk közös kanonikus alakban. Alkalmazzuk a legnagyobb közös osztó és a legkisebb közös többszörös szokásos képletét (3.1.20. Gyakorlat). A kitevőkre bizonyítandó azonosságok pontosan azok lesznek, amit a 8.5.5. Gyakorlatban már bebizonyítottunk, hiszen a kitevők nemnegatív egész számok, amelyek láncot alkotnak a $\leq$ rendezésre, ahol az egyesítést a max, a metszetet a min függvény adja meg. Ezért a disztributivitás fönnáll.

Valójában a következőről van szó. Jelölje P a pozitív egészek hálóját az oszthatóság által megadott rendezésre, N pedig a nemnegatív egészek hálóját a $\leq$ rendezésre. Legyen p prímszám, és jelölje $\varphi_p(n)$ az $n > 0$ egészben a p kitevőjét. Ez a leképezés (szürjektív) hálóhomomorfizmus P-ből N-be (ezt fejezi ki a legnagyobb közös osztó és a legkisebb közös többszörös szokásos képlete). Továbbá a φ_p homomorfizmusok magjainak metszete a 0_P,

hiszen ha két számban minden prím ugyanazon a kitevőn szerepel, akkor a két szám megegyezik. Ezért ezek a homomorfizmusok a P egy szubdirekt felbontását adják, ahol a tényezők mind N-nel izomorfak (8.4.15. Következmény). Mivel N lánc, így disztributív, tehát minden szubdirekt hatványa is az.

Legyen P_n az n pozitív egész pozitív osztóinak a hálója az oszthatóságra nézve. Az előző bekezdésben leírt gondolatmenet most azt mutatja, hogy a P_n láncok direkt szorzata. Valóban, ha $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, akkor a φ_{p_i} leképezés most a 0 és α_i közötti egész számok láncába képez, ami $\alpha_i + 1$ elemű. A kapott szubdirekt felbontás azonban most a teljes direkt szorzat, hiszen ha $(\beta_1, \dots, \beta_n)$ egy eleme e láncok direkt szorzatának, akkor ő a $p_1^{\beta_1} \dots p_k^{\beta_k} \mid n$ számnak felel meg. Röviden: minden szám osztóhálója láncok direkt szorzatával izomorf.

Az eddigiekből a részcsoporthálókra vonatkozó állítás már nyilvánvaló, hiszen $\mathbb{Z}^+$ részcsoporthálója a nemnegatív egészek osztóinak hálójával, az n-edrendű ciklikus csoport részcsoporthálója pedig az n pozitív osztóinak hálójával izomorf a 4.3.21. Állítás miatt. (A megfeleltetés a részcsoportok és a számok között mindkét irányban rendezéstartó, tehát háló-izomorfizmus.)

8.5.8. A θ_I reflexivitása és szimmetriája nyilvánvaló, előbbi azért, mert I nem üres. Ha $x \equiv y$ és $y \equiv z$, akkor van olyan $c, d \in I$, hogy $x \vee c = y \vee c$ és $y \vee d = z \vee d$. A $c \vee d \in I$ elem mutatja, hogy $x \equiv z$. Tegyük föl, hogy $x \equiv y$, ekkor $x \vee c = y \vee c$ alkalmas $c \in I$-re. Tetszőleges z esetén nyilván $x \vee z \equiv y \vee z$, a disztributivitás miatt pedig

$$(x \wedge z) \vee (c \wedge z) = (x \vee c) \wedge z = (y \vee c) \wedge z = (y \wedge z) \vee (c \wedge z)\,.$$

Mivel I ideál, $c \wedge z \leq c \in I$, és így $x \wedge z \equiv y \wedge z$. Tehát θ_I kongruencia (8.2.35. Gyakorlat). A dualitás elve miatt ρ_F is kongruencia. Az (1) megmutatásához még azt kell belátni, hogy I osztálya θ_I-nek. Ha $c, d \in I$, akkor $c \vee d \in I$-vel egyesítve ugyanazt az elemet kapjuk, tehát $c \equiv d$. Megfordítva, ha $x \equiv d$, ahol $d \in I$, akkor $x \vee c = d \vee c$ alkalmas $c \in I$-re, de akkor $x \leq d \vee c \in I$, tehát $x \in I$.

Tegyük föl, hogy a (2)-ben szereplő feltétel igaz, és $x \equiv y$ $(\theta_I \wedge \rho_F)$. Ekkor alkalmas $c \in I$-re $x \vee c = y \vee c$, és alkalmas $f \in F$-re $x \wedge f = y \wedge f$. A feltétel miatt $c \leq f$, így

$$y = (y \vee c) \wedge y = (x \vee c) \wedge y = (x \wedge y) \vee (c \wedge y) \leq x \vee (f \wedge y) = x \vee (f \wedge x) = x$$

(közben az elnyelési tulajdonságot és a disztributivitást használtuk, továbbá azt, hogy a két hálóművelet monoton). Az x és y cseréjével $x \leq y$ adódik, tehát $x = y$.

Végül a (3) igazolásához legyen L legalább háromelemű disztributív háló. Ekkor van olyan $c \in L$, amely nem legkisebb és nem legnagyobb elem. Legyen $I = (c]$ a c által generált főideál (vagyis a c-nél kisebb vagy egyenlő elemek halmaza), és $F = [c)$. Ekkor teljesül a (2)-beli feltétel, ezért $\theta_I \wedge \rho_F = 0_L$. A szubdirekt irreducibilitás miatt e két kongruencia egyike nulla, ami nem lehet, mert az I legalább kételemű, és osztálya θ_I-nek, az F pedig szintén legalább kételemű, és osztálya ρ_F-nek.

8.5.12. Az $m(x, y, z) \leq M(x, y, z)$ egyenlőtlenség nyilván következik az óriás-törpe elvből. A szimmetria és a dualitás miatt ahhoz, hogy ezek többségi kifejezések, elég belátni, hogy $m(x, x, z) = z$. Ez igaz, mert

$$m(x, x, z) = (x \wedge x) \vee (x \wedge z) \vee (x \wedge z) = x \vee (x \wedge z) = x$$

az elnyelési tulajdonság és az idempotencia miatt. Végül ha L disztributív, akkor

$$\begin{aligned} m(x, y, z) &= \big(x \wedge (y \vee z)\big) \vee (y \wedge z) = \\ &= \big(x \vee (y \wedge z)\big) \wedge \big((y \vee z) \vee (y \wedge z)\big) = \big(x \vee (y \wedge z)\big) \wedge (y \vee z) = M(x, y, z) \end{aligned}$$

(háromszor alkalmaztuk a disztributivitást).

8.5.16. A Jónsson-lemma szerint az M_3 által generált varietás szubdirekt irreducibilisei az M_3 részalgebráinak homomorf képei közül a szubdirekt irreducibilisek, vagyis az M_3 mellett csak a kételemű háló (a négyelemű és háromelemű hálók egyike sem szubdirekt irreducibilis, hiszen ezek vagy C_2^2-nel izomorfak, vagy láncok). Hasonlóan $\mathsf{V}(N_5)$ szubdirekt irreducibilisei csak az N_5 és a kételemű háló. Így egyik varietás sem része a másiknak, ezért mindegyikben igaz egy olyan azonosság, amelyik a másikban nem teljesül.

8.5.17. Tegyük föl, hogy az a elemnek b és c is komplementuma. Ekkor

$$c = 0 \vee c = (a \wedge b) \vee c = (a \vee c) \wedge (b \vee c) = 1 \wedge (b \vee c) = b \vee c \geq b\,.$$

A b és c cseréjével $b \geq c$ adódik, tehát $b = c$.

8.5.19. Csak azt kell végiggondolni, hogy a 8.5.4. Gyakorlat megoldásában megadott megfeleltetés a komplementumképzés műveletét is tartja.

8.5.20. Az x' elemnek x és x'' is komplementuma. A komplementum egyértelműsége (8.5.17. Gyakorlat) miatt tehát $x = x''$. A disztributivitás miatt

$$(x \wedge y) \wedge (x' \vee y') = (x \wedge y \wedge x') \vee (x \wedge y \wedge y') = 0 \vee 0 = 0\,.$$

Ennek duálisa $(x \vee y) \vee (x' \wedge y') = 1$. Ezt x helyett x'-re és y helyett y'-re alkalmazva $(x' \vee y') \vee (x \wedge y) = 1$ adódik. Ezért $x \wedge y$-nak komplementuma $x' \vee y'$. A második De Morgan azonosság az elsőnek a duálisa.

8.5.21. Elég megmutatni, hogy a θ_I kongruencia a komplementumképzés műveletével is kompatibilis. Tegyük föl, hogy $x \equiv y\ (\theta)$, ekkor létezik olyan $c \in I$, melyre $x \vee c = y \vee c$. Mindkét oldal komplementumát véve $x' \wedge c' = y' \wedge c'$ adódik a 8.5.20. Gyakorlat miatt. Ezt c-vel egyesítjük. A disztributivitást alkalmazva

$$(x' \wedge c') \vee c = (x' \vee c) \wedge (c' \vee c) = (x' \vee c) \wedge 1 = x' \vee c\,.$$

Hasonlóan $(y' \wedge c') \vee c = y' \vee c$, vagyis $x' \vee c = y' \vee c$, és így $x' \equiv y'\ (\theta_I)$.

8.5.23. A gyűrűaxiómák levezethetők volnának közvetlen számolással is, egyszerűbb azonban azt mondani, hogy a kételemű $\{0, 1\}$ Boole-algebrában a szimmetrikus differencia nyilván a szokásos összeadás, a metszet pedig a szokásos szorzás, és így a $\mathbb{Z}_2$ gyűrűt kapjuk, ami tényleg gyűrű, és igaz benne, hogy $x^2 = x$ és $x + x = 0$. A többi Boole-algebra pedig ennek szubdirekt hatványa, ezért $\mathbb{Z}_2$-ről minden gyűrűaxióma öröklődik a megadott két műveletre.

Most tegyük föl, hogy az R egységelemes gyűrűben érvényes az $x^2 \approx x$ azonosság. Ekkor

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y\,,$$

és ezért $xy + yx = 0$. Speciálisan $y = 1$ esetén $x + x = 0$. Azaz a karakterisztika 2, és így $xy = -yx = yx$, vagyis a kommutativitás is adódik. Az Olvasóra hagyjuk annak igazolását, hogy a megadott három műveletre Boole-algebrát kapunk, és hogy a kétféle ideálfogalom megegyezik.

8.5.24. Csak a lánc, valamint az első sor hálói disztributívak. Például a D_1 és D_2 azért nem, mert van N_5-tel izomorf részhálójuk, és N_5 nem disztributív (8.5.3. Gyakorlat). A C_2^2 és a C_2^3 lesznek Boole-hálók.

8.5.25. Tudjuk a 8.4.11. Feladat miatt, hogy véges sok véges algebra által generált varietásban minden végesen generált algebra véges. Márpedig Stone tétele miatt a disztributív hálók és a Boole-algebrák varietása is generálható egy kételemű algebrával.

8.5.26. Az nyilvánvaló, hogy az Útmutatóban megadott $\sim$ tényleg ekvivalencia-reláció az X halmazon. (A reflexivitás igazolásához ki kell használni, hogy C egységeleme az egész X halmaz, hiszen az egységelem Boole-algebrákban művelettel van kijelölve, és így részalgebra egységeleme ugyanaz, mint az eredeti algebráé. Hasonlóképpen $\emptyset \in C$.)

Ha kielemezzük a Stone-tétel bizonyítását, akkor láthatjuk, hogy az abból kapott C és X esetében a $\sim$ reláció triviális: a 0_X-szel egyezik meg. Ennek oka az, hogy a szubdirekt felbontás elkészítésekor csupa különböző kongruenciát használtunk (vagyis mindegyik kongruenciához csak egy tényezőt vettünk be a felbontásba). Ha a $\sim$ reláció triviális, akkor az alábbi bizonyítás egyszerűbbé válik (ezért az Olvasó nyugodtan tegye föl, hogy ez a helyzet).

Legyen Z a $\sim$ reláció egy osztálya, $z \in Z$ és $y \notin Z$. Ekkor a $\sim$ definíciója miatt van olyan $Y \in C$, hogy z és y közül pontosan az egyik van Y-ban. Feltehetjük (az Y halmazt a komplementumára cserélve, ha szükséges), hogy $z \in Y$ és $y \notin Y$. Mivel Z a z-nek az osztálya a $\sim$ relációnál, $Z \subseteq Y$. Készítsünk el minden $y \notin Z$-re egy ilyen Y halmazt. E véges sok halmaz metszete is C-ben van (hiszen C részalgebra), és Z-vel egyenlő. Vagyis $\sim$ minden osztálya C-beli. Mivel véges sok osztály van, és C részalgebra, osztályok tetszőleges uniója is C-beli. Láttuk továbbá, hogy $\emptyset \in C$, és így C izomorf a $\mathcal{P}(X')$ Boole-algebrával, ahol X' a $\sim$ osztályainak a halmaza.

Másféle bizonyítást is kaphatunk az állításra a következőképpen. Ha B véges Boole-algebra, akkor legyen X az atomoknak (a 0 fedőinek) a halmaza. Nem nehéz kiszámolni, hogy B minden eleme egyértelműen állítható elő atomok egyesítéseként (vagyis az alatta lévő

atomoknak az egyesítése, de kevesebb atomnak nem egyesítése). Ekkor pedig $B \cong \mathcal{P}(X)$ (vö. 8.6.34. Feladat). Egy harmadik bizonyítást a 8.6.37. Feladatban látunk majd.

8.5.27. Csak az Útmutató utolsó bekezdésében leírt állítást bizonyítjuk. Tekintsük az összes $\varphi : \{y_1, \ldots, y_n\} \to \{0, 1\} = L$ függvényt. A szabad algebrákról szóló Birkhoff-tétel (8.3.26. Tétel) bizonyítása szerint minden ilyen φ függvényhez fölveszünk egy koordinátát, és az L Boole-algebra ennyi példányának tekintjük a direkt szorzatát. A φ függvényt egyértelműen meghatározza azoknak az i számoknak az I halmaza, amelyekre $\varphi(y_i) = 1$, ezt pedig megfeleltethetjük az Útmutatóban definiált $x_I \in X$ elemnek. Vagyis az L^X direkt hatványról van szó, amelynek elemeit (a 8.5.4. Gyakorlatban megadott megfeleltetéssel) az X részhalmazainak is tekinthetjük.

Nem nehéz kiszámolni, hogy a Birkhoff-tételbeli $\psi : \{y_1, \ldots, y_n\} \to L^X$ függvény az y_i elemhez azt az $Y_i \subseteq X$ halmazt rendeli, amely pontosan azokból az x_I elemekből áll, amelyekre $i \in I$. De az Útmutatóban szereplő X_i halmaznak is ugyanezek az elemei, vagyis $X_i = Y_i$, és így a Birkhoff-tétel bizonyítása azt mondja, hogy az $X_1, \ldots, X_n$ halmazok szabad generátorrendszert alkotnak az általuk generált részalgebrában.

8.5.28. A 8.5.27. Feladat Útmutatójában bevezetett jelöléseket használjuk. E feladat fenti „második" megoldásából világos, hogy a szabad disztributív háló Birkhoff-féle konstrukciója ugyanazokat az $X_i \subseteq X$ halmazokat eredményezi, mint a szabad Boole-algebráké, csak az a különbség, hogy Boole-algebrák esetében ezek a teljes $\mathcal{P}(X)$-et generálják, míg disztributív hálók esetében ennek csak egy részhalmazát (hiszen komplementumképzést nem használhatunk). Így persze a szabad disztributív háló elemszáma legfeljebb 2^{2^n}.

Az alsó becsléshez legyen $K \subseteq \{1, 2, \ldots, n\}$, és messük el azokat az X_i halmazokat, ahol $i \in K$. A kapott X_K azokból az $x_I \in X$ elemekből áll, melyekre $K \subseteq I$. Ha $K_1, \ldots, K_m$ egyforma elemszámú halmazok, akkor az $Y = X_{K_1} \cup \ldots \cup X_{K_m}$ is eleme a szabad disztributív hálónak. Az Y halmazból visszakapható $K_1, \ldots, K_m$: tekintsük az Y összes x_I elemét, és keressük meg az így kapott I halmazok közül a tartalmazásra minimálisakat. Ezek pont $K_1, \ldots, K_m$ lesznek, hiszen ezek közül egyik sem tartalmazza a másikat az egyforma elemszám miatt. Ez azt jelenti, hogy bármely rögzített k esetén a hálónknak legalább annyi eleme van, mint ahány részhalmaza az X halmaz k elemű részhalmazaiból álló halmaznak.

8.5.29. Tekintsük az Útmutatóban konstruált faktoralgebrát. Tegyük föl, hogy ebben a nulla elemnek van egy fedője. Ez egy Y/θ_I osztály, ahol $Y \subseteq X$ szükségképpen végtelen halmaz (különben Y/θ_I a nulla elem lenne). Vágjuk az Y halmazt két végtelen Y_1 és Y_2 részre (például úgy, hogy kiveszünk belőle $y_1, y_2, \ldots$ elemeket, és az Y_1 a páros indexű y_i elemekből áll, az Y_2 pedig az Y többi eleméből). Ekkor a $0 < Y_1/\theta_I < Y/\theta_I$ (ami ellentmond annak, hogy Y/θ_I fedi a nullát). Ha ugyanis $Y_1/\theta_I = Y/\theta_I$ lenne, akkor θ_I definíciója szerint van olyan Z véges részhalmaza X-nek, hogy $Y \cup Z = Y_1 \cup Z$, ami ellentmond annak, hogy Y_2 végtelen halmaz.

8.5.30. Az (1) és (2) nyilvánvaló, a (3) abból következik, hogy ha θ maximális kongruencia, akkor L/θ egyszerű, így szubdirekt irreducibilis disztributív háló, tehát kételemű.

A (3) közvetlen számolással is igazolható, ez azonban nagyon hasonlít a 8.5.8. Feladat megoldásához, amit az előző mondatban fölhasználtunk. Ezt a feladatot a (4) bizonyításához is fölhasználhatnánk, mert segítségével az állítást visszajátszhatnánk az L/θ_I hálóra (az Olvasó számára jó gyakorló feladat ezt végiggondolni). Egyszerűbb azonban az alábbi, közvetlen gondolatmenet (amivel a Stone-tételre is új bizonyítást adhatunk).

A (4) igazolásához legyen I maximális az L azon ideáljai között, amelyek az F filtertől diszjunktak. Tegyük föl, hogy $x, y \notin I$, de $x \wedge y \in I$. Azok az e elemek, amelyekhez létezik olyan $c \in I$, hogy $e \leq c \vee x$, egy ideált alkotnak, amely az I-t és x-et is tartalmazza. Az I maximalitása miatt ez az ideál már nem diszjunkt F-től, tehát valamelyik ilyen $e \in F$, és így a megfelelő $c \vee x$ is eleme F-nek, hiszen F filter. Ugyanígy van olyan $d \in I$, hogy $d \vee y \in F$. De akkor a disztributivitás miatt

$$F \ni (c \vee x) \wedge (d \vee y) = (c \wedge d) \vee (c \wedge y) \vee (x \wedge d) \vee (x \wedge y)\,.$$

Mind a négy metszet I-beli, és így az egyesítésük is, ami ellentmond annak, hogy I és F diszjunkt. Ezzel (4)-et beláttuk. Az (5) bizonyítását az Útmutatóban leírtak alapján az Olvasóra hagyjuk.

8.6. Moduláris hálók.

8.6.1. Ha θ és ρ felcserélhetők, akkor legyen $h \in H$ és $k \in K$. Mivel $1\ \theta\ h\ \rho\ hk$, ezért $(1, hk) \in \rho \circ \theta$, azaz van olyan g, hogy $1K = gK$ és $gH = hkH$. Így $g^{-1}hk \in H$, és $hk = g(g^{-1}hk) \in KH$. Tehát $HK \subseteq KH$. A H és K illetve a θ és ρ cseréjével látjuk, hogy $KH \subseteq HK$ is teljesül.

A megfordítás is hasonló számolás, de abból is következik, hogy ha $HK = KH$, akkor HK részcsoport (4.4.29. Gyakorlat), és mind $\theta \circ \rho$, mint $\rho \circ \theta$ könnyen láthatóan a HK baloldali mellékosztályaiból kapott partíció.

8.6.8. Ha $x \leq z$, akkor a disztributivitás miatt

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) = x \vee (y \wedge z)\,,$$

hiszen $x \wedge z = x$. Ezért (1) igaz. Ha $x \leq z$, akkor $(x \vee y) \wedge z \geq x \vee (y \wedge z)$ az óriás-törpe elv miatt, ezért (2) is teljesül.

Disztributív hálóban a fenti átalakítás miatt $(x \vee y) \wedge z \leq x \vee (y \wedge z)$ mindig teljesül, hiszen $x \wedge z \leq x$. Tegyük most föl, hogy az L hálóban igaz a (2)-beli egyenlőtlenség. Ezt kétszer alkalmazva (először y helyett z-re és z helyett $x \vee y$-ra)

$$(x \vee z) \wedge (x \vee y) \leq x \vee \big(z \wedge (x \vee y)\big) \leq x \vee \big(x \vee (y \wedge z)\big) = x \vee (z \wedge y)\,,$$

vagyis beláttuk a disztributív szabályt (az óriás-törpe elv miatt elég ez az egyenlőtlenség).

8.6.9. A 8.6.7. Definícióban szereplő moduláris tulajdonság önmagába megy át, ha dualizáljuk (ekkor $x \leq z$ átváltozik $x \geq z$-re), majd az x és z változókat megcseréljük.

8.6.12. Az Útmutatóban lerajzolt „halgerinc-háló” elemeit alulról fölfelé haladva generálhatjuk úgy, hogy felváltva a-val, illetve c-vel egyesítünk, és közben mindig b-vel metszünk. A halgerinc magassága, és így egy három elemmel generált háló elemszáma akármilyen nagy (véges) szám lehet. Mivel a három elemmel generált szabad hálónak ezek mind homomorf képei, annak elemszáma végtelen.

8.6.14. A moduláris szabályt úgy is meg lehet jegyezni, hogy az a disztributivitás gyengített változata: metszetbe be szabad egyesíteni az egyik tagnál kisebbel, és egyesítésbe be szabad metszeni az egyik tagnál nagyobbal. Ennek alapján

$$[x \wedge (y \vee z)] \vee [z \wedge (x \vee y)] = \big([x \wedge (y \vee z)] \vee z\big) \wedge (x \vee y) = \big((x \vee z) \wedge (y \vee z)\big) \wedge (x \vee y)\,.$$

Az első lépésben $x \wedge (y \vee z)$-vel egyesítettünk be a $z \wedge (x \vee y)$ metszetbe, a másodikban z-vel az $x \wedge (y \vee z)$ metszetbe.

8.6.21. A Jordan–Dedekind-tétel az ilyen láncokról szól, csak azt kell meggondolni, hogy amikor a bizonyításban az intervallum-izomorfizmus tételt alkalmazzuk, akkor csoportelméleti izomorfiát is kapunk az első izomorfizmus-tétel miatt.

8.6.27. Az Útmutatóban bevezetett jelöléseket használjuk. A $c \wedge q_j$ elemek metszete b, és így az intervallum-izomorfizmusnál nekik megfelelő $p_i \vee (c \wedge q_j)$ elemek metszete a b-nek megfelelő p_i. De p_i metszet-irreducibilis, ezért van olyan j, hogy e metszet egyik tagja maga p_i, ami az izomorfizmusnál visszafelé haladva azt jelenti, hogy $c \wedge q_j = b$. Tehát p_i-t sikerült q_j-re cserélni.

Tegyük föl most, hogy $n \neq m$, hanem például $n < m$. Cseréljük ki az első felbontás elemeit sorra a második felbontás elemeire. Végül a b egy olyan felbontását kapjuk néhány q_j metszeteként, amelynek legfeljebb n tagja van. Ez lehetetlen akkor, ha a b-nek a $q_1 \wedge \ldots \wedge q_m$ felbontása rövidíthetetlen volt.

Felhívjuk a figyelmet arra, hogy az eljárás közben kapott felbontásokról nem állítjuk, hogy rövidíthetetlenek. Érdemes ezt a gondolatmenetet összevetni a 7.2.19. Gyakorlat megoldásával. Ha F független rendszer, G pedig generátorrendszer egy vektortérben, és azt akarjuk bizonyítani, hogy $|F| \leq |G|$, akkor az F elemeit cseréljük G elemeire. A függetlenségnek a fenti bizonyításban a rövidíthetetlenség felel meg. A lineáris algebrai gondolatmenetben fontos volt, hogy cseréléskor F elemszáma ne csökkenjen, a fenti gondolatmenetben azonban erre nem kellett ügyelnünk. Ennek oka az, hogy a fenti állítás lineáris algebrai analogonja csak annyi, hogy egy vektortérben bármely két bázis elemszáma egyforma. Ha F és G bázisok, akkor a lineáris algebrai bizonyításban sem kell ügyelni arra, hogy F elemszáma ne csökkenjen: ha indirekt föltesszük, hogy F és G elemszáma különböző, akkor a kisebbik elemeit fogjuk cserélni a nagyobbik elemeire.

Megjegyezzük még, hogy ez az analógia a lineáris algebrai függetlenség-fogalommal pontossá tehető (lásd a 8.6.34. Feladatot).

8.6.28. Csak M_3 és a disztributívak (a C_8 és az első sor hálói, vö. 8.5.24. Gyakorlat).

8.6.29. Ha a-nak $b \le c$ is komplementuma, akkor a modularitás miatt

$$c = 1 \wedge c = (b \vee a) \wedge c = b \vee (a \wedge c) = b \vee 0 = b\,.$$

8.6.30. Ha $a \le c \le b$, és d a c komplementuma az egész hálóban, akkor $e = (d \vee a) \wedge b$ komplementuma lesz c-nek az $[a, b]$ intervallumban. Valóban, a modularitás miatt

$$c \wedge e = c \wedge [(d \vee a) \wedge b] = c \wedge (d \vee a) = (c \wedge d) \vee a = 0 \vee a = a\,,$$

és $c \le b$ miatt, szintén a modularitást alkalmazva

$$c \vee e = c \vee [(d \vee a) \wedge b] = [c \vee (d \vee a)] \wedge b = 1 \wedge b = b\,.$$

8.6.31. Legyen $x \le z$, akkor a dimenzió-egyenlőség miatt

$$d\big((x \vee y) \wedge z\big) = d(x \vee y) + d(z) - d\big((x \vee y) \vee z\big)\,.$$

Itt $(x \vee y) \vee z = y \vee z$, hiszen $x \le z$, és a dimenzió-egyenlőséget még egyszer alkalmazva a következő kifejezést kapjuk:

$$d(x) + d(y) + d(z) - d(x \wedge y) - d(y \vee z)\,.$$

A $d\big(x \vee (y \wedge z)\big)$ kifejezést a dimenzió-egyenlőség kétszeri alkalmazásával hasonló módon kifejtve ugyanez a kifejezés adódik. Mivel $x \vee (y \wedge z) \le (x \vee y) \wedge z$, és e két elem magassága megegyezik, ezért egyenlőek, vagyis beláttuk a modularitást.

8.6.32. Az L magassága három, és így a 8.6.31. Gyakorlat miatt a modularitás igazolásához elég a dimenzió-egyenlőséget ellenőrizni. Ez nyilvánvaló, ha x és y összehasonlíthatók. Ezen kívül $\{x, y\}$-ra csak három lehetőség van: két pont, pont és egyenes, illetve két egyenes. Mindegyik eset könnyen elintézhető azzal, hogy két különböző egyenes metszete pont (aminek magassága 1); két különböző pont egyesítése egyenes (aminek a magassága 2); végül egyenes és rajta nem fekvő pont metszete üres, egyesítése pedig az egész sík.

Az L egyszerű. Ezt ugyanúgy igazolhatjuk, mint azt, hogy M_3 egyszerű (8.2.37. Gyakorlat), vagy hogy a partícióháló egyszerű (8.2.41. Feladat). A bizonyítás azon múlik, hogy L intervallumaiban az elemeknek elég sok komplementuma van. A részletek kidolgozását az Olvasóra hagyjuk.

Vegyük a síkon egy háromszög három csúcsát és a súlypontját. Az ezek által generált részháló végtelen. Valóban, az első lépésben megkapjuk a háromszög oldalfelező pontjait. Az ezek alkotta háromszögnek a súlypontja ugyanaz, mint az eredeti háromszögé, tehát ennek a kisebb háromszögnek is megkapjuk az oldalfelező pontjait. És így tovább, egyre kisebb háromszögeket kapunk, és így végtelen sok pont lesz az eredeti négy pont által generált hálóban. Ebből következik, hogy a négy elemmel generált szabad moduláris háló elemszáma is végtelen, hiszen a most generált részháló a szabadnak homomorf képe.

8.6.33. Ha a atom, akkor a dimenzió-egyenlőség miatt $d(x) \le d(x \vee a) \le d(x)+1$, hiszen az atomok magassága 1, és ha a nincs x alatt, akkor $d(x \vee a) = d(x) + 1$ (hiszen ekkor $d(x \wedge a) = 0$). Ebből látszik az is, hogy atomok tetszőleges egyesítésének magassága legfeljebb a tagok száma lehet.

Ha tehát az Útmutatóban leírt procedúrát végezzük, akkor $d(c \vee a_1 \vee \ldots \vee a_i) = d(c)+i$ mindegyik i-re. Mivel L véges magasságú, az eljárás véges sok lépésben véget ér. Ekkor viszont $c \vee a_1 \vee \ldots \vee a_k = 1$ teljesül, hiszen az 1 előáll atomok egyesítéseként. Legyen $b = a_1 \vee \ldots \vee a_k$, akkor a fenti megjegyzés miatt $d(b) \le k$, és így

$$d(c) + k = d(c \vee b) = d(c) + d(b) - d(c \wedge b) \le d(c) + k - d(c \wedge b)\,,$$

ahonnan $d(c \wedge b) \le 0$. Ezért b komplementuma c-nek.

Beláttuk tehát, hogy L komplementumos, és így minden intervalluma is komplementumos (8.6.30. Gyakorlat). Ha $c \in L$, akkor jelölje d a c alatti atomok egyesítését, és legyen e a d komplementuma a $[0, c]$ intervallumban. Ekkor e alatt nem lehet atom. A Jordan–Dedekind-tétel és a véges magasság miatt azonban minden nem nulla elem alatt van atom. Ezért $e = 0$, vagyis $d = c$. Tehát c atomok egyesítése.

A feladat állítására egy másik bizonyítást találhatunk a 8.6.34. Feladat megoldásában, ami a függetlenség fogalmán alapszik.

8.6.34. Tegyük föl, hogy $a_1, \ldots, a_n$ atomok, és az a egyesítésük rövidíthetetlen. A függetlenség igazolásához elég belátni, hogy ha $b = a_1 \vee \ldots \vee a_{n-1}$, akkor $b \wedge a_n = 0$ (hiszen ugyanez a bizonyítás működik bármely másik a_i elhagyásakor is, csak az a_i elemeket kell permutálni). Mivel a_n atom, ha $b \wedge a_n$ nem nulla, akkor csak a_n lehet, vagyis $a_n \le b$. De akkor $a = b \vee a_n = b$, ami ellentmond a rövidíthetetlenségnek. Ezzel (1)-et beláttuk.

A (2) bizonyításához elég megmutatni, hogy

$$a_1 \wedge (a_2 \vee \ldots \vee a_n \vee a) = 0$$

(hiszen az a_i elemeket ismét permutálhatjuk). Legyen $b = a_2 \vee \ldots \vee a_n$. Tudjuk, hogy $a_1 \wedge b = 0$ és $(a_1 \vee b) \wedge a = 0$. Így az Útmutatóban szereplő azonosság miatt

$$a_1 \wedge (b \vee a) \le (a_1 \vee b) \wedge (b \vee a) = b \vee \big((a_1 \vee b) \wedge a\big) = b \vee 0 = b\,.$$

De akkor $a_1 \wedge (b \vee a) \le a_1 \wedge b = 0$.

A (3) igazolásához legyen $I \subseteq \{1, 2, \ldots, n\}$ esetén a_I az a_i elemek egyesítése, ahol $i \in I$ (speciálisan $a_\emptyset = 0$ és $a_{\{i\}} = a_i$). Nyilván elég belátni, hogy ezek részhálót alkotnak, vagyis hogy $a_I \wedge a_J = a_{I \cap J}$. Legyen $b = a_{I-J}$, $c = a_{I \cap J}$ és $d = a_{J-I}$. Ismét az Útmutatóban szereplő azonosság miatt

$$a_I \wedge a_J = (b \vee c) \wedge (d \vee c) = c \vee \big((b \vee c) \wedge d\big)\,.$$

Jelölje K az I és J szimmetrikus differenciáját. Persze $b \vee c = a_K$, és K diszjunkt az $I \cap J$ halmaztól. Ezért elég megmutatni, hogy ha $U, V \subseteq \{1, 2, \ldots, n\}$ és $U \cap V = \emptyset$, akkor $a_U \wedge a_V = 0$ (mert ebből $(b \vee c) \wedge d = 0$ következik).

Ezt V elemszáma szerinti indukcióval végezzük. Ha V üres, akkor az állítás nyilvánvaló. Tegyük föl, hogy $V = W \cup \{j\}$, ahol W-nek eggyel kevesebb eleme van, mint V-nek. Az

indukciós feltevés miatt $a_U \wedge a_W = 0$. Alkalmazzuk a (2)-ben bizonyított állítást az a_U, az a_W és az a_j elemekre. Az a_U és az a_W független, mert $a_U \wedge a_W = 0$. Az $a_1, \ldots, a_n$ függetlensége miatt $(a_U \vee a_W) \wedge a_j = 0$ (hiszen $j \notin U \cup W$). Így (2) miatt a_U, a_W, a_j függetlenek, vagyis $0 = a_U \wedge (a_W \vee a_j) = a_U \wedge a_V$. Ezzel a (3) állítást is igazoltuk.

A 8.6.33. Feladat állításának bizonyításához tegyük föl, hogy $c \in L$. Az 1 előáll véges sok a_i atom egyesítéseként, válasszuk ki ezek közül az $a_1, \ldots, a_n$-et úgy, hogy c-vel együtt független rendszert alkossanak, de több a_i-t már ne lehessen bevenni úgy, hogy a rendszer független maradjon. (Ezt a véges magasság és (3) miatt megtehetjük.) Az ezek generálta részháló (3) miatt komplementumos, és c-t tartalmazza, ezért elég megmutatni, hogy a legnagyobb eleme, vagyis $d = c \vee a_1 \vee \ldots \vee a_n$ az L háló egységeleme. Tegyük föl, hogy nem, akkor van olyan a_i, hogy a_i nincs d alatt. Mivel a_i atom, $a_i \wedge d = 0$. De akkor (2) miatt a $c, a_1, \ldots, a_n$ rendszer a_i-vel bővítve is független, ami a maximalitásnak ellentmond.

8.6.35. Legyen d az A algebrának Malcev-kifejezése, és jelöljük ugyanígy a hozzá tartozó kifejezésfüggvényt is. A d a $B \leq A \times A$ algebrán komponensenként működik. A B szimmetriáját bizonyítandó tegyük föl, hogy $(a, b) \in B$. Mivel B reflexív, $(a, a), (b, b) \in B$, és így

$$d\big((a, a), (a, b), (b, b)\big) = \big(d(a, a, b), d(b, b, a)\big) = (b, a)\,.$$

Ez a pár B-ben van, mert B zárt az d-hez tartozó kifejezésfüggvényre. Így B tényleg szimmetrikus. A tranzitivitás igazolásához tegyük föl, hogy $(a, b), (b, c) \in B$. Ekkor

$$d\big((a, b), (b, b), (b, c)\big) = \big(d(a, b, b), d(b, b, c)\big) = (a, c) \in B\,.$$

8.6.36. Érdemes az A elemeire úgy gondolni, mint egy páros gráf éleire, amelyek a B és C között vezetnek. Tegyük föl, hogy $(b_1, c_1), (b_1, c_2), (b_2, c_2) \in A$. A d Malcev-függvényt (komponensenként) alkalmazva

$$d\big((b_1, c_1), (b_1, c_2), (b_2, c_2)\big) = \big(d(b_1, b_1, b_2), d(c_1, c_2, c_2)\big) = (b_2, c_1) \in A\,.$$

Ez azt jelenti, hogy ha $(b_1, c_1) \in A$, akkor a b_1/θ osztály minden b_2 elemére $(b_2, c_1) \in A$. Ugyanígy, ha $(b_2, c_2) \in A$, akkor a c_2/ρ osztály minden c_1 elemére $(b_2, c_1) \in A$. Ezt a két észrevételt egymás után alkalmazva azt kapjuk, hogy ha egy θ-osztály és egy ρ-osztály között megy egy A-beli él, akkor e két osztály között minden él be van húzva. Továbbá egy θ-osztály csak egyetlen ρ-osztállyal lehet „szomszédos”, a ρ definíciója miatt (és fordítva).

Mindebből világos, hogy a φ kölcsönösen egyértelmű megfeleltetés a θ-osztályok és a ρ-osztályok között, és az is, hogy A elemei pontosan azok a párok, amelyek az egymásnak megfelelő osztályokat kötik össze.

8.6.37. Egy tényezős szubdirekt szorzat természetesen izomorf az egyetlen tényezőjével. Legyen A az $S_1, \ldots, S_n$ szubdirekt szorzata, ahol S_i egyszerű. Vetítsük A-t az első $n-1$ tényezőre (vagyis vegyük A minden elemének az első $n-1$ komponensét). Az így kapott $B \leq S_1 \times \ldots \times S_{n-1}$ szubdirekt szorzat lesz, ami az indukciós feltevés miatt izomorf néhány S_i direkt szorzatával. Az A viszont tekinthető a B és az S_n szubdirekt szorzatának. Megmutatjuk, hogy A vagy B-vel, vagy $B \times S_n$-nel izomorf (és ezzel készen is leszünk).

Alkalmazzuk az előző 8.6.36. Feladatot az $A \leq B \times S_n$ szubdirekt szorzatra. Mivel S_n egyszerű, a ρ kongruenciára csak két lehetőség van: az 1 és a 0. Az első esetben $A = B \times S_n$ (hiszen akkor B/θ is egyelemű). A második esetben viszont az első projekció izomorfizmus A és B között, hiszen minden $b \in B$-hez pontosan egy olyan $s \in S_n$ van, melyre $(b, s) \in A$.

Az Olvasónak azt javasoljuk, adjon másik bizonyítást is az állításra a 8.6.34. Feladat (és a 8.2.32. Állítás) fölhasználásával.

Speciális esetként tekintsük a Boole-algebrák varietását, amely a 8.6.5. Állítás miatt kongruencia-felcserélhető. Stone tétele szerint minden véges Boole-algebra a kételemű Boole-algebra szubdirekt hatványa, és a kételemű Boole-algebra egyszerű, ezért azt kapjuk, hogy minden véges Boole-algebra néhány tényező direkt szorzatával, vagyis a kételemű Boole-algebra egy direkt hatványával izomorf.

8.6.38. Az Útmutató jelöléseivel a D és a $H \times \{1\}$ egyesítése a 8.6.35. Feladat miatt a G egy kongruenciájának megfelelő részcsoport lesz $G \times G$-ben. Ennél a kongruenciánál H minden eleme kongruens az egységelemmel, és ezért a megfelelő normálosztó legalább akkora, mint az N. Másfelől viszont az N-hez tartozó B részalgebra nyilván tartalmazza D-t is és $H \times \{1\}$-et is, tehát a keresett egyesítés a B. A modularitást alkalmazva

$$[(H \times \{1\}) \vee D] \wedge (N \times \{1\}) = (H \times \{1\}) \vee [D \wedge (N \times \{1\})]\,.$$

A bal oldal $B \wedge (N \times \{1\}) = N \times \{1\}$, a jobb oldal viszont $H \times \{1\}$, hiszen $D \wedge (N \times \{1\})$ csak az egységelemből áll. Ezért $H = N$, vagyis H normálosztó.

8.7. Galois-kapcsolat és fogalom-analízis.

8.7.7. A 8.7.6. Lemma állítását hivatkozás nélkül használni fogjuk. Vegyük észre először, hogy ha $X \subseteq Y$, akkor $X^\sharp \supseteq Y^\sharp$, innen pedig $X^{\sharp\flat} \subseteq Y^{\sharp\flat}$. Az $X^{\sharp\flat}$ nyilván zárt, és tartalmazza X-et. Ha $X \subseteq U^\flat$, akkor $X^{\sharp\flat} \subseteq U^{\flat\sharp\flat} = U^\flat$. Ezért $X^{\sharp\flat}$ tényleg az X-et tartalmazó legszűkebb zárt halmaz, és így (1) igaz. A (2) közvetlenül adódik ebből, hiszen $X^{\sharp\flat\sharp\flat} = (X^\sharp)^{\flat\sharp\flat} = X^{\sharp\flat}$. A (3) is világos, hiszen az X akkor és csak akkor zárt, ha az őt tartalmazó legszűkebb zárt halmaz saját maga.

Végül ha X az X_i zárt halmazok metszete, akkor $X \subseteq X_i$ miatt $\overline{X} \subseteq \overline{X_i} = X_i$, és így $\overline{X}$ része az X_i halmazok metszetének, ami X. Tehát X zárt, és (4) is teljesül.

8.7.9. Az állítást valós fölött úgy szokás bizonyítani, hogy belátjuk: W és $W^\perp$ egymás komplementumai az $\mathbb{R}^n$ altérhálójában. Véges karakterisztikájú T esetében ez általában nem igaz (hiszen egy vektor lehet önmagára ortogonális). Sőt, ez például komplex fölött is előfordulhat, ezért ott az ortogonalitás fogalmát módosítják (ennek mikéntjével itt nem foglalkozunk, lásd [**10**], 7. és 8. Fejezet).

Vegyünk a W altérben egy bázist, és írjuk ezek koordinátáit egy M mátrix soraiba. Ekkor $W^\perp$ elemei pontosan az $Mv = 0$ feltételnek eleget tevő v vektorok lesznek. Mivel M rangja $\dim W$, a dimenziótétel miatt az M magterének, vagyis $W^\perp$-nak a dimenziója $n - \dim W$. Ezt kétszer alkalmazva azt kapjuk, hogy $W^{\perp\perp}$ dimenziója ugyanaz, mint W dimenziója. De $W \subseteq W^{\perp\perp}$, és így a dimenziók egyenlősége miatt e két altér is megegyezik. Ezért tényleg minden altér zárt halmaz.

8.7.10. Először azt igazoljuk, hogy T^n minden W altere zárt. A lineáris leképezések előírhatósági tétele segítségével könnyen konstruálhatunk olyan C lineáris transzformációt, amelynek magja pontosan a W altér. Ekkor $\{C\}^\sharp = W$, vagyis W tényleg zárt.

Annak igazolására, hogy a balideálok is zártak, az Útmutatóban leírt megoldást folytatjuk. Legyen $C \in L$ egy maximális rangú transzformáció, föltehetjük, hogy C idempotens (hiszen $C \in L$ esetén $DC \in L$). Mivel $C \in L$, a C magtere tartalmazza W-t. Tegyük föl, hogy van olyan $v \notin W$, amelyre $C(v) = 0$. Ekkor $W = L^\sharp$ miatt van olyan $C_v \in L$, hogy $C_v(v) \neq 0$. A C_v-t alkalmas DC_v-vel helyettesítve föltehető, hogy $C_v(v) = v$. Legyen $F = C_v + C - C_vC$. Ekkor $F(v) = C_v(v) = v$, ha pedig u benne van C képterében, akkor $C(u) = u$, és ezért $F(u) = C_v(u) + u - C_v(u) = u$. Vagyis az $F \in L$ képtere bővebb a C képterénél (hiszen v nincs az C képterében, mert akkor $C(v) = v$ teljesülne). Ez az ellentmondás bizonyítja, hogy C magtere W. Az előírhatósági tétel segítségével könnyű megmutatni, hogy minden olyan transzformáció, amelynek magtere W-t tartalmazza, DC alakban írható, és így L-beli. Vagyis $W^\flat \subseteq L$, és így beláttuk, hogy minden balideál zárt.

A 8.7.12. Feladat megoldása utáni megjegyzés egy másik bizonyítást ad az állításra.

8.7.11. Ha tetszőlegesen veszünk relációkat, akkor az ezekkel kompatibilis függvények nyilván klónt alkotnak, vagyis zártak a kompozícióra, és tartalmazzák a projekciókat. Azt kell megmutatni, hogy minden klón előáll ilyen módon (vagyis hogy minden klón zárt halmaz). Ha adott egy K klón, akkor ez a C-t algebrává teszi. Jelölje F_n a C fölött n elemmel generált szabad algebra alaphalmazát. Ez a 8.3.26. Tétel bizonyítása miatt a C^k részhalmazának tekinthető, ahol $k = |C|^n$ (hiszen ennyi függvény van egy n elemű halmazból C-be, lásd A.2.3. Állítás). Megmutatjuk, hogy ezek a relációk a K klónt határozzák meg.

Az világos, hogy az F_n relációk kompatibilisek K-val, hiszen részalgebrákról van szó. Megfordítva, tegyük föl, hogy egy n-változós f függvény tartja az F_n relációt. Az F_n algebra szabad generátorait jelölje $x_1, \ldots, x_n$, akkor tehát $f(x_1, \ldots, x_n)$ is eleme az F_n halmaznak. Ezért létezik olyan t formális kifejezés a K által meghatározott τ típusban, hogy

$t^{F_n}(x_1, \dots, x_n) = f(x_1, \dots, x_n)$. Mivel ezek szabad generátorok, $t^C = f$ (a 8.4.6. Gyakorlat miatt). Tehát f kifejezésfüggvénye a (K elemeivel, mint műveletekkel ellátott) C algebrának, vagyis előáll, mint K-beli függvények kompozíciója (vagy projekció). De K zárt a kompozícióra, így $f \in K$.

Az előző bizonyítás elmondható formális kifejezések használata nélkül is. Az F_n algebrát úgy kapjuk meg az $x_1, \dots, x_n$ generátorokból, hogy K elemeit komponensenként hatva alkalmazzuk ezekre. Így van olyan $g \in K$, hogy a g-t komponensenként alkalmazva éppen $f(x_1, \dots, x_n)$ adódik. Ekkor $f = g$, vagyis $f(c_1, \dots, c_n) = g(c_1, \dots, c_n)$ tetszőleges $c_1, \dots, c_n \in C$ elemekre, mert van olyan j komponense a C^k direkt hatványnak, hogy minden i-re az x_i-nek a j-edik komponense pont c_i.

8.7.12. Ha M egy $n \times n$-es mátrix és $v \in T^n$, akkor $Mv = 0$ akkor és csak akkor, ha v ortogonális M soraira (a 8.7.9. Gyakorlat értelmében). Legyen L balideál, és a 8.7.10. Feladat jelölését használva készítsük el a $U = (W^\sharp)^\perp$ alteret. Ez két rendezésfordító bijekció egymásutánja, tehát rendezéstartó bijekció a balideálok és az alterek között. Az U altér pontosan az L-beli mátrixok sorvektoraiból áll, az L pedig azokból a mátrixokból, amelyek sorai U-ban vannak, és így ez a feladatban megadott megfeleltetés.

Az állítást közvetlenül, mátrixokkal való számolással is bizonyíthatjuk. Legyen $E_{i,j}$ az a mátrix, amelyben az i-edik sor j-edik eleme 1, a többi elem nulla. Könnyű belátni, hogy az $E_{i,j}M$ mátrixban az i-edik sor megegyezik az M mátrix j-edik sorával, a többi sor pedig nulla. Legyen L balideál, az L-beli mátrixok soraiból álló altér az U, és tegyük föl, hogy az M mátrix mindegyik sora U-beli. Ezek a sorok tehát az $M_1, \dots, M_n \in L$ mátrixok alkalmas sorai. Ezekből a mátrixokból balszorzás és összeadás segítségével M-et megkaphatjuk, tehát $M \in L$. Vagyis L minden olyan mátrixot tartalmaz, amelynek a sorai U-beliek. Hasonlóan könnyű meggondolni, hogy U altér, továbbá, hogy ha W tetszőleges altér, akkor azok a mátrixok, amelyek sorai W-beliek, balideált alkotnak. A részleteket az Olvasóra bízzuk.

Ez lehetővé teszi, hogy a 8.7.10. Feladatra második megoldást adjunk. Ha ugyanis tudjuk már, hogy az $U \leftrightarrow b(U)$ megfeleltetés rendezéstartó bijekció, akkor a $b(U) \leftrightarrow U^\perp$ megfeleltetés rendezésfordító bijekció lesz, és persze $U^\perp = b(U)^\sharp$. A részletek kidolgozását itt is az Olvasóra hagyjuk.

8.8. Kategóriák és funktorok.

8.8.3. Az $\alpha \circ \varphi = \beta \circ \varphi$ azt jelenti, hogy minden $a \in A$-ra $\alpha\big(\varphi(a)\big) = \beta\big(\varphi(a)\big)$. Ha φ szürjektív, akkor $\varphi(a)$ minden B-beli értéket fölvesz, tehát $\alpha(b) = \beta(b)$ minden $b \in B$-re, és így $\alpha = \beta$. Ha viszont φ nem szürjektív, akkor megadhatunk olyan α és β leképezéseket, amelyek φ értékkészletén megegyeznek, de egy azon kívüli (B-beli) elemen nem. Ezekre tehát $\alpha \neq \beta$, de $\alpha \circ \varphi = \beta \circ \varphi$. Ezért (1) igaz.

A $\varphi \circ \alpha = \varphi \circ \beta$ azt jelenti, hogy $\varphi\big(\alpha(c)\big) = \varphi\big(\beta(c)\big)$ minden $c \in C$-re. Ha φ injektív, akkor innen $\alpha(c) = \beta(c)$ minden c-re, vagyis $\alpha = \beta$. Ha viszont φ nem injektív, mondjuk $\varphi(a) = \varphi(b)$, ahol $a \neq b$, akkor legyen α a konstans a és β a konstans b leképezés. Ezek különböznek, de $\varphi \circ \alpha = \varphi \circ \beta$. Ezért (2) is teljesül.

Ha $\varphi : A \to B$ homomorfizmus, akkor $\varphi(a) = \varphi(b)$ (de $a \neq b$) esetén legyen C az x által generált szabad algebra, és válasszuk az α és β homomorfizmusokat úgy, hogy $\alpha(x) = a$ és $\beta(x) = b$ legyen. Ebből látszik, hogy a (2) tulajdonság minden varietásban jellemzi az injektivitást.

Ugyanakkor a $\mathbb{Z} \to \mathbb{Q}$ identikus (nem szürjektív) beágyazás a gyűrűk varietásában teljesíti az (1) tulajdonságot. Ennek okát csak érzékeltetjük: ha $\alpha, \beta : \mathbb{Q} \to R$ homomorfizmusok, akkor könnyen láthatóan $\alpha(1/2) = 2\alpha(1/2)\beta(1/2) = \beta(1/2)$.

8.8.5. Legyen az A_i objektumoknak A a π_i morfizmusokkal, B pedig a ρ_i morfizmusokkal a direkt szorzata. A direkt szorzat definíciója miatt van olyan $\psi : B \to A$ morfizmus, hogy $\pi_i \circ \psi = \rho_i$ minden i-re. A szerepeket megcserélve olyan $\varphi : A \to B$ is létezik, amelyre $\rho_i \circ \varphi = \pi_i$ minden i-re. Az A és B „izomorfiája" azt jelenti, hogy $\varphi \circ \psi = id_B$ és $\psi \circ \varphi = id_A$. Ez a direkt szorzat definíciójában szereplő egyértelműségi kitétel miatt igaz. Ugyanis $\rho_i \circ \varphi \circ \psi = \rho_i$, de persze $\rho_i \circ id_B = \rho_i$, az egyértelműség miatt tehát $\varphi \circ \psi = id_B$. Ugyanez a gondolatmenet szerepelt a 8.8.2. Tétel bizonyításában is.

8.8.7. Az (1) speciális esete (3)-nak (hiszen a halmazok olyan speciális algebrák, amelyeknél a műveletek halmaza üres). Tekintsük az Útmutatóban megadott π_i homomorfizmusokat. A (2) esetében ha $\varphi_i : M_i \to N$, akkor a $\psi : M \to N$ egyetlen lehetősége, hogy az $(\ldots, m_i, \ldots)$ elemet $\sum \varphi_i(m_i)$-be vigye. Ez az összeg értelmes, hiszen csak véges sok nem nulla tagja van, és a kapott ψ könnyen láthatóan homomorfizmus is.

A (3) esetében ha $\varphi_i : F(X_i) \to A$, akkor tekintsük azt a $\varphi : X \to A$ leképezést, amelyre $x_i \in X_i$ esetén $\varphi(x_i) = \varphi_i(x_i)$. Ez egyértelműen kiterjeszthető egy $\varphi : F(X) \to A$ homomorfizmussá, ami nyilván megfelel a feltételeknek.

8.8.10. Ha $\varphi : X \to Y$ halmazok közötti leképezés, akkor legyen $F(\varphi)$ a φ egyértelmű kiterjesztése $F(X) \to F(Y)$ homomorfizmussá. Ez nyilván tartja a kompozíciót, azaz kovariáns funktor. Megfordítva, ha $\psi : H \to K$ csoporthomomorfizmus, akkor legyen $G(\psi) = \psi$, ami halmazleképezés, és persze G az identikus leképezés lévén szintén tartja a kompozíciót. A $\mathrm{Hom}\big(M, G(K)\big)$ elemei tetszőleges M-ből K alaphalmazába menő függvények. Ezek egyértelműen kiterjeszthetők egy $F(M) \to K$ homomorfizmussá, amelyek pontosan $\mathrm{Hom}\big(F(M), K\big)$ elemei (és persze $\mathrm{Hom}\big(F(M), K\big)$ minden eleme megkapható ily módon).

11.9. Hibajavító kódok

9.1. Alapfogalmak.

9.1.5. Ha u és v összesen t helyen tér el, v és w pedig s helyen, akkor u-ból $s+t$ változtatással w-t tudunk csinálni, ami a háromszög-egyenlőtlenséget bizonyítja. Előfordulhat, hogy ugyanazon a helyen változtatunk kétszer, sőt az is, hogy a második változtatás az elsőt visszacsinálja, és ezért nem mindig áll egyenlőség.

A topológiában *metrikának* egy olyan nemnegatív valós értékű $d(u, v)$ „távolságfüggvényt" neveznek, amelyre a háromszög-egyenlőtlenségen kívül még az is teljesül, hogy $d(u, v) = d(v, u)$, továbbá hogy $d(u, v)$ akkor és csak akkor nulla, ha $u = v$. Ezek a Hamming-távolságra nyilvánvalóan igazak.

9.1.6. Egy u kódszót legfeljebb t helyen megváltoztatva akkor és csak akkor nem kaphatunk egy másik kódszót, ha u-tól mindegyik kódszó t-nél nagyobb távolságra van. Ez minden u-ra pontosan akkor teljesül, ha a kód minimális távolsága t-nél nagyobb.

Ha a kódban vannak olyan $u \neq w$ szavak, amelyek távolsága legfeljebb $2t$, akkor az u betűit ennek a $2t$ helynek a felén w megfelelő betűjére változtatva egy olyan v szót kapunk, amelynek távolsága w-től is legfeljebb t, és így a kód nem t-hibajavító. Megfordítva, ha a kód nem t-hibajavító, vagyis vannak olyan $u \neq w$ kódszavak, melyeket legfeljebb t helyen megváltoztatva ugyanazt a v szót kapjuk, akkor u és w távolsága legfeljebb $2t$ lehet a háromszög-egyenlőtlenség miatt, tehát a kód minimális távolsága legfeljebb $2t$.

9.1.10. Ez a kódolás akármilyen nagy k esetén érzékeli, ha pontosan 1 hiba történt, vagyis a kód minimális távolsága kettő. Ennek oka az, hogy a kódhoz tartozó szavak pontosan azok, amelyekben a betűk összege nulla mod 2, és ha egy helyen a szót megváltoztatjuk, akkor ez az összeg is megváltozik.

Ugyanakkor 1 hibát már nem lehet kijavítani még $k = 1$ esetén sem, mert ha 01 érkezett, akkor az eredeti üzenet 00 és 11 egyaránt lehetett. Érzéketlen a kód a betűk cseréjére is.

9.1.11. Ha az $u_1 \dots u_9$ sorozat ellenőrző jegye u_{10}, akkor

$$\sum_{i=1}^{10} i u_i \equiv u_{10} + 10u_{10} = 11u_{10} \equiv 0 \ (11) \, .$$

Ha az $u_1 \dots u_{10}$ sorozat egyetlen helyen megváltozik, és az eredményt $v_1 \dots v_{10}$ jelöli, akkor $\sum_{i=1}^{10} i v_i$ már biztosan nem lesz 11-gyel osztható. Ha ugyanis a változás az i-edik helyen történik ($1 \leq i \leq 10$), akkor az eredeti $\sum i u_i$ összeget egy iw számmal változtatjuk meg, ahol $1 \leq |w| \leq 10$, és így iw biztosan nem lehet osztható 11-gyel (hiszen 11 prímszám). Ezért ez a kód 1-hibajelző.

Tegyük most föl, hogy a küldés során u_i és u_{i+1} megcserélődik, ahol $1 \leq i \leq 9$. Ekkor a $\sum i u_i$ összeg $\big(iu_i + (i+1)u_{i+1}\big) - \big(iu_{i+1} + (i+1)u_i\big) = u_{i+1} - u_i$-vel változott meg, ami $u_i \neq u_{i+1}$ esetén szintén nem lehet 11-gyel osztható. Ezért a szomszédos jegyek cseréjét is észrevesszük.

9.2. Lineáris kódok.

9.2.4. A G generátormátrix rangja k (hiszen a kód, vagyis a képtér k-dimenziós). Ezért a mátrixnak van k darab lineárisan független sora. Permutáljuk át a sorokat úgy, hogy ezek az első k helyre kerüljenek. Ezáltal a C altér minden vektorának a koordinátái is permutálódnak, de a vektor súlya (és így a kód minimális távolsága) nem változik meg. Nevezzük ezt a kódot D-nek, a kapott mátrixot H-nak.

A H első k sora egy invertálható M mátrixot ad, legyen $K = HM^{-1}$. Ekkor a K mátrix képtere továbbra is D, tehát ugyanazt a kódot kapjuk, de ennek a mátrixnak az első k sora már az egységmátrix, tehát az ezzel való kódolás szisztematikus.

9.2.6. Keressünk egy olyan $B : Q^n \to Q^{n-k}$ lineáris leképezést, melynek magtere C. (Egy ilyet úgy kaphatunk, hogy a C altér $b_1, \dots, b_k$ bázisát kiegészítjük a Q^n egy $b_1, \dots, b_n$ bázisává, és B-t a lineáris leképezések előírhatósági tétele alapján úgy definiáljuk, hogy a $b_1, \dots, b_k$ vektorokat nullába, a $b_{k+1}, \dots, b_n$ vektorokat pedig Q^{n-k} egy bázisába vigye.) Jelölje P a B mátrixát a szokásos bázisban (amelynek elemei az egységmátrix oszlopai). Ekkor $[Bv] = [B][v] = P[v]$, és mivel a szokásos bázist választottuk, a v mátrixa, azaz $[v]$ maga a v oszlopvektor lesz. Így Pv tényleg pontosan akkor nulla, ha v a kódhoz tartozik.

Legyen most $P \in Q^{(n-k)\times n}$ egy tetszőleges mátrix, és $B(v) = Pv$. A P pontosan akkor ellenőrző mátrix, ha B magja C, ami a dimenziótétel miatt azzal ekvivalens, hogy B (és így P) rangja $n-k$, továbbá B magja tartalmazza C-t. Ez utóbbi állítást úgy fogalmazhatjuk át, hogy $PGu = 0$ minden $u \in Q^k$-ra, vagyis hogy $PG = 0$.

Ebből az utolsó állítás is következik: a megadott két mátrixra $PG = 0$ szorzással ellenőrizhető, az pedig világos, hogy P utolsó $n - k$ oszlopa független.

9.2.8. Ha a w vektor első nem nulla komponense az i-edik, akkor a fennmaradó $m-i$ komponens mindegyikét q-féleképpen választhatjuk, tehát ilyen vektorból q^{m-i} van. Ezeket a számokat kell összeadni i lehetséges értékeire, azaz $1 \le i \le m$ esetén. Ekkor pontosan a feladatban szereplő összeget kapjuk.

Érdemes meggondolni a következőt (ami egy második megoldáshoz is elvezet). Vegyük Q^m nem nulla vektorait, és tekintsük rajta a „párhuzamosság” ekvivalencia-relációt (két vektor akkor ekvivalens, ha egymás nem nulla skalárszorosai). Minden osztályban $q - 1$ vektor van (hiszen ennyi nem nulla skalárral szorozhatunk meg egy vektort, hogy egy vele párhuzamos vektort kapjunk). Ezért az osztályok száma $(q^m - 1)/(q - 1)$. Másrészt azonban mindegyik osztályban pontosan egy olyan vektor van, amelynek az első nem nulla komponense 1 (hiszen a vektort eloszthatjuk az első nem nulla komponensével).

9.2.10. Azt kell megmutatni, hogy a Hamming-kód esetében a 9.1.7. Hamming-korlátban egyenlőség áll. Most $t = 1$, tehát ez az egyenlet

$$q^{n-k} = \frac{q^n}{|C|} = \binom{n}{0} + \binom{n}{1}(q-1) = 1 + n(q-1)\,.$$

Mivel a Hamming-kód $k = n-m$-dimenziós, a baloldalon q^m áll, tehát az állítás következik a 9.2.8. Gyakorlatból.

9.2.11. Most $Q = \mathrm{GF}(3)$, tehát $q = 3$, legyen $m = 3$. Ekkor a 9.2.8. Gyakorlat miatt $n = 13$, és így a kód dimenziója $13 - 3 = 10$. Ha Q elemeit 1, 2, X-nek feleltetjük meg, és a hasábokba a kódszavakat írjuk (összesen 3^{10} kódszó van, tehát ennyi hasáb kell), akkor a Hamming-kód perfektsége (9.2.10. Gyakorlat) miatt minden Q^{13}-beli szóhoz (tehát a nyerő tippsorozathoz is) van olyan általunk kitöltött hasáb, amely attól legfeljebb 1 helyen tér el.

9.3. Polinomkódok.

9.3.2. Az $u_1 \dots u_k$ sorozatnak az $u(x) = u_1 x^{k-1} + \dots + u_k$ polinomot akarjuk megfeleltetni. Ezért válasszuk az $x^{k-1}, x^{k-2}, \dots, x, 1$ bázist a k-nál kisebb fokú polinomok vektorterében. Ekkor a fenti $u_1 \dots u_k$ sorozathoz tartozó polinom koordinátavektora ebben a bázisban az az oszlopvektor lesz, amelyben a koordináták felülről lefelé haladva éppen $u_1, \dots, u_k$. Ugyanez elmondható a Q^n vektortérről, és az $x^{n-1}, x^{n-2}, \dots, x, 1$ bázisról.

A kódolás az $A\big(u(x)\big) = g(x)u(x)$ leképezéssel történik. A 9.2.2. Definíció előtti megjegyzések szerint a keresett G generátormátrixot úgy kaphatjuk meg, hogy vesszük ennek a lineáris leképezésnek a mátrixát a fenti bázispárban. Valóban, ekkor az $[A(u)] = [A][u]$ összefüggés miatt a kódszavak halmaza tényleg a $G[u]$ alakú oszlopvektoroknak megfelelő sorozatok halmaza lesz.

A G mátrix oszlopaiba tehát a $g(x)x^i$ polinomok együtthatói kerülnek. Az első oszlopba g együtthatóit írjuk, az oszlop tetején kezdjük, a legmagasabb fokú tagnál kezdve. A második oszlop első eleme nulla, ezután g együtthatói következnek, az első oszlophoz képest eggyel lejjebb csúsztatva. A harmadik oszlopban a harmadik elemnél kezdünk, és így tovább. A kimaradó helyekre nullák kerülnek. Az eredmény a következő:

$$\begin{bmatrix}
a_{n-k} & 0 & 0 & \dots & 0 \\
a_{n-k-1} & a_{n-k} & 0 & \dots & 0 \\
a_{n-k-2} & a_{n-k-1} & a_{n-k} & \dots & 0 \\
\vdots & \vdots & \vdots & & \vdots \\
a_1 & a_2 & a_3 & \dots & a_k \\
a_0 & a_1 & a_2 & \dots & a_{k-1} \\
0 & a_0 & a_1 & \dots & a_{k-2} \\
\vdots & \vdots & \vdots & & \vdots \\
0 & 0 & 0 & \dots & a_0
\end{bmatrix}$$

(n sor van, és k oszlop; az utolsó oszlopban szereplő együtthatókat úgy kell érteni, hogy $a_i = 0$, ha $i > n - k$).

9.3.4. A 9.3.3. Állítás bizonyítása most is működik, hiszen most is olyan determinánst kapunk, amelynek az oszlopai páronként különböző kvóciensű, nem nulla elemű mértani sorozatot alkotnak.

9.3.10. Mivel $\alpha^{2^r-1} = 1$, az α gyöke az $x^{2^r} - x$ polinomnak, és így a GF(2^r) testnek az eleme (6.7.6. Tétel), a rendje miatt pedig generálja e test multiplikatív csoportját. Jelölje m_i az α^i minimálpolinomját $Q = \mathrm{GF}(2)$ fölött. Ennek foka a $Q(\alpha_i)$ dimenziója Q fölött (6.1.17. Következmény). Tehát m_1 foka r, és mindegyik m_i foka legfeljebb r. A négyzetre emelés relatív automorfizmus Q fölött, ezért α^{2i} gyöke m_i-nek, tehát $m_i = m_{2i}$ minden i-re. Amikor tehát a 9.3.6. Definíció alapján kiszámítjuk a g polinomot, akkor elegendő az $m_1, m_3, \ldots, m_{2t-1}$ polinomok legkisebb közös többszörösét venni. Ennek foka így legfeljebb rt, a kód dimenziója pedig $k = n - \mathrm{gr}(g) \geq n - rt$.

Ha $t = 1$, akkor $g = [m_1, m_2] = [m_1, m_1] = m_1$. A Q^r vektortér elemei (mint oszlopvektorok) kölcsönösen egyértelmű, lineáris megfeleltetésben állnak a GF(2^r) test elemeivel. A kételemű test fölött két nem nulla vektor akkor és csak akkor párhuzamos, ha egyenlő. Ezért az $m = r$-hez tartozó Hamming-kód ellenőrző mátrixának oszlopait tekinthetjük a GF(2^r) nem nulla elemeinek is. Ezek pontosan az α elem hatványai, írjuk az oszlopokat az $\alpha^{n-1}, \alpha^{n-2} \ldots, \alpha^2, \alpha, 1 = \alpha^n$ sorrendben. Ekkor a $v_1 \ldots v_n$ szó pontosan akkor van benne ebben a Hamming-kódban, ha $v_1\alpha^{n-1} + \ldots + v_n = 0$, vagyis ha a hozzá tartozó $v(x)$ polinomnak gyöke az α. Ezek a polinomok viszont a $g = m_1$ minimálpolinom többszörösei, vagyis a BCH-kód elemei.

9.4. Ciklikus kódok.

9.4.3. Ha $v(x)$ a C egy $v_1 \ldots v_n$ kódszavához tartozó polinom, akkor

$$xv(x) = x(v_1x^{n-1} + v_2x^{n-2} + \ldots + v_n) = (v_2x^{n-1} + v_3x^{n-2} + \ldots + v_nx + v_1) + v_1(x^n - 1)\,.$$

A C kód ciklikussága miatt $w(x) = v_2x^{n-1} + v_3x^{n-2} + \ldots + v_nx + v_1$ is C-beli kódszóhoz tartozó polinom. Így tetszőleges $f \in Q[x]$-re

$$x\big(v(x) + f(x)(x^n - 1)\big) = w(x) + \big(v_1 + xf(x)\big)(x^n - 1)\,.$$

Ezért a $v(x) + f(x)(x^n - 1)$ alakú polinomok I halmaza (ahol $v(x)$ befutja a C kódszavaihoz tartozó polinomokat, $f \in Q[x]$ pedig tetszőleges), zárt az x-szel való szorzásra. Ez a polinomhalmaz nyilván altér, és így minden polinommal való szorzásra is zárt, vagyis ideál $Q[x]$-ben. A $Q[x]$ főideálgyűrű (5.5.3. Tétel), tehát van olyan $g \in Q[x]$ polinom, hogy I a g összes polinomszorosaiból áll. Mivel $x^n - 1 \in I$, ezért $g(x) \mid x^n - 1$. A kódszavakhoz tartozó polinomok is I-ben vannak, tehát g többszörösei. Megfordítva, ha $g(x)u(x)$ foka n-nél kisebb (és így benne van a g által generált polinomkódban), akkor $g \in I$ miatt

$$g(x)u(x) = v(x) + f(x)(x^n - 1)$$

alkalmas v-re és f-re. Innen átrendezéssel $(x^n - 1) \mid g(x)u(x) - v(x)$, ami a fokszámok miatt csak úgy lehet, hogy $g(x)u(x) = v(x)$. Ezért $g(x)u(x)$ egy C-beli kódszóhoz tartozó polinom.

Az állítást úgy is bizonyíthattuk volna, hogy a $Q[x]/(x^n - 1)$ faktorgyűrű elemeit azonosítjuk Q^n-nel. Ekkor a kódszavak ebben a faktorgyűrűben alkotnak ideált. Ez a számolást kicsit egyszerűsíti, de fogalmilag nehezebbé teszi.

V. rész

Függelék

A. A SZÜKSÉGES ELŐISMERETEK ÖSSZEFOGLALÁSA

A tudomány egész haladása semmi egyéb, mint fokozatos lemondás a világ egyszerűségéről.

Stanisław Lem: *Szénanátha (Murányi Beatrix fordítása)*

A.1. Halmazelmélet és logika

Az alábbi halmazelméleti fogalmak egy része középiskolából ismerős, a többit pedig a szövegben menet közben vezetjük be, amikor egyúttal példákat is mutatunk rájuk. Mégis hasznosnak gondoljuk az alábbi összefoglalót, ahol meg lehet találni a tömör definíciókat. Szót ejtünk néhány olyan szabályról is, amelyek segíthetnek abban, hogy elkerüljük a legtipikusabb, tapasztalatlanságból eredő logikai hibákat.

A halmaz összességet, kollekciót jelent, olyan dolgot, amelynek elemei vannak (mindegyik elem egyszer szerepelhet, és a sorrendjük nem számít). A matematikában a „halmaz" és a „halmaz eleme" alapfogalmak, nem definiáljuk őket (de az összes többi fogalmat ezekre vezethetjük vissza). Azt, hogy h eleme a H halmaznak úgy jelöljük, hogy $h \in H$ (vagy $H \ni h$). A halmazok elemeit kapcsos zárójelek között sorolhatjuk fel, például $\{1, 2, 3\}$ az a halmaz, amelynek elemei 1, 2 és 3,

$$\{x \in \mathbb{Z} : x^2 = 1\}$$

pedig azokat az egész számokat jelöli, amelyek négyzete 1. Itt $\mathbb{Z}$ az egész számok halmaza, a : jel után pedig bármilyen másmilyen feltételt is írhatunk. Ha X véges halmaz, akkor az elemeinek számát $|X|$ fogja jelölni.

Azt mondjuk, hogy B *részhalmaza* A-nak, jelben $B \subseteq A$ (vagy $A \supseteq B$), ha B minden eleme A-nak is eleme. Minden halmaznak részhalmaza önmaga, továbbá a $\emptyset$-val jelölt *üres halmaz*, amelynek egyetlen eleme sincs, ezek a *triviális részhalmazok*. Az X-től különböző részhalmazokat *valódi részhalmaznak* nevezzük.

A halmazok között műveleteket értelmezhetünk. Az A és B halmazok *uniója* azokból az elemekből áll, amelyek A és B valamelyikében benne vannak, jele $A \cup B$. Az A és B halmazok *metszete* azokból az elemekből áll, amelyek mind A-ban, mind B-ben benne

vannak, jele $A \cap B$. Két halmaz *diszjunkt*, ha metszetük az üres halmaz, azaz ha nincs közös elemük.

Az A és B halmazok *különbsége* azokból az elemekből áll, amelyek A-ban benne vannak, de B-ben nincsenek benne, jele $A - B$ (vagy néhány könyvben $A \setminus B$). Ennek speciális esete a komplementum fogalma. Ha A részhalmaza X-nek, akkor A *komplementuma* az $X - A$ halmaz, jele A' (vagy néha $\overline{A}$). Ezt olyankor szokás használni, ha X rögzített, és ennek a részhalmazait vizsgáljuk. Két halmaz *szimmetrikus differenciáján* azoknak az elemeknek a halmazát értjük, amelyek a két halmazból pontosan egyben vannak benne. Az A és B szimmetrikus differenciája tehát $(A - B) \cup (B - A)$.

Az unió műveletének fontos tulajdonsága, hogy *asszociatív*, azaz tetszőleges A, B, és C halmazok esetén

$$(A \cup B) \cup C = A \cup (B \cup C)\,.$$

Valóban, mindkét halmazban azok az elemek vannak benne, amelyek A, B és C valamelyikében benne vannak. Ezt szokás zárójelek nélkül, $A \cup B \cup C$-vel jelölni. Végtelen sok halmaz uniójáról is beszélhetünk, ebben azok az elemek vannak, amelyek a résztvevő halmazok valamelyikének elemei. Ugyanígy asszociatív a metszet művelete is, végtelen sok halmaz metszetét analóg módon definiálhatjuk.

Másik fontos műveleti tulajdonság a *kommutativitás*, ami azt jelenti, hogy

$$A \cup B = B \cup A \quad \text{és} \quad A \cap B = B \cap A\,.$$

tetszőleges A és B halmazokra. Végül tetszőleges A, B és C halmazokra teljesül kétféle *disztributivitás* is:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \quad \text{és} \quad (A \cap B) \cup C = (A \cup C) \cap (B \cup C)\,.$$

További fontos halmazok közötti művelet a *Descartes-szorzat* fogalma. Ha A és B halmazok, és $a \in A$, $b \in B$, akkor az (a, b) *rendezett pár* annyiban különbözik az $\{a, b\}$ halmaztól, hogy (a, b) esetében számít az a és b elemek sorrendje (vagyis $a \neq b$ esetén $(a, b) \neq (b, a)$), és $a = b$ is lehetséges (míg az $\{a, a\}$ halmaz csak egyeleműnek számít). Az összes (a, b) párok halmazát, ahol $a \in A$ és $b \in B$, az A és B halmazok Descartes-szorzatának nevezzük, és $A \times B$-vel jelöljük. Nyilván $A \times B$ elemszáma az A és B elemszámának a szorzata. Ha kettőnél több halmaz adott, például $A_1, \ldots, A_n$, akkor beszélünk az

$$A_1 \times \ldots \times A_n$$

Descartes-szorzatról is, ennek elemei az $(a_1, \ldots, a_n)$ *rendezett n-esek*, ahol $a_i \in A_i$ mindegyik i-re. Ezt a fogalmat végtelen sok tényező esetében is használni fogjuk.

Azt, hogy f az A halmazból a B halmazba vezető függvény, úgy írjuk, hogy $f : A \to B$. Ha $f(a) = b$, akkor alkalmazzuk az $f : a \mapsto b$ jelölést is. Az f függvény *értékkészlete* azoknak a $b \in B$ elemeknek a halmaza, amelyeket f értékként fölvesz, vagyis van olyan $a \in A$, hogy $f(a) = b$. Az $f : A \to B$ *szürjektív*, ha értékkészlete az egész B. Az f *injektív*, ha A különböző elemeihez B különböző elemeit rendeli, vagyis $a_1 \neq a_2$ esetén

$f(a_1) \neq f(a_2)$. Az injektív függvényeket (különösen algebrai struktúrák között a művelettartókat) szokás *beágyazásnak* is hívni. Az $f : A \to B$ *bijektív* vagy *kölcsönösen egyértelmű* ha injektív is és szürjektív is.

Ha H véges halmaz, akkor minden $f : X \to X$ leképezésre f akkor és csak akkor szürjektív, ha injektív. Ha viszont H végtelen, akkor létezik olyan $f : H \to H$ leképezés, ami injektív, de nem szürjektív, és olyan is, ami szürjektív, de nem injektív.

Két véges halmaz nyilván akkor és csak akkor egyenlő elemszámú, ha van közöttük kölcsönösen egyértelmű megfeleltetés. Ezt a definíciót végtelen halmazokra is ki szokás terjeszteni, ilyenkor nem elemszámról, hanem *számosságról* beszélünk. *Megszámlálhatóan végtelennek* nevezzük azokat a halmazokat, amelyek kölcsönösen egyértelmű megfeleltetésben állnak a pozitív egész számok halmazával. Meg lehet mutatni, hogy az összes egész számok, sőt az összes racionális számok halmaza is megszámlálhatóan végtelen, de a valós számoké már nem az. Az X halmaz számosságát $|X|$ fogja jelölni.

Az X halmaz *identikus leképezése* az az id_X függvény, amely X mindegyik eleméhez önmagát rendeli. Ha $f : A \to B$ és $g : B \to A$, akkor f és g egymás *inverzei*, ha mindegyik „visszacsinálja", amit a másik elvégez, azaz ha $f\big(g(b)\big) = b$ minden $b \in B$-re, és $g\big(f(a)\big) = a$ minden $a \in A$-ra. Az f függvénynek akkor és csak akkor van inverze, ha bijekció. A függvények között a legfontosabb művelet a kompozíció (lásd 2.2.3. Definíció), amely szintén asszociatív (2.2.4. Gyakorlat).

Egy X halmazon *relációt* értelmezünk, ha bármely két eleméről megmondjuk, hogy relációban állnak-e. Ilyen például az oszthatóság vagy a $\leq$ az egész számok halmazán. Formailag egy reláció az $X \times X$ egy részhalmaza. Azt, hogy x és y az R relációban áll, $x\ R\ y$ vagy $(x, y) \in R$ jelöli. Az R reláció

(1) *reflexív*, ha $x\ R\ x$ minden $x \in X$-re;
(2) *szimmetrikus*, ha $x\ R\ y$-ból következik, hogy $y\ R\ x$ minden $x, y \in X$-re;
(3) *tranzitív*, ha $x\ R\ y$-ből és $y\ R\ z$-ből $x\ R\ z$ következik bármely $x, y, z \in X$ esetén.

Ha mind a három tulajdonság teljesül, akkor R *ekvivalencia-reláció*. Ezek az X halmaz *partícióival* (vagyis páronként diszjunkt halmazokra való felosztásaival) állnak kölcsönösen egyértelmű megfeleltetésben (lásd 4.4.6. Tétel).

A halmazelmélet nevezetes tétele Zorn lemmája, amit algebrában is, analízisben is sokat használnak. Mi bizonyítás nélkül idézzük. Tegyük fel, hogy X egy halmaz, és legyen $\mathcal{L}$ egy halmazrendszer az X halmazon (ez azt jelenti, hogy $\mathcal{L}$ elemei az X bizonyos részhalmazai).

A.1.1. Definíció. Egy $\mathcal{L}$ halmazrendszert *láncnak* hívunk, ha bármely két L_1 és L_2 elemére $L_1 \subseteq L_2$ vagy $L_2 \subseteq L_1$.

Az Olvasót megkérjük, hogy az állítás elolvasása előtt ismételje át a maximális elem fogalmát (4.4.23. Definíció).

A.1.2. Tétel [Zorn-lemma]. *Legyen $\mathcal{X}$ az X halmaz részhalmazaiból álló halmazrendszer, amely rendelkezik a következő tulajdonsággal: bárhogyan is választjuk ki $\mathcal{X}$ egy olyan nem üres $\mathcal{L}$ részrendszerét, amelyik lánc, az $\mathcal{L}$ elemeinek uniója is eleme az $\mathcal{X}$ halmazrendszernek. Ekkor az $\mathcal{X}$-nek van maximális eleme.*

Például a Zorn-lemma segítségével mutatható meg, hogy minden vektortérben van bázis. Ebben a bizonyításban $\mathcal{X}$ a lineárisan független halmazokból álló halmazrendszer.

Az emberiség az 1900-as évek elején jött rá arra, hogy a halmaz naív fogalmával probléma van, ellentmondásra, paradoxonokra vezet. Egy példa a következő. Ha bármit betehetünk egy halmazba, akkor speciálisan beszélhetünk az összes halmazok halmazáról is. Ez persze halmaz, tehát eleme önmagának. Már ez önmagában is problematikusnak látszik. Konkrétan ellentmondásra is lehet jutni, ha az összes olyan halmazok H halmazát tekintjük, amelyek nem elemei önmaguknak (próbálja meg az Olvasó: abból is ellentmondást kap, ha H eleme önmagának, és abból is, ha H nem eleme önmagának).

A kiutat az jelenti, hogy a most kapott „ellentmondást" a következőképpen fogjuk föl: beláttuk, hogy azok a halmazok, amelyek nem elemei önmaguknak, nem alkotnak halmazt! Tehát nem minden összességet, kollekciót tekintünk halmaznak (például a túl „nagyokat" nem). Pontos axiómákkal lehet szabályozni, hogy mik is a halmazok, ilyen például a *Zermelo-Fraenkel-féle* axiómarendszer, amelyből az egész matematika felépíthető. Ezek az axiómák megengedik a matematikában megszokott halmazokat (halmazok uniója is halmaz, egy halmaz összes részhalmaza is halmazt alkot, és így tovább).

Ugyanakkor vannak helyzetek, amikor a nagyon nagy „nem-halmazokról" mégiscsak beszélni szeretnénk. Például szeretnénk tételeket kimondani, amelyek minden halmazra érvényesek (vagy minden vektortérben igazak). Az ilyen esetekben nem halmazról, hanem *osztályról*, például az összes halmazok osztályáról beszélünk. Az osztály pontosan definiált fogalom, amelyből nem kapunk ellentmondást a fenti értelemben (feltéve, hogy maga a halmazelmélet is ellentmondásmentes). Egy algebrai struktúra (például egy csoport) alaphalmaza csakis halmaz lehet, osztály nem.

Kurt Gödel szenzációs tétele, hogy a halmazelmélet (vagy a számelmélet) ellentmondásmentességét nem lehet bebizonyítani. Általában belátta, hogy minden valamirevaló axiómarendszerben van *megoldhatatlan* probléma, amit se bizonyítani, se megcáfolni nem lehet. Ezek a (logikához tartozó) tételek a huszadik század talán legfontosabb eredményei, mert nem valamiféle technikai problémáról, hanem magáról az emberi gondolkodásról, annak a határairól szólnak.

A halmazelméletből szükséges tudnivalók ismertetése után a matematikai logikára térünk. A mindennapi beszédben is használunk logikai műveleteket. Jelölje A azt a mondatot, hogy „esik az eső", B pedig azt, hogy „felhős az ég". Ekkor azt a mondatot, hogy „esik az eső és felhős az ég" így rövidíthetjük: „A és B". Hasonlóan értjük azt is, hogy „A vagy B", vagy azt, hogy „nem A" (ez tehát azt rövidíti, hogy „nem esik az eső"). Ez utóbbit $\neg A$-nak írjuk.

Az „A és B" jelentése egyértelmű: ez akkor igaz, ha A is és B is igaz. A „vagy" műveletet azonban sokféle értelemben használjuk a köznapi életben. Gondoljunk csak az

alábbi mondatokra:

„Ez a villamos átmegy a Petőfi-hídon, vagy a Margit-hídon."

„Vagy fagyit kapsz, vagy perecet."

„Vagy eszel, vagy olvasol."

Ezek egészen másképp kapcsolják össze a két részállítást. Az első igaz, ha a villamos akármelyik hídon is átmegy, de akkor is igaz, ha mindkettőn átmegy. A második állítás kizárja azt, hogy a gyerek fagyit és perecet is kapjon, de az egyiket biztosan megkapja. Tehát ez az összetett állítás akkor igaz, ha a két részállítás közül pontosan az egyik teljesül. A harmadik állítás is kizárja, hogy a két részállítás egyszerre teljesüljön, de megengedi, hogy egyik se legyen igaz (hiszen nem muszáj minden pillanatban vagy enni, vagy olvasni, az állítás azt kívánja csak, hogy egyszerre ne történjen a kettő).

A matematikában zavart keltene, ha nem tudnánk pontosan, hogy a „vagy" szót melyik értelemben használjuk. Ezért megállapodunk abban, hogy a „vagy" mindig a fenti legelső, megengedő értelemben szerepel. Tehát az „A vagy B" csak akkor hamis, ha A is és B is hamis, különben igaz.

Az első fontos tudnivaló a tagadás szabályaira vonatkozik. Ha C azt jelenti, hogy „ez a gyerek lány", D pedig azt, hogy „ez a gyerek szőke", akkor az, hogy

„nem igaz, hogy ez a gyerek lány és szőke"

így rövidíthető: „$\neg(C$ és $D)$". Ez ***nem azt jelenti,*** hogy „ez a gyerek nem lány ***és*** nem szőke", hanem azt, hogy „ez a gyerek nem lány ***vagy*** nem szőke". Gondoljunk csak bele: a fent kiemelt mondat a szőke fiúkra és a barna lányokra is teljesül. Ugyanígy a

„nem igaz, hogy ez a gyerek lány vagy szőke"

azt jelenti, hogy „ez a gyerek nem lány és nem szőke", és nem azt, hogy „ez a gyerek nem lány vagy nem szőke". Ezt az észrevételt általánosítják De Morgan szabályai:

„C és D" tagadása „$\neg C$ vagy $\neg D$",

„C vagy D" tagadása „$\neg C$ és $\neg D$".

Nagyon fontos a „ha A, akkor B" típusú mondat is, annyira, hogy erre is bevezetünk jelölést: $A \implies B$-vel fogjuk rövidíteni (ezt a műveletet *implikációnak* hívják). Az $A \implies B$ akkor hamis, ha A igaz, de B mégis hamis. Erről ismét példamondatokkal győzhetjük meg magunkat. Legyen A az az állítás, hogy az n szám hattal osztható, B pedig az, hogy n páros. Az $A \implies B$ következtetés ekkor azt mondja, hogy „ha egy szám hattal osztható, akkor páros". Ezt igaznak érezzük, hiszen ha egy számból 6-ot ki tudunk emelni, akkor 2-t is. Ha $n = 6$, akkor A és B is igaz. Ha $n = 2$, akkor A nem igaz, de B igaz. Ha $n = 7$, akkor sem A, sem B nem igaz, de ez még mindig nem rontja el a következtetést. Csak akkor lenne baj, ha találnánk egy 6-tal osztható páratlan számot, tehát amire A igaz, de B mégis hamis.

Hamis állításból tehát minden következik! Ha $0 = 1$, akkor minden ember örökké él. Ugyanígy az üres halmazban található minden szám egyszerre páros és páratlan; az üres halmazban található mindegyik háromszög szabályos és derékszögű is.

Az Olvasónak érdemes meggondolnia, hogy az $A \implies B$ ugyanazt jelenti, mint hogy „nem A, vagy B”. Ismét egy példamondattal érvelve: „ha elmész, megharagszom” ugyanazt jelenti, mint hogy „nem mész el, vagy megharagszom”. Azt, hogy $A \implies B$, szokás úgy is mondani, hogy *A elégséges feltétele B*-nek, vagy hogy *B szükséges feltétele A*-nak.

Egy implikációt nem lehet büntetlenül megfordítani! Abból, hogy $A \implies B$, általában nem következik, hogy $B \implies A$. A fenti példát folytatva: nem igaz, hogy minden páros szám hattal osztható, hiszen például az $n = 2$ ellenpélda. Ugyanakkor érvényes a következő szabály:

$$\text{Ha } A \implies B \text{ igaz, akkor } \neg B \implies \neg A \text{ is igaz.}$$

Például igaz az, hogy „ha egy szám páratlan, akkor nem osztható hattal”. Másképp fogalmazva: ha egy implikációt meg akarunk fordítani, akkor mindkét tagját tagadnunk kell. Ezt a *kontrapozíció* szabályának nevezzük.

Ha $A \implies B$ és $B \implies A$ is teljesül, akkor ezt úgy jelöljük, hogy $A \iff B$, és azt mondjuk, hogy *A ekvivalens B*-vel. Ezt úgy szokás fogalmazni, hogy „A akkor és csak akkor, ha B”, vagy rövidebben „A pontosan akkor, ha B”.

Sokszor hallunk ilyesfajta mondatokat is: „az osztályban van barna gyerek”, vagy „mindegyik fa beteg”. Ezeket a $\exists$ („létezik”) és $\forall$ („minden”) jelek segítségével rövidíthetjük. Például

$$(\forall x)(\exists y)(x < y)$$

így fordítható le: „minden számnál van nagyobb szám”. E két jelet *kvantoroknak* hívjuk, az első az egzisztenciális, a második az univerzális kvantor.

Az „és” és a „vagy” műveletekhez hasonlóan a kvantorokat tartalmazó állítások tagadása is külön figyelmet érdemel. A szabály is hasonló: ahogy az „és” és a „vagy” jelek kicserélődnek, ugyanúgy a kvantorokat is meg kell cserélni, amikor a „nem” műveletet átvisszük rajtuk. Például annak az állításnak, hogy „mindegyik fa beteg”, a tagadása az, hogy „van olyan fa, amelyik nem beteg”. Ugyanígy annak, hogy „az osztályban van barna gyerek”, a tagadása az, hogy „az osztályban mindegyik gyerek nem barna”, vagy köznapibban „az osztályban egyik gyerek sem barna”. Általában a szabály a következő:

$$\text{„}(\forall x)F(x)\text{” tagadása „}(\exists x)\neg F(x)\text{”},$$
$$\text{„}(\exists x)F(x)\text{” tagadása „}(\forall x)\neg F(x)\text{”}.$$

Érdemes még megemlíteni kétféle bizonyítási módszert. Ha azt akarjuk bebizonyítani, hogy $A \implies B$, akkor a kontrapozíció szabálya szerint elég azt megmutatni, hogy $\neg B$-ből következik $\neg A$, vagy másképpen: ha feltesszük, hogy A és $\neg B$ is igaz, akkor ellentmondást kapunk. Vagyis feltesszük a bizonyítandó állítás tagadását, és ellentmondásra jutunk. Ezt *indirekt bizonyításnak* nevezzük, a könyvben rengeteg példát találunk ilyenre.

A másik bizonyítási módszer a teljes indukció. Ha egy állítást minden pozitív egész n számra be akarunk látni, akkor elég megmutatni $n = 1$ esetén, továbbá annak feltételezésével, hogy $n - 1$-re igaz, megmutatni n-re is. Praktikusan: az állítás n-re való megmutatásához felhasználhatjuk, hogy igaz $n - 1$-re.

Ez valójában az indirekt bizonyítás egy formája, mert a következőképpen is fogalmazhatjuk. Tegyük, fel, hogy az állítás nem igaz. Legyen n a legkisebb olyan szám, amire az állítás hamis. Ez azt jelenti, hogy az összes n-nél kisebb számra már igaz. Tehát valójában nemcsak $n - 1$-re, hanem az összes n-nél kisebb számra feltehetjük, hogy az állítás igaz, miközben n-re próbáljuk igazolni azt.

A.2. Kombinatorika

A.2.1. Tétel. *Ha van n tárgyunk, akkor ezeket*

$$n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n = \prod_{i=1}^{n} i$$

különböző módon tudjuk sorba rakni. Az itt szereplő $n!$ szám neve: n faktoriális. *Megállapodás szerint $0! = 1$ (lásd a 2.2.43. Gyakorlatot).*

A.2.2. Tétel. *Ha van n tárgyunk, és ebből k darabot akarunk kiválasztani (a sorrendre való tekintet nélkül), akkor ezt*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{k!}$$

különböző módon tehetjük meg. Az itt szereplő kifejezés az „n alatt a k” binomiális együttható. *Megállapodás szerint ennek értéke nulla, ha $k > n$, vagy ha $k < 0$.*

A.2.3. Állítás. *Egy n elemű halmazból egy k elemű halmazba képző függvények száma n^k.*

A.2.4. Tétel. *Egy n elemű halmaz összes részhalmazainak száma 2^n. Ha $n \geq 1$, akkor a páros- illetve páratlan elemszámú részhalmazok száma egyaránt 2^{n-1} (lásd az 1.5.22. Feladat megoldását).*

Használni fogjuk az alábbi két gráfelméleti tételt is. A gráfokkal kapcsolatos elemi fogalmakat ismertnek tételezzük fel (ezek csak kevés helyen jönnek az anyagban elő).

A.2.5. Tétel. *Egy n csúcsú összefüggő gráfnak legalább $n - 1$ éle van, és pontosan akkor van ennyi, ha a gráf fa, vagyis nincsen benne kör.*

A.2.6. Definíció. A $G = (A, B, E)$ *páros gráf*, ha a csúcshalmaza a diszjunkt A és B halmazok uniója, és sem A-n, sem B-n belül nem megy él.

Az előbbi jelölésben E az élek halmazát szokta jelenteni. Könnyű belátni, hogy egy gráf akkor és csak akkor páros, ha minden köre páros hosszúságú. Az alábbi jóval nehezebb, de igen hasznos tétel.

A.2.7. Tétel [König–Hall–Ore-tétel]. *Legyen G páros gráf. Pontosan akkor léteznek olyan diszjunkt élek, amelyek az A minden elemét lefedik, ha tetszőleges $X \subseteq A$ esetén az X-beli pontok B-beli szomszédainak száma legalább annyi, mint az X elemszáma.*

A.3. Analízis

A.3.1. Tétel. *Ha f valós együtthatós polinom, akkor a hozzá tartozó $f^* : \mathbb{R} \to \mathbb{R}$ polinomfüggvény folytonos.*

A.3.2. Tétel [Bolzano tétele]. *Legyen f folytonos függvény az $[a, b]$ zárt intervallumon. Ha $f(a) < 0$ és $f(b) > 0$, akkor van olyan $a < c < b$, melyre $f(c) = 0$.*

A.3.3. Lemma. *Legyen f valós együtthatós polinom, melynek főegyütthatója pozitív. Ekkor van olyan c valós szám, hogy $x > c$ esetén $f(x) > 0$ (azaz „elég nagy" x értékekre $f(x)$ már pozitív lesz).*

Bizonyítás. Legyen $f(x) = a_0 + \ldots + a_n x^n$, ahol $a_n > 0$. A háromszög-egyenlőtlenséget (1.4.2. Tétel) felhasználva $x \geq 1$ esetén

$$|a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}| \leq \big(|a_0| + \ldots + |a_{n-1}|\big) x^{n-1} .$$

Ez kisebb, mint $a_n x^n$, ha még

$$x > \big(|a_0| + \ldots + |a_{n-1}|\big)/a_n$$

is teljesül. Ezért az ilyen x-ekre $f(x) > 0$. □

Az alábbi tételt érdemes összevetni a 3.3.8. Tétellel, és az azt követő megjegyzésekkel.

A.3.4. Tétel. *Páratlan fokú valós együtthatós polinomnak van valós gyöke.*

Az algebra alaptételétől független bizonyítás. Mivel f-nek és $-f$-nek ugyanazok a gyökei, feltehetjük, hogy f főegyütthatója pozitív. Az előző lemma szerint f felvesz pozitív értéket. Most tekintsük a $-f(-x)$ polinomot. Mivel f páratlan fokú, ennek a főegyütthatója szintén pozitív. Az előző lemma szerint van olyan d valós szám, hogy $-x > d$ esetén $-f(-x) > 0$. Vagyis x helyébe $-x$-et írva $x < -d$ esetén $f(x) < 0$. Beláttuk tehát, hogy f pozitív és negatív értéket is felvesz, és így Bolzano tétele miatt van valós gyöke. □

A.4. Számelmélet

Az alábbiakban emlékeztetünk néhány olyan számelméleti definícióra és tételre, amelyet a könyvünkben felhasználunk. Általános hivatkozásként Freud Róbert és Gyarmati Edit [**11**] könyvét ajánljuk. Elsőként az Euler-függvénnyel kapcsolatos tudnivalókat foglaljuk össze.

A.4.1. Definíció. Ha n pozitív egész, akkor a $\varphi(n)$ *Euler-függvény* a $0, 1, \ldots, n-1$ számok közül az n-hez relatív prímek száma.

Természetesen ha a $0, 1, \ldots, n-1$ helyett az $1, 2, \ldots, n$ számok között (vagy bármely más teljes maradékrendszerben) számoljuk meg az n-hez relatív prím számokat, akkor ugyanazt az eredményt kapjuk.

A.4.2. Tétel. *Az Euler-függvény multiplikatív, azaz ha n és m relatív prím pozitív egészek, akkor $\varphi(nm) = \varphi(n)\varphi(m)$. Innen következik, hogy ha n kanonikus alakja $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, ahol egyik α_i kitevő sem nulla, akkor*

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \ldots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right).$$

Elemi számelméleti okoskodásokkal adódik a fenti képletből az alábbi két állítás, amit a könyvben felhasználunk.

A.4.3. Állítás. *Legyen n pozitív egész.*

(1) *A $\varphi(n)$ értéke akkor és csak akkor 1, ha $n = 1$ vagy $n = 2$.*
(2) *A $\varphi(n)$ értéke akkor és csak akkor páratlan, ha $n = 1$ vagy $n = 2$.*

Azt, hogy az Euler-függvény multiplikatív, most be fogjuk bizonyítani, mert a bizonyításból egy olyan összefüggés adódik, amire szükségünk lesz. Ehhez emlékeztetjük az Olvasót néhány definícióra. A 2.2. Szakaszban láttuk, hogy amikor a $0, 1, \ldots, n-1$ számokkal modulo n végezzük a műveleteket, akkor egy $\mathbb{Z}_n$ egységelemes gyűrűt kapunk, amelynek az invertálható elemei pontosan azok a $0 \leq i < n$ számok, amelyek n-hez relatív prímek. Ezeknek a halmazát $\mathbb{Z}_n^\times$-tel jelöltük. Vagyis $\mathbb{Z}_n^\times$ elemszáma pontosan $\varphi(n)$. A $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ az olyan (a, b) rendezett párok halmazát jelöli, amelyekre $a \in \mathbb{Z}_n^\times$ és $b \in \mathbb{Z}_m^\times$. Ennek a halmaznak az elemszáma tehát $\varphi(n)\varphi(m)$.

A.4.4. Tétel. *Tegyük fel, hogy n és m relatív prím pozitív egészek. Ekkor létezik olyan $g : \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \to \mathbb{Z}_{nm}^\times$ kölcsönösen egyértelmű megfeleltetés, hogy tetszőleges $a, a' \in \mathbb{Z}_n$ és $b, b' \in \mathbb{Z}_m$ esetén*

$$g(a *_n a', b *_m b') = g(a, b) *_{mn} g(a', b').$$

(ebben a képletben $*_n$ a modulo n szorzás műveletét jelöli, lásd 1.1.4. Definíció). Speciálisan $\varphi(nm) = \varphi(n)\varphi(m)$.

Bizonyítás. Kényelmesebb a g megfeleltetés f inverzét megkonstruálni. Ha $c \in \mathbb{Z}_{nm}^\times$, akkor vegyük a c szám n-nel való osztási maradékát, ezt jelölje a. Hasonlóképpen legyen b a c szám m-mel való osztási maradéka, és $f(c) = (a, b)$.

A definíció szerint $0 \leq a < n$. Megmutatjuk, hogy a és n relatív prímek. Valóban, ha volna egy $d > 1$ közös osztójuk, akkor $a \equiv c\ (n)$ miatt d osztaná c-t is, ami lehetetlen, mert c és nm relatív prímek. Ezért $a \in \mathbb{Z}_n^\times$. Ugyanígy adódik, hogy $b \in \mathbb{Z}_m^\times$. Az f tehát a $\mathbb{Z}_{nm}^\times$ halmazt a $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ halmazba képzi. Ahhoz, hogy belássuk, hogy bijektív, meg kell mutatnunk, hogy f szürjektív és injektív.

Legyen $(a, b) \in \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$, és tekintsük az

$$\left.\begin{aligned} x &\equiv a\ (n) \\ x &\equiv b\ (m) \end{aligned}\right\}$$

szimultán kongruenciarendszert. Ennek a kínai maradéktétel szerint van megoldása, és ez egyértelmű modulo nm. Ezért pontosan egy olyan c megoldás van, amelyre $0 \leq c < nm$. Belátjuk, hogy $c \in \mathbb{Z}_{nm}^{\times}$, azaz hogy $(c, nm) = 1$. Tegyük fel ennek ellenkezőjét. Ekkor van olyan q prím, melyre $q \mid c$ és $q \mid nm$. Ezért vagy $q \mid n$, vagy $q \mid m$. Az első esetben $c \equiv a\ (n)$ miatt $q \mid a$ is teljesül, azaz q közös osztója a-nak és n-nek. Ez lehetetlen, mert $a \in \mathbb{Z}_n^{\times}$, azaz $(a, n) = 1$. A második esetben, amikor $q \mid m$, a $(b, m) = 1$ feltétellel kerülünk ellentmondásba. Tehát tényleg $c \in \mathbb{Z}_{nm}^{\times}$. A maradékos osztás egyértelműsége miatt $f(c) = (a, b)$. Tehát f tényleg szürjektív.

Az, hogy f injektív, a kínai maradéktétel egyértelműségi állításából következik. Ha ugyanis $f(c) = f(c') = (a, b)$, akkor c is és c' is megoldása a fenti szimultán kongruenciarendszernek. Tehát $c \equiv c'\ (nm)$. Mivel $0 \leq c, c' < nm$, ezért $c = c'$. Tehát f bijektív, és ezzel φ multiplikativitását beláttuk.

Definiáljuk a g függvényt az f inverzének. Ha tehát $g(a, b) = c$ és $g(a', b') = c'$, akkor $f(c) = (a, b)$ és $f(c') = (a', b')$. Szeretnénk kiszámítani $f(c *_{nm} c')$ értékét, azaz a $c *_{nm} c'$ szám maradékát modulo n és modulo m. A modulo nm szorzás definíciója az, hogy az egész számok között kiszámított szorzatot még redukálni kell modulo nm. Így viszont $c *_{nm} c' \equiv cc'\ (n)$ is teljesül, tehát elegendő a cc' maradékát kiszámolni. Tudjuk, hogy $c \equiv a\ (n)$ és $c' \equiv a'\ (n)$, ezért $cc' \equiv aa\ (n)$. Így cc' maradéka ugyanaz, mint aa' maradéka, azaz $a *_n a'$. Hasonló számolással kapjuk, hogy $c *_{nm} c'$ mod m vett maradéka $b *_m b'$. Tehát $f(c *_{nm} c') = (a *_n a', b *_m b')$. Másképp fogalmazva $g(a *_n a', b *_m b') = c *_{nm} c'$, és ezzel az állítást beláttuk. □

A.4.5. Definíció. A $\mu(m)$ *Möbius-függvényt* a következőképpen definiáljuk: ha az m pozitív egész szám s darab különböző prím szorzata, akkor $\mu(m) = (-1)^s$, egyébként pedig $\mu(m) = 0$.

Természetesen $\mu(1) = (-1)^0 = 1$, hiszen az 1 nulla darab prím szorzata (üres szorzat). A Möbius-függvény egy fontos tulajdonságát fogalmazza meg a következő állítás.

A.4.6. Állítás. *Tetszőleges m pozitív egészre*

$$\sum_{d \mid m} \mu(d) = \begin{cases} 1 & \text{ha } m = 1, \\ 0 & \text{ha } m \neq 1. \end{cases}$$

Bizonyítás. Az állítás $m = 1$ esetén nyilvánvaló. Tegyük fel, hogy $m > 1$, és legyenek $p_1, \ldots, p_s$ az m szám különböző prímosztói. A $\mu(d)$ értéke 0, kivéve ha d különböző prímek szorzata, azaz $p_1 \cdot \ldots \cdot p_s$ egy rész-szorzata. Ha páratlan sok prímet szorzunk össze, akkor $\mu(d) = -1$, ha páros sokat, akkor $\mu(d) = 1$. Vagyis a fenti összeg értéke akkor lesz nulla, ha a $\{p_1, \ldots, p_s\}$ halmaznak ugyanannyi páratlan elemű részhalmaza van, mint páros elemű. Ez $s \geq 1$ (vagyis $m > 1$) esetén igaz a A.2.4. Tétel miatt. □

A.5. Lineáris algebra

Általában Freud Róbert [**10**] könyvének terminológiáját követjük, azonban a vektorokat egyszerűen kisbetűkkel, a mátrixokat és a lineáris leképezéseket pedig nagybetűkkel jelöljük: u, M, A. Az $m \times m$-es egységmátrix jele E_m. Az alábbi tételeket azért idézzük, mert ezeket a könyvünk harmadik fejezetében alkalmazzuk, ahol lineáris algebrai ismereteket még nem tételezünk föl.

A.5.1. Definíció. *Vandermonde-determinánsnak* nevezzük az alábbi determinánst:

$$V(z_1, \ldots, z_n) = \begin{vmatrix} z_1^{n-1} & \ldots & z_n^{n-1} \\ \vdots & \ldots & \vdots \\ z_1 & \ldots & z_n \\ 1 & \ldots & 1 \end{vmatrix},$$

továbbá az ebből transzponálással, valamint a sorok (oszlopok) sorrendjének megfordításával kapható determinánsokat is.

A.5.2. Tétel. *A fenti Vandermonde-determináns értéke*

$$\prod_{1 \le i < j \le n} (z_i - z_j)\,.$$

A.5.3. Tétel [A determinánsok szorzástétele]. *Legyen T test, és M, N a T fölötti $n \times n$-es mátrixok. Ekkor*

$$\det(MN) = \det(M)\det(N)\,.$$

Egy M (négyzetes) mátrix akkor és csak akkor invertálható, ha determinánsa nem nulla. Ha M és N négyzetes mátrixok, és MN az egységmátrix, akkor M és N egymás kétoldali inverzei, vagyis NM is az egységmátrix.

A.5.4. Tétel. *Ha T test, $M \in T^{m\times m}$, $N \in T^{n\times n}$, $X \in T^{n\times m}$, O az $m \times n$-es nullmátrix, akkor*

$$\det \begin{bmatrix} M & O \\ X & N \end{bmatrix} = \det(M)\det(N)\,.$$

A transzponált determinánsra vonatkozó tétel miatt az állítás akkor is igaz, ha a nullák nem a jobb fölső, hanem a bal alsó sarokban vannak.

Ezt az állítást a legegyszerűbb m szerinti indukcióval, az első sor szerinti kifejtéssel igazolni. Következik azonban a determináns Laplace-féle kifejtéséből is.

B. PÉLDÁK, TÁBLÁZATOK

B.1. A körosztási polinomok

A 3.9. Szakasz feladataiban a Φ_n körosztási polinom kiszámítását visszavezettük arra az esetre, amikor $n > 1$ páratlan, négyzetmentes, nem prím egész szám. Most az ilyen indexű körosztási polinomokat soroljuk fel, $n \leq 105$-ig bezárólag.

$$\Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

$$\Phi_{21} = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{33} = x^{20} - x^{19} + x^{17} - x^{16} + x^{14} - x^{13} + x^{11} - x^{10} + x^9 - x^7 + x^6 - x^4 + \\ + x^3 - x + 1$$

$$\Phi_{35} = x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - x^{11} + \\ + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1$$

$$\Phi_{39} = x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - x^{17} + x^{15} - x^{14} + x^{12} - x^{10} + \\ + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{51} = x^{32} - x^{31} + x^{29} - x^{28} + x^{26} - x^{25} + x^{23} - x^{22} + x^{20} - x^{19} + x^{17} - x^{16} + x^{15} - \\ - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{55} = x^{40} - x^{39} + x^{35} - x^{34} + x^{30} - x^{28} + x^{25} - x^{23} + x^{20} - x^{17} + \\ + x^{15} - x^{12} + x^{10} - x^6 + x^5 - x + 1$$

$$\Phi_{57} = x^{36} - x^{35} + x^{33} - x^{32} + x^{30} - x^{29} + x^{27} - x^{26} + x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - \\ - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{65} = x^{48} - x^{47} + x^{43} - x^{42} + x^{38} - x^{37} + x^{35} - x^{34} + x^{33} - x^{32} + x^{30} - x^{29} + x^{28} - \\ - x^{27} + x^{25} - x^{24} + x^{23} - x^{21} + x^{20} - x^{19} + x^{18} - x^{16} + x^{15} - x^{14} + x^{13} - \\ - x^{11} + x^{10} - x^6 + x^5 - x + 1$$

$$\Phi_{69} = x^{44} - x^{43} + x^{41} - x^{40} + x^{38} - x^{37} + x^{35} - x^{34} + x^{32} - x^{31} + x^{29} - x^{28} + \\ + x^{26} - x^{25} + x^{23} - x^{22} + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + \\ + x^{9} - x^{7} + x^{6} - x^{4} + x^{3} - x + 1$$

$$\Phi_{77} = x^{60} - x^{59} + x^{53} - x^{52} + x^{49} - x^{48} + x^{46} - x^{45} + x^{42} - x^{41} + x^{39} - x^{37} + \\ + x^{35} - x^{34} + x^{32} - x^{30} + x^{28} - x^{26} + x^{25} - x^{23} + x^{21} - x^{19} + x^{18} - x^{15} + \\ + x^{14} - x^{12} + x^{11} - x^{8} + x^{7} - x + 1$$

$$\Phi_{85} = x^{64} - x^{63} + x^{59} - x^{58} + x^{54} - x^{53} + x^{49} - x^{48} + x^{47} - x^{46} + x^{44} - x^{43} + \\ + x^{42} - x^{41} + x^{39} - x^{38} + x^{37} - x^{36} + x^{34} - x^{33} + x^{32} - x^{31} + x^{30} - x^{28} + \\ + x^{27} - x^{26} + x^{25} - x^{23} + x^{22} - x^{21} + x^{20} - x^{18} + x^{17} - x^{16} + x^{15} - \\ - x^{11} + x^{10} - x^{6} + x^{5} - x + 1$$

$$\Phi_{87} = x^{56} - x^{55} + x^{53} - x^{52} + x^{50} - x^{49} + x^{47} - x^{46} + x^{44} - x^{43} + x^{41} - x^{40} + \\ + x^{38} - x^{37} + x^{35} - x^{34} + x^{32} - x^{31} + x^{29} - x^{28} + x^{27} - x^{25} + x^{24} - x^{22} + \\ + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^{9} - x^{7} + x^{6} - x^{4} + \\ + x^{3} - x + 1$$

$$\Phi_{91} = x^{72} - x^{71} + x^{65} - x^{64} + x^{59} - x^{57} + x^{52} - x^{50} + x^{46} - x^{43} + x^{39} - x^{36} + \\ + x^{33} - x^{29} + x^{26} - x^{22} + x^{20} - x^{15} + x^{13} - x^{8} + x^{7} - x + 1$$

$$\Phi_{93} = x^{60} - x^{59} + x^{57} - x^{56} + x^{54} - x^{53} + x^{51} - x^{50} + x^{48} - x^{47} + x^{45} - x^{44} + \\ + x^{42} - x^{41} + x^{39} - x^{38} + x^{36} - x^{35} + x^{33} - x^{32} + x^{30} - x^{28} + x^{27} - x^{25} + \\ + x^{24} - x^{22} + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^{9} - x^{7} + \\ + x^{6} - x^{4} + x^{3} - x + 1$$

$$\Phi_{95} = x^{72} - x^{71} + x^{67} - x^{66} + x^{62} - x^{61} + x^{57} - x^{56} + x^{53} - x^{51} + x^{48} - x^{46} + \\ + x^{43} - x^{41} + x^{38} - x^{36} + x^{34} - x^{31} + x^{29} - x^{26} + x^{24} - x^{21} + x^{19} - x^{16} + \\ + x^{15} - x^{11} + x^{10} - x^{6} + x^{5} - x + 1$$

$$\Phi_{105} = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + \\ + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + \\ + x^{12} - x^{9} - x^{8} - 2x^{7} - x^{6} - x^{5} + x^{2} + x + 1$$

B.2. Néhány érdekesebb csoport

Ezen az oldalon a legfeljebb harminc elemű csoportokat tekintjük át, p és q végig különböző prímszámokat jelölnek.

- Egyelemű csoport izomorfia erejéig csak egy van.
- Minden p rendű csoport ciklikus, és így $\mathbb{Z}_p^+$-szal izomorf. Ilyen csoport összesen tíz van, a lehetséges rendek 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.
- Minden p^2 rendű csoport kommutatív (4.10.3. Tétel), és a véges Abel-csoportok alaptétele miatt $\mathbb{Z}_p^+ \times \mathbb{Z}_p^+$-szal vagy $\mathbb{Z}_{p^2}^+$-szal izomorf. Ilyen csoport összesen kétszer három van, a lehetséges rendek 4, 9, 25.
- Ha a csoport rendje p^3, akkor három kommutatív és két nemkommutatív csoport van. A kommutatívak $\mathbb{Z}_{p^3}^+$, $\mathbb{Z}_{p^2}^+ \times \mathbb{Z}_p^+$ és $(\mathbb{Z}_p^+)^3$. A nemkommutatívak $p = 2$ esetén a D_4 diédercsoport, és a Q kvaterniócsoport, ha pedig p páratlan, akkor az $\mathrm{U}(3, \mathbb{Z}_p)$ és a 4.10.11. Feladatban leírt csoport. Összesen ötször két csoportról van szó, a lehetséges rendek 8 és 27.
- Ha a csoport rendje $2p$, ahol p páratlan prím, akkor a 4.7.40. Gyakorlat miatt vagy a D_p diédercsoportról, vagy a $\mathbb{Z}_{2p}^+$ ciklikus csoportról van szó. Ilyen csoport kétszer öt van, a lehetséges rendek 6, 10, 14, 22, 26.
- Ha a csoport rendje pq, ahol $p > q$ páratlan prímek, akkor a 4.10.18. Következmény miatt $q \nmid p - 1$ esetén csak ciklikus lehet, egyébként van egyetlen ilyen rendű nemkommutatív csoport is (4.10.35. Feladat). Ezért 15 rendű csoport egy, 21 rendű csoport kettő van.

12 rendű csoport öt van: két kommutatív, és három nemkommutatív. Ezek az A_4, a $D_6 \cong D_3 \times \mathbb{Z}_2^+$, és a 4.8.32. Feladat (6) pontjában szereplő csoport.

16 rendű csoport tizennégy van: öt kommutatív és kilenc nemkommutatív. Ezek közül az alábbi, páronként nem izomorf csoportokat tanultuk: D_8, $D_4 \times \mathbb{Z}_2^+$, $Q \times \mathbb{Z}_2^+$.

18 rendű csoport öt van: két kommutatív, és három nemkommutatív, melyek közül a D_9 és az $S_3 \times \mathbb{Z}_3^+$ csoportokat ismerjük.

20 rendű csoport is öt van: két kommutatív és három nemkommutatív, melyek közül csak a D_{10} diédercsoportról beszéltünk.

24 rendű csoport tizenöt van: három kommutatív és tizenkét nemkommutatív, melyek közül az egyik az S_4, és további hat az eddig említett csoportokból direkt szorzással kapható.

28 rendű csoport négy van: két kommutatív, és két nemkommutatív, D_{14} és $D_7 \times \mathbb{Z}_2^+$.

30 rendű csoport négy van: egy kommutatív, és három nemkommutatív, ezek D_{15}, $D_5 \times \mathbb{Z}_3^+$ és $D_3 \times \mathbb{Z}_5^+$.

Összesen tehát izomorfia erejéig pontosan 92 darab legfeljebb harminc rendű csoport létezik. (Ez nem a matematikusok találmánya, hanem a világ tulajdonsága, olyan univerzális állandó, mint például a fénysebesség.)

1. táblázat. A sporadikus egyszerű csoportok jele, rendje és felfedezőik.

M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	Mathieu
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	Mathieu
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	Mathieu
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	Hall, Janko
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Suzuki
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	Higman, Sims
McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	McLaughlin
Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	Conway, Leech
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	Held/Higman, McKay
Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Fischer
Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	Fischer
Fi'_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	Fischer
HN	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	Harada, Norton/Smith
Th	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	Thompson/Smith
B	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$	Fischer/Sims, Leon
M	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot$ $\cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	Fischer, Griess
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	Janko
$O'N$	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	O'Nan/Sims
J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	Janko/Higman, McKay
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	Lyons/Sims
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	Rudvalis/Conway, Wales
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	Janko/Norton, Parker, Benson, Conway, Thackray

2. táblázat. Az egymilliónál kisebb rendű egyszerű csoportok: $\mathrm{PSL}(2, q)$.

$\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong A_5$	$60 = 2^2 \cdot 3 \cdot 5$
$\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$	$168 = 2^3 \cdot 3 \cdot 7$
$\mathrm{PSL}(2,9) \cong A_6 \cong S_4(2)'$	$360 = 2^3 \cdot 3^2 \cdot 5$
$\mathrm{PSL}(2,8) \cong R(3)'$	$504 = 2^3 \cdot 3^2 \cdot 7$
$\mathrm{PSL}(2,11)$	$660 = 2^2 \cdot 3 \cdot 5 \cdot 11$
$\mathrm{PSL}(2,13)$	$1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$
$\mathrm{PSL}(2,17)$	$2448 = 2^4 \cdot 3^2 \cdot 17$
$\mathrm{PSL}(2,19)$	$3420 = 2^2 \cdot 3^2 \cdot 5 \cdot 19$
$\mathrm{PSL}(2,16)$	$4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$
$\mathrm{PSL}(2,23)$	$6072 = 2^3 \cdot 3 \cdot 11 \cdot 23$
$\mathrm{PSL}(2,25)$	$7800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13$
$\mathrm{PSL}(2,27)$	$9828 = 2^2 \cdot 3^3 \cdot 7 \cdot 13$
$\mathrm{PSL}(2,29)$	$12180 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$
$\mathrm{PSL}(2,31)$	$14880 = 2^5 \cdot 3 \cdot 5 \cdot 31$
$\mathrm{PSL}(2,37)$	$25308 = 2^2 \cdot 3^2 \cdot 19 \cdot 37$
$\mathrm{PSL}(2,32)$	$32736 = 2^5 \cdot 3 \cdot 11 \cdot 31$
$\mathrm{PSL}(2,41)$	$34440 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 41$
$\mathrm{PSL}(2,43)$	$39732 = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$
$\mathrm{PSL}(2,47)$	$51888 = 2^4 \cdot 3 \cdot 23 \cdot 47$
$\mathrm{PSL}(2,49)$	$58800 = 2^4 \cdot 3 \cdot 5^2 \cdot 7^2$
$\mathrm{PSL}(2,53)$	$74412 = 2^2 \cdot 3^3 \cdot 13 \cdot 53$
$\mathrm{PSL}(2,59)$	$102660 = 2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 59$
$\mathrm{PSL}(2,61)$	$113460 = 2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61$
$\mathrm{PSL}(2,67)$	$150348 = 2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 67$
$\mathrm{PSL}(2,71)$	$178920 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 71$
$\mathrm{PSL}(2,73)$	$194472 = 2^3 \cdot 3^2 \cdot 37 \cdot 73$
$\mathrm{PSL}(2,79)$	$246480 = 2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 79$
$\mathrm{PSL}(2,64)$	$262080 = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$
$\mathrm{PSL}(2,81)$	$265680 = 2^4 \cdot 3^4 \cdot 5 \cdot 41$
$\mathrm{PSL}(2,83)$	$285852 = 2^2 \cdot 3 \cdot 7 \cdot 41 \cdot 83$
$\mathrm{PSL}(2,89)$	$352440 = 2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 89$
$\mathrm{PSL}(2,97)$	$456288 = 2^5 \cdot 3 \cdot 7^2 \cdot 97$
$\mathrm{PSL}(2,101)$	$515100 = 2^2 \cdot 3 \cdot 5^2 \cdot 17 \cdot 101$
$\mathrm{PSL}(2,103)$	$546312 = 2^3 \cdot 3 \cdot 13 \cdot 17 \cdot 103$
$\mathrm{PSL}(2,107)$	$612468 = 2^2 \cdot 3^3 \cdot 53 \cdot 107$
$\mathrm{PSL}(2,109)$	$647460 = 2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 109$
$\mathrm{PSL}(2,113)$	$721392 = 2^4 \cdot 3 \cdot 7 \cdot 19 \cdot 113$
$\mathrm{PSL}(2,121)$	$885720 = 2^3 \cdot 3 \cdot 5 \cdot 11^2 \cdot 61$
$\mathrm{PSL}(2,125)$	$976500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 31$

3. táblázat. A többi egymilliónál kisebb rendű egyszerű csoport.

A_7	$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$
PSL(3, 3)	$5616 = 2^4 \cdot 3^3 \cdot 13$
$U_3(3) \cong G_2(2)'$	$6048 = 2^5 \cdot 3^3 \cdot 7$
M_{11}	$7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$
PSL(3, 4)	$20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$
PSL(4, 2) $\cong A_8$	$20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$
$U_4(2) \cong S_4(3)$	$25920 = 2^6 \cdot 3^4 \cdot 5$
$Sz(8)$	$29120 = 2^6 \cdot 5 \cdot 7 \cdot 13$
$U_3(4)$	$62400 = 2^6 \cdot 3 \cdot 5^2 \cdot 13$
M_{12}	$95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$
$U_3(5)$	$126000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7$
J_1	$175560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
A_9	$181440 = 2^6 \cdot 3^4 \cdot 5 \cdot 7$
PSL(3, 5)	$372000 = 2^5 \cdot 3 \cdot 5^3 \cdot 31$
M_{22}	$443520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
J_2	$604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
$S_4(4)$	$979200 = 2^8 \cdot 3^2 \cdot 5^2 \cdot 17$

B.2.1. Tétel. *Az alábbi,* 10 *generátorral és* 27 *definiáló relációval megadott G csoport szóproblémája nem oldható meg. Ez azt jelenti, hogy nem lehet olyan számítógépes programot írni, amely az $a, b, c, d, e, p, q, r, t, k$ generátorokkal felírt tetszőleges két szóról eldönti, hogy ezek a G csoportban egyenlőek-e, vagy sem.*

$$
\begin{aligned}
G = \langle a,\ b,\ c,\ d,\ e, p,\ q,\ r,\ t,\ k \mid \\
& p^{10}a = ap,\ p^{10}b = bp,\ p^{10}c = cp,\ p^{10}d = dp,\ p^{10}e = ep, \\
& aq^{10} = qa,\ bq^{10} = qb,\ cq^{10} = qc,\ dq^{10} = qd,\ eq^{10} = qe, \\
& ra = ar,\ rb = br,\ rc = cr,\ rd = dr,\ re = er, \\
& pacqr = rpcaq,\ p^2adq^2r = rp^2daq^2, \\
& p^3bcq^3r = rp^3cbq^3,\ p^4bdq^4r = rp^4dbq^4, \\
& p^5ceq^5r = rp^5ecaq^5,\ p^6deq^6r = rp^6edbq^6, \\
& p^7cdcq^7r = rp^7cdceq^7,\ p^8ca^3q^8r = rp^8a^3q^8, \\
& p^9da^3q^9r = rp^9a^3q^9,\ pt = tp,\ qt = tq, \\
& a^{-3}ta^3k = ka^{-3}ta^3\rangle\,.
\end{aligned}
$$

(Lásd a megjegyzéseket a 208. oldalon.)

C. MI AZ ALGEBRA?

Ha végigpillantunk a tudomány történetén, beláthatjuk: nagyon valószínűvé teszi, hogy a jövő képét az határozza meg, amit ma nem tudunk, és ami nem látható előre.

Stanisław Lem: *Az Úr hangja*
(Murányi Beatrix fordítása)

A címben föltett kérdésre nagyon sokféle válasz lehetséges. Aki végigolvassa ezt a könyvet (és remélhetőleg más matematika-könyveket is), annak kialakul a képe az algebráról. Mégis megkísérelünk egyfajta — szükségszerűen szubjektív — összefoglalót adni. Ez egyaránt szól azoknak, akik most nyitják ki először a könyvet, és azoknak, aki már végigrágták magukat rajta. Az alábbiakat érdemes többször is elolvasni, hiszen a fölsorolt elvek konkrét tudás birtokában újabb és újabb értelmet nyernek, egyre érthetőbbekké válnak.

Középiskolai tapasztalatunk az, hogy az algebrában számolni szoktunk. Ha például egy geometria-példát akarunk megoldani, és sikerül fölírni egy egyenletet, akkor ennek megoldása már az algebra témakörébe tartozik. Az algebrista dolga az, hogy az embereknek megkönnyítse a számolások elvégzését.

A számolás fogalma egészen általános. A mindennapi életben mondhatjuk ezt olyankor is, ha el akarjuk dönteni, melyik úton haladva jutunk el leggyorsabban a Magas-Tátrába, vagy hogy beáldozzuk-e a vezérünket egy sakkpartiban a mattadás érdekében. Az algebrában számoláson elsősorban azt értjük, hogy *műveleteket végzünk*. Ezek lehetnek a klasszikus műveletek: összeadás, kivonás, szorzás, osztás, de más is, például két egész szám legnagyobb közös osztójának a meghatározása.

Műveleteket nem csak számokkal végzünk. Középiskolában megtanultunk egyenleteket rendezni, és ilyenkor ismeretlent tartalmazó (formális) kifejezésekkel számolunk. Beszélni szoktunk függvények összegéről is, például a $\sin x + \cos x$ függvényről. Szükséges lehet annak kiszámítása, hogy a síkon egy tükrözés és egy forgatás egymás utáni elvégzése milyen transzformációt eredményez. Ilyenkor geometriai transzformációkkal végzünk műveletet: az egymás után alkalmazás, más néven *kompozíció* műveletét. A matematikában, a fizikában a fentieken kívül még sok olyan dolgot fedeztek föl (például vektorokat, tenzorokat, kvaterniókat), amelyekkel számolni érdemes.

Amikor sok ember mindenfélével számolni akar, az a jó, ha az algebrista egyszerre tud segíteni nekik, olyan általánosan, ahogy csak lehet. Ha valakinek sok olyan feladatot kell

megoldania, amely mind másodfokú egyenletre vezet, akkor nem érdemes minden egyenlettel az algebristához szaladnia, jobban jár, ha az algebrista megmutatja neki a megoldóképletet. A lineáris algebra a geometriai transzformációk kompozíciójának kiszámítását úgy könnyíti meg, hogy minden síkbeli transzformációhoz egy számnégyest (úgynevezett mátrixot) rendel, és megadja, hogy a két transzformáció kompozíciójának mátrixát milyen szabályokkal határozhatjuk meg.

A matematika erős oldala mindig is az volt, hogy sok hasonló problémát *egyszerre* tudott megoldani, alkalmas módszerek kidolgozásával. Az ezt elősegítő egyik alapvető eszköz az *absztrakció*. Ez azt jelenti, hogy sok hasonló dolognak megragadjuk a közös vonásait, ezekből kiindulva valami érdekeset fedezünk föl, amit azután a kiinduló dolgok mindegyikére alkalmazhatunk (olyanokra is, amire korábban nem is gondoltunk).

> Amikor az ősember rájött, hogy két tigris meg két tigris az négy tigris, de ugyanúgy két dárda meg két dárda az négy dárda, akkor hatalmas lépést tett a szám fogalmának megalkotása felé. Az „egész szám" tehát egy absztrakt fogalom, a $2 + 2 = 4$ pedig egy absztrakt tétel. Ez azt is maga után vonja, hogy két űrhajó meg két űrhajó az négy űrhajó (amire az ősember feltehetőleg nem gondolt). Hasonlóképpen absztrakció eredménye a másodfokú egyenlet fogalma is, a megoldóképlet pedig egy absztrakt tételnek tekinthető.

Az absztrakciót a matematika minden ága alkalmazza. Az algebra abban speciális, hogy *struktúrákban* gondolkodik, és ezek szerkezetét akarja földeríteni. Ezt először az egész számok példáján érzékeltetjük (amelyek ugyan nem struktúrák a szó algebrai értelmében, de mint láttuk, absztrakció eredményei).

> Nevezetes eredmény, hogy minden egész szám egyértelműen fölbontható prímszámok szorzatára. Ez megadja a számok „szerkezetét", tehát egyfajta struktúratételnek tekinthető. Lehetővé teszi bizonyos kérdések gyors megválaszolását (például hogy egy számnak hány osztója van, mi két szám legkisebb közös többszöröse). Persze nem minden probléma megoldásában segít (például azokéban kevésbé, amelyekben összeadás is szerepel).

Mi az, hogy algebrai struktúra? Középiskolából tudjuk, hogy a szorzás *asszociatív*, vagyis $(ab)c = a(bc)$ tetszőleges számokra teljesül. Ez a szabály érvényes akkor is, ha függvényeket, vagy ha mátrixokat szorzunk. Ilyenkor az algebrista a következőt mondja.

> „Ne foglalkozzunk azzal, hogy *miket* szorzunk össze, csak azzal, hogy a szorzásnak mik a tulajdonságai. Nevezzük el félcsoportnak azt a struktúrát, amelyről csak annyit tudunk, hogy az elemeit asszociatív módon össze lehet szorozni. Az én dolgom az, hogy az ilyen struktúrákat vizsgáljam, minél többet, mélyebbet tudjak mondani róluk, a legjobb esetben teljesen le tudjam írni a szerkezetüket. Mivel az elemekről semmit sem tettem föl, mindenki tudja majd alkalmazni az eredményeimet, aki egy asszociatív művelettel találkozik."

Természetesen nagyon sokféle struktúra és tulajdonság van, amit ily módon vizsgálni lehet. Két olyan fontos feltétel van, amelynek teljesülnie kell ahhoz, hogy egy struktúrát érdemes is legyen vizsgálni.

- Elég speciális legyen ahhoz, hogy nemtriviális eredményeket lehessen bizonyítani.
- Elég általános legyen ahhoz, hogy a kapott eredmények sokféleképpen alkalmazhatók legyenek.

Az algebrában szereplő fogalmak ennek megfelelően származhatnak az alkalmazásokból, de eredhetnek abból a belső szükségszerűségből is, hogy az algebrai vizsgálatokat hatékonnyá, áttekinthetővé, egyszerűvé tegyük.

Ha egy struktúra szerkezetét teljesen föl lehet deríteni, akkor *struktúratételről* beszélünk. Ilyen a véges Abel-csoportok alaptétele, a véges egyszerű csoportok klasszifikációja, a véges testek leírása, vagy a Wedderburn–Artin-tétel. Ide tartozó egyszerűbb eredmény a ciklikus csoportok és a prímtestek *osztályozása* is.

Az imént hangsúlyoztuk, hogy a vizsgált struktúrákban csak a műveletek tulajdonságai számítanak, az elemek mibenléte nem. Ha az elemeket kicseréljük, de a műveleteket „ugyanúgy" végezzük, akkor a két struktúrát azonosnak tekintjük. Ezt pontosabban úgy fogalmazhatjuk, hogy a két struktúra elemei között van egy olyan megfeleltetés, amely *tartja a műveleteket*. Más szóval a két struktúra *izomorf*, a szerkezetük ugyanaz.

Általában két struktúra között egy „szerkezettartó" leképezést *homomorfizmusnak* nevezünk. Ez talán az algebra legfontosabb fogalma, mert lehetővé teszi, hogy a struktúrákat ne önmagukban, hanem egymáshoz való viszonyaikban vizsgáljuk. Az izomorfizmusok is homomorfizmusok, ezek fontosságát már láttuk. Sokszor előfordul az is, hogy egy bonyolult struktúrában föltett kérdés megválaszolásához elegendő egy olyan egyszerűbb struktúra vizsgálata, amelybe a bonyolult struktúrából homomorfizmus vezet, azt *reprezentálja*.

Például ha a kérdés az, hogy az 100000000007 számot elő lehet-e állítani két négyzetszám összegeként, akkor minden számot reprezentáljunk a néggyel való osztási maradékával. Összeg maradéka a maradékok összege, szorzat maradéka a maradékok szorzata, ezért ez a leképezés „szerkezettartó" (tartja az összeadást és a szorzást). Mivel négyzetszám néggyel osztva nullát vagy egyet ad maradékul, két négyzetszám összegének maradéka három biztosan nem lehet, és így a fenti szám nem áll elő két négyzetszám összegeként.

Homomorfizmusnak tekinthetjük a mérés aktusát is a természettudományokban, hiszen a mérőszám a vizsgált dolog egy egyszerűen kezelhető reprezentánsa. A mérőszám hozzárendelése „szerkezettartó" leképezés, ezt fejezik ki a természeti törvények. Például ha két biliárdgolyó összeütközik, akkor a tömegek, a mozgásmennyiségek összeadódnak. Egy fizikai kérdést, mondjuk azt, hogy a biliárdasztalon lévő golyók ütközések sorozata után kerülhetnek-e egy megadott állapotba, megválaszolhatunk negatívan úgy, hogy kiszámítjuk a rendszer energiáját a kezdő és a végső állapotban. Ha más mennyiséget kapunk, akkor a végső állapot nem jöhet létre. Ez a fenti, négyzetszámokról szóló feladat analogonja. A mérések eredményei általában az algebra legfontosabb objektumainak elemei (számok, vektorok), és az ezekkel végzendő műveletek motivációja is sokszor a fizikából származik (például a vektorok összeadását levezethetjük az erők viselkedéséből is).

Ennél még általánosabb elvként magát az absztrakció folyamatát is homomorfizmusnak képzelhetjük. Amikor elvonatkoztatunk az elemek mibenlététől, ugyanolyan egyszerűsítést hajtunk végre, mint az előbbi két példában, és ez lehetővé teszi, hogy a lényegre koncentráljunk. A valós számok esetében elhagyhatjuk a műveleteket, és csak arra figyelhetünk, hogy mely számok vannak egymáshoz „közel". Ekkor az analízis *topológiai* szemléletmódjához jutunk. Ha viszont a rendezést és a távolságot hanyagoljuk el, és a műveletekre figyelünk, akkor a valós számok összességét, mint algebrai struktúrát, azaz mint *testet* vizsgálhatjuk.

„Szerkezettartó” hozzárendelésre fontos példa az *invariánsok* fogalma is. Az invariáns olyan dolog, ami egy rendszernek jellemzője, a rendszer átalakulásai során nem változik. Ilyen például az energia, a mozgásmennyiség a fizikában. Ha gyerekek dobálnak labdákat egymásnak, akkor az változhat, hogy kinél éppen hány labda van, de a labdák össz-száma invariáns marad. Az algebrában az invariánsok szerepe különösen fontos, ha azt akarjuk megállapítani, hogy két struktúra izomorf-e.

Például két vektortér akkor és csak akkor izomorf, ha a dimenziójuk megegyezik. Ezért a vektorterek teljes osztályozásához szükséges egyetlen invariáns a dimenzió. Csoportoknál invariáns a huszadrendű elemek száma a csoportban, hiszen izomorfizmusnál ez is megőrződik.

Néha olyan szerencsénk van, hogy a megismerni kívánt bonyolult struktúrából rengeteg homomorfizmust találunk egyszerűbb struktúrákba, eleget ahhoz, hogy a kiinduló struktúra szerkezetét ezek teljesen meghatározzák. Például egy pont egy koordinátájának kiszámítása homomorfizmus, de ha a pont „összes” koordinátáit megadjuk, akkor ezzel a pontot is meghatároztuk. Ugyanígy egy részecske állapotát leírhatjuk hat „koordináta” segítségével (három hely- és három sebesség-koordináta). Ha egy algebrai struktúrát sikerül az így leírt módon megfognunk, akkor *szubdirekt felbontásról* beszélünk.

Az algebrában a *fogalmak* és a *módszerek* legalább annyira fontosak, mint a tételek. Egy-egy tételt el lehet felejteni, de az alkalmazott módszerek megragadnak, és így lehetővé válik, hogy az erre alkalmas problémákat „algebrista” gondolkodásmóddal támadjuk meg. A helyes fogalmak felismerésének módját az alábbi, klasszikus hindu történet példázza.

Vak fakírok az erdőben sétálva találkoztak egy állattal. Az egyik felkiáltott: „Ez egy kígyó!”, mikor megsimogatta az ormányát. „Nem, ez egy fa!”, mondta egy másik, aki a lábát tapogatta. A harmadik az állat testét falnak érzékelte, a negyedik a fülét papírnak, az ötödik a farkát kötélnek. Amikor azonban este elbeszélgettek a tapasztalataikról, egész jó képet sikerült kialakítaniuk az elefántról (amit korábbi tapasztalataik segítségével „mértek” meg).

Azt, hogy egy fogalmat az általánosság melyik szintjén érdemes vizsgálni, magától a fogalomtól, és a felvetett kérdéstől függ. Ezt úgy kell elképzelni, mint amikor megismerünk egy hegységet, ahová kirándulni járunk. A konkrét problémák megoldása annak felel meg, hogy le kell küzdenünk meredek emelkedőket, bozótos részeket. Eleinte ezeket ki sem tudjuk kerülni. Csak évek során jön meg az az áttekintési képességünk, hogy már minden pillanatban tudjuk: a hegység egészéhez képest hol vagyunk, merre mi van, milyen távolságban, és az hogyan érhető el. Ez a megismerési folyamat az egyéni tanulásra éppen úgy vonatkozik, mint magának a matematikának a fejlődésére. A jobb áttekintés a matematikában sokszor az általánosság szintjének emelkedését jelenti. Minderre fontos példát szolgáltatnak az alábbiak.

- Elem rendjével először a komplex egységgyökök kapcsán találkozunk, amikor azt vizsgáljuk, hogy egy komplex szám mely hatványai lesznek 1-gyel egyenlők. Kiderül, hogy ezek a „jó” kitevők mindig egy alkalmas egész szám összes többszörösei. Ugyanez a jelenség lép föl akkor is, ha azt kérdezzük, hogy egy geometriai transzformációt hányszor kell alkalmazni ahhoz, hogy minden pontot önmagába vigyen. Az „elefánt” ebben az esetben a csoportelméleti elemrend lesz. Az újabb fakír azonban észreveszi, hogy a lineáris

transzformációknál tanult minimálpolinomnak is vannak a fentiekhez hasonló tulajdonságai. A végső, „még magasabb szintű elefánt” tehát az elemrendnek az a fogalma, ami a modulusok elméletében szerepel.
- A véges Abel-csoportok alaptétele és a Jordan-féle normálalakról szóló tétel esetében a „helyes” (közös) általánossági szint a főideálgyűrűk fölötti modulusok alaptétele.
- A számelmélet alaptételét tárgyalhatjuk külön az egész számokra, és test fölötti polinomokra. Közös általánosításként szerepel az euklideszi gyűrű, illetve a főideálgyűrű fogalma. Ennél is tovább léphetünk, ha ideálok primér felbontásait nézzük (Noether–Lasker-tétel), vagy akár ennek a hálóelméleti általánosítását (Kuros–Ore-tétel).
- A direkt szorzat fogalmának legáltalánosabb definíciója a kategóriaelméletből származik. A direkt szorzat belső jellemzése általános algebrákban kongruenciákkal történik. Csoportokban és gyűrűkben is módosítanunk kell ezen, hogy a normálosztókkal illetve ideálokkal történő jellemzést megtaláljuk.
- A generált részstruktúra megkapható úgy, mint a generátorokat tartalmazó részstruktúrák metszete (ez a teljes hálók szintje). Az elemeit le lehet írni úgy, mint a a generátoroknak a term-függvényeknél fölvett értékeit (ez az általános algebrák szintje). Konkrét struktúrákban mindig új feladat, hogy ez a leírás milyen formában lehetséges (lineáris kombinációkkal a vektorterekben, modulusokban, szavakkal a csoportokban, normálformákkal a Boole-algebrákban).

Az algebrai módszerek alapja az, hogy, mint már említettük, struktúrákban gondolkodunk. A teljesség igénye nélkül megemlítünk néhány további, tipikus algebrai módszert.

- A *direkt szorzatra bontás* során a struktúrákat egyszerűbb alkotóelemekből állítjuk össze. Olyanokból, amelyekben már könnyebb számolni. A *szubdirekt szorzat* szerkezete nehezebben kezelhető, de több struktúrát bonthatunk szubdirekt szorzatra, mint direkt szorzatra.
- Hasonló fontosságú a *faktorstruktúra* fogalma is, amely azt teszi lehetővé, hogy hasonló tulajdonságú elemeket egymással azonosítsunk. Példa erre az a technika, amelynek segítségével a törteket bevezetjük a hányadostest nevű konstrukció révén (és a $2/4$ és $3/6$ törteket egyenlővé tesszük).
- A *reprezentációk* olyan homomorfizmusok, amelyek egy struktúrából egy másfajta struktúrába képeznek, ahol általában már jól lehet számolni. Például egy csoport elemeihez mátrixokat vagy permutációkat, egy Boole-algebra elemeihez halmazokat rendelhetünk.
- Ennek ellentéteképpen sokszor *szabadon* építünk bizonyos objektumokat, és ezekből kapjuk meg a vizsgált struktúrát egy homomorfizmus képeként.
- A *Gauss-elimináció* egy konkrét algoritmus, amit eredetileg lineáris egyenletrendszerek megoldására fejlesztettek ki. Alkalmas azonban mátrixok inverzének, determinánsának és Jordan-alakjának, továbbá kvadratikus alakok négyzetösszeg alakjának kiszámítására is.

A most leírt szemléletmód különösen alkalmas arra, hogy az egyes problémák megoldására egy másik területről származó módszereket alkalmazzunk. Az ilyen „interdiszciplináris” hozzáállás mindig nagyon megtermékenyítő.

Például egyenletek megoldásainak vizsgálatára testeket, ezek megértéséhez pedig csoportokat használunk a Galois-elmélet keretében. Hasonló fontosságú a Pontrjagin-dualitás, amely a diszkrét és kompakt topologikus csoportok elméletét kapcsolja össze.

Végül egy általános megjegyzést szeretnénk tenni a matematikáról. A matematika fejlődése nem olyan egyszerű folyamat, hogy megoldjuk a gyakorlatban, vagy a más tudományokban fölmerülő problémákat. Azért nem, mert sokszor előfordul, hogy ezeket a problémákat nem tudjuk megoldani azonnal. Gyakori tapasztalat, hogy ilyenkor segíthet a megoldásban a matematika egy másik területe, egy olyan terület, amelyet eredetileg egészen más célból, más problémák megoldása végett fejlesztettek ki. Példaként érdemes megemlíteni az RSA titkosítási rendszert, amelyet manapság állandóan alkalmaznak, és amely annak köszönheti a megszületését, hogy az emberiség egy másik, teljesen elvontnak és alkalmazhatatlannak tűnő problémát vizsgált: azt, hogy nagyon nagy számokat milyen eljárással lehet gyorsan prímtényezőkre bontani.

> A jó problémák azok, amelyek új, még feltáratlan területekre, új jelenségek megértésére vezetnek. A keletkező elméletek azután már sokszor gyakorlati alkalmazásokat is adnak. Jó példa erre, hogy az egyenletek megoldóképletének vizsgálata a Galois-elmélet kifejlődéséhez vezetett, ennek segítségével értettük meg a véges testek szerkezetét, ezeket pedig, szinte váratlan módon, alkalmazni lehet a híradástechnikában, pontosabban a kódelméletben.

A matematika most leírt fejlődési folyamata hasonlít ahhoz, ahogy az Élet terjeszkedik, és egyre újabb területeket vesz birtokába. Eleinte a véletlenen, például mutációkon, tengeráramlatok szeszélyein múlik, hogy egy-egy organizmus „megpróbálkozik-e" valami újdonsággal. Azután „követői" is akadnak, akik közül nagyon sok elpusztul. De lassan kiderül az „igazság": a helyes stratégia, amivel az új körülményekhez alkalmazkodni lehet. Ugyanígy számos matematikai kísérletet kell tennünk, problémákat megoldanunk, tételt bizonyítanunk, elméletet készítenünk, míg végül a helyes irányra rábukkanunk, és az „elefántot" megtaláljuk.

A matematikát tehát nem egy (tétel)gyárhoz, vagy csirkefarmhoz érdemes hasonlítani, hanem inkább a természethez, ahol minden mindennel összefügg. Egy-egy terület életképességét nemcsak az eredményei szabják meg, hanem az is, hogy hogyan tud beilleszkedni az egészbe, milyen kapcsolatokat tud teremteni. A fejlődést sokszor belső törvényszerűségek szabályozzák, ezek egy kifejeződési formája a matematika *esztétikuma*. A matematikusok által izgalmasnak, érdekesnek, szépnek tartott kérdések megválaszolása számtalanszor vezetett döntő áttöréshez. Olyan ötletek merülhetnek így föl, amelyekhez máshogy el sem juthattunk volna. A matematikát alkalmazni szándékozók azután meglátogathatják a természetet, és megtalálhatják azt az erdei gyümölcsöt, gombát, amire éppen szükségük van.

Ha kirándulunk a természetben, akkor meg is erősödünk. A matematikával való foglalkozás pedig megerősíti az általános emberi gondolkodásnak egy nagyon fontos fajtáját: azt, amikor szisztematikusan végig kell gondolnunk valamit. Ez lehet köznapi dolog, mondjuk bútortologatási stratégia egy zsúfolt lakásban, de lehet számítástechnikai probléma, vagy akár jogi kérdés is. Mindezt problémamegoldással, fogalmak, bizonyítások megértésével edzhetjük. A matematikának része a matematikai logika, amely ezt a fajta gondolkodásmódot vizsgálja, és teljes megbízhatósággal kezeli.

Tárgymutató

Ö, Ő

P

R

Irodalom

[1] E. Berlekamp: *Algebraic Coding Theory.* Aegean Park Press, Laguna Hills, CA, 1984.

[2] G. Birkhoff, T. C. Bartee: *A modern algebra a számítógéptudományban.* Műszaki Könyvkiadó, 1974.

[3] S. Burris, H. P. Sankappanavar: *Bevezetés az univerzális algebrába.* Tankönyvkiadó, Budapest, 1988.

[4] S. Burris, H. P. Sankappanavar: *A course in universal algebra.* Springer kiadó, 1981. Letölthető a `http://www.thoralf.uwaterloo.ca/htdocs/ualg.html` címről.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson: *Atlas of finite groups: Maximal subgroups and ordinary characters for simple groups.* Oxford University Press, Oxford, 1985.

[6] Czédli Gábor, B. Szendrei Mária, Szendrei Ágnes: *Absztrakt algebrai feladatok.* Polygon kiadó, Szeged, 2005.

[7] Czédli Gábor, Szendrei Ágnes: *Geometriai szerkeszthetőség*. Polygon kiadó, Szeged, 1997.

[8] D. K. Fagyejev, I. Sz. Szominszkij: *Felsőfokú algebrai feladatok.* TypoTEX kiadó, 2000.

[9] W. Feit, J. G. Thompson: Solvability of groups of odd order. *Pacific J. Math.*, **13** (1963), 775-1029.

[10] Freud Róbert: *Lineáris Algebra*. ELTE Eötvös kiadó, Budapest, 1996.

[11] Freud Róbert, Gyarmati Edit: *Számelmélet*. Nemzeti Tankönyvkiadó, Budapest, 2000.

[12] Fried Ervin: *Algebra I.* Nemzeti Tankönyvkiadó, Budapest, 2000.

[13] Fried Ervin: *Algebra II.* Nemzeti Tankönyvkiadó, Budapest, 2002.

[14] Györfi László, Győri Sándor, Vajda István: *Információ- és kódelmélet.* TypoTEX kiadó, 2002.

[15] D. Hobby, R. McKenzie: *The structure of finite algebras* (Tame congruence theory). American Mathematical Society *Contemporary Mathematics* Series 76, 1988. Letölthető a `http://www.ams.org/online_bks/conm76/` címről.

[16] Saunders Mac Lane: *Categories for the Working Mathematician.* Volume 5 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1971.

[17] Ken C. Pohlmann: *Principles of Digital Audio.* McGraw-Hill, 2000.

[18] Hao Wang: *A Logical Journey.* From Gödel to Philosophy. MIT Press, 1997.

Az ábrák jegyzéke

Tartalom