KISS EMIL

BEVEZETÉS AZ ALGEBRÁBA

A gyakorlatok és a feladatok megoldásai

A könyvet és a megoldásokat lektorálta:
Dr. Freud Róbert egyetemi docens

ISBN 978-963-9664-48-7
ISSN 1788-1811

Budapest, 2007

Stanisław Lem *emlékének,*
aki mindannyiunknál messzebbre látott.

Tartalom

1. fejezet

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 fölülvonás 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 egyszerűbb számolással igazolható. Az 1.1.5-beli azonosságok igazolásához írjuk föl 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 fölülvonás 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 $3 *_5 x = 2$. 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 $a *_5 x = b$. Nullával nem tudunk osztani, hiszen ha $a = 0$, akkor $b \neq 0$ 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 látni, 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 $x^2 + 5y^2 = 26$ 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 $\mathbb{Z}$-beli kiszámítása helyett gyorsabb, 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 $3 * 1 = 3$. (Még gyorsabb, ha a negyedik hatványt a $3 * 3$ négyzetre emelésével számítjuk ki.) Láthatjuk, hogy a hatványok ebben az esetben periodikusan ismétlődnek, tehát nagyon nagy kitevőkre is gyorsan kiszámíthatnánk őket. Ezzel a módszerrel könnyű ellenőrizni az $5 \mid a^5 - a$ osztható-ságot, és ugyanígy számolhatjuk ki azt is, hogy $5 \mid a^4 - 1$ 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 sem $6k+2$, sem $6k+5$ alakú.
(2) $6 \mid a^5 - 1 \iff$ az a szám $6k+1$ alakú.
(3) $6 \mid a^2 - 1 \iff$ az a szám $6k+1$ vagy $6k-1$ (rövid jelöléssel $6k \pm 1$) alakú. Másképp fogalmazva: az oszthatóság akkor áll fenn, ha 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. 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 mod 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) el kellene tudni osztani kettővel. De ezt meg lehet tenni modulo 101, hiszen $13 = \overline{114}$, vagyis a feladatban 13 helyett 114-et (vagy -88-at) 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, hogy 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 $20 = \overline{121}$, 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.

1.1.17. Nem fedhető le. A bizonyítás ötlete hasonló ahhoz, amit az 1.1.1. Kérdés esetében alkalmaztunk a 100×100-as tábla esetén, csak most a modulo 2 maradékokat írjuk a sakktáblára. Egyszerűbb úgy fogalmazni hogy 0 és 1 fölírása helyett a mezőket világosra és sötétre festjük, ahogy az a sakktáblán amúgy is szokásos. Ekkor a két hiányzó mező ugyanolyan színű, tehát a maradékon különbözik a világos és sötét mezők száma, márpedig ha létezne lefedés, akkor nem különbözne.

1.1.18. Ha $m \mid k$, akkor a lefedés például soronként lehetséges. Ha nem, akkor számozzuk meg a sakktábla mezőit az 1.1.1. Kérdés megoldásában látott 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 föl a sakktáblára. Az 1.1.3. Gyakorlat megoldásában szereplő vagdosási eljárással azt kapjuk, hogy ha r a 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 föl, 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.

Így az első kérdésre adott megoldásban, amikor már kijött, hogy $p = \pm 3$, *nem kell ellenőrizni, hogy* p^2+2 *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 akkor és csak 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 megkapjuk 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, tegyük föl, hogy u megoldása a $z^2-az+b=0$ egyenletnek. Ekkor $u^2-au+b=0$, így

$$z^2-az+b=z^2-az+b-(u^2-au+b)=(z-u)\big(z-(a-u)\big)\,.$$

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.

1.2.5. Az $(u+v)^3=(u^3+3uv^2)+v(3u^2+v^2)$ összefüggés miatt az első esetben

$$\left(-\frac{5}{2}+\frac{\sqrt{-3}}{2}\right)^3=\left(-\frac{125}{8}-3\cdot\frac{5}{2}\cdot\frac{-3}{4}\right)+\frac{\sqrt{-3}}{2}\left(3\cdot\frac{25}{4}+\frac{-3}{4}\right),$$

és ez $-10+\sqrt{-243}$, hiszen $9\cdot\sqrt{-3}=\sqrt{-9^2\cdot 3}=\sqrt{-243}$. A másik köbre emelés is hasonló.

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 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 csak akkor tudjuk elvégezni, ha ismerünk egy megoldást, márpedig a cél éppen a megoldások megkeresése. 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 megoldás: $7 + \sqrt{50} = (1+\sqrt{2})^3$ 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 fölcserélődik 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 fölírva, 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 E.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

$$(x+y)z = \big((a+c)+(b+d)i\big)(e+fi) = \\ = (ae + ce - bf - df) + (af + cf + be + de)i\,.$$

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 $1241 = 4 \cdot 310 + 1$, ezért a végeredmény $(1+i)^{1241} = (-4)^{310}(1+i) = 2^{620} + 2^{620}i$.
(4) Az eredmény 8.

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. Feltehetjük, hogy $b \neq 0$, hiszen valós számból tudunk négyzetgyököt vonni. 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 szakaszban más módszerrel is be fogjuk látni. A fenti képletet nem érdemes megtanulni, inkább a levezetéséhez használt módszert (vagy a következő szakaszban 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 egyenletre 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 $x = 0$ 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.

(7) Az $x = a + bi$ alakot behelyettesítve $a = 2a$ adódik, azaz $a = 0$. Ezért a megoldások a tisztán képzetes számok.

1.3.15. Ha $z = a + bi$ és $w = c + di$, akkor $\overline{z \cdot w} = (ac - bd) - (ad + bc)i = \overline{z} \cdot \overline{w}$.

1.3.16. Az (1) és (3) lesz igaz.

(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 a 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

1.4.2. Az eredmények a következők.

(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 $-1 - \sqrt{3}i = 2(\cos 240^\circ + i \sin 240^\circ)$.

1.4.4. Az Olvasót arra biztatjuk, hogy a megoldást geometriailag gondolja végig, mi algebrai bizonyítást adunk. Legyen $z = r(\cos\alpha + i \sin\alpha) = s(\cos\beta + i \sin\beta)$. Mivel r és s pozitív valós számok, továbbá $|\cos\alpha + i \sin\alpha| = |\cos\beta + i \sin\beta| = 1$, ezért $r = |z| = s$. 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. A megfordítás nyilvánvaló.

1.4.6. 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

$$r(\cos\alpha + i \sin\alpha) = z = uw = ts\big(\cos(\gamma + \beta) + i \sin(\gamma + \beta)\big).$$

A trigonometrikus alak egyértelműségéből $r = st$, és $\alpha = \beta + \gamma$ (pontosabban $\alpha - (\beta + \gamma)$ a 360° egész számú többszöröse). Ezért

$$z/w = (r/s)\big(\cos(\alpha - \beta) + i \sin(\alpha - \beta)\big).$$

Vagyis a hosszakat osztani kell, a szögeket pedig kivonni (modulo 360°).

1.4.7. 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 a hossza, vagyis *z és w távolsága.*

1.4.8. Vigyázzunk, a $\cos\alpha - i \sin\alpha$ szám nincs trigonometrikus alakban, ennek szöge ugyanis $-\alpha$ (vagy $2\pi - \alpha$). Az eredmények:

(1) $\cos 300^\circ + i \sin 300^\circ$.

(2) $(\sqrt{6}/2)(\cos 315^\circ + i \sin 315^\circ)$.
(3) $\cos(90^\circ - \alpha) + i \sin(90^\circ - \alpha)$.
(4) $\cos 2\alpha + i \sin 2\alpha$. (A törtet bővítsük $\cos\alpha$-val, majd alkalmazzuk a hányados trigonometrikus alakjáról szóló képletet, lásd 1.4.6. Gyakorlat.)

1.4.9. 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 $x + 3 \le -2$ egyenlőtlenséget kapjuk. Innen $x \le -5$, tehát a keresett alakzat egy félsík, amelyet az $x = -5$ egyenletű függőleges egyenes határol.
(2) Ha $z = x + yi$, akkor $x + 1 \ge y - 3$ adódik, vagyis $y \le x + 4$. 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, akkor egy kör egyenletét kell felismernünk. Jobb azonban, ha közvetlenül okoskodunk. A $|z-1-i|$ szám az 1.4.7. Gyakorlat 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. Így a másik két csúcs a $\mathrm{Re}(z) = -1/2$ függőleges egyenesen van.
(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 egyenletből $z = 4 \pm \sqrt{17}$ 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) A $(z-1)/(z+1)$ törtet a nevező konjugáltjával bővítve a számláló $(z-1)(\overline{z}+1) = (|z|^2-1)+(z-\overline{z})$ lesz. 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.
(9) A $z = x + iy$ helyettesítéssel $(x + 2)^2 + y^2 = 4$ adódik, vagyis ez a $(-2, 0)$ középpontú, 2 sugarú kör. Ezt *Apollóniusz-körnek* nevezik: azon pontok mértani helye, amelyek távolságának aránya két adott ponttól állandó (ha az arány 1, akkor a két pont felező merőlegesét kapjuk).

1.4.10. A keresett transzformációk a következők.

(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 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.

1.4.11. Az eredmények a következők.

(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 w-be tenni, ami azt jelenti, hogy a végpontja $i(z-w)+w$-ben lesz. Mindez az 1.4. ábráról (22. oldal a tankönyvben) is leolvasható.
(7) Ha x a keresett pont, akkor az x-ből z-be mutató vektor $\pm 90^\circ$-kal történő elforgatottja x-ből w-be mutat. 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. *Második megoldás.* A w csúcsból z-t $\pm 90^\circ$-kal elforgatva az eredmény $\pm i(z-w)+w$, ez a két keresett négyzet z-vel átellenes csúcsa. Ezért a keresett középpont ennek és a z számnak a számtani közepe.
(8) Legyen $\varepsilon = \cos 120^\circ + i \sin 120^\circ$, ekkor $\varepsilon^2 = \overline{\varepsilon} = \cos 240^\circ + i \sin 240^\circ$. Az előzőhöz hasonlóan $(w-\varepsilon z)/(1-\varepsilon)$, illetve $(w-\varepsilon^2 z)/(1-\varepsilon^2)$ adódik. *Második megoldás.* A háromszög harmadik csúcsát megkaphatjuk 60°-os elforgatással. A keresett középpont a háromszög súlypontja, vagyis a három csúcshoz tartozó számok számtani közepe.

1.4.12. A négyzet négy csúcsa legyen A, B, C, D, pozitív körüljárás szerint. Ekkor az AB oldalra kifelé írt négyzet középpontja az előző feladat (7) pontja miatt $(B+Ai)/(1+i)$. A másik három négyzet középpontját ugyanígy kapjuk. A szemközti négyzetek középpontját összekötő két vektor tehát

$$\frac{1}{1+i}\big((B+Ai)-(D+Ci)\big), \quad \text{illetve} \quad \frac{1}{1+i}\big((C+Bi)-(A+Di)\big).$$

Az első vektor i-szerese a második, így a kettő egyenlő hosszú és merőleges.

1.4.13. 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 1.4.11. Gyakorlat (8) pontja miatt az AB csúcsra kifelé írt szabályos háromszög középpontja

$$X = \frac{1}{1-\varepsilon}(A-\varepsilon B).$$

Analóg módon írhatjuk föl 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.

1.4.14. 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 látókörívén 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.

1.4.15. Legyenek a négyszög csúcsai rendre 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.

1.4.16. Az Útmutatóban leírtak alapján legyen $\varepsilon = \cos(x/2)+i\sin(x/2)$. A keresett összeg $\varepsilon^2+\varepsilon^4+\ldots+\varepsilon^{2n}$ képzetes része. A mértani sort összeadva az eredmény

$$\varepsilon^2\frac{\varepsilon^{2n}-1}{\varepsilon^2-1} = \varepsilon^{n+1}\frac{\varepsilon^n-(1/\varepsilon^n)}{\varepsilon-(1/\varepsilon)}\,.$$

De $\varepsilon-(1/\varepsilon) = 2i\sin(x/2)$ és $\varepsilon^n-(1/\varepsilon)^n = 2i\sin(nx/2)$. Így

$$\sin x+\sin(2x)+\ldots+\sin(nx) = \frac{\sin\big((n+1)x/2\big)\sin(nx/2)}{\sin(x/2)}\,,$$

és

$$\cos x+\cos(2x)+\ldots+\cos(nx) = \frac{\cos\big((n+1)x/2\big)\sin(nx/2)}{\sin(x/2)}\,.$$

A végeredmény birtokában az állítás már komplex számok nélkül is igazolható, n szerinti indukcióval. Egy *harmadik megoldást,* amelyhez nem kell előre tudni a fenti végeredményt, a következőképpen kaphatunk. A $\sin\alpha\sin\beta = \big(\cos(\alpha-\beta)-\cos(\alpha+\beta)\big)/2$ ismert azonosság, amely következik a cos függvény addíciós képletéből. Ezért

$$\sin(kx)\sin(x/2) = (1/2)\left[\cos\Big(\big(k-(1/2)\big)x\Big)-\cos\Big(\big(k+(1/2)\big)x\Big)\right].$$

Ezt $k = 1, 2, \ldots, n$-re összeadva a tagok nagy része kiesik (egy úgynevezett *teleszkopikus összeget* kapunk), ahonnan

$$\big(\sin x+\sin(2x)+\ldots+\sin(nx)\big)\sin(x/2) = (1/2)\left[\cos(x/2)-\cos\Big(\big(n+(1/2)\big)x\Big)\right].$$

A $\sin\alpha\sin\beta = \big(\cos(\alpha-\beta)-\cos(\alpha+\beta)\big)/2$ képletet ismételten alkalmazva ez a fenti alakra hozható.

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

$$w^n = s^n(\cos n\beta+i\sin n\beta) = r(\cos\alpha+i\sin\alpha)\,.$$

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 2π egész többszörösével változtatja meg.

1.5.5. Ha $|z|>1$, akkor $1<|z|<|z|^2<|z|^3<\ldots$, azaz nem lesz közöttük egyenlő. Sőt az egész kitevőkre sem, mert $1 = |z|^0 > |z|^{-1} > \ldots$ meg egyre kisebb lesz. Ugyanez a helyzet akkor, ha $|z|<1$, mert akkor minden egyenlőtlenség 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. Az 1 első, a -1 második egységgyök.

1.5.9. Először képzeljük azt, hogy a bolha 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.

Számozzuk be az n-szög csúcsait a $0, 1, \ldots, n-1$ számokkal, és képzeljük azt, hogy a bolha a 0 sorszámú csúcsról indul. Ha k-asával ugrál, akkor m lépést megtéve a km-es csúcson lesz (pontosabban ennek az n-nel való osztási maradékán). 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

$$\frac{n}{(n,k)} \,\Big|\, m$$

(az elemi számelméletből ismert állítást használtunk föl, amit általánosabban belátunk majd a 3.1.24. Gyakorlatban). 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.

1.5.14. 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 gyökvonás képlete szerint a 8-adik gyökök hossza $\sqrt[8]{2}$, szögeik $41, 25^\circ + k \cdot 45^\circ$, ahol $0 \le k < 8$.
(4) Ezek azok a $2n$-edik egységgyökök, amelyek nem n-edik egységgyökök. Szögeik a $2\pi/2n$ páratlan többszörösei, hosszuk 1.

1.5.15. Elég meghatározni a rendeket, mert ezután a válasz a következő gyakorlat megoldásából leolvasható. Az 1.5.11. 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.

1.5.16. 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.

1.5.17. 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 $4 = o(i) \mid d$.

1.5.18. 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 1.5.11. Állítást használjuk föl. Az ε szöge a 360°-nak $k/512$-szöröse, ahol $(k, 512)$=1. Speciálisan k páratlan szám. Mivel a $-i$ szöge a 360°-nak $-1/4$-szerese, ezért $-i\varepsilon$ szöge a 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.

1.5.19. 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 $n \mid 2d$-ből $n \mid d$, 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 1.5.11. Állítást használjuk. Legyen ε szöge 360°-nak k/n-szerese, ahol $(k, n) = 1$. Mivel -1 szöge 360°/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.

1.5.20. Az első esetben a tizenkettedik egységgyököket kapjuk, mindegyiket kétszer, a másodikban a negyvenkettedikeket, mindegyiket egyszer.

1.5.21. Az (1)-ben 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 (n, m)-edik egységgyökök, így számuk (n, m).

A (2) esetében ha $\varepsilon^m = 1$ és $\eta^n = 1$, akkor nyilván $(\varepsilon\eta)^{mn} = 1$.

Végül (3)-at látjuk be. 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 föl, 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 az állítás.

1.5.22. Elsőnek az n-edik egységgyökök összegét számítjuk ki. Hogyan fogná föl 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. Ez a megoldás elemi geometriával teljesen precízzé tehető.

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 fölírva. 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.

1.5.23. A binomiális tételt alkalmazzuk először az $(1+1)^n$ összegre.

$$2^n = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}.$$

Hasonlóan fölírva 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 föl 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

$$\operatorname{Re}\big((1+i)^n\big) = \binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \binom{n}{6} + \binom{n}{8} - + \ldots .$$

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 $X - Y = \operatorname{Re}\big((1+i)^n\big)$ és $X + Y = B = 2^{n-1}$. Ebből a két egyenletből pedig a keresett X kifejezhető: $X = \big(2^{n-1} + \operatorname{Re}((1+i)^n)\big)/2$. Az $(1+i)^n$ értékét trigonometrikus alakban számíthatjuk ki, az eredmény $2^{n/2}\big(\cos(2n\pi/8) + i\sin(2n\pi/8)\big)$, aminek a valós része $2^{n/2}\cos(2n\pi/8)$. A feladatban $n = 1867$, így a végeredmény $X = 2^{1865} - 2^{932}$.

1.5.24. 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 képzetes részt véve

$$\sin(nx) = \binom{n}{1} \cos^{n-1} x \sin x - \binom{n}{3} \cos^{n-3} x \sin^3 x + \binom{n}{5} \cos^{n-5} x \sin^5 x \ldots ,$$

valós részt véve

$$\cos(nx) = \cos^n x - \binom{n}{2} \cos^{n-2} x \sin^2 x + \ldots + (-1)^j \binom{n}{2j} \cos^{n-2j} x \sin^{2j} x \ldots$$

(itt $\sin^2 x$ helyére $1 - \cos^2 x$-et írva $\sin x$ teljesen eltüntethető).

2. fejezet

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. Mindkét fajta beszorzást az teszi lehetővé, hogy a komplex számok műveleteire érvényes a disztributivitás.

2.1.9. $(x^3+3x^2+2)-(x^3+3x-4) = 3x^2-3x+6$ és $(x^2+ix+3)(x^2+i) = x^4+ix^3+(3+i)x^2-x+3i$. 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 $(a_1+b_1)\ldots(a_n+b_n)$ 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 $x_1x_2\ldots x_n$ 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.

2.1.12. Az Útmutatóban leírtakat folytatjuk. Az összegben szereplő $(\varepsilon^{j-k})^{j+k}$ tagok közül n darab lesz olyan, ahol $j-k$ egy előre rögzített ℓ szám (a kitevőkkel mod n számolunk): minden k értékhez pontosan a $j = k+\ell$-hez tartozó. Ekkor $j+k = 2k+\ell$, vagyis

$$S\overline{S} = \sum_{\ell=0}^{n-1}\sum_{k=0}^{n-1}(\varepsilon^{\ell})^{2k+\ell} = \sum_{\ell=0}^{n-1}\varepsilon^{\ell^2}\left(\sum_{k=0}^{n-1}(\varepsilon^{2\ell})^k\right).$$

A zárójelben álló összeg az 1.5.22. Gyakorlat mintájára, mértani sorként kiszámítható: ha $\varepsilon^{2\ell} = 1$, akkor n-nel egyenlő, egyébként nulla. Az $\varepsilon^{2\ell}$ akkor lesz 1, ha $\ell = n$, továbbá ha n páros és $\ell = n/2$. Ez utóbbi esetben például trigonometrikus alak segítségével kapjuk, hogy ε^{ℓ^2} értéke 1, ha n osztható néggyel, különben pedig -1. Ezért $|S|$ értéke $\sqrt{n}$, ha n páratlan, nulla, ha n néggyel osztva 2 maradékot ad, végül $\sqrt{2n}$, ha $4 \mid n$.

Ha $n = 2$, akkor $S = 0$. Tegyük föl, hogy p páratlan prím, és vizsgáljuk először azt az esetet, amikor $p \equiv 1\ (4)$. Az E.4.8. Tétel miatt van olyan b egész, hogy $b^2 \equiv -1\ (p)$. A $j \mapsto bj$ kölcsönösen egyértelmű

megfeleltetés a mod p maradékosztályok halmazán, hiszen $(b, p) = 1$. Ezért az S összeg az $\varepsilon^{(bj)^2}$ számok összege is, ahol $0 \le j \le n-1$. De $(bj)^2 \equiv -j^2$, vagyis ez utóbbi összeg az S konjugáltjával egyenlő. Tehát $S = \overline{S}$, és mivel $|S| = \sqrt{p}$, ezért $S = \pm\sqrt{p}$. (Az eredmény előjele attól függ, hogy melyik ε primitív egységgyökből indulunk ki.)

Tegyük most föl, hogy $p \equiv 3$ (4). Mivel $(-j)^2 = j^2$, ezért az S összeg minden 1-től különböző tagja kétszer szerepel ebben az összegben. A $\overline{S}$ összegben az 1 kivételével szintén minden tag kétszer szerepel, ezek az E.4.8. Tétel szerint éppen azok az egységgyökök, amelyek S-ben nem szerepelnek, viszont mindegyik egységgyök szerepel valamelyik összegben. Ezért $S + \overline{S}$ az összes p-edik egységgyökök összegének kétszerese, azaz nulla (1.5.22. Gyakorlat). Innen $|S| = \sqrt{p}$ miatt $S = \pm i\sqrt{p}$.

2.2. A szokásos számolási szabályok

2.2.2. A tényezők száma szerinti indukcióval bizonyítunk: 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 asszociativitás miatt $A * B = (a_1 * C) * B = a_1 * (C * B)$. 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. Nyilván $f \circ id = id \circ f = f$ minden f függvényre (helyettesítsünk be tetszőleges $x \in X$-et), azaz *id* neutrális elem. Belátjuk, hogy ez az egyetlen neutrális elem (ez a 2.2.8. Gyakorlatból is következik). Ha az e függvény neutrális elem, akkor az $e \circ id = id$ egyenletbe x-et helyettesítve $e(x) = x$, vagyis $e = id$.

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 föl, hogy v balinverze, w pedig jobbinverze u-nak. A $*$ művelet 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 függvények akkor 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* 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 pontosan akkor balinvertálható, ha injektív.

Ha f-nek van jobbinverze, azaz olyan g, melyre $f \circ g = e$, akkor f *szürjektív*függvény, 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 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-ban, 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 elég 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.

2.2.17. Tekintsük az egész számok csoportját az összeadásra. Ebben a nemnegatív egészek halmaza zárt az összeadásra, tartalmazza a 0 neutrális elemet, mégsem részcsoport, mert például az 1-ek nincs ellentettje.

2.2.18. Az Útmutatóban megadott példában az egész számok halmaza neutrális elem, hiszen tetszőleges X részhalmazával elmetszve X-et kapjuk. Álljon T a páros számok halmazának összes részhalmazaiból. Ez zárt a metszetképzésre, a páros számok halmaza neutrális elem, és ez nem ugyanaz, mint az egész számok halmaza.

2.2.20. Tegyük föl 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 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 fölcserélhetők. 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 $0 \leq n < k$, 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}. Ha $n \leq 0$, akkor $a^n = b^{-n}$ miatt ugyancsak b^{k-n} mindkét oldal. Így beláttuk az állítást akkor, ha $m \leq 0$ és n tetszőleges. Az m és n szerepének megcserélésével azt az esetet is megkapjuk, amikor $n \leq 0$ és m tetszőleges.

2.2.22. 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 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.

2.2.26. 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.

2.2.28. 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 2.2.22. Feladatban bizonyított $u(-s) = -(us)$ összefüggésre is.

Megfordítva, tegyük föl, hogy az $u \neq 0$ 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, és az állítás megfordítása is igaz.

2.2.30. Ez pontosan ugyanaz a gondolatmenet, mint a 2.2.29. 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. A megfordítás nem igaz: az egész számok gyűrűjében a 2 nem bal oldali nullosztó, de nincsen balinverze.

2.2.32. 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, mert kihasználtuk 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 egy olyan algebrai állítás bizonyítására, ahol a számelméletet már nem alkalmazhatjuk (5.3.5. Tétel).

Belátjuk, hogy a $\mathbb{Z}_m$ gyűrű 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.

2.2.35. Ha a megadott halmaz egy gyűrűnek része, és a műveletek is „ugyanazok”, akkor elegendő a 2.2.26. Feladatban megadott tulajdonságokat ellenőrizni. Ezt nagyon sokszor használjuk majd az alábbiakban.

(1) Ez részteste $\mathbb{C}$-nek. Ennek ellenőrzéséhez 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 $z + w = (a + c) + (b + d)i$ és $zw = (ac - bd) + (ad + bc)i$ 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 hasonlít, azzal a kivétellel, hogy 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 $z\bar{z} = |z|^2$ összefüggés miatt azt kapjuk, hogy $(a^2 + b^2)(c^2 + d^2) = 1$. De mindkét tényező nemnegatív egész, és így szorzatuk csak úgy lehet 1, ha mindkettő 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: 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 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 föl 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 3.5.18. 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 könnyű belátni, 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 föl 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.

2.2.36. 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, 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 2.4.29. Feladatban látni fogjuk, hogy nullosztómentes gyűrűben egy részgyűrű egységeleme csak az eredeti gyűrű egységeleme lehet.)

2.2.37. Az (1) – (4) állításokat a 2.2.20. Gyakorlatban már beláttuk (csak a művelet jele ott szorzás volt; a (4) állításban persze föl 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 nulla a 2.2.22. 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 a 2.2.22. Feladat segítségével az egyenlőség $n = -m$-re is adódik.

2.2.38. 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. Végül az $xa = b$ egyenlet egyetlen megoldása nyilván $x = b$, azaz a jobbosztás egyértelműen elvégezhető.

2.2.39. Az (1) igazolásához tegyük föl, hogy e bal oldali egységelem, és legyen $b \in S$. Ekkor b-nek van balinverze, vagyis olyan $c \in S$, hogy $cb = e$. A c elemnek is van balinverze, azaz olyan d, hogy $dc = e$. Ekkor $b = eb = (dc)b = d(cb) = de$, de innen $be = (de)e = d(ee) = de = b$. Mivel ez minden b-re igaz, beláttuk, hogy e jobb oldali egységelem is. Speciálisan $b = de = d$, tehát a b elemnek c kétoldali inverze.

A (2) megmutatásához legyen $b \in S$ tetszőleges elem, és jelölje e az $xb = b$ egyenlet (egyik) megoldását, azaz $eb = b$. Ha $c \in S$, akkor legyen f megoldása a $by = c$ egyenletnek, tehát $bf = c$. Ekkor $ec = e(bf) = (eb)f = bf = c$, azaz e bal oldali egységelem. Az $xb = e$ egyenlet megoldhatósága miatt S minden b elemének van e-re nézve balinverze. Az (1) állítás miatt tehát S csoport.

2.2.40. A $(\sqrt{2}-1)^n(\sqrt{2}+1)^n = 1$ összefüggésből látszik, hogy $\sqrt{2}+1$ minden hatványa invertálható. Ez végtelen sok különböző szám, mert $\sqrt{2}+1 > 1$.

2.2.41. 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.

2.2.42. 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 $k = 0$, 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.

2.2.43. Csak a (3)-beli leképezés nem művelettartó.

(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 $+_{100}$, 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 meggondolni, hogy tetszőleges gyűrűben a $\varphi(x) = nx$ leképezés minden n egészre tartja az összeadást (a 2.2.37. Gyakorlat miatt).

2.2.44. 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 $e_2 = \varphi(e_1)$.

♫ Az előző bekezdésbeli bizonyítás úgy is elmondható, hogy $e_1 g = g$ miatt $\varphi(e_1)\varphi(g) = \varphi(g)$, ahonnan $\varphi(g)$-vel egyszerűsítve $e_2 = \varphi(e_1)$. Mi itt a g? A G_1 csoport tetszőleges eleme. Van-e ilyen g? Van, mert tudjuk, hogy egy csoport nem lehet üres, ha mást nem is, az egységelemet biztosan tartalmazza. De akkor a legegyszerűbb, ha g-t eleve e_1-nek választjuk, így kapjuk az előző bekezdésbeli bizonyítást.

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.)

2.2.45. Bár a feladat szempontjából ez nem lényeges, a 2.2.35. Gyakorlat szerint itt tényleg két testről van szó. Legyen $\varphi : T \to S$ kölcsönösen egyértelmű művelettartó leképezés. Az előző 2.2.44. 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.

2.2.46. 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 veszünk (és akkor a többi $n-j$ zárójelből a-t vesszük ki). Az E.2.2. Tétel szerint ez $\binom{n}{j}$-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 2.2.19. Definíció utáni megjegyzéseket).

2.3. A polinomok alaptulajdonságai

2.3.4. Legyen $f(x) = \sum_{i=0}^{n} a_i x_i$, $g(x) = \sum_{i=0}^{m} b_i x_i$, $h(x) = \sum_{i=0}^{\ell} c_i x_i$. 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. Az $f\big(g(x)\big)$ nyilván polinom. Ha $f(x) = a_0 + \ldots + a_n x^n$ foka n, akkor $a_i \neq 0$ esetén $a_i\, p(x)^i$ foka $i\,\mathrm{gr}(p)$ (hiszen a 2.3.2. Tétel szerint szorzat foka a fokok összege). Ezek $\mathrm{gr}(p) \neq 0$ esetén csupa különböző fokú polinomok, és ezért az összegük, vagyis $f\big(g(x)\big)$ foka e fokok maximuma, vagyis $n\mathrm{gr}(p)$ lesz. Ha g konstans, akkor persze $f\big(g(x)\big)$ is konstans, és vagy nulladfokú, vagy a nullapolinom.

2.3.7. 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.

2.3.8. Jelölje fölülvonás, azaz $\overline{a}$ az a egész szám maradékát mod m. Legyen $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ és $h(x) = c_0 + c_1 x + \ldots + c_\ell x^\ell$. 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

$$\overline{a_0 c_k + \ldots + a_k c_0}\,.$$

Ez a két együttható tényleg egyenlő, hiszen a fölülvonás leképezés összeg- és szorzattartó (1.1.6. Állítás). Beláttuk tehát, hogy $\overline{f}\ \overline{h} = \overline{fh}$. Hasonlóan, de egyszerűbb számolással igazolható, hogy $\overline{f} + \overline{h} = \overline{f+h}$.

2.3.9. 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 $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ és $g(x) = c_0 + c_1 x + \ldots + c_n x^n$. Ekkor

$$(f+g)^*(b) = (a_0 + c_0) + (a_1 + c_1)b + \ldots + (a_n + c_n)b^n\,,$$

és

$$f^*(b) + g^*(b) = (a_0 + a_1 b + \ldots + a_n b^n) + (c_0 + c_1 b + \ldots + c_n b^n)\,.$$

Ez a két összeg nyilván egyenlő. Hasonlóan igazolható az $(fg)^*(b) = f^*(b)g^*(b)$ összefüggés is, bár a számolás picit bonyolultabb.

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-elrendezésből 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 $f^*(b)=B$ adódik (hiszen $x-b$ nullává válik).

2.4.8. Mivel egy gyöktényező főegyütthatója 1, és az egységelem egyetlen gyűrűben sem 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 nullapolinom a 2.4.7. Tétel miatt. Ezért f a konstans c polinom.

2.4.12.

(1) Ezekből (egyszerre) kiemelhető az $n-1$ darab $(x-a_i)$ gyöktényező mindegyike, ahol $i\neq j$. Mivel a polinom $n-1$-edfokú, már csak egy konstans szorzó maradhat.

(2) Az a_j-t behelyettesítve e konstans értékét meghatározhatjuk. Az eredmény:

$$f_j(x)=\frac{(x-a_1)\ldots(x-a_{j-1})(x-a_{j+1})\ldots(x-a_n)}{(a_j-a_1)\ldots(a_j-a_{j-1})(a_j-a_{j+1})\ldots(a_j-a_n)}\,.$$

Ez a *Lagrange-féle alappolinom* tényleg $n-1$-edfokú.

(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 $i\neq j$), a megmaradó tag pedig $b_jf_j(a_j)=b_j$ lesz, hiszen $f_j(a_j)=1$. Az f nyilván legfeljebb $n-1$-edfokú (lehet nulla is).

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. Az eredmény $(1/2)x^3-(3/2)x^2+x+3$ (bármelyik interpolációval).

2.4.15. 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 $f(x)=(x-2)(x^5+2x^4+x^2+x+2)+8$.

2.4.16. Az (1) esetben a j-edik tag kiszámításához j darab szorzás, összesen $(n^2+n)/2$ szorzás kell. A (2) esetben b^n értékét $n-1$ szorzással számíthatjuk ki, és menet közben a b^j hatványokat is megkapjuk. Ezeket felhasználva még n szorzás, összesen $2n-1$ szorzás történik. Végül a Horner-elrendezést használva összesen n-szer kell szorozni.

2.4.17. Ha $f(x)=a_nx^n+\ldots+a_0$, 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. Ha f egész együtthatós,

akkor akár a fentiekből, akár a 2.4.6. Állításból adódik, hogy $f(x) - f^*(b) = (x-b)g(x)$, ahol g egész együtthatós. Innen $x = a$ helyettesítéssel a kívánt oszthatóságot kapjuk.

2.4.18. Az Útmutatóbeli 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 $x = b$ helyettesítéssel $d_0 = 0$ adódik. Mivel $R[x]$ 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.

2.4.19. Pontosan akkor, ha m összetett szám. Ha $m = ab$, ahol $1 < a, b < m$, akkor az ax elsőfokú polinomnak (legalább) két gyöke van: a 0 és a b. Ha m prím, akkor $\mathbb{Z}_m$ nullosztómentes (2.2.31. Állítás), és így a 2.4.7. Tétel miatt minden polinomnak legfeljebb annyi gyöke van, mint a foka.

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 (2.4.17. Gyakorlat), akár g-t $(x-10)h(x) + 10$ alakban fölírva 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. Az Útmutatóban készített $g(x) = f(x) - cx^k(x-a_1)\ldots(x-a_n)$ polinom is egész együtthatós, és az $a_1, \ldots, a_n$ helyeken ugyanazokat az értékeket veszi fel, mint f. Mivel a kivonásnál f főegyütthatója kiesik, g foka alacsonyabb, mint f foka. Ez az ellentmondás bizonyítja az állítást.

2.4.22. 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 f 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".

2.4.23. Az Útmutatóbeli utolsó állítás világos: mivel $g(x)$ egész együtthatós, ezért a 2.4.17. Gyakorlat miatt $g(x+km) - g(x)$ osztható $x + km - x = km$-mel, és ez m-mel osztva is egész szám. De alkalmas k-ra $x + km > r$, azaz $f(x+km)$ egész a feltevés szerint, és így $f(x)$ is az.

2.4.24. Legyen az $n+1$ egymás utáni hely $b, b+1, \ldots, b+n$. Ha f-et ezen az $n+1$ helyen interpoláljuk, akkor magát f-et kapjuk az interpoláció egyértelműsége miatt, hiszen f csak n-edfokú. Írjuk föl $0 \le j \le n$

esetén a j-edik Lagrange-féle interpolációs alappolinomot ezekre a helyekre (2.4.12. Gyakorlat). Ennek nevezője $(-1)^j\, j!(n-j)!$, ami osztója $n!$-nak, hiszen az $\binom{n}{j}$ binomiális együtthatónak $j!(n-j)!$ a nevezője. Ezért $n!\,f(x)$ egész együtthatós.

Az állítást n szerinti indukcióval igazoljuk, tegyük föl, hogy az n-nél kisebb fokú polinomokra igaz. Legyen f főtagja $(c/n!)x^n$, az előzőek szerint c egész szám. Ha

$$g(x) = f(x) - c\binom{x}{n},$$

akkor a kivonásnál $(c/n!)x^n$ kiesik, és így g legfeljebb $n-1$-edfokú (esetleg a nullapolinom, de akkor készen vagyunk). A g polinom is egész értéket vesz föl a $b, b+1, \ldots, b+n$ helyeken, és így az indukciós feltevés miatt a kívánt alakban írható. Így az f keresett felírását kapjuk.

2.4.25. A 2.4.24. Feladat szerint a g polinomot kereshetjük

$$g(x) = c_{10}\binom{x}{10} + \ldots + c_0\binom{x}{0}$$

alakban. Az $x = 0$ értéket behelyettesítve $c_0 = g(0) = 1$. Ezt tudva $x = 1$-et helyettesítve $c_1 = 1$, és így tovább, valamennyi c_j-re 1 adódik.

Ehelyett persze némi kísérletezéssel is megsejthetjük, hogy

$$g(x) = \binom{x}{0} + \binom{x}{1} + \ldots + \binom{x}{10}$$

megfelelő polinom lesz. Ugyanis a binomiális tételt az $(1+1)^j$ összegre alkalmazva $g(j) = 2^j$ ha $0 \le j \le 10$, azaz g megfelel a feltételeknek, és mivel foka legfeljebb 10, az interpolációs polinom egyértelműsége (igazából a 2.4.10. Következmény) miatt ez a legalacsonyabb fokú ilyen polinom. Az $(1+1)^{11}$ összeget kifejtve kapjuk, hogy $g(11) = 2^{11} - 1 = 2047$.

2.4.26. Az $f(x)-5$ polinomnak négy, páronként különböző egész gyöke van, és ezért ez a polinom fölírható $(x-a)(x-b)(x-c)(x-d)q(x)$ alakban, ahol $a, b, c, d \in \mathbb{Z}$ és $q(x) \in \mathbb{Z}[x]$. Ha $f(n) = 12$, akkor tehát $(n-a)(n-b)(n-c)(n-d)q(n) = 7$. Ez lehetetlen, mert a 7 prímszám, és az $n-a, n-b, n-c, n-d$ különböző egész számok közül legfeljebb egy lehet 1 és egy másik -1.

2.4.27. Legyen $0 \neq r \in R$. 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.

2.4.28. 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 gyűrű 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.

2.4.29. Álljon S azokból a függvényekből, melyeknek a 2 szám gyöke. Ez a 2.2.26. 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 (2.2.28. Gyakorlat) miatt innen $e = f$.

2.4.30. Az állítás a 2.4.2. Gyakorlat bizonyos értelemben vett általánosítása. A szorzattartást egy konkrét példán vizsgáljuk meg. Legyen $f(x) = a + bx$ és $g(x) = c + dx$. Ekkor

$$f(x)g(x) = (a+bx)(c+dx) = ac + (ad+bc)x + bdx^2\,.$$

Ezért azt kell belátni, hogy az S gyűrűben

$$(ae+bs)(ce+ds) = ace + (ad+bc)s + bds^2\,.$$

A bal oldalon a szorzást elvégezve a disztributivitás miatt

$$aece + aeds + bsce + bsds$$

adódik. A 2.2.37. Gyakorlat (5) pontja szerint $r(ns) = n(rs)$ tetszőleges gyűrűben teljesül, ahol r és s gyűrűelemek, n pedig egész szám. Ezért a fenti összeg $ace^2 + ades + bcse + bds^2$ alakban írható. Mivel e egységelem, a kívánt eredményt kapjuk. Az általános számolás ugyanígy működik, csak a képletek bonyolultabbak, a részletek kidolgozását az Olvasóra hagyjuk. Fontos észrevenni, hogy s hatványai egymással és az egységelemmel is fölcserélhetők. Valójában pontosan azért definiáltuk a polinomok között műveleteket azon a módon, ahogy definiáltuk, hogy a behelyettesítés homomorfizmus legyen.

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 kiszámításához használjuk föl, hogy szorzat 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 föl, 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 2.2.28. Gyakorlat szerint. Ha $k < m$, akkor tehát $g(x) = (x-b)^{m-k} h(x)$ 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 föl:

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

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 1.5.14 (2) (sőt az 1.2.9.) Gyakorlatban, az eredmény $\pm1\pm i$ 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 kiemelésekor kapott 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	$\boxed{0}$
1	1	1	1	$\boxed{0}$	
1	1	2	$\boxed{3}$		

$$x^4-x^3-x+1=$$
$$=(x-1)(x^3-1)=$$
$$=(x-1)^2(x^2+x+1)\,.$$

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 végül is

$$x_1^2 + \ldots + x_n^2 = \sigma_1^2 - 2\sigma_2 \quad (\text{ha } n \geq 2).$$

Ezt az összefüggést általánosítjuk majd a 2.7.8. Tételben.

2.5.14. A gyökök és együtthatók összefüggése (2.5.9. Következmény) szerint 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

$$\begin{aligned}
\sigma_1 &= b_1 + b_2 + b_3 + b_4 = (-1)^1 a_3/a_4 = 0\,,\\
\sigma_2 &= b_1b_2 + b_1b_3 + b_1b_4 + b_2b_3 + b_2b_4 + b_3b_4 = (-1)^2 a_2/a_4 = 0\,,\\
\sigma_3 &= b_1b_2b_3 + b_1b_2b_4 + b_1b_3b_4 + b_2b_3b_4 = (-1)^3 a_1/a_4 = -1\,,\\
\sigma_4 &= b_1b_2b_3b_4 = (-1)^4 a_0/a_4 = 3/2\,.
\end{aligned}$$

Tehát a gyökök összege nulla, szorzata $3/2$, négyzetösszege a 2.5.13. Feladat 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 föl 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 polinom gyökei reciprokainak összegét tehát a g polinomból mint a gyökök összegét olvashatjuk le.

2.5.15. Az $x^n - 1$ polinom gyökei pontosan az n-edik egységgyökök. Ilyenből n darab van (1.5.4. Tétel), és ezek a 2.4.7. Tétel miatt egyszerre is kiemelhetők. Mivel $x^n - 1$ foka n, egy konstans polinom „marad", ami az $x^n - 1$ főegyütthatója, vagyis 1 (lásd 2.5.1. Gyakorlat). Ezért valóban

$$x^n - 1 = (x - \varepsilon_1)\ldots(x - \varepsilon_n)\,.$$

Speciálisan $x^4 - 1 = (x-1)(x-i)(x+1)(x+i)$.

Az n-edik egységgyökök összegét, szorzatát és négyzetösszegét már meghatároztuk az 1.5.22. Gyakorlatban, a mostani eszköztárunk azonban gyorsabb megoldást kínál. Az $\varepsilon_1 \ldots \varepsilon_n$ 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

$$\varepsilon_1 \ldots \varepsilon_n = \sigma_n(\varepsilon_1, \ldots \varepsilon_n) = (-1)^n a_0/a_n = (-1)^n \cdot (-1)/1 = (-1)^{n+1}$$

(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:

$$\varepsilon_1 + \ldots + \varepsilon_n = \sigma_1(\varepsilon_1, \ldots \varepsilon_n) = (-1)^1 a_{n-1}/a_n.$$

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. Feladatot használjuk föl. Az $x^n - 1$ polinomban az x^{n-2}-es tag a_{n-2} együtthatója nulla ha $n > 2$, ezért $\sigma_2(\varepsilon_1, \ldots \varepsilon_n)$ 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 (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 (1.4.7. 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 2.2.28. Gyakorlat 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 sémája 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 fölött 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. A 2.5.13. Feladatból kapjuk, hogy $2(ab + ac + bc) = (a + b + c)^2 - (a^2 + b^2 + c^2) = 4$. Legyen $f(x) = (x-a)(x-b)(x-c)$, ekkor a gyökök és együtthatók összefüggése miatt $f(x) = x^3 - 3x^2 + 2x + q$. Ide a, b, c-t helyettesítve, majd összeadva $7 - 3 \cdot 5 + 2 \cdot 3 + 3q = 0$ adódik, azaz $q = 2/3$ (ez mellesleg $-abc$-vel egyenlő). Az $af(a) + bf(b) + cf(c) = 0$ összefüggésből $(a^4 + b^4 + c^4) - 3 \cdot 7 + 2 \cdot 5 + q \cdot 3 = 0$, ahonnan $a^4 + b^4 + c^4 = 9$. Hasonlóan $a^5 + b^5 + c^5 = 29/3$ és $a^6 + b^6 + c^6 = 19/3$. Ilyen a, b, c számok léteznek: megfelelnek az $x^3 - 3x^2 + 2x + 2/3$ polinom (komplex) gyökei. Ezt ellenőrizhetjük a gyökök és együtthatók összefüggése alapján, a fenti számolások megfordításával. (A gyökök közelítőleg $-0{,}24$ és $1{,}62 \pm 0{,}39i$.)

2.5.17. 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).

Megjegyezzük, hogy nemcsak a $\mathbb{Z}_2$, hanem bármely véges test fölött találhatunk hasonló példát. Valóban, lesz olyan $n \neq m$, hogy az x^n és x^m polinomokhoz ugyanaz a polinomfüggvény tartozik (hiszen véges testben csak véges sok polinomfüggvény lehetséges). Ezért nincs olyan véges test, ahol minden polinomfüggvény meghatározza a gyökök multiplicitását.

2.5.18. 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 föl, 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:

$$\begin{aligned} p_5 &= ix_1x_2x_3x_4^2 - x_1^2x_3^3 + 2x_1^2x_2x_3x_4 - 6x_1^2x_2^2x_4 - x_1^2x_2^2x_3 + \pi x_1^2x_2^3\,,\\ p_4 &= 3x_1^3x_2\,,\\ p_1 &= x_4\,; \end{aligned}$$

itt p_5 tagjai már lexikografikusan növő sorrendben vannak fölírva. A p polinom főtagja $3x_1^3x_2$, ezért p^7 főtagja $3^7x_1^{21}x_2^7$. Viszont p^7 foka $7\cdot 5 = 35$, 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 $f \in R[x_1,\dots,x_n]$. 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 $\mathbf{b}=(b_1,\dots,b_n)$-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).

Mivel definíció szerint $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$, ezért tetszőleges n-határozatlanú polinom

$$f = g_0 + g_1 x_n + \ldots + g_k x_n^k$$

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

$$f(\mathbf{b}) = a_0 + a_1 b_n + \ldots + a_k b_n^k .$$

A gyakorlat többi állítását is a fenti módon, n szerinti indukcióval igazolhatjuk. Amikor a 2.4.30. Gyakorlatot általánosítjuk, akkor vigyáznunk kell: az állítás csak kommutatív S gyűrű esetében marad érvényben (de legalábbis a behelyettesítendő elemeknek páronként fölcserélhetőknek kell lenniük).

2.6.10. Bizonyítsunk n szerinti indukcióval. Egyváltozós polinomokra tudjuk az állítást a polinomok azonossági tétele 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

$$f = g_0 + g_1 x_n + \ldots + g_m x_n^m ,$$

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 $n = 0$ 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. Az Útmutatóbeli jelöléseket alkalmazzuk, k szerinti indukciót alkalmazunk. Egy pont esetében nyilván jól interpolál egy konstans polinom. Tegyük föl, hogy van olyan f, ami már az első $k-1$ helyen a megadott értéket veszi föl. Ha találunk olyan g polinomot, amelyre $g(\mathbf{a}^j) = 0$, ha $1 \le j \le k-1$, 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, $\mathbf{a}^k = (a_1^k, \ldots, a_n^k)$ és $\mathbf{a}^j = (a_1^j, \ldots, a_n^j)$ sem egyenlő, azaz valamelyik koordinátájuk különbözik. Jelölje a(z egyik) megfelelő indexet $u(j)$, tehát akkor tudjuk, hogy $a^j_{u(j)} \neq a^k_{u(j)}$. 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 föl, hogy $m_1 \ge m_2 \ge \ldots \ge m_n$ 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 $H(\sigma_1, \sigma_2, \sigma_3)$ összes tagját kiszámolni túl 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 $y_1 y_3^3$-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 világos, hogy az $s_i(x_1, \ldots, x_n)$ hatványösszegbe x_n helyére nullát helyettesítve 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 az $n = 4$ speciális esetben közös nevezőre hozással már a 2.5.14. Gyakorlatban láttuk). 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 $x_i^2x_j$ (ahol $i \neq j$) háromszor (úgy, mint $x_ix_ix_j$, $x_ix_jx_i$, $x_jx_ix_i$), végük az $x_ix_jx_k$ (ahol az i, j, k páronként különböző) hatszor (az indexeknek ugyanis hatféle lehetséges sorrendje van). De az $x_i^2x_j$ 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:

$$s_3 - \sigma_1s_2 + \sigma_2s_1 - 3\sigma_3 = 0\,.$$

Nyilván $s_1 = \sigma_1$, továbbá a Newton–Girard-formulákból (vagy a 2.5.13. Feladatból) $s_2 = \sigma_1^2 - 2\sigma_2$. 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 $a+b+c = 0$, $ab+ac+bc = 3$, és $abc = -1$. Ezért $a^2b^2c^2 = (abc)^2 = 1$, 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 $-2abc(a+b+c)=0$. 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 $k_1+2k_2+\ldots+nk_n$. 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 $k_1+2k_2+\ldots+nk_n=k$, és így f tényleg fölírható 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 $k_1+k_2+\ldots+k_n$, ezért minden levont tagra fenn kell álljon a $k_1+k_2+\ldots+k_n\le m$ egyenlőtlenség is.

A most kapott képletek behatárolják, hogy egy adott f fölírásakor 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 fölírását az elemi szimmetrikus polinomokkal.

Ekkor $m=3=k$, és így $k_1+2k_2+\ldots+nk_n=3$ (és $k_1+\ldots+k_n\le 3$, de ez kevesebbet mond ebben az esetben, mint az előző feltétel). Mivel mindegyik k_i egész szám, látjuk, hogy $k_4=\ldots=k_n=0$, 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 meghatározhatjuk alkalmas helyettesítésekkel. 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 $2=2b+8$, 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 $a=3$.

2.7.18. Az Útmutatóban bevezetett jelöléseket használjuk. Az f_N együtthatói a $b_1,\dots,b_n$-eknek *egész együtthatós* szimmetrikus polinomjai. Ezért ezek fölírhatók az elemi szimmetrikus polinomok *egész együtthatós* polinomjaként. Mivel f normált és egész együtthatós, a $b_1,\dots,b_n$ elemi szimmetrikus polinomjainak az értékei egész számok. Ezeket egész együtthatós polinomba helyettesítve egész számot kapunk, és így f_N tényleg egész együtthatós.

Az f_N együtthatóit a háromszög-egyenlőtlenség (1.4.3. Tétel) segítségével becsülhetjük meg. Mindegyik együttható a $b_1^N,\dots,b_n^N$ elemi szimmetrikus polinomja, azaz egy legfeljebb 2^n tagú összeg, amelyben minden tag abszolút értéke 1. Ezért $f_N(x)$ minden együtthatója abszolút értékben legfeljebb 2^n.

Mivel n rögzített szám, ez összesen csak véges sokféle polinom lehet, és ezeknek összesen is csak véges sok gyökük van. A b_j^N lehetséges értékei e véges sok gyök közül kerülnek ki (miközben N befutja a pozitív egészeket). Tehát mindegyik b_j-nek csak véges sok pozitív kitevőjű hatványa van. Mivel $b_j\ne 0$ (hiszen abszolút értéke 1), ezért b_j egységgyök (különben minden hatványa különböző lenne az 1.5.8. Tétel miatt).

2.7.19. Jelölje x_1 kitevőjét P_i-ben m_i. Mivel $P_{i+1}\prec P_i$, ezért $m_{i+1}\le m_i$. Vagyis az $m_1,m_2,\dots$ sorozat monoton fogyó, és mivel nemnegatív egészekből áll, van olyan k, hogy onnantól kezdve egy állandó m értéket vesz föl. Dobjuk el az első $k-1$ darab P_i polinomot. Ezzel feltehetjük, hogy mindegyik P_i-ben az x_1 kitevője ugyanaz az m szám.

Ha ezt tudjuk, akkor $P_{i+1}\prec P_i$ miatt az x_2 kitevőinek sorozata is monoton fogy. Ez ismét stabilizálódik, és véges sok P_i kidobásával elérhetjük, hogy már x_2 kitevője is minden P_i polinomban ugyanaz a szám

legyen (ez persze nem feltétlenül egyenlő az x_1-nek az m kitevőjével). Az eljárást folytatva azt kapjuk, hogy mindegyik x_j kitevője mindegyik megmaradt P_i polinomban ugyanaz (vagyis nem függ i-tól). De akkor a megmaradó P_i polinomok már csak egy R-beli együtthatóban különbözhetnek, ami ellentmond annak, hogy $P_i \succ P_{i+1}$ minden i-re.

3. fejezet

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 úgy, hogy az egyik tényezőt egy nem nulla konstanssal megszorozzuk, a másikat pedig ugyanezzel elosztjuk. De $\mathbb{Z}_2$ egyetlen nem nulla eleme az 1, és így ezen a módon 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. Azaz $x^2+1=1(x^2+1)=2(2x^2+2)$.

3.1.4. Mintabizonyításként a (3) állítást mutatjuk meg. 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 $r\mid t$.

A többi állítás hasonlóan igazolható. A (2) utolsó állításánál föl kell használni, hogy nullosztómentes gyűrűben minden nem nulla elemmel szabad egyszerűsíteni (2.2.28. Gyakorlat).

3.1.5. Ha $0\mid s$, akkor van olyan $a\in R$, melyre $a\cdot 0=s$. De (a 2.2.22. Feladat 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. Legyen R egységelemes, kommutatív gyűrű. Ekkor 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 $g(x)=b_0+\ldots+b_nx^n\in R[x]$, melyre

$$f(x)=rg(x)=rb_0+\ldots+rb_nx^n\,.$$

Tehát f minden együtthatója r-nek többszöröse. Az állítás megfordításának igazolásához tegyük föl, hogy $f(x)=a_0+\ldots+a_nx^n$ minden együtthatója r-rel osztható. Ekkor $a_j=rb_j$ alkalmas $b_0,\ldots,b_n\in R$ elemekre. Így

$$f(x)=r(b_0+\ldots+b_nx^n)\,,$$

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).

3.1.17. Pozitív egész számok esetében két felbonthatatlan akkor és csak akkor asszociált, ha egyenlő. Így minden pozitív egész fölírható kanonikus alakban úgy is, hogy nem szerepel egységtényező: az egyenlő felbonthatatlanokat összevonjuk. Speciálisan az 1 üres szorzatként írható (2.2.42. 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.

3.1.18. A kanonikus alak egyértelműsége precízen a következőt jelenti. Tegyük föl, 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 $\alpha_i = \beta_j = \alpha$.

3.1.20. Tegyük föl, 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 $u \sim v$.

3.1.21. 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 $r \mid 0$. Így $(0, 0) = 0$. Ha $(r, s) = 0$, akkor $0 \mid r$, tehát $r = 0$, és hasonlóan $s = 0$.

3.1.22. 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 fölírható

$$r = ep_1^{\alpha_1} \dots p_m^{\alpha_m} \quad \text{és} \quad s = fp_1^{\beta_1} \dots p_m^{\beta_m}$$

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 fölírható $t = gp_1^{\gamma_1} \dots p_m^{\gamma_m}$ 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 a pozitív egészek esetében), 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 fölírható $v = gp_1^{\gamma_1} \dots p_m^{\gamma_m}$ 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 3.1.20. 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.

3.1.24. Tegyük föl, 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, ezért $(r, s)t \sim t$. Másfelől viszont r közös osztója rt-nek és st-nek, vagyis $r \mid (rt, st) \sim (r, s)t \sim t$. Tehát tényleg $r \mid t$.

3.1.26. 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 föl, 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.

♫ A gyakorlat második állítása a 3.1.27. Gyakorlatból is adódik, hiszen alaptételes gyűrűben bármely két elemnek van kitüntetett közös osztója (3.1.22. Gyakorlat). Hasznos azonban, ha az Olvasó megismer egy közvetlen bizonyítást is, most ez következik. Ugyanígy érdemes megpróbálkozni a 3.1.23. Tétel közvetlen bizonyításával alaptételes gyűrűk esetén.

Legyen R alaptételes gyűrű, és p felbonthatatlan eleme R-nek. Ekkor p nem nulla és nem egység, meg kell mutatni, hogy prímtulajdonságú. Tegyük föl, 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 fölírhatjuk felbonthatatlanok szorzataként. Legyen $r = p_1 \dots p_m$, $s = q_1 \dots q_n$ és $t = z_1 \dots z_k$. Ekkor

$$pz_1 \dots z_k = pt = rs = p_1 \dots p_m q_1 \dots q_n .$$

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.

3.1.27. Legyen p felbonthatatlan elem. Ekkor p nem nulla, nem egység, és mindegyik osztója vagy egység, vagy p-nek asszociáltja. Tegyük föl, 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) csak egység lehet. A 3.1.24. Gyakorlat szerint tehát $p \mid s$.

3.1.28. Tegyük föl, 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 tényezőnek. 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. 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 3.2.19. Gyakorlatot is).

3.1.30. Ez a gyakorlat azt járja körül, hogy a felbonthatatlan illetve prím elemek definíciójában (3.1.13, illetve 3.1.25) mennyire volt szükséges külön kikötni, hogy a szóban forgó 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.

3.1.31. Ismét a 3.1.22. 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.

3.1.32. Tudjuk a 2.2.35. (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 végül is 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 az [1] könyv 7.4. és 7.5. szakaszában ismerkedhet meg.

3.1.33. 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 $rx = r$. Innen $rxs = rs$, majd r-rel egyszerűsítve $xs = s$ teljesül minden $s \in R$ esetén, azaz x egységeleme R-nek. (Ez a gondolatmenet a későbbi 5.3.4. Lemma bizonyítása.)

Ha tehát $e \in R$ minden elemnek osztója, akkor $e \mid e$ miatt R egységelemes, kivéve ha $e = 0$, amikor a 2.2.22. 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 osztható néggyel. Megfordítva, ha egy nem nulla szám néggyel osztható $\mathbb{Z}$-ben, vagyis $4k$ alakú, akkor $2(2k)$ a páros számok körében készített (egyik) 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, 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.

3.1.34. 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 3.1.32. Gyakorlat mintájára járunk el. Tegyük föl, 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. Ezzel (1)-et beláttuk, és azt is, hogy 3 osztói csak ± 1 és ± 3.

A (2) esetében a válasz nemleges. Tegyük föl ugyanis, hogy $d \in R$ kitüntetett közös osztója 9-nek és $3(2 + i\sqrt{5})$-nek. Mivel 3 közös osztója e két számnak, $3 \mid d$, azaz $d = 3r$ alkalmas $r \in R$ elemre. Hasonlóképpen $2 + i\sqrt{5} \mid d$ is teljesül. Mivel $d \mid 9$, ezért $r \mid 3$. Az előzőek szerint $r = \pm 1$ vagy $r = \pm 3$.

Mindkettő lehetetlen, az $r = \pm 1$ azért, mert akkor $d = \pm 3$, és ennek $2 + i\sqrt{5}$ nem osztója, az $r = \pm 3$ pedig azért, mert akkor $d = \pm 9$, ami nem osztója $3(2 + i\sqrt{5})$-nek.

3.1.35. 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 csupa legalább negyedfokú tag szerepel, továbbá olyan másodfokú tagok konstansszorosai, amelyek valamelyik tényezőnek is tagjai. Így xy nem szerepelhet a szorzatban, és ezért a megadott halmaz zárt a szorzásra. A 2.2.26. Feladat miatt tehát R tényleg részgyűrű. Az R egységelemes, hiszen $1 \in R$, és mivel $\mathbb{R}[x, y]$ szokásos gyűrű, R is nullosztómentes és kommutatív.

Belátjuk, hogy az x^3y^2 és az x^2y^3 polinomoknak nincs R-ben kitüntetett közös osztója. Az x^3y^2 osztói $\mathbb{R}[x, y]$-ban nyilván az $x^n y^m$ (valós) konstansszorosai, ahol $n \leq 3$ és $m \leq 2$. Az R-ben ezek közül például x^2y nem osztó, mert $(x^3y^2)/(x^2y) = xy \notin R$. Vagyis x^3y^2 osztói R-ben (konstansszoros erejéig) 1, x^2, x^3, y^2, xy^2, x^3y^2. Hasonlóan fölírhatjuk x^2y^3 osztóit is, a közösek 1, x^2, y^2 (konstansszorosai). Ezek között pedig nincs olyan, ami a többinek többszöröse lenne.

3.1.36. Azt, hogy R szokásos gyűrű, ugyanúgy bizonyíthatjuk be, mint ahogy $\mathbb{R}[x]$-ről megmutattuk, hogy szokásos gyűrű: itt is igaz lesz, hogy a főtagok szorzata a szorzat főtagja. Belátjuk, hogy x-nek minden osztója cx^r alakú, ahol $c \in \mathbb{R}$, és $0 \leq r \leq 1$ 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 $r' \leq r$ és $s' \leq s$ 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 fölírható $cx^{r/2}$ 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 91. 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 föl, 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 helyettesítjük 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 fölírva 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 3.2.17. 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 3.2.7. Tétel bizonyítását érdemes követni.

3.2.4. A 2 konstans polinom osztói $\mathbb{Z}[x]$-ben csak ± 1 és ± 2 (mert 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. Ugyanakkor 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.

3.2.5. Ha f és g valamelyike nulla, akkor a kitüntetett közös osztójuk a másik lesz. 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, $r_1 = 0$ (azaz $g \mid f$), akkor a kitüntetett közös osztó g lesz. Ez persze nem látszik ránézésre, csak ha az osztást elvégezzük.

♫ 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.

3.2.6. 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.

3.2.8. 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. 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 többszörösei 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.

Az 1.5.8. 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).

3.2.11. 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 egység.

3.2.13. A 3.2.3. Gyakorlat (vagy a 3.2.7. Tétel) szerint egy T test fölötti $T[x]$ polinomgyűrűben bármely két f és g polinomnak van kitüntetett közös osztója. 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.

3.2.14. Tegyük föl, hogy van olyan nem konstans polinom $T[x]$-ben, amely nem bontható föl irreducibilisek szorzatára. Válasszunk ezek közül egy minimális fokszámú f polinomot. A minimalitás azt jelenti, hogy az f-nél kisebb fokú nem konstans 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.

3.2.16. A hányados $x/2 - 1/2$, a maradék $(5/2)x - (7/2)$.

3.2.17. 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

$$x - 1 = (-x)(x^5 - 1) + (1 + x^3)(x^3 - 1) .$$

Az általános eljárást a 3.2.3. Gyakorlat megoldásában írtuk le.

3.2.18. Nem végezhető el. Az osztónak, vagyis a 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).

3.2.19. 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. A megfordítás nyilvánvaló.

3.2.20. A lényeg 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.

3.2.21. A 3.2.6. Gyakorlat szerint mindegy, hogy az $(f, g) \in S[x]$ kitüntetett közös osztót $T[x]$-ben, vagy $S[x]$-ben számítjuk-e ki. A $T[x]$-ben $x - b$ közös osztója f-nek és g-nek, ezért osztója a kitüntetett közös osztónak is. Vagyis (f, g) nem konstans polinom. De $(f, g) \mid g$ az $S[x]$-ben, és mivel g irreducibilis S fölött, az (f, g) vagy konstans, vagy g-nek asszociáltja (azaz konstansszorosa). Az előbbit kizártuk, az utóbbi esetben viszont $g \sim (f, g) \mid f$ miatt $g \mid f$.

3.2.22. 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.

3.2.23. Nulla lesz a maradék. Ha csak a maradékra vagyunk kíváncsiak, és az osztó 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 racionális számok, hiszen az $x^4 + x^2 + 1$ osztandó és az $x^2 + x + 1$ 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 $b = 0$.

Egy lehetséges általánosítás, hogy $x^4 + x^2 + 1$ helyett az $f(x) = x^{2n} + x^n + 1$ polinomot tekintjük. 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.

Másik megoldásként az $x^{2n} + x^n + 1 = (x^{3n} - 1)(x^n - 1)$ összefüggést felhasználva az $x^{2n} + x^n + 1$ polinomot gyöktényezőkre bonthatjuk $\mathbb{C}[x]$-ben. Ha $3 \nmid n$, akkor nyilván $x - \varepsilon_1$ és $x - \varepsilon_1$ is közöttük van, és egyszerre is kiemelhetők.

Harmadik megoldás: $x^4+x^2+1 = x^4+2x^2+1-x^2 = (x^2+1)^2-x^2 = (x^2+1+x)(x^2+1-x)$.

3.2.24. 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.

Erre a gyakorlatra is könnyen adhatunk második megoldást egyszerű azonos átalakításokkal.

3.2.25. Mivel f maradéka 2 az $x-1$-gyel osztva, ezért $f(1)=2$, a másik feltétel miatt pedig $f(2)=1$. Ha $f(x)=(x-1)(x-2)q(x)+(ax+b)$, akkor $x=1$ és $x=2$ helyettesítéssel $2=a+b$ és $1=2a+b$, ahonnan $ax+b=-x+3$.

3.2.26. 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 $k\le\ell$, 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 fölírva a kitüntetett közös osztó képletéből (3.1.22. Gyakorlat (3)) is ezt az eredményt kapjuk.

3.3. Gyökök és irreducibilitás

3.3.7. Az indukciónak azt a formáját alkalmaztuk, amit a 3.2.1. Tétel bizonyításában. Ha $\mathrm{gr}(f)=0$, akkor az indukciós feltevés üres. Ekkor z és $\overline{z}$ nem gyökei f-nek, ezt az esetet a bizonyítás elején intéztük el.

3.3.11. A polinomot (hacsak nem a nullapolinomról van szó) fölírhatjuk $g(x)x^k$ 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.

3.3.13. Az első három polinom esetében úgy érdemes eljárni, hogy a polinomot $\mathbb{C}$ fölött 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:

$$\begin{aligned} x^4-1 &= (x-1)(x+1)(x^2+1)\,,\\ x^4+1 &= (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)\,,\\ x^4+9 &= (x^2-\sqrt{6}x+3)(x^2+\sqrt{6}x+3)\,. \end{aligned}$$

Az $x^6-4x^3+3=0$ egyenlet az $y=x^3$ helyettesítéssel 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:

$$x^6-4x^3+3 = (x-1)(x^2+x+1)(x-\sqrt[3]{3})(x^2+\sqrt[3]{3}x+\sqrt[3]{9})\,.$$

3.3.14. Figyelnünk kell arra, hogy a felsorolt négy gyűrű fölött nemcsak az irreducibilis polinomok mások, hanem az egységek is. Ennek megfelelően egy $\mathbb{C}$ fölötti 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, tehát 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 $\mathbb{Z}$ fölötti felbontás:

$$2\cdot 3\cdot(x^2-2)\cdot(x^2+1)\,.$$

Ezt csak úgy variálhatjuk, hogy páros sok tényezőt -1-gyel beszorzunk.

3.3.15. Az x^n-1 kanonikus alakja $\mathbb{C}$ fölött $(x-\varepsilon_1)\dots(x-\varepsilon_n)$, ahol $\varepsilon_1,\dots,\varepsilon_n$ az n-edik egységgyökök (2.5.15. Feladat). Hasonlót mondhatunk x^m-1-ről is. A 3.1.22. Gyakorlat szerint tehát a keresett kitüntetett közös osztó a közös gyöktényezők szorzata, vagyis $x^{(n,m)}-1$ (1.5.21. Gyakorlat). Ugyanez az eredmény $\mathbb{Q}$ fölött is (3.2.6. Gyakorlat).

3.3.16. A 3.3.6. Lemma miatt a polinomnak $1-i$ is hatszoros gyöke, és ezért

$$(x-1-i)^6(x-1+i)^6g(x)=(x^2-2x+2)^6g(x)$$

alakban írható. Ez a szorzat akkor lesz tizenkettedfokú, ha $g(x)$ egy r konstans. Ez az r az eredeti polinom főegyütthatója, tehát valós. (Ez abból is következik, hogy mivel $(x^2-2x+2)^6$ valós együtthatós, $g(x)$ is az a 3.2.2. Állítás miatt.) Tehát a keresett polinomok pontosan az $r(x^2-2x+2)^6$ polinomok, ahol $r\neq0$ valós szám.

3.3.17. A racionális gyöktesztet alkalmazzuk (3.3.10. Tétel). Ha p/q racionális gyöke ennek a polinomnak, ahol p és q relatív prím egészek, akkor $p\mid5$ és $q\mid2$. 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

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

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).

3.3.18. Mivel $0<j<m$, az $f(x)+mx^j$-nek és az $f(x)$-nek ugyanaz a konstans tagja és a főegyütthatója. Ezért ha a racionális gyöktesztet az $f(x)+mx^j$ polinomra alkalmazzuk, akkor a p/q gyökjelöltek m-től függetlenül mindig ugyanazok, és a számuk $f(0)\neq0$ miatt véges. Minden egyes p/q gyökhöz legfeljebb egy m-érték tartozhat, hiszen $m(p/q)^j=-f(p/q)$ és $p/q\neq0$. Ezért tényleg csak véges sok m lesz megfelelő. Az viszont elérhető, hogy az 1 gyök legyen, azaz $m=-f(1)$ mindig megoldás.

3.3.19. Ha $c>0$, akkor $\mathbb{C}$ fölött gyöktényezős alakra bontva, a 3.3.13. 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 3.3.12. 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, azaz ha $c=4b^4$ alkalmas $b>0$ egészre.

Ha $c < 0$, akkor legyen $d = -c > 0$. Ebben az esetben, ismét a $\mathbb{C}$ fölötti 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.

3.3.20. Az előző gyakorlat alapján például $n^4 + 4 \cdot 16^m = (n^2 - 2^{m+1}n + 2^{2m+1})(n^2 + 2^{m+1}n + 2^{2m+1})$. Azt kell elérnünk, hogy ez a felbontás nemtriviális legyen. Ez $m \geq 1$ esetén így is van, mert a két tényező $(n \pm 2^m)^2 + 2^{2m} \geq 2^{2m} > 1$.

3.3.21. 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 pontosan 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 föl 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 36. 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.

3.3.22. 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 2.2.20. Gyakorlat (3) pontjában leírt tulajdonságát a többszörös fogalmára átalakítva). A binomiális tételből 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 2.2.46. Gyakorlatban fogalmaztunk meg.)

A most bizonyított állításból 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 $f(x) = a_0+a_1x+\dots+a_nx^n \in \mathbb{Z}_p[x]$, 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 $f(x^p)$.

3.3.23. A $\mathbb{Z}_2$ fölötti irreducibilitás vizsgálatához érdemes átfutni a 3.3.21. 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 $x^5+x+1 = (x^3+x^2+1)(x^2+x+1)$ 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 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 3.3.22. 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 $17-1 = 16$-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 végül is $x^4+1 = (x+2)(x-2)(x+8)(x-8)$.

x^8+1 az előzőek szerint $(x^2+2)(x^2-2)(x^2+8)(x^2-8)$. Ezért

$$x^8+1=(x+7)(x-7)(x+6)(x-6)(x+3)(x-3)(x+5)(x-5)$$

(mert itt is mindegyik négyzetgyökvonás elvégezhető).

$x^{17}+1=(x+1)^{17}$, 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.

3.3.24. Ez is hasonló a 3.3.12. 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 $\mathbb{R}$ fölötti felbontás irreducibilisek szorzatára.

A racionális gyökteszt segítségével megállapíthatjuk, hogy az x^4-10x^2+1 polinomnak nincs racionális gyöke (ennél számolósabb lenne 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 3.3.12. 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 egyik sem ad $\mathbb{Q}$ fölötti felbontást. A 3.3.12. Példa gondolatmenete szerint tehát x^4-10x^2+1 irreducibilis $\mathbb{Q}$ fölött.

A $\mathbb{Z}_5$ fölött a $\sqrt{6}$ 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 $\mathbb{Z}_5$ fölött, 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:

$$x^4-10x^2+1=(x^2-10x+1)(x^2+10x+1)\,.$$

Persze ezeket a felbontásokat némi ügyeskedéssel közvetlenül is megkaphatjuk, ha az együtthatókat picit megváltoztatjuk, például $\mathbb{Z}_5$ fölött $x^4-10x^2+1=x^4-4=(x^2+2)(x^2-2)$, de ez nem általános módszer.

♫ Aki ismeri számelméletből a kvadratikus maradékok elméletét (vagyis 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 mod p vizsgálata sokszor segít az irreducibilitás eldöntésében. A 111. oldalon található táblázatban szerepel több ilyen módszer is, de a fenti

polinom irreducibilitását egyik sem bizonyítja (például az eddigiek alapján könnyű belátni, hogy $x^4 - 10x^2 + 1$ egyik 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 föl, 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 fölcserélve 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. Az egységek az R egységei lesznek, mint konstans polinomok. Ezt a 3.1.11. Gyakorlat megoldásához hasonlóan igazolhatjuk, csak most azt kell felhasználnunk, hogy szorzásnál a fokszámok a többváltozós polinomok esetében is összeadódnak (2.6.3. Gyakorlat), és így nem konstans, azaz nullánál nagyobb fokú polinom nem lehet egység.

3.4.14. Az Útmutatóban leírt megoldásvázlat egyes lépéseihez fűzünk megjegyzéseket. A $\mathbb{C}[x_1, \ldots, x_n]$ polinomgyűrű a 3.4.12. Tétel szerint alaptételes, és az egységek a nem nulla konstans polinomok (3.4.13. Gyakorlat). Mivel minden komplex számból vonhatunk n-edik gyököt, ezért a $\mathbb{C}[x_1, \ldots, x_n]$-beli teljes n-edik hatványok asszociáltjai maguk is teljes n-edik hatványok: ha $b^n = c$, akkor $cq^n = (bq)^n$.

Ha $f^n + g^n = h^n$, de mondjuk f és g nem relatív prímek, hanem van egy közös p prímosztójuk, akkor $p \mid h^n$, azaz $p \mid h$. Az egyenletet p^n-nel egyszerűsítve ismét megoldást kapunk, ahol a szereplő polinomok fokai már kisebbek. Hasonlóan láthatjuk, hogy h is relatív prím f-hez és g-hez.

Az $x^n - 1$ polinom gyökei az n-edik egységgyökök. A gyökténye zős alakban x helyére h/g-t helyettesítve és g^n-nel szorozva a kiinduló azonosság adódik. Ha d közös osztója $h - \varepsilon^j g$-nek és $h - \varepsilon^k g$-nek, akkor kivonással kapjuk, hogy $d \mid (\varepsilon^k - \varepsilon^j)g$, azaz $d \mid g$, de akkor $d \mid h$ is teljesül. Mivel g és h relatív prímek, d csak konstans lehet. Ezért a $h - \varepsilon^j g$ polinomok tényleg páronként relatív prímek.

Az f^n kanonikus alakjában minden prím kitevője n-nel osztható. Ezt páronként relatív prím polinomok szorzatára bontottuk. Mivel minden prím ezek közül csak egyben szerepelhet, e tényezőkre is igaz, hogy minden prímosztójuk kitevője n-nel osztható. Így mindegyik $h - \varepsilon^j g$ egy teljes n-edik hatvány asszociáltja, és ezért a fenti megjegyzés szerint maga is teljes n-edik hatvány.

Az $\varepsilon u^n + w^n = (\varepsilon + 1)v^n$ összefüggésben az ε és $\varepsilon + 1$ beolvasztható u^n-be, illetve w^n-be. Ezért az egyenlet egy újabb megoldását kaptuk. Az u, v, w egyike sem lehet nulla, mert akkor f is nulla lenne. Ha mindhárom konstans, akkor könnyen láthatóan g és h is konstans, és így f is, ami lehetetlen. Végül ha g és h foka legfeljebb N, akkor u, v, w mindegyike legfeljebb N/n fokú. Ezért tényleg olyan nemtriviális megoldást kaptunk, amely kisebb fokú polinomokból áll.

♫ A teljes indukciónak azt a formáját, amit a megoldásban használtunk, a 3.2.1. Tétel bizonyítása előtti apró betűs részben magyaráztuk el.

3.4.15. $30x^3 - 30 = 2 \cdot 3 \cdot 5 \cdot (x - 1) \cdot (x^2 + x + 1)$. 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).

3.4.16. Mivel R nullosztómentes, egy nem nulla konstans R-beli polinom minden felbontása csakis nulladfokú, azaz konstans polinomok szorzatára történhet. Egy ilyen felbontás pontosan akkor triviális R-ben, ha $R[x]$-ben az, mert a 3.1.11. Gyakorlat szerint R és $R[x]$ egységei ugyanazok. Így egy konstans polinom

pontosan 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. Ezért 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. A felbontás $R[x]$-beli egyértelműségéből tehát az R-beli egyértelműség adódik.

3.4.17. 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 fölírható $\mathbb{Q}[x]$-beli irreducibilisek szorzataként. A 3.4.7. második Gauss-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 föl 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.

3.4.18. 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 3.1.22. 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 a 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.

3.4.19. 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 fölötti polinomgyűrű is alaptételes, kihasználtuk, hogy test fölötti polinomgyűrű alaptételes (amikor $\mathbb{Z}[x]$-et vizsgáltuk, akkor a $\mathbb{Q}[x]$-ben használtuk az alaptételt), tehát erre nem kaptunk új bizonyítást.

3.4.20. Nyilván $f \neq \pm 1$. Tegyük föl, hogy $f = gh$ nemtriviális felbontás, $\operatorname{gr}(g) = m$, és így $\operatorname{gr}(h) = n-m$. Az ominózus $2n + 1$ hely mindegyikén $g(x)$ és $h(x)$ egyike 1 vagy -1 lesz. Ezért összesen vagy legalább $n + 1$ darab 1-es, vagy legalább $n + 1$ darab -1-es fordul elő. Az első esetben vagy g vesz föl több, mint m helyen 1-et, és így a polinomok azonossági tétele miatt $g(x)$ konstans 1, vagy pedig h vesz föl több, mint $n - m$ helyen 1-et, tehát $h(x)$ lesz konstans 1. Ugyanez a bizonyítás, amikor a -1-ek vannak többségben.

3.4.21. Keressük meg az $f \in \mathbb{Z}[x]$ legfeljebb k-adfokú g osztóit $\mathbb{Z}[x]$-ben a következőképpen. Legyen $f = gh$ (ahol $h \in \mathbb{Z}[x]$). Ekkor $f(m) = g(m)h(m)$ 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 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 föl 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 nf akkor és csak akkor irreducibilis $\mathbb{Q}$ fölött, ha nem bomlik alacsonyabb fokú, egész együtthatós polinomok szorzatára.

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 3.1.36. 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 3.1.22. Gyakorlat, (2) pont).

3.5.3. Tegyük föl, 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. Ekkor f felbontható nála alacsonyabb fokú, racionális együtthatós polinomok szorzatára. Legyenek ezek $g(x) = b_0 + \ldots + b_k x^k$ és $h(x) = c_0 + \ldots + c_\ell x^\ell$, ahol $\mathrm{gr}(g) = k < n$ és $\mathrm{gr}(h) = \ell < n$. 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 $i \leq k$ miatt $k \geq n$. Ez ellentmond a $k < n$ feltételnek.

3.5.4. 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 pontosan 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.

3.5.5. Ha az f polinomot szorzattá lehet bontani: $f = gh$, akkor az összes eltoltjait is 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, ha $a \neq 0$. 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, műveletartó 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.

Helyettesítsünk most x helyébe $p(x)$-et. A fenti gondolatmenet szerint ha f reducibilis, akkor $f\big(p(x)\big)$ is az lesz. Megfordítva ez nem igaz, például az x irreducibilis polinomba x^2-et helyettesítve nyilván reducibilissé válik.

3.5.6. Tegyük föl, 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. De akkor szorzatuk főegyütthatója osztható kilenccel, ami nem igaz: ez a főegyüttható ugyanis 6.

3.5.7. 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.

3.5.8. Mindkét állítás bizonyításának kulcsa a következő észrevétel:

$$x^n f(1/x) = x^n(a_n/x^n + \ldots + a_1/x + a_0) = a_n + \ldots + a_1 x^{n-1} + a_0 x^n = g(x)\,.$$

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.

3.5.10. 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 (3.3.21. Gyakorlat), és mivel a főegyütthatója páratlan, irreducibilis $\mathbb{Q}$ fölött is (lásd 3.5.11. Gyakorlat, (4) pont).

3.5.11. 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 föl, 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

$$\mathrm{gr}(\overline{g}) \leq \mathrm{gr}(g) < \mathrm{gr}(f) = \mathrm{gr}(\overline{f})\,,$$

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.

3.5.12. 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.

3.5.13. 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 3.9.9. Tétel miatt (is) irreducibilisek.

(1) $3x^7 - 6x^6 + 6x^2 + 3x - 2$: irreducibilis, fordított Schönemann–Eisenstein-kritérium ($p = 3$).
(2) $3x^7 + x^6 + 6x^2 + 2x - 2$: reducibilis, a -1 gyöke (ez a racionális gyökteszt segítségével található meg).
(3) $3x^7 - 6x^6 + 6x^2 + 2x - 2$: irreducibilis, Schönemann–Eisenstein ($p = 2$).
(4) $x^{16} + 1$: irreducibilis, $x \to x + 1$ helyettesítés után Schönemann–Eisenstein $p = 2$-re. Ennek kiszámítását a 3.5.15. Feladat mintájára érdemes elvégezni (lásd 3.9.24. Gyakorlat).
(5) $x^{16} + 2$: irreducibilis, Schönemann–Eisenstein ($p = 2$).
(6) $x^4 - 14x^2 + 9$: irreducibilis, a 3.3.24. Feladat módszerével, gyökei $\pm\sqrt{2} \pm \sqrt{5}$.
(7) $x^4 - x^2 + 1$: irreducibilis, a 3.3.19. Gyakorlat módszerével, gyökei a tizenkettedik primitív egységgyökök, $\mathbb{R}$ fölötti felbontása $(x^2 + 1)^2 - (\sqrt{3}x)^2 = (x^2 - \sqrt{3}x + 1)(x^2 + \sqrt{3}x + 1)$.
(8) $3x^7 + 6x - 18$: irreducibilis, Schönemann–Eisenstein ($p = 2$).
(9) $x^5 + 4$: irreducibilis, $x \to x + 1$ helyettesítés után Schönemann–Eisenstein-kritérium ($p = 5$).
(10) $x^3 + 9$: irreducibilis, mert harmadfokú, és nincs racionális gyöke (az egyetlen valós gyöke a $-\sqrt[3]{9}$, irracionális szám).
(11) $x^5 + 729$: irreducibilis, $y = x/3$ helyettesítéssel $(x^5 + 729)/243 = y^5 + 3$, Schönemann–Eisenstein $p = 3$-ra.
(12) $x^{10} - x^5 + 1$: 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.
Második megoldásként $x^{10} - x^5 + 1 = (x^{15} + 1)/(x^5 + 1)$, nyilván $x^2 - x + 1 \mid x^3 + 1 \mid x^{15} + 1$, de a nevezőhöz relatív prím, mert $x^2 - x + 1 \mid x^6 - 1$, és az euklideszi algoritmus triviálisan végigszámolható $x^6 - 1$ és $x^5 + 1$ esetében (ezek kitüntetett közös osztója $x + 1$).
(13) $x^{20} + 20$: irreducibilis, Schönemann–Eisenstein ($p = 5$).
(14) $x^4 + 25$: irreducibilis, a 3.3.19. Gyakorlat eredménye szerint.
(15) $x^6 + 32$: irreducibilis, $y = x/2$ helyettesítéssel $(x^6 + 32)/32 = 2y^6 + 1$, fordított Schönemann–Eisenstein $p = 2$-re.
(16) $x^4 + 4x + 1$: irreducibilis, $x \to x + 1$ helyettesítés után Schönemann–Eisenstein ($p = 2$).
(17) $x^4 - 2x + 1$: reducibilis, az 1 gyöke.
(18) $x^4 + x^3 + 1$: irreducibilis, mert $\mathbb{Z}_2$ fölött is az (3.3.21. Gyakorlat), és a főegyüttható 1 (3.5.11. Gyakorlat (4) pont).
(19) $x^4 + x^3 + 4$: irreducibilis, mert $\mathbb{Z}_3$ fölött egy első- és egy harmadfokú irreducibilis szorzata, viszont $\mathbb{Z}$ fölött csak két másodfokú szorzata lehetne, mert nincs racionális gyöke (lásd a 3.5.9. Példa megoldását).
(20) $x^4 + x^3 + x^2 + 1$: irreducibilis, ez a 3.5.9. Példában szereplő polinomhoz tartozó reciprok polinom (lásd 3.5.8. Feladat).

3.5.14. 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 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.

(1) $x^5+5x+26$: irreducibilis, $x \to x-1$ helyettesítés után Schönemann–Eisenstein ($p=5$).
(2) x^6+1: reducibilis, az ismert azonosság szerint $(x^2+1)(x^4-x^2+1)$.
(3) x^3+7x-3: irreducibilis, mert harmadfokú, és a racionális gyökteszt miatt nincs racionális gyöke.
(4) $x^4+3x^3+x^2+1$: reducibilis, a -1 gyöke.

3.5.15. 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 (3.3.22. 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.

3.5.16. 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-kritérium 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.

Ahhoz, hogy a Schönemann–Eisenstein-tétel általános formáját kimondjuk, szükség van a hányadostest fogalmára, ezért ez az 5.7.9. Gyakorlatban szerepel.

3.5.17. Tegyük föl, hogy 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 $\big(x+h(x)\big)^k-x^k$ osztható $x+h(x)-x=h(x)$-szel az $a-b \mid a^k-b^k$ összefüggés miatt, és így $f(x)$-szel is. Ezért $f(x) \mid f\big(x+h(x)\big)-f(x)$, ahonnan $f(x) \mid f\big(x+h(x)\big)$.

Belátjuk, 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.

♫ Hogyan lehet rájönni a megoldás ötletére? Keressünk olyan $g(x)$-et, hogy $f\big(g(x)\big)$-nek legyenek „kezelhető" gyökei. Ha például $f(\alpha)=0$ és $g(\alpha)=\alpha$, akkor α gyöke $f\big(g(x)\big)$-nek is. Ez teljesül, ha $g(x)-x$-nek α gyöke. Kézenfekvő tehát $g(x)-x$-et f többszörösének választani.

Ha az Olvasó már jártasságra tett szert a Galois-elméletben (6. fejezet), akkor a következőképpen is rájöhet a megoldásra. Legyen $\mathrm{gr}(f)=n$ és $\mathrm{gr}(g)=m$, ekkor $f\big(g(x)\big)$ foka nm. Ha c komplex gyöke $f\big(g(x)\big)$-nek,

akkor $b = g(c)$ gyöke f-nek, és $b = g(c) \in \mathbb{Q}(c)$ miatt $\mathbb{Q}(b)$ részteste $\mathbb{Q}(c)$-nek. Ha $f\big(g(x)\big)$ irreducibilis, akkor $|\,\mathbb{Q}(c) : \mathbb{Q}\,| = nm$. De $|\,\mathbb{Q}(b) : \mathbb{Q}\,| \le n$ és $|\,\mathbb{Q}(c) : \mathbb{Q}(b)| \le m$, mert c gyöke a $g(x) - b$ polinomnak, mely $\mathbb{Q}(b)$-beli együtthatós. A testbővítések fokának szorzástétele miatt ez csak úgy lehetséges, hogy mindkét esetben egyenlőség áll, azaz $g(x) - b$ irreducibilis $\mathbb{Q}(b)$ fölött. Azt, hogy ez ne legyen igaz, a legkönnyebb úgy elérni, ha biztosítjuk, hogy $g(x) - b$-nek legyen gyöke $\mathbb{Q}(b)$-ben, például maga b. Megjegyezzük, hogy a most bizonyított állítás megfordítása is igaz: ha f irreducibilis $\mathbb{Q}$ fölött, és $g(x) - b$ irreducibilis $\mathbb{Q}(b)$ fölött, akkor $f\big(g(x)\big)$ irreducibilis $\mathbb{Q}$ fölött. Valóban, legyen c komplex gyöke $g(x) - b$-nek, ekkor c foka nm a szorzástétel miatt, és így $f\big(g(x)\big)$ a c minimálpolinomja lesz.

3.5.18. Tegyük föl, hogy $\sqrt[3]{4} = a + b\sqrt[3]{2}$, és tekintsük az $f(x) = x^2 - ax - b$ és $g(x) = x^3 - 2$ racionális együtthatós polinomokat. Ezeknek $\sqrt[3]{2}$ közös valós gyöke, továbbá $x^3 - 2$ a Schönemann–Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött. Ezért a 3.2.21. Gyakorlat miatt $x^3 - 2$ osztója $x^2 - ax - b$-nek $\mathbb{Q}[x]$-ben. Ez lehetetlen a fokszámok miatt.

3.5.19. Legyen $f(x) = a_0 + a_1x + \ldots + a_nx^n$, ahol $a_0 = f(0)$ és a_n nem nulla komplex számok, és $g(x) = a_n + a_{n-1}x + \ldots + a_0x^n$ az f-hez tartozó reciprok polinom. A 3.5.8. Feladat szerint g gyökei (multiplicitással számolva) az f gyökeinek reciprokai. Ezért f akkor és csak akkor teljesíti a feladat feltételét, ha f és g gyöktényezős alakja csak egy nem nulla konstans c szorzóban tér el egymástól (itt felhasználtuk az algebra alaptételét), azaz ha $g(x) = cf(x)$. Az együtthatókat összehasonlítva

$$a_n = ca_0\,,\ a_{n-1} = ca_1\,,\ \ldots,\ a_0 = ca_n\,.$$

Az első és utolsó egyenletet összeszorozva $a_na_0 = c^2a_0a_n$, ami azzal ekvivalens, hogy $c^2 = 1$, azaz $c = \pm 1$.

3.5.20. A 3.5.19. Gyakorlat szerint ha $f(x) = a_nx^n + \ldots + a_0$ egy n-edfokú reciprok polinom, akkor az antiszimmetrikus esetben $a_i = -a_{n-i}$ minden i-re. Ezeket az egyenleteket összeadva azonnal látszik, hogy a polinomnak gyöke az 1 (ha f foka páros, akkor a „középső” együttható nulla lesz, hiszen megegyezik az ellentettjével). A szimmetrikus esetben $a_i = a_{n-i}$ minden i-re. 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. Mivel a fok páratlan, nincs „középső” tag, ezért f-nek is gyöke a -1. Az 1 és a -1 reciproka is önmaga, ezért ha az $x + 1$ vagy az $x - 1$ gyöktényezőt elvesszük a polinomból, akkor a megmaradó polinom gyökeire továbbra is igaz, hogy minden gyök ugyanolyan multiplicitású, mint a reciproka. Ha tehát az összes ilyen gyöktényezővel leosztunk, akkor csakis páros fokú, szimmetrikus reciprok polinom maradhat (különben a fentiek szerint 1 vagy -1 továbbra is gyök lenne).

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:

$$0 = \frac{x^6 + x^5 - x^4 - x^2 + x + 1}{x^3} = \Big(x^3 + \frac{1}{x^3}\Big) + \Big(x^2 + \frac{1}{x^2}\Big) - \Big(x + \frac{1}{x}\Big)\,.$$

Legyen $z = x + (1/x)$, ekkor négyzetre, illetve köbre emeléssel

$$z^2 = \Big(x^2 + \frac{1}{x^2}\Big) + 2 \quad \text{és} \quad z^3 = \Big(x^3 + \frac{1}{x^3}\Big) + 3\Big(x + \frac{1}{x}\Big)\,.$$

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.

3.6. A derivált és a többszörös gyökök

3.6.7. 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.

3.6.8. 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.

3.6.9. Ilyen például $f(x)=x^9+x^8$ a $\mathbb{Z}_2$ fölött. A 3.6.3. Állítás bizonyításából látszik, hogy általában olyan $f(x)=(x-b)^8q(x)$ polinomot érdemes keresni, amelyre $8q(b)=0$ (de $q(b)$ és $q'(b)$ nem nulla). A második kérdés megválaszolásához legyen $g(x)=x^8q(x)$ a $\mathbb{Z}_2$ fölött. Ekkor $8q(0)=0$ minden q-ra, arra van még szükség, hogy $xq'(x)$-nek a 0 háromszoros gyöke legyen, de q-nak ne legyen gyöke. Ha $q'(x)=x^2$, akkor például $q(x)=x^3+1$ megfelelő, ekkor $g(x)=x^{11}+x^8$.

3.6.10. Tegyük föl, hogy b az f-nek pontosan ℓ-szeres gyöke. Ekkor $\ell\geq 1$, mert b gyöke f-nek, és így a 3.6.5. 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 nyilván szükséges, hogy b gyöke legyen f-nek, hiszen például x^k+1 deriváltjának a $b=0$ szám $k-1$-szeres gyöke, de x^k+1-nek nem gyöke.

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.

3.6.11. Ha $f'=0$, akkor f konstans, és így $f'\mid f$ pontosan akkor igaz, ha f is nulla. Tegyük föl, hogy $f'\neq 0$. Legyen $b\in\mathbb{C}$ gyöke f'-nek. Mivel $f'\mid f$, a b szám gyöke f-nek is. Az előző 3.6.10. Gyakorlat szerint ha b az f'-nek $k-1$-szeres gyöke, akkor f-nek k-szoros gyöke. Ezért f/f' osztható $x-b$-vel, vagyis f/f'-nek gyöke f' mindegyik gyöke. De f/f' elsőfokú polinom, hiszen $\mathrm{gr}(f')=\mathrm{gr}(f)-1$. Ezért f'-nek csak egy gyöke lehet, és így $f(x)=c(x-b)^k$. Az ilyen alakú polinomok nyilván megfelelnek.

3.6.12. A 3.6.5. 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 a 3.6.12. 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.

3.6.13. Ha $b\in\mathbb{C}$ 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 $k-1$, azaz b az (f,f')-nek 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 3.2.6. 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 $k>1$ esetén egy komplex szám akkor és csak akkor k-szoros gyöke f-nek, ha $k-1$-szeres gyöke (f,f')-nek (vö. 3.6.10. Gyakorlat).

3.6.14. 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 (3.3.22. 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.

3.6.15. Legyen S test és $g \in S[x]$ egy S fölött irreducibilis polinom. Tegyük föl, hogy g-nek van többszörös gyöke egy S-nél bővebb T testben. Ekkor ez gyöke g'-nek is. A 3.2.21. Gyakorlat miatt $g(x)$ osztója $g'(x)$-nek $S[x]$-ben. Ha $g' \neq 0$, akkor g' foka kisebb g foknál, és így g nem oszthatja g'-t. Tehát csak a $g' = 0$ eset az, ami egyáltalán előfordulhat.

Ha $S = \mathbb{Q}$, akkor ez lehetetlen, hiszen ekkor g konstans polinom lenne, márpedig g-ről föltettük, hogy nem konstans (hiszen irreducibilis).

Ha $S = \mathbb{Z}_2$, és $g(x) = a_0 + \ldots + a_nx^n$, akkor

$$g'(x) = a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1} = 0$$

akkor és csak akkor teljesül, ha g páratlan indexű együtthatói nullával egyenlők, vagyis

$$g(x) = a_0 + a_2x^2 + \ldots + a_{2k}x^{2k}$$

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 (3.3.22. Feladat),

$$g(x) = (a_0 + a_2x + \ldots + a_{2k}x^k)^2 .$$

Ez ellentmond annak, hogy g irreducibilis. Tehát ilyen g 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.

A feladat második kérdésére is igenlő a válasz, azaz ha $(f, f') \neq 1$ teljesül egy $\mathbb{Q}$ vagy $\mathbb{Z}_2$ fölötti f polinomra, akkor f-nek van többszörös tényezője $\mathbb{Q}$-ban, illetve $\mathbb{Z}_2$-ben. Az Útmutatóban leírtakat folytatjuk. Mivel b közös gyöke f-nek és f'-nek, ezért b legalább kétszeres gyöke f-nek (3.6.6. Következmény). A g-nek viszont b csak egyszeres gyöke, ezért b gyöke f/g-nek is. A 3.2.21. Gyakorlat miatt g osztója f/g-nek, azaz $g^2 \mid f$.

3.6.16. Érdemes általában meggondolni (például n szerinti indukcióval), hogy

$$(f_1f_2 \ldots f_n)' = \sum_{i=1}^{n} f_1 \ldots f_{i-1}f_i'f_{i+1} \ldots f_n .$$

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.

3.6.17. Mivel f legalább másodfokú, az f' legalább elsőfokú, és így az algebra alaptétele miatt van egy komplex b gyöke. Ekkor $c = -f(b)$ megfelelő lesz. Ehhez a 3.6.6. Következmény miatt elég megmutatni, hogy b közös gyöke $f(x) - f(b)$-nek és a deriváltjának. Ez nyilvánvaló, hiszen ez a derivált $f'(x)$.

3.6.18. Az $f(x)$ a c értéket akkor és csak akkor veszi föl 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

3.7.9. 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 ennek $(-1)^1/a$-szorosa (3.7.6. Definíció), azaz $b^2 - 4ac$.

♫ A gyökök és együtthatók összefüggése miatt $a(\alpha_1 + \alpha_2) = -b$ és $a\alpha_1\alpha_2 = c$. Innen is azonnal adódik, hogy $a^2(\alpha_1 - \alpha_2)^2 = b^2 - 4ac$.

A 3.7.8. Állítás szerint a diszkrimináns 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.

3.7.10. 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.

3.7.12. 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, mert 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 rezultánsának kiszámítását az Olvasó remélhetőleg már nem kézzel, hanem a `Maple` program `factor(resultant(f,g,y))` parancsa segítségével végezte, és így az eredményt rögtön szorzattá alakítva kapta meg:

$$z^5(z+1)^4(z-1)^2(z-2)(z^2+2z+2)(z^2-2z-1)\,.$$

Azt gondolhatnánk, hogy ennek mindegyik gyöke megoldáshoz vezet, hiszen végig normált polinomok rezultánsát vettük, vagyis 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 $z = 2$ végül is nem vezet az egyenletrendszer megoldásához.

Az összes gyököt ugyanígy végigszámolni fáradságos volna. Egyszerűbb, ha az f helyett az egyenletrendszer második és harmadik egyenletének a rezultánsát számoljuk ki, ez $h(y, z) = y^2 + y - (z^2 + z)$. 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, 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. Mindezt a `Maple` program

```
solve( {x^2-y-z-1, y^2-x-z-1, z^2-x-y-1}, {x,y,z} );
```

parancsa segítségével ellenőrizhetjük.

3.8. A harmad- és negyedfokú egyenlet

3.8.3. Tegyük föl, hogy az $x^3+px+q = 0$ egyenletnek b legalább kétszeres gyöke. Mivel a gyökök összege nulla, a harmadik gyök $-2b$ lesz. A gyökök és együtthatók összefüggése miatt $p = -3b^2$ és $q = -2b^3$. Behelyettesítve látjuk, hogy $D = (q/2)^2 + (p/3)^3 = 0$.

A 3.8.1. Tétel szerint az egyenlet gyökei (multiplicitásokkal is) $u + v$, $\varepsilon u + \varepsilon^2 v$, $\varepsilon^2 u + \varepsilon v$, ahol ε primitív harmadik egységgyök és $uv = -p/3$. Ha $D = 0$, akkor u is és v is a $-q/2$ szám köbgyökei. Ezért három eset van. Ha $u = v$, akkor $\varepsilon u + \varepsilon^2 v = \varepsilon^2 u + \varepsilon v$. Ha $u = \varepsilon v$, akkor $u + v = \varepsilon^2 u + \varepsilon v$. Végül ha $u = \varepsilon^2 v$, akkor $u + v = \varepsilon u + \varepsilon^2 v$. Tehát mindegyik esetben van többszörös gyök.

Tegyük most föl, hogy p és q valós. Ha $D > 0$, akkor u és v választható valós számnak. Valóban, ilyenkor mindkét köbgyök alatt valós szám áll, és ezeknek van valós köbgyöke, csak azt kell meggondolni, hogy az $uv = -p/3$ teljesíthető-e. A 3.8.1. Tétel bizonyításában láttuk, hogy ha $p \neq 0$, akkor u-nak a köbgyök bármelyik értéke választható, és $v = -p/3u$ ekkor szintén valós lesz. Ha pedig $p = 0$, akkor u választható a valós $-q$ szám valós köbgyökének, v pedig nullának.

Tehát $u = v$, ahonnan azt kapjuk, hogy $\varepsilon u+\varepsilon^2 v$ konjugáltja $\varepsilon^2 u+\varepsilon v$ (hiszen ε és ε^2 egymás konjugáltjai). Ez a két gyök különböző, hiszen az egyenletnek $D > 0$ miatt nincs többszörös gyöke. Ezért egyikük sem lehet valós.

Végül tegyük föl, hogy (p, q valós és) $D < 0$. A $p = 0$ eset most nem lehetséges, mert akkor $D = (q/2)^2$ nemnegatív lenne. Így u a köbgyök bármelyik értékének választható. A Cardano-képletben a két köbgyök alatt most konjugált számok állnak, ezért a köbgyökvonás elvégezhető úgy, hogy v az u konjugáltja legyen, csak be kell látni, hogy ez a v érték megfelelő, azaz $uv = -p/3$. Mivel u és v konjugáltak, uv valós szám. Tudjuk továbbá, hogy $(uv)^3 = (-p/3)^3$ (mert ez a köbgyökök bármelyik értékére igaz). Mivel a köbgyökvonás a valós számok között egyértelmű, ezért tényleg $uv = -p/3$.

Tehát $u = \overline{v}$. Ekkor viszont közvetlen számolással ellenőrizhető, hogy az egyenlet mindegyik gyöke önmagának a konjugáltja, azaz valós (mert mindegyik gyök két konjugált komplex szám összege).

♫ Ha az Olvasó végigszenvedte ezt a kifejezetten hosszadalmas diszkussziót, akkor értékelheti csak igazán a 3.8.2. Tétel elegáns, diszkriminánst felhasználó bizonyítását.

3.8.4. Tegyük föl először, hogy $q^2 - 4pr = 0$. Ha $p \neq 0$, akkor $q^2 - 4pr$ a polinom diszkriminánsa. Mivel ez nulla, van kétszeres gyök, így a polinom $p(x - \alpha)^2 = [\sqrt{p}(x - \alpha)]^2$, hiszen 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, nevezetesen $\sqrt{r}$ négyzete.

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 a bizonyítás ugyanaz, mint az előbb, csak most figyelni kell arra is, hogy nem minden racionális számból vonható négyzetgyök. Az eredmény a következő: 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 $q^2 - 4pr = 0$.

3.8.6. A szokásos módon D jelöli a Cardano-képletben a négyzetgyök alatti kifejezést.

(1) $x^3-6ix-i+8 = 0$: ennél az egyenletnél D teljes négyzet, mert $D = (4-i/2)^2-(2i)^3 = (4+i/2)^2$. 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 $u+v = (1+\sqrt{3}/2)+(1/2+\sqrt{3})i$, $\varepsilon u+\varepsilon^2 v = (1-\sqrt{3}/2)+(1/2-\sqrt{3})i$ és $\varepsilon^2 u+\varepsilon v = -2-i$. Itt $\varepsilon = \cos 120^\circ + i \sin 120^\circ$ primitív harmadik egységgyök, lásd a 3.8.1. Tétel bizonyítását. Természetesen u másik két értékéből is kiindulhattunk volna, akkor más sorrendben kapjuk ugyanezeket a gyököket.

(2) $x^3 + 12x - 16i = 0$: ennél az egyenletnél $D = 0$, és így u (például) $2(\cos 30^\circ + i \sin 30^\circ)$, ehhez $v = -4/u = 2(\cos 150^\circ + i \sin 150^\circ)$. Innen $x^3+12x-16i = (x-2i)^2(x+4i)$, a $2i$ kétszeres gyök.

(3) $x^3 - 21x + 20 = 0$: ekkor $D = -243$, 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 (egyik) 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 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 $(-1 \pm \sqrt{5})/2$.

3.8.7. 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 3.3.24. Feladatban használt felbontások. A kapott észrevételt a 3.8.9. Gyakorlatban általánosítjuk.

3.8.8. 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 3.8.5. 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 3.8.5. 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 $8(x-u_1)(x-u_2)(x-u_3)$ lesz, azaz (1) igaz. 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. Így (2) is igaz.

A 3.8.5. 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.

3.8.9. A 3.8.8. 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 $(x-\alpha_2)(x-\alpha_3)$.

3.8.10. 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 3.8.4. 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 polinom felbomlik két racionális együtthatós, másodfokú polinom szorzatára.

Megfordítva, tegyük föl, hogy f két másodfokú, racionális együtthatós polinom szorzata. 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 3.8.8. 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 3.8.4. Gyakorlat szerint erre teljesül a (2) és (3) pontbeli 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 egy racionális szám négyzete, ha a négyszerese, vagyis $b^2 - 4d$ az.

3.8.11. A harmadfokú rezolvens most $(8u - 4b)(u^2 - d)$, amiből (4) azonnal következik. Az (5) állítás következménye a 3.8.10. Feladatnak. Valóban, tegyük föl először, hogy f reducibilis. Ekkor ebben a feladatban (1), (2) és (3) valamelyike teljesül. Ha ez (3), akkor $u = b/2$, és $(b/2)^2 - d$ egy racionális szám négyzete, azaz $b^2 - 4d$ is. Ha ez (2), akkor $u = \pm\sqrt{d}$ esetén $\pm\sqrt{d} - b$ egy racionális szám négyzete, az $u = b/2$ eset pedig nem lehetséges, mert ekkor $2u - b + a^2/4 = 0$. Végül ha (1) teljesül, azaz f-nek van egy racionális α gyöke, akkor $-\alpha$ is racionális gyök. Így $x^2 - \alpha^2$ osztója f-nek, vagyis f előáll két másodfokú, racionális együtthatós polinom szorzataként is, ezért a 3.8.10. Feladat utolsó előtti megjegyzése miatt (2) és (3) valamelyike ebben az esetben is teljesül. Az Olvasó megpróbálhat erre az irányra közvetlen, a harmadfokú rezolvenst nem használó bizonyítást is adni.

Megfordítva, ha (5) teljesül, akkor hasonlóan ellenőrizhető, hogy (2) és (3) egyike igaz. De most meg is kell adnunk az f polinom felbontásait. Ha a $\sqrt{b^2 - 4d} = e_1 \in \mathbb{Q}$, akkor

$$f(x) = \big(x^2 - (-b + e_1)/2\big)\big(x^2 - (-b - e_1)/2\big),$$

ha $\sqrt{2\sqrt{d} - b} = e_2 \in \mathbb{Q}$, akkor a 3.8.10. Feladat megoldását végigszámolva

$$f(x) = \big(x^2 - e_2x + \sqrt{d}\big)\big(x^2 + e_2x + \sqrt{d}\big),$$

végül ha $\sqrt{-2\sqrt{d}-b}=e_3\in\mathbb{Q}$, akkor

$$f(x)=\left(x^2-e_3x-\sqrt{d}\right)\left(x^2+e_3x-\sqrt{d}\right).$$

Az utolsó két esetben $\sqrt{d}$ nyilvánvalóan racionális, mert e_2, illetve e_3 az.

3.8.12. Az x^4-2 esetében $b=0$ és $d=-2$, ami nem négyzetszám, és ezért $\pm2\sqrt{d}-b$ 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 (3.3.24. Feladat). Ebben az esetben a 96, 12 és 8 értékek adódnak, amelyek nem négyzetszámok.

3.8.13. Ezt az egyenletet, a negyedfokú egyenlethez 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 két harmadik primitív egységgyökök $-1/2\pm i\sqrt{3}/2$, a két hatodik $1/2\pm i\sqrt{3}/2$, a négy tizenkettedik $\pm\sqrt{3}/2\pm i/2$. 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). Az 1.5.13. Tétel szerint ezek közül az 1 kivételével mindegyik primitív p-edik egységgyök is, hiszen az $1,\dots,p-1$ 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. (Az Olvasó kereshet elemi számelméleti bizonyítást is: csoportosítsuk az $1/n,2/n,\dots,n/n$ törteket egyszerűsítés után a nevezőjük szerint.)

3.9.8. 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 pillanatok alatt kiszámolja a mai otthoni számítógépeinken is, 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 index, 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.

3.9.11. A rekurziós képlet alapján, ha p prím, akkor

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{\Phi_1 \Phi_p \dots \Phi_{p^{k-1}}} = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1},$$

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:

$$\Phi_{p^k}(x) = \frac{y^p - 1}{y - 1} = 1 + y + \dots + y^{p-1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \dots + x^{(p-1)p^{k-1}}.$$

3.9.12. Legyen n pozitív, páratlan egész. Az 1.5.19. 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 az E.4.3. Állítás szerint $\varphi(n)$ páros szám (kivéve ha $n = 1$ vagy 2).

3.9.13. Láttuk, hogy $\Phi_1(x) = x - 1$. Ha p prím, akkor a 3.9.3. Gyakorlat miatt $\Phi_p(x) = 1 + x + \dots + x^{p-1}$. A további prímhatvány-indexű körosztási polinomok a 20-as indexig a 3.9.11. 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, 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 3.9.15. Feladatot).

3.9.14. Tudjuk, hogy $x^{n/d} - 1$ azoknak az $x - \eta$ gyökténye zőknek 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 $\sum_{d|(n/m)} \mu(d)$. Az E.4.6. Állítás miatt ez az összeg 1, ha $n/m = 1$, és nulla egyébként.

3.9.15. A feladatra két megoldást adunk. Az első rövid számolás, ami felhasználja a 3.9.14. Feladatban bizonyított összefüggést. A második bizonyítás hosszabb, de nagyon tanulságos, mert gyakoroljuk általa az elemrend fogalmát.

Az első bizonyításban 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 3.9.14. 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 azt adja, hogy $o(\eta^{n/m}) = o(\eta)/(o(\eta), n/m)$. Ha $o(\eta) = n$, akkor ez $n/(n, n/m) = n/(n/m) = m$. Megfordítva, tegyük föl, hogy $o(\eta)/(o(\eta), n/m) = m$. Azaz

$$o(\eta) = (o(\eta), n/m)m = (o(\eta)m, n) = \big(m, n/o(\eta)\big)o(\eta)\,.$$

Itt kétszer használtuk a kitüntetett közös osztó kiemelési tulajdonságát. (A második esetben is szabad ezt megtenni, azaz $o(\eta) \mid n$ teljesül, 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 $p \mid n$, 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 igazolja.

♫ A bizonyítást másképp is befejezhettük volna, miután már igazoltuk, hogy $o(\eta) = n$ esetén $o(\eta^{n/m}) = m$. Ebből ugyanis következik, hogy $\Phi_n(x)$ osztója $\Phi_m(x^{n/m})$-nek, és mivel normált polinomokról van szó, elég megmutatni, hogy a fokuk egyenlő. Ehhez a $\varphi(n) = (n/m)\varphi(m)$ azonosságot kell ellenőrizni, ami könnyen megtehető az E.4.2. Tétel segítségével.

3.9.16. Az előző feladat alapján elég a négyzetmentes indexű körosztási polinomokat ismerni, mert ha 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. Az eredmények a következők: $\Phi_{36}(x) = \Phi_6(x^6) = x^{12}-x^6+1$, $\Phi_{72}(x) = \Phi_6(x^{12}) = x^{24}-x^{12}+1$, $\Phi_{144}(x) = \Phi_6(x^{24}) = x^{48}-x^{24}+1$, végül a 3.9.13. Gyakorlat eredményét felhasználva $\Phi_{100}(x) = \Phi_{10}(x^{10}) = x^{40}-x^{30}+x^{20}-x^{10}+1$.

3.9.17. Tegyük föl, hogy θ egy mn-edik egységgyök. Mivel m és n relatív prímek, léteznek olyan x és y egész számok, melyekre $nx + my = 1$. Ekkor $\theta = \theta^{nx+my} = \theta^{nx}\theta^{my}$. Mivel $(\theta^{nx})^m = (\theta^x)^{mn} = 1$, ezért θ^{nx} egy m-edik egységgyök, és hasonlóan θ^{my} egy n-edik egységgyök. Tegyük most föl, hogy θ *primitív* nm-edik egységgyök. A hatvány rendjének képlete szerint θ^{nx} rendje $mn/(mn, nx)$. 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 megmutatjuk, hogy ez a szorzat-előállítás egyértelmű. Tegyük föl, hogy $\eta\varepsilon = \eta'\varepsilon'$, ahol η és η' is m-edik egységgyökök, továbbá ε és ε' is n-edik egységgyökök. Átrendezve $\eta/\eta' = \varepsilon'/\varepsilon$. A bal oldalon egy m-edik, a jobb oldalon egy n-edik egységgyök van, így a bal oldal rendje m-nek, a jobb oldalé n-nek osztója. Mivel $(m, n) = 1$, 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 1.5.21. 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 az mn-edik primitív egységgyököket adják, és így számuk $\varphi(mn)$.

A $S(n)$ függvény multiplikativitásának bizonyításához szorozzuk össze az m-edik és az n-edik primitív egységgyökök összegét. Ekkor az eddig bizonyítottak miatt pontosan az mn-edik primitív egységgyökök összegét, azaz $S(mn)$-et kapjuk.

3.9.18. Belátjuk, hogy az n-edik primitív egységgyökök összege $\mu(n)$ (ahol μ az E.4.5. Definícióban megadott Möbius-függvény), szorzatuk pedig mindig 1, kivéve az $n = 2$ esetet, amikor -1. 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 az E.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.)

A szorzatra vonatkozó összefüggés levezetéséhez a $\prod_{d|n} \Phi_d(x) = x^n - 1$ konstans tagját kell tekinteni (azaz nullát helyettesíteni). Így $\prod_{d|n} \Phi_d(0) = -1$, 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 E.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 $n = 2$.

♫ A szorzatról szóló állítást az Olvasónak érdemes bebizonyítania úgy is, hogy minden primitív n-edik egységgyököt párosít az inverzével (ami szintén primitív n-edik egységgyök). Az összegről szóló állítás nyilvánvaló abban az esetben, ha n prímhatvány (hiszen ekkor ismerjük a körosztási polinom együtthatóit a 3.9.11. Gyakorlat miatt), az általános esetet pedig megmutathatjuk a 3.9.17. Gyakorlat utolsó állításának fölhasználásával is (hiszen a Möbius-függvény nyilvánvalóan multiplikatív).

3.9.19. 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.

3.9.20. Eljárhatnánk az előző feladatban látott módon is, a rekurziót páros n esetén $\Phi_2(x) = x + 1$-gyel leosztva. Ennél egyszerűbb azonban, ha ennek a feladatnak az *eredményét* használjuk fel. Ha $n = 4m$, akkor a 3.9.15. 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 3.9.12. 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.

3.9.21. 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 3.9.18. Feladat miatt 1, kivéve az $m = 2$ esetet, amikor -1, ez adja a mínusz 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.

3.9.22. $\mathbb{Z}$ 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

$$\Phi_4(x) = (x-2)(x+2)\,, \quad \Phi_{12}(x) = (x^2+2x-1)(x^2-2x-1)\,.$$

Az eredményeket vessük össze a 3.9.23. Feladatnak, továbbá a 6.7.20. Feladat (4) pontjának az állításával.

3.9.23. Legyen n a legkisebb ellenpélda az állításra. Végig $\mathbb{Z}_p[x]$-ben számolunk (de nem írjuk ki a fölülvonásokat). Tekintsük a $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggést. A d szám egyértelműen fölírható $d = p^j m'$ 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 belátott $\sum_{d|p^k} \varphi(d) = p^k$ 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 $\prod_{m'|m} \Phi_{m'}(x) = x^m - 1$, azt kapjuk, hogy

$$\prod_{d|n} \Phi_d(x) = \left(\prod_{m'|m} \Phi_{m'}(x) \right)^{p^k} = (x^m - 1)^{p^k} = x^{mp^k} - 1 = x^n - 1$$

(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, így $\Phi_n(x)=\Phi_m(x)^{\varphi(p^k)}$, amit bizonyítani kellett. Valamivel talán egyszerűbb a számolás, ha a fenti módszerrel csak az $n=pm$ esetet intézzük el, majd alkalmazzuk a 3.9.15. Feladatot.

3.9.24. A 3.9.11. 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 $\Phi_{p^k}(x+1)$ mindegyik együtthatója osztható p-vel, kivéve a főegyütthatót. A Schönemann–Eisenstein-kritérium tehát teljesül.

3.9.25. A 3.9.24. Gyakorlat és a 3.9.12. Feladat alapján látjuk, hogy prímhatványra, illetve páratlan prímhatvány kétszeresére a körosztási polinom egy eltoltja tényleg teljesíti a Schönemann–Eisenstein-kritérium feltételét. Megfordítva, tegyük föl, 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 $p\nmid n$. A 3.9.23. 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 3.6.14. Gyakorlat). Így $\varphi(m)=1$, ahonnan (az E.4.3. Állítás szerint) $m=1$ vagy 2.

3.9.26. Az Útmutató jelöléseit használjuk. A keresett sokszög oldalait képzeljük a komplex számsík vektorainak. Mivel a sokszög mindegyik szöge egyenlő, alkalmas elforgatással feltehető, hogy a sokszög j-edik oldalvektora $a_j\varepsilon^j$, ahol a_j a megfelelő oldal hossza (hiszen ε_j hossza 1). Mivel az oldalvektorok összege nulla, $a_0+a_1\varepsilon+a_2\varepsilon^2+\ldots+a_{n-1}\varepsilon^{n-1}=0$. Megfordítva, ha ez az egyenlőség teljesül, akkor az $a_j\varepsilon^j$ vektorokat egymás után fűzve megfelelő sokszöget kapunk. Ezzel beláttuk az Útmutató első állítását.

Tegyük föl indirekt, hogy $n=p^k$, ahol p prím, és a keresett sokszög mégis létezik. Ekkor ε gyöke az $f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ polinomnak. Az ε gyöke $g(x)=\Phi_n(x)$-nek is, ami irreducibilis $\mathbb{Q}$ fölött, ezért a 3.2.21. Gyakorlat miatt Φ_n osztója f-nek. Legyen $f(x)=h(x)\Phi_n(x)$, ekkor h foka $(p^k-1)-(p^k-p^{k-1})=p^{k-1}-1$. Jelölje c a h polinom konstans tagját. A 3.9.11. Gyakorlat miatt $\Phi_n(x)$ az $x^{p^{k-1}}$-nek is polinomja, és konstans tagja 1 (hiszen $n\geq 3$). Ezért ha a $h(x)\Phi_n(x)$ szorzást elvégezzük, akkor a szorzatban a konstans tag is és $x^{p^{k-1}}$ együtthatója is c lesz. Azaz f-nek van két egyforma együtthatója, ami feltevésünknek ellentmond.

Most tegyük föl, hogy $n=mk$, ahol $(m,k)=1$ és $m,k>1$. Legyen η egy primitív m-edik, θ pedig egy primitív k-adik egységgyök, és tekintsük a

$$\sum_{i,j}(ik+j)\eta^i\theta^j$$

összeget, ahol $1\leq j\leq k$ és $0\leq i<m$. A 3.9.17. Gyakorlat szerint $\eta^i\theta^j$ befutja az $mk=n$-edik egységgyököket, az együtthatók pedig nyilván az $1,\ldots,n$ számok. Elegendő tehát megmutatni, hogy ez az összeg nullával egyenlő. Mivel $k>1$, a $\theta+\theta^2+\ldots+\theta^k$ a k-adik egységgyökök összege, azaz nulla (1.5.22. Gyakorlat). Rögzített i mellett az $ik\eta^i\theta^j$ tagok összege a fenti összeg $ik\eta^i$-szerese, tehát szintén nulla. Így ezeket i-re összegezve is nullát kapunk. Össze kell még adni a $j\eta^i\theta^j$ tagokat. Itt először a j-t rögzítjük, és az $\eta^0+\eta^1+\ldots+\eta^{m-1}=0$ összefüggést használjuk föl.

4. fejezet

Csoportok

4.1. Példák szimmetriacsoportokra

4.1.1. 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.

4.1.3. A 2.2.4. Gyakorlat szerint a kompozíció asszociatív. A 2.2.7. Gyakorlat szerint az identikus leképezés neutrális elem. Végül a 2.2.11. Gyakorlat szerint a kétoldali inverz is létezik. E gyakorlatok megoldása független attól, hogy a kompozíciót milyen sorrendben végezzük el.

4.1.9. A 4.1.7. Állítás miatt az eltolásokat is felbonthatjuk két tükrözés szorzatára, itt a két egyenesnek az eltolás irányára merőlegesnek kell lennie, de ezen belül az egyik tetszőlegesen választható. Legyen e az az egyenes, ami az adott f forgatás középpontján átmegy, és merőleges a megadott eltolás irányára. Ha t jelöli az e-re tükrözést, akkor $f = t_1 t$ és a megadott eltolás is tt_2 alakban írható alkalmas t_1, t_2 tükrözésekre. Ekkor a forgatás és az eltolás kompozíciója $t_1 t_2$ lesz, azaz eltolás vagy forgatás (attól függően, hogy a két tengely párhuzamos-egyenlő-e, vagy metsző). Hasonlóképpen gondolhatjuk meg, hogy ha a forgatást és az eltolást a másik sorrendben szorozzuk össze, akkor is eltolást vagy forgatást kapunk. Az egyenesek szögeit vizsgálva láthatjuk, hogy egy eltolás és egy α szögű forgatás bármely sorrendben vett kompozíciója szintén α szögű forgatás lesz, kivéve, ha a forgatás az identitás.

4.1.10. Legyen f a forgatás, t a tükrözés. A 4.1.6. Állítás szerint $f = tt_2$, ahol t_2 alkalmas, P-n átmenő egyenesre való tükrözés. Ezért $tf = ttt_2 = t_2$. Hasonlóan láthatjuk, hogy ft is egy P-n átmenő egyenesre való tükrözés.

4.1.15. A P pont akkor és csak akkor akkor fixpontja f-nek, ha $g(P)$ fixpontja gfg^{-1}-nek. Valóban, gfg^{-1} nyilvánvalóan fixálja $g(P)$-t. Megfordítva, ha $gfg^{-1}(Q) = Q$, akkor g^{-1}-et alkalmazva kapjuk, hogy f fixálja $P = g^{-1}(Q)$-t, tehát $Q = g(P)$ tényleg az f egy fixpontjának g-nél vett képe.

4.1.16. A $\overrightarrow{PP'}$ vektorral való r eltolást a következőképpen jellemezhetjük. Ha Q tetszőleges pont a síkon akkor Q' pontosan akkor lesz $r(Q)$, ha a $PP'Q'Q$ négyszög paralelogramma (ami lehet elfajuló is). Mivel g egybevágóság, ezért a $g(P)g(P')g(Q')g(Q)$ négyszög is paralelogramma. A grg^{-1} transzformáció a $g(Q)$ pontot $g(Q')$-be viszi. A sík minden pontja $g(Q)$ alakú, hiszen g bijekció, ezért grg^{-1} a $\overrightarrow{g(P)g(P')}$ vektorral való eltolás.

4.1.17. Az e egyenesre való t tükrözést a következőképpen jellemezhetjük. Ha Q tetszőleges pont a síkon, akkor Q' pontosan akkor lesz $t(Q)$, ha e a QQ' felező merőlegese, vagy ha $Q = Q'$ az e egyenesen van. Mivel g egybevágóság, ugyanez a mondat elmondható a $g(Q)$ és $g(Q')$ pontokra, valamint a $g(e)$ egyenesre, és ezért a $g(Q)$ és $g(Q')$ tükörképek a $g(e)$-re. A gtg^{-1} transzformáció $g(Q)$-t $g(Q')$-be viszi. A sík minden pontja $g(Q)$ alakú, hiszen g bijekció, ezért gtg^{-1} minden pontot tükröz $g(e)$-re.

4.1.18. Tegyük föl először, hogy $0^\circ \leq \alpha \leq 180^\circ$. A P pont körüli α szögű, pozitív irányú f forgatást a következőképpen jellemezhetjük. Ha Q tetszőleges pont a síkon, akkor Q' pontosan akkor lesz $f(Q)$, ha PQQ' egy olyan egyenlő szárú (esetleg elfajuló), pozitív körüljárású háromszög, melynek szárai $PQ = PQ'$, és a P csúcsnál lévő szög α. Mivel g egybevágóság, ezért $g(P)g(Q)g(Q')$ is egyenlő szárú

háromszög, melynek szárai $g(P)g(Q) = g(P)g(Q')$, és a $g(P)$ csúcsnál lévő szög α. Ha g mozgás, akkor $g(P)g(Q)g(Q')$ is pozitív körüljárású, egyébként negatív körüljárású. Ezért $g(Q')$ a $g(Q)$-nak a $g(P)$ körüli α szögű elforgatottja, mégpedig pozitív irányba, ha g mozgás, és negatív irányba különben. A gfg^{-1} transzformáció $g(Q)$-t $g(Q')$-be viszi. A sík minden pontja $g(Q)$ alakú, hiszen g bijekció, ezért gfg^{-1} minden pontot $g(P)$ körül α szöggel forgat a megfelelő irányba.

Ezzel $0^\circ \le \alpha \le 180^\circ$ esetén beláttuk az állítást. Ha $180^\circ \le \alpha \le 360^\circ$, akkor alkalmazzuk a fentieket f inverzére, ami a $360^\circ - \alpha$ (ami ugyanaz, mint a $-\alpha$) szögű forgatás. Kiderül, hogy $gf^{-1}g^{-1}$ forgatás $g(P)$ körül $-\alpha$ szöggel, ha g mozgás, és α szöggel egyébként. Mivel $gf^{-1}g^{-1}$ nyilván az gfg^{-1} inverze, ezzel az állítást f-re is igazoltuk.

4.1.20. Az $\varepsilon(z-w)+w = \varepsilon z + (1-\varepsilon)w$ képletből láthatjuk, hogy ez a forgatás az $(1-\varepsilon)w$ vektorral való eltolásnak és az origó körüli α szögű forgatásnak a kompozíciója.

4.1.21. Legyen a két forgatás f_1 és f_2, ahol $f_j(z) = \varepsilon_j(z-w_j)+w_j = \varepsilon_j z + (1-\varepsilon_j)w_j$ $(j=1,2)$ és $\varepsilon_j = \cos\alpha_j + i\sin\alpha_j$. Ekkor

$$f_2 f_1(z) = \varepsilon_2\varepsilon_1 z + \varepsilon_2(1-\varepsilon_1)w_1 + (1-\varepsilon_2)w_2\,.$$

Ha ez forgatás, akkor az egyetlen olyan pont, amely önmagába képződik, a forgatás centruma lesz. Ezért az $f_2f_1(z) = z$ egyenletet kell megoldani. Ez mindig megtehető, ha $\varepsilon_2\varepsilon_1 \neq 1$, vagyis ha a két forgatás szögének összege nem nulla. Az f_1f_2 forgáscentruma

$$w = \frac{\varepsilon_2(1-\varepsilon_1)w_1 + (1-\varepsilon_2)w_2}{(1-\varepsilon_1\varepsilon_2)}\,, \quad \text{és} \quad f_1f_2 = \varepsilon_1\varepsilon_2(z-w)+w\,.$$

Ezért ilyenkor tényleg forgatást kapunk.

4.1.27. Igen. Egy 1×1-es (ε) mátrix pontosan akkor unitér, ha $\varepsilon^{-1} = \overline{\varepsilon}$, azaz ha $|\varepsilon| = 1$. Ez kölcsönösen egyértelmű, művelettartó módon megfeleltethető a $z \mapsto \varepsilon z$ forgatásnak a síkon.

4.1.28. Ha a harmadik bázisvektort a forgatás tengelyének irányában választjuk, az első kettőt pedig a rá merőleges síkban, akkor a mátrix a következő lesz:

$$\begin{bmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Ennek determinánsa $\cos^2\alpha + \sin^2\alpha = 1$, a sajátértékek pedig $\cos\alpha \pm i\sin\alpha$ és 1.

4.1.29. Kétféle megoldást is mutatunk, az elsőt elemi geometriával, a másodikat lineáris algebra felhasználásával. Legyen $f \in \mathrm{SO}(3)$.

Ha f nem az identitás, akkor van olyan P pont, hogy $f(P) \neq P$. Az O origó rajta van a P és $f(P)$ pontok S_1 felező merőleges síkján, jelölje t az S_1 síkra tükrözést. Ekkor $tf(P) = P$, és így az $e_1 = OP$ egyenes fixen marad tf-nél. Ezért tf az e_1-re merőleges, O-n átmenő S_2 síkot is önmagába képzi (hiszen minden egybevágóság szögtartó). Mivel f mozgás, tf nem az, és így a tf transzformáció hatása az S_2 síkon a 4.1.13. Állítás miatt, csak egy S_2-beli e_2 egyenesre való tükrözés lehet (hiszen O fixpontja). Ekkor az e_2 és e_1 által kifeszített S_3 sík minden pontja fixen marad tf-nél. Az S_3-ra az origóban állított e_3 merőleges tehát tf-nél önmagába megy, és így vagy az origóra tükröződik, vagy minden pontja helyben marad. Ez utóbbi lehetetlen, mert akkor tf az identitás lenne, ami nem irányításváltó. Ezért tf az S_3 síkra tükrözés. Így $f = t(tf)$ az S_3 és S_1 síkok e_2 metszésvonala körüli forgatás.

A lineáris algebrai megoldáshoz legyen $f \in \mathrm{SO}(3)$, és jelölje $\lambda_1, \lambda_2, \lambda_3$ az f karakterisztikus polinomjának gyökeit (ezek sajátértékei f-nek). Ha valamelyik λ_i valós, akkor a hozzá tartozó sajátvektort f a λ_i-szeresébe viszi, és mivel f távolságtartó, $\lambda_i = 1$ vagy $\lambda_i = -1$.

Mivel páratlan fokú, valós együtthatós polinomnak mindig van valós gyöke (3.3.9. Következmény), a λ_i számok között van valós, például λ_1. Az f mozgás, így a determinánsa $\lambda_1\lambda_2\lambda_3 = 1$. Ha λ_2 vagy λ_3 nem valós, akkor egymás komplex konjugáltjai, hiszen a karakterisztikus polinom valós együtthatós. De akkor

$\lambda_2\lambda_3 = |\lambda_2|^2$, ami pozitív valós szám. Ezért $\lambda_1 > 0$, és így $\lambda_1 = 1$. Ha viszont λ_2 és λ_3 is valós, akkor vagy $\lambda_1 = \lambda_2 = \lambda_3 = 1$, vagy pedig két -1 fordul elő közöttük. Átszámozással ekkor is feltehető, hogy $\lambda_1 = 1$.

Jelölje e a $\lambda_1 = 1$-hez tartozó sajátvektornak az (origón átmenő) egyenesét. Ezt az egyenest a transzformáció pontonként önmagába viszi, és ezért az e-re merőleges, origón átmenő S sík is önmagába megy. Legyen g az f megszorítása az S síkra, azt kell belátnunk, hogy g forgatás. Válasszunk az S síkban két bázisvektort, a harmadikat pedig az e egyenesen. Ebben fölírva f mátrixát, majd a determinánst kiszámítva azt kapjuk, hogy $1 = \det(f) = \det(g) \cdot 1$. Ezért g mozgás, ami fixálja az origót, és így a 4.1.13. Állítás miatt forgatás.

4.1.30. Az állítás elemi geometriával igazolható a 4.1.18. Gyakorlat mintájára.

4.1.31. A keresett tükrözés rtr^{-1} (a 4.1.17. Gyakorlat miatt). Az z szám képe $\overline{z - ic} + ic = \overline{z} + 2ic$.

♫ *Második megoldás.* Legyen s a keresett tükrözés. A 4.1.7. Állítás miatt $st = r^2$, ahonnan $s = r^2t^{-1}$. Ez ugyanaz, mint a fenti eredmény, mert a 4.1.16. Gyakorlat szerint $trt^{-1} = r^{-1}$, azaz $t^2 = id$ miatt $rt^{-1} = tr^{-1}$.

4.1.32. Legyen t az e egyenesre való tükrözés, r pedig a v vektorral való eltolás. Jelölje u a v vetületét az e egyenesre, r_1 pedig az u-val való eltolást. Elemi geometriával könnyű megmutatni, hogy $t_1 = r_1^{-1}rt$ egy alkalmas, e-vel párhuzamos egyenesre való tükrözés. Persze $rt = r_1t_1$, és ez a leképezés csúsztatva tükrözés, ha $u \neq 0$, azaz r_1 nem az identitás, különben pedig a t_1 tükrözés.

Komplex számokkal is elvégezhetjük a fenti számolást. Feltehető, hogy e a valós tengely és $v = a + bi$. Ekkor $u = a$ és $t_1 : z \mapsto \overline{z} + bi$, ami a 4.1.17. Gyakorlat szerint tükrözés az $\mathrm{Im}(z) = b/2$ egyenesre. A $(tr)^{-1} = r^{-1}t^{-1}$ összefüggést használva látható, hogy ha a fordított sorrendben szorzunk, azaz eltolást komponálunk tükrözéssel, akkor szintén tükrözést vagy csúsztatva tükrözést kapunk.

Harmadik megoldásként megmutatjuk, hogy három tükrözés szorzata mindig tükrözés vagy csúsztatva tükrözés. Legyenek t_1, t_2, t_3 tükrözések. Ha a három tükörtengely iránya egyenlő, akkor a 4.1.7. Állítás szerint $t_1t_2 = t_4t_3$, ahol t_3 alkalmas tükrözés (az kell, hogy t_1 és t_2 tengelyének távolsága ugyanaz legyen, mint t_4 és t_3 tengelyének távolsága). De akkor $t_1t_2t_3 = t_4$, azaz tükrözés.

A második eset, hogy t_1 és t_2 tengelye metsző. Ekkor t_1t_2 forgatás, és a 4.1.6. Állítás szerint t_1t_2 fölírható t_4t_5 alakban, ahol t_4 és t_5 tükrözések, és t_5 tengelye merőleges t_3 tengelyére. Így t_5t_3 középpontos tükrözés, írjuk föl t_6t_7 alakban, ahol t_6 tengelye párhuzamos vagy egyenlő t_4 tengelyével, ekkor t_6 és t_7 tengelye merőleges. Tudjuk, hogy $t_1t_2t_3 = t_4t_5t_3 = t_4t_6t_7$. Ha $t_4 = t_6$, akkor a végeredmény t_7, azaz tükrözés. Ha nem, akkor t_4t_6 olyan eltolás, amelynek iránya merőleges t_6 tengelyére, és így a t_7 tengelyével egyenlő irányú. Ezért ekkor a végeredmény csúsztatva tükrözés.

A harmadik eset, hogy t_2 és t_3 tengelye metsző, ez a második esettel azonos módon intézhető el (csak a szorzások sorrendjét kell megfordítani). Érdemes észrevenni, hogy ha az r eltolás iránya párhuzamos a t tükrözés tengelyével, akkor $rt = tr$ ugyanaz a csúsztatva tükrözés.

4.1.33.

(1) Tekintsük azt a kört, ami R-en átmegy, és középpontja P, továbbá azt a másikat, amelyik R-en átmegy és középpontja Q. Mivel f távolságtartó, az $f(R)$ pontnak mindkét körvonalon rajta kell lennie. A két körvonal azonban csak két pontban metszi egymást, az egyik R, a másik pedig R tükörképe a PQ egyenesre. (Ez akkor is igaz, ha valamelyik kör a P ponttá fajul, és a két kör érintheti is egymást R-ben.)

(2) Vegyük észre, hogy (1) szerint ha f két különböző pontot fixál, akkor az ezeket összekötő egyenes minden pontja fixpont. Ha tehát f a $P \neq Q$ mellett még egy ezektől különböző R pontot is fixál, akkor az RP és RQ egyenesek pontjai is fixen maradnak. További alkalmas egyenesek behúzásával látjuk, hogy a sík minden pontja fixpont. Ha viszont R az R' tükörképébe megy f-nél, akkor jelölje t a PQ egyenesre való tükrözést. Ekkor tf^{-1} már fixálja P, Q, R mindegyikét, tehát az előzőek szerint az identitás. Innen jobbról f-fel szorozva $t = f$ adódik.

(3) Legyen $Q \neq P$ tetszőleges pont, és g egy olyan P körüli forgatás, mely Q-t elviszi $f(Q)$-ba. Ekkor $g^{-1}f$ fixálja P-t is és Q-t is, ezért (2) miatt vagy az identitás, vagy a PQ egyenesre való t tükrözés.

Az első esetben $f = g$, tehát f forgatás. A másodikban $f = gt$, ami a 4.1.10. Gyakorlat szerint tengelyes tükrözés. Mivel P fixen marad, a tengely átmegy a P ponton.

(4) Legyen P tetszőleges pont és g az az eltolás, amelyre $g(P) = f(P)$. Ekkor $g^{-1}f$ fixálja P-t, tehát (3) miatt vagy P körüli forgatás, vagy egy P-n átmenő egyenesre való t tükrözés. Az első esetben f egy forgatás és egy eltolás kompozíciója, ami a 4.1.9. Gyakorlat miatt forgatás vagy eltolás. Mivel f-nek nincs fixpontja, csak eltolás lehet. A második esetben $f = gt$, ami a 4.1.32. Gyakorlat miatt tükrözés, vagy csúsztatva tükrözés. Mivel f fixpontmentes, csakis csúsztatva tükrözés lehet.

A 4.1.13. Állítás igazolásához már csak azt kell ellenőrizni, hogy a felsorolt transzformációk mindegyike előáll legfeljebb három tükrözés kompozíciójaként. A forgatások és az eltolások két tükrözéssel kaphatók (4.1.6. és 4.1.7. Állítások), és így a csúsztatva tükrözés az egyetlen, amelyhez három tükrözés kell (az eltolás-részéhez kettő).

4.1.34. A P-t eltolhatjuk R-be, majd a Q-nak ennél az eltolásnál vett képét S-be forgathatjuk. Ezért van legalább egy olyan g mozgás, ami a feltételeknek eleget tesz. Ha f egy másik ilyen transzformáció, akkor $g^{-1}f$ fixálja a P és Q pontokat, és így a 4.1.33. Gyakorlat miatt vagy az identitás, vagy a PQ egyenesre való t tükrözés. Az első esetben $f = g$, a másodikban $f = gt$. Tehát a keresett egybevágóságok száma kettő, amelyek közül g mozgás, gt nem az.

4.1.35. A 4.1.18. Gyakorlatból láthatjuk, hogy a sík mozgáscsoportja nem kommutatív. Valóban ha $P \neq Q$ a sík pontjai és r a P-t Q-ba képező eltolás f pedig egy P körüli 90 fokos forgatás, akkor rfr^{-1} a Q körüli 90 fokos forgatás (de ha a csoport kommutatív lenne, akkor f-fel kellene egyenlőnek lennie). Ennél egyszerűbben is gondolkozhatunk: az f egyetlen fixpontja P, az rfr^{-1} egyetlen fixpontja viszont Q, tehát nem lehetnek egyenlőek.

Egy P középpontú körvonal mozgásai a P körüli forgatások. Ezek csoportja kommutatív, hiszen egy α és β szögű forgatás szorzata mindkét sorrendben az $\alpha + \beta$ szögű forgatás.

Végül a 4.1.18. Gyakorlatból az is adódik, hogy ha f a P körüli 90 fokos forgatás, és t egy P-n átmenő egyenesre való tükrözés, akkor tft^{-1} a P körüli -90 fokos forgatás, tehát nem egyenlő f-fel. Ezért a kör egybevágóságainak csoportja nem kommutatív.

4.1.36. Ha $g(P) = P$, akkor $gf(P) = fg(P) = f(P)$, tehát $f(P)$ is fixpontja g-nek. Vagyis ha Y a g fixpontjainak halmaza, akkor $f(Y) \subseteq Y$. Az $fg = gf$ egyenlőséget balról és jobbról f inverzével szorozva $gf^{-1} = f^{-1}g$ adódik. Ezért f^{-1} is fölcserélhető g-vel, és így az iménti bizonyításból $f^{-1}(Y) \subseteq Y$. Az f-et alkalmazva $Y \subseteq f(Y)$, tehát $Y = f(Y)$.

4.1.37. Pontosan akkor, ha a két egyenes egyenlő, vagy merőleges. Valóban, jelölje t_i az e_i-re való tükrözést. Ha $t_1t_2 = t_2t_1$, akkor a 4.1.36. Gyakorlat miatt t_1 az e_2 egyenest önmagába viszi és így e_2 vagy e_1-gyel egyenlő, vagy arra merőleges. Ha egyenlők, akkor $t_1 = t_2$, ezek fölcserélhetők. Ha merőlegesek, akkor t_1t_2 és t_2t_1 is a metszéspontjukra való tükrözés a 4.1.6. Állítás szerint.

♫ A gyakorlat egésze könnyen megkapható a 4.1.6. és a 4.1.7. Állításokból is. De felhasználhatjuk a 4.1.17. Gyakorlatot is, hiszen $t_1t_2 = t_2t_1$ azzal ekvivalens, hogy t_1-nek a t_2-vel vett konjugáltja t_1.

4.1.38. Jelölje f_i az e_i körüli, 180 fokos forgatást. Ha $e_1 = e_2$, akkor f_1f_2 az identitás. Ha nem, akkor e_1 és e_2 egy S síkot határoznak meg. Legyen e_3 az S-re az e_1 és e_2 egyenesek P metszéspontjában emelt merőleges. Ezt mindkét forgatás P-re tükrözi, és így f_1f_2 az e_3 minden pontját helyben hagyja. Az S síkon az f_i tükrözés az e_i egyenesre, a kompozíciójuk tehát a P körüli, 2α szögű forgatás a 4.1.6. Állítás miatt. Ezért f_1f_2 az e_3 egyenes körüli 2α szögű forgatás.

A 4.1.37. Gyakorlat gondolatmenetét alkalmazva láthatjuk, hogy f_1 akkor és csak akkor cserélhető föl f_2-vel, ha a két tengely egyenlő, vagy merőleges.

4.1.39. Ha f nem az identitás, akkor van olyan P, hogy $f(P) \neq P$. Legyen S e két pont felező merőleges síkja, O pedig az őket összekötő szakasz felezőpontja. Mivel f^2 az identitás, $f\big(f(P)\big) = P$, ezért a $Pf(P)$ egyenest f saját magába képzi. Egy pont akkor és csak akkor eleme az S síknak, ha P-től és $f(P)$-től ugyanakkora távolságra van. Ezért f az S síkot saját magába képzi, és így $f(O) = O$. Tehát f az S síknak

olyan egybevágósági transzformációja, amelynek négyzete az identitás. A 4.1.13. Állítás miatt ez vagy az identitás, vagy az O pontra tükrözés, vagy pedig egy O-n átmenő egyenesre tükrözés.

Legyen t az S síkra való tükrözés. Ekkor tf fixálja a P pontot, és ezért a $Pf(P)$ egyenest is. Ezért $f = ttf$ a $Pf(P)$ egyenest O-ra tükrözi. Így a következő lehetőségek adódnak.

(1) f az identitás.
(2) f síkra tükrözés.
(3) f középpontos tükrözés.
(4) f forgatás egy egyenes körül 180 fokkal.

4.1.40. Akkor és csak akkor, ha $n = 1$. Ha $n = 1$, akkor 1×1-es mátrixokról van szó, amelyek nyilván fölcserélhetők. 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 2.2.22. Feladat).

4.2. Permutációk előjele és ciklusfelbontása

4.2.3. 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.

4.2.4. 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 nemkommutatív csoport. Ha $n > 3$, akkor az f permutációt kiterjeszthetjük az $\{1, 2, \ldots, n\}$ 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 fölcserélhető elemet kapunk. Ezért $n \geq 3$ esetén S_n nem kommutatív. Az S_1 és S_2 csoportok viszont Abel-félék. Ez közvetlenül is ellenőrizhető, de általában is könnyen adódik, hogy minden legfeljebb kételemű csoport kommutatív. Később belátjuk majd, hogy a prímelemű csoportok is kommutatívak.

4.2.7. Mindkét oldal könnyen kiszámolhatóan az alábbi permutáció.

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

4.2.8. 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 föl 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.

4.2.10. Az igaz, hogy $f \circ g$ és $g \circ f$ általában különbözők, viszont $\mathrm{sg}(f)$ és $\mathrm{sg}(g)$ egész számok, és ezért fölcserélhetők. Így persze $f \circ g$ és $g \circ f$ előjele mindig ugyanaz lesz.

4.2.18. Mindkét ciklus az a permutáció, amely az x_j elemet x_{j+1}-be viszi (ahol $1 \leq j < k$), az x_k-t x_1-be, az X összes többi elemét pedig saját magába.

4.2.20. 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.

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.

4.2.22. Az egyelemű ciklusokat akár kiírjuk, akár nem, a permutáció nyilván nem változik (hiszen minden egyelemű ciklus az identitás). Hasonlóképpen egy-egy ciklus fölírását akármelyik eleménél elkezdhetjük. A diszjunkt ciklusokra bontás ezektől a változtatásoktól és a sorrendtől eltekintve lesz egyértelmű. Ez látszik a 4.2.21. 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.

4.2.23. 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.

4.2.25. 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 fölírást 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 (4.2.24. 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. Végül is (1234)(35)(1432)(35) = (345) adódik, ami páros permutáció. (Azt, hogy ez páros permutáció, az eredeti (1234)(35)(1432)(35) alakból is láthatjuk, hiszen abban négy páros hosszú ciklus, vagyis négy páratlan permutáció szerepel.)

Az $(12345)(234)(12345)^{-1}$ szorzatban egy ciklus inverze szerepel. Általában

$$(x_1, x_2, \ldots, x_{k-1}, x_k)^{-1} = (x_k, x_{k-1}, \ldots, x_2, x_1)\,,$$

hiszen az inverznél a körön a nyilak mentén visszafelé haladunk. Az eredmény (345), ami páros.

Az $[(12)(23)(34)]^{1222}$ permutáció 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.

Végezetül 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 mennyié, 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 szám is helyet cserél. Az előjelet a kapott transzpozíciók számából olvashatjuk le. A végeredmény: ez a permutáció pontosan akkor páros, ha n néggyel osztva nullát vagy egyet ad maradékul.

4.2.26. Mivel (12) és (345) diszjunkt ciklusok, ezért egymástól függetlenül, diszjunkt halmazokon operálnak (lásd a 4.2.20. 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, vagyis hatosával periodikusan ismétlődnek az alábbi táblázat szerint:

$$[(12)(345)]^1 = (12)(345) \qquad [(12)(345)]^2 = (354)$$
$$[(12)(345)]^3 = (12) \qquad [(12)(345)]^4 = (345)$$
$$[(12)(345)]^5 = (12)(354) \qquad [(12)(345)]^6 = id\,.$$

Tehát hat különböző hatvány van, és $f^k = f^\ell$ akkor és csak akkor, ha $6 \mid k - \ell$.

4.2.27. Lásd a 2.2.5. Feladat megoldását. Második megoldásként a 4.2.23. Gyakorlatból látjuk, hogy szomszédos elemek cseréjével minden ciklus előáll.

4.2.28. 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

$$(i, i+1) = f^{i-1}(12)f^{n-i+1}\,.$$

Így mozdulatainkkal bármely két szomszédos lap megcserélhető. A 4.2.27. 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.

4.2.29. Most az (13) és az (1234) permutációkról van szó, és nem kapjuk meg S_4 minden elemét. Egy ilyen bizonyításban kellemetlen, 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 fölírjuk 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.

4.2.30. 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 fölírható hármasciklusok szorzataként.

Tekintsük 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

$$(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)\,.$$

4.2.31. Tegyük föl, hogy $f \circ (1, 2, \ldots, n) = (1, 2, \ldots, n) \circ f$, és jelölje i az $f(1)$ elemet. Tudjuk, hogy j-t az $(1, 2, \ldots, n)$ 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

$$f(2) = \big(f \circ (1, 2, \ldots, n)\big)(1) = \big((1, 2, \ldots, n) \circ f\big)(1) = i +_n 1\,.$$

Az 1 helyett 2-t helyettesítve $f(3) = i +_n 1 +_n 1 = i +_n 2$, és így tovább, $f(j) = i +_n (j-1) = j +_n (i-1)$. Vagyis f az $(1, 2, \ldots, n)$ ciklus $i - 1$-edik hatványa. Ezek nyilván fölcserélhetők $(1, 2, \ldots, n)$-nel, így összesen n darab f permutáció felel meg a feltételeknek.

4.2.32. Amikor kiszámítjuk az $(1, 2, \ldots, n)$ ciklus k-adik hatványát, akkor az 1-ből elindulva k-asával lépegetünk egy n hosszúságú körön. Ezért a „bolhás” 1.5.9. Feladat szerint $n/(n, k)$ lépésben érünk vissza a kiindulópontra. Vagyis az 1 (és bármelyik másik elem is) egy $n/(n, k)$ hosszú ciklusba kerül. (Érdemes ezt például az $(123456)^4 = (153)(264)$ esetében ellenőrizni.) Vagyis $(1, 2, \ldots, n)^k$ egyforma hosszú diszjunkt ciklusok szorzata.

Megfordítva, tegyük föl, hogy adva van tetszőlegesen k darab m hosszú diszjunkt ciklus szorzata. Vegyük az $(1, 2, \ldots, km)^k$ permutációt, ez a fentiek szerint szintén k darab m hosszú diszjunkt ciklus szorzata (csak más számok vannak a ciklusokban). Tehát át tudjuk számozni az $(1, 2, \ldots, km)$ 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 $(1324)^2 = (12)(34)$.)

4.2.33. Tegyük föl, 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 föl, 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.

4.2.34. Minden k hosszú ciklus $k-1$ transzpozíció szorzata (4.2.23. Gyakorlat). Ha S_n egy permutációját diszjunkt ciklusok szorzatára bontjuk, akkor ezek összhossza legfeljebb n, és így összesen legfeljebb $n-1$ transzpozíció szerepel.

Az $(1, 2, \ldots, n)$ 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 $(1, 2, \ldots, n)$ ciklus többszöri alkalmazásával bármelyik pontból bármelyik pontba el lehet jutni. Így az előző feladat (2) állítása miatt a G gráf összefüggő, és az E.2.5. Tétel miatt legalább $n-1$ éle van.

4.2.35. Az Útmutatóban leírtakat folytatva tegyük föl, 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. Izomorfizmus, ciklikus csoportok

4.3.2. Legyen $G = \{e, b\}$ és $H = \{f, c\}$ a két csoport, ahol e, illetve f a két neutrális elem. Ekkor $e*x = x*e = x$ és $f*y = y*f = y$. Továbbá $b*b = b$ nem lehet, mert b-vel egyszerűsítve $b = e$ adódna. Ezért $b*b = e$, és hasonlóan $c^2 = f$. De akkor az $e \mapsto f$ és $b \mapsto c$ megfeleltetés izomorfizmus: az $e*e$, $e*b$, $b*e$, $b*b$ szorzatok mindegyikét tartja.

4.3.4. 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 (mint permutáció) 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.

4.3.5. Ha $\varphi : G \to H$ és $\psi : H \to K$ homomorfizmusok, akkor $\psi \circ \varphi : G \to K$ is szorzattartó, hiszen

$$\begin{aligned}(\psi\circ\varphi)(xy) &= \psi\big(\varphi(xy)\big) = \psi\big(\varphi(x)\varphi(y)\big) = \\ &= \psi\big(\varphi(x)\big)\psi\big(\varphi(y)\big) = (\psi\circ\varphi)(x)(\psi\circ\varphi)(y)\,.\end{aligned}$$

Tegyük föl, 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.

4.3.6. 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.

4.3.7. Tegyük föl, 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

$$h_1h_2 = \psi(g_1)\psi(g_2) = \psi(g_1g_2) = \psi(g_2g_1) = \psi(g_2)\psi(g_1) = h_2h_1\,.$$

Az állítás megfordítására ellenpélda az, ha egy nemkommutatív G csoport (egyetlen) homomorfizmusát tekintjük az egyelemű csoportba. Ilyen például az S_n szimmetrikus csoport, ha $n \geq 3$ (4.2.4. Gyakorlat). Kevésbé triviális példa, ha ψ az előjelképzés az S_n csoportból a kommutatív $\{1, -1\}$ csoportba. Ellenpéldát kapunk akkor is, ha a determinánsképzést, mint homomorfizmust tekintjük a (legalább) kétszer kettes invertálható mátrixok szorzáscsoportján.

4.3.10. Ha az Olvasónak gondot jelent az alábbiak követése, akkor próbálja meg az 1.5. szakaszban leírt bizonyításokat átvinni az általános esetre. Mi a 3.2.9. 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 föl, 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 3.2.9. 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 1.5.10. Tétel bizonyításában. Végül ha $o(g) = 1$, akkor $g = g^1 = 1$, vagyis g az egységelem (aminek tényleg már az első hatványa is 1).

4.3.11. A 4.1.13. Állításban osztályoztuk a sík egybevágóságait.

(1) Az identitás az egyetlen elem, aminek a rendje 1.
(2) A nem identikus eltolások rendje végtelen.
(3) Az α szögű forgatás rendje ugyanaz, mint a $\cos\alpha + i \sin\alpha$ komplex szám rendje, hiszen a két csoport izomorf. Ez utóbbit az 1.5.11. Állításban határoztuk meg.
(4) A tengelyes tükrözések rendje 2.
(5) Egy csúsztatva tükrözés rendje végtelen (ha nem tükrözésről van szó), mert a négyzete nemtriviális eltolás.

4.3.14. A hatványozás azonosságai (2.2.20. 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.

4.3.15. 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 föl, 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

$$\psi(g^n) = \psi\big((g^{-1})^k\big) = \big(\psi(g^{-1})\big)^k = \big(\psi(g)^{-1}\big)^k = \psi(g)^n .$$

4.3.16. 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.

4.3.18. 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 $k = 1, 5, 7, 11$.

4.3.19. Tegyük föl, 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 $h = \psi(g) = \psi(b^n) = \psi(b)^n$.

A megfordításra ellenpélda, ha egy nem ciklikus G csoport (egyetlen) homomorfizmusát tekintjük az egyelemű csoportba, vagy ha a ψ az előjelképzést tekintjük az S_n szimmetrikus csoportból a ciklikus $\{1, -1\}$ csoportba. Ellenpéldát kapunk akkor is, ha a determinánsképzést, mint homomorfizmust tekintjük egy véges test fölötti legalább kétszer kettes mátrixok között, mert minden véges test multiplikatív csoportja ciklikus (4.3.22. Tétel).

4.3.25. Egy Abel-csoportban könnyen láthatóan mindig részcsoportot alkot az összes olyan g elem, 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).

4.3.28. Semelyik kettő nem izomorf, mert $\mathbb{R}^+$-nak a nullán kívül nincs véges rendű eleme, $\mathbb{R}^\times$-ben csak az 1 és -1 véges rendű, $\mathbb{C}^\times$-ben viszont végtelen sok véges rendű elem van (a komplex egységgyökök).

4.3.29. 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.

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 bizonyítani a 4.4.22. 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 a 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.

4.3.30. 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.

4.3.31. A 4.3.12. Állítást alkalmazva a 4.2.25. 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 $n > 1$).

4.3.32. 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 föl, hogy $(1, x_1, \ldots, x_{n-1}) = (1, y_1, \ldots, y_{n-1})$. Az 1 elem 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.

4.3.33. A 4.3.12. 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 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 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 $\{a, b, c, d\}$-t már kiválasztottuk, 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.

4.3.34. Mivel $(n, n/m) = n/m$, ezért a hatvány rendjének képlete szerint $o\big(g^{n/m}\big) = n/(n/m) = m$. 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. A gyakorlat első állítása miatt g-nek van p rendű hatványa.

4.3.35. 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.

4.3.36. A hatvány rendjének képletét (4.3.10. 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 $o(h) = mn$.

4.3.37. Az első állítás igaz a 4.3.23. Lemma miatt. A második állítás nem igaz. Például a 4.3.29. Gyakorlat szerint a $\mathbb{Z}_8^\times$ csoportban három másodrendű elem van, holott $\varphi(2) = 1$.

4.3.38. Ha ε rendje 3^k és η rendje 3^ℓ, ahol például $k \leq \ell$, akkor az $\varepsilon\eta$ számot 3^ℓ-edik hatványra emelve 1-et kapunk, tehát $\varepsilon\eta$ rendje osztója 3^ℓ-nek, és így 3-hatvány. Mivel az elemek rendjei végesek, az inverzre való zártságot nem kell ellenőrizni. Ez a csoport nem ciklikus, hiszen minden elemének csak véges sok hatványa van, a csoport viszont végtelen.

4.3.39. Legyen $o(g) = n$ és $o(h) = m$, ekkor $(gh)^{nm} = (g^n)^m(h^m)^n = 1$, 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 fölcserélhetők, a g rendje 2, a h rendje 3, de a $gh = (23)$ szorzat rendje 2, és nem 6.

4.3.40. Az $(ab)^2 = 1$ összefüggést balról a-val, jobbról pedig 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 ellenpélda. Ebben négy forgatás és négy tükrözés van, valamennyinek a negyedik hatványa az identitás. Ugyanakkor egyik tengelyes tükrözés sem cserélhető föl egy 90 fokos forgatással. Ez közvetlen geometriai megfontolásokkal vagy a 4.1.23. Állítás segítségével látható be.

4.3.41. 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. Az Olvasót arra biztatjuk, hogy e második bekezdés módszerével is hozza ki az állítás másik irányát, amit az előző bekezdésben elemien (rend nélkül) igazoltunk.

♫ 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 $o(a) \mid k$.

4.4. Mellékosztályok, Lagrange tétele

4.4.1. Ha H részcsoport, akkor $a, b \in H$ esetén $b^{-1} \in H$, és így $ab^{-1} \in H$. Megfordítva, tegyük föl, 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 föl, 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, hogy $Hh = H$.

4.4.14. Nyilván $a = a1 \in aH$. Ha $a \in bH$, akkor az aH és bH mellékosztályoknak van közös eleme (az a elem), és így megegyeznek.

♫ Az Olvasó 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 $hH = H$.

4.4.15. A keresett mellékosztályok a következők (mindegyiket kétszer soroltuk föl, hiszen két elemük van).

$$\begin{aligned} idH &= \{id, (12)\} & Hid &= \{id, (12)\} \\ (12)H &= \{(12), id\} & H(12) &= \{(12), id\} \\ (123)H &= \{(123), (13)\} & H(123) &= \{(123), (23)\} \\ (132)H &= \{(132), (23)\} & H(132) &= \{(132), (13)\} \\ (13)H &= \{(13), (123)\} & H(13) &= \{(13), (132)\} \\ (23)H &= \{(23), (132)\} & H(23) &= \{(23), (123)\}. \end{aligned}$$

Három bal oldali és három jobb oldali mellékosztály van, ezek azonban egymással nem mind egyenlők: ugyan $idH = (12)H = H(12) = Hid$, de a másik két bal oldali mellékosztály, azaz $(123)H = (13)H$ és $(132)H = (23)H$ különbözik a másik két jobb oldali mellékosztálytól, azaz $H(123) = H(23)$-tól és $H(132) = H(13)$-tól is. Mind a bal oldali, mind a jobb oldali mellékosztályok S_3-nak egy-egy (különböző) partícióját alkotják:

$$\big\{id, (12) \,\big|\, (123), (13) \,\big|\, (132), (23)\big\}, \quad \text{illetve} \quad \big\{id, (12) \,\big|\, (123), (23) \,\big|\, (132), (13)\big\}.$$

4.4.16. Ha $g(Q) = P$, akkor $f^{-1}(P) = Q$ (azaz $f(Q) = P$) pontosan akkor teljesül, ha $h = fg^{-1} \in H$, azaz ha $f = hg$. Ezért a kérdéses f elemek a Hg mellékosztályt alkotják.

Tegyük föl, hogy $P \neq Q$, belátjuk, hogy a kapott $Hg = \{f : f(Q) = P\}$ jobb oldali mellékosztály nem bal oldali mellékosztály H szerint.

♫ Ez szemléletesen világos: Hg azokból a transzformációkból áll, amelyek Q-t P-be viszik, a $g'H$ pedig azokból, amelyek P-t a rögzített $R = g'(P)$-be viszik, és ez a két halmaz érezhetően nem ugyanaz.

Tegyük föl, hogy $Hg = g'H$ és legyen $R = g'(P)$. Ha r az az eltolás, amely Q-t P-be viszi, akkor $r \in Hg = g'H$, tehát $r(P) = R$. Ha k a 90 fokos forgatás P körül, akkor $kr(Q) = P$, azaz $kr \in Hg = g'H$. Ezért $kr(P) = R$. Vagyis az $R = r(P)$ pont megegyezik a P körüli 90 fokos elforgatottjával. Így $r(P) = R = P$, azaz r az identitás, ami ellentmond annak, hogy $r(Q) = P \neq Q$.

4.4.17. 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.

4.4.18. Ha aH bal oldali mellékosztály, akkor $(aH)^{-1} = H^{-1}a^{-1} = Ha^{-1}$, ami egy jobb oldali mellékosztály. Ugyanígy egy jobb oldali mellékosztály komplexusinverze bal oldali mellékosztály lesz. Mivel inverz inverze az eredeti mellékosztály, egy kölcsönösen egyértelmű megfeleltetést kaptunk a bal és jobb oldali mellékosztályok halmaza között.

♫ Azt nem tehetjük meg, hogy az aH mellékosztályhoz a Ha mellékosztályt rendeljük, mert ez a megfeleltetés általában nem jóldefiniált. Ha ugyanis adott egy M bal oldali mellékosztály, melynek a és b is elemei, akkor $M = aH = bH$, de nem biztos, hogy $Ha = Hb$ is teljesül, és így nem tudhatjuk, hogy M-hez Ha-t vagy Hb-t rendeljük-e hozzá. Például a 4.4.15. Gyakorlat megoldása szerint $(123)H = (13)H$, de $H(123) \neq H(13)$ az S_3 csoport $H = \{id, (12)\}$ részcsoportjára.

4.4.22. Legyen $\overline{a}$ az a-nak az n-nel való osztási maradéka. Ez is relatív prím n-hez, és ezért eleme a $\mathbb{Z}_n^\times$ csoportnak. E csoport rendje $\varphi(n)$, és így a 4.4.21. 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.

4.4.24.

(1) Igen, az osztályok a $\mathbb{Z}^+$ csoport $1848\,\mathbb{Z}^+$ részcsoportja szerinti mellékosztályok (a számelmélet nyelvén 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, ahány eleme f értékkészletének. 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 $f(a) = u$.

4.4.25. 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 4.3.27. 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 (4.3.29. Gyakorlat). A két triviális részcsoporton kívül tehát három másodrendű részcsoport van, amit egy-egy másodrendű elem az egységelemmel együtt alkot.

Az A_4 csoport elemei a hármasciklusok, melyek rendje 3, a két diszjunkt transzpozíció szorzataként írható permutációk, amelyek másodrendűek, és az identitás. Legyen H negyedrendű részcsoportja A_4-nek. Negyedrendű csoportban az elemek rendje 1, 2 és 4 lehet. Mivel negyedrendű elem nincs A_4-ben, ezért H-ban az identitás mellett 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.

♫ A szorzás helyett észrevehetjük azt is, hogy ezek a permutációk egy olyan téglalap szimmetriái, amely nem négyzet, és ezért részcsoportot alkotnak S_4-ben (4.5.17. Gyakorlat).

4.4.26. Legyen a kérdéses körvonal középpontja P, ekkor a körvonal egybevágóságai a P körüli forgatások (ezek a mozgások, amelyek egy H részcsoportot alkotnak), továbbá a P-n átmenő egyenesekre való tükrözések (4.1.13. Állítás). Legyenek t és s ilyen tükrözések. Ekkor $f = ts$ egy P körüli forgatás (4.1.6. Állítás). Ezért $s = tf$, vagyis s benne van a tH mellékosztályban. Ez rögzített t mellett minden s tükrözésre igaz, és így a H szerinti bal mellékosztályok H és tH, azaz H indexe 2.

A sík mozgáscsoportja esetében hasonlóan járunk el. Rögzítsünk egy t tengelyes tükrözést a síkon. A 4.1.13. Állításban felsorolt transzformációkat végignézve láthatjuk, hogy ha g nem mozgás, akkor tg már az. Ezért a mozgások K részcsoportja szerint csak két bal mellékosztály van: K és tK.

♫ Valójában a mozgás definíciójából adódik, hogy két mellékosztály van, az irányítástartó transzformációk a mozgások, az irányításváltók pedig a másik mellékosztály elemei. Azért alkotnak ezek is csak egyetlen mellékosztályt, mert ha g és h irányításváltó transzformációk, akkor g^{-1} is az, és így $g^{-1}h$ már irányítástartó. Ehhez már csak azt kell hozzátenni, hogy a gyakorlatban szereplő mindkét csoportban van is irányításváltó transzformáció (tengelyes tükrözés).

4.4.27. 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.

4.4.28. Ha G véges, akkor a $|G : H| = |G|/|H|$ összefüggés felhasználásával azonnal adódik a gyakorlat utolsó állítása, 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 $|K : H|$ 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 $|G : H| = k|G : K|$.

4.4.29. Megmutatjuk, hogy ha H és K részcsoportok a G csoportban, 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 oldali mellékosztály előáll egy H szerinti és egy K szerinti bal oldali mellékosztály metszeteként. Így $|G : (H \cap K)| \leq |G : H| \cdot |G : K|$.

♫ A megoldáshoz hozzátartozik, hogy ez a becslés nem javítható, vagyis hogy $|G : (H \cap K)| = |G : H| \cdot |G : K|$ előfordulhat. Erre a legtriviálisabb példa az, amikor $H = K = G$. Megfelel a $G = \mathbb{Z}_8^\times$ csoportban $H = \{1, 3\}$ és $K = \{1, 5\}$ is. A 4.9. szakaszban definiált direkt szorzat segítségével további példákat is könnyen mutathatunk.

4.4.30. A $h \mapsto ghg^{-1}$ megfeleltetés a g-vel való konjugálás, ami a G csoportot önmagára képző izomorfizmus (4.3.4. Gyakorlat), és így minden részcsoportot egy vele izomorf részcsoportba visz. Nyilván $gH = gHg^{-1}g = Kg$, tehát az utolsó állítás is igaz.

4.4.31. Az ab alakú szorzatokat kell megszámolni, ahol $a \in A$ és $b \in B$. Az (a, b) párok száma $|A||B|$, tehát azt kell megmutatni, hogy mindegyik ab szorzatot $|A \cap B|$-féleképpen kapjuk meg. Legyen a és b rögzített, és tegyük föl, hogy $ab = a_1b_1$, ahol $a_1 \in A$ és $b_1 \in B$. Innen $a^{-1}a_1 = bb_1^{-1}$, jelölje ezt az elemet c. Ekkor $c = a^{-1}a_1 \in A$ és $c = bb_1^{-1} \in B$, tehát $c \in A \cap B$. Nyilván $a_1 = ac$ és $b_1 = c^{-1}b$. Megfordítva, ha $c \in A \cap B$, akkor az $a_1 = ac \in A$ és $b_1 = c^{-1}b \in B$ elemekre $ab = a_1b_1$. Ezért az olyan (a_1, b_1) párok, ahol $ab = a_1b_1$, kölcsönösen egyértelmű megfeleltetésben állnak $A \cap B$ elemeivel.

4.4.32. 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 $o(g) = 2$.

4.4.33. 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 föl, 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 4.3.23. 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.

4.4.34. 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. Pálya és stabilizátor

4.5.7. Egy négyzetnek nyolc 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 alkotja a D_4 csoportot.

A négyzet középpontja csak önmagába mehet D_4 elemeinél, ez tehát egyelemű pálya. A két átló egyenesének többi pontja mind négy-négy helyre mehet, tehát négyelemű pályákat kapunk. Ugyanez a helyzet az oldalfelező merőlegesek pontjaival is. A többi pontnak mind a nyolc képe különböző lesz.

A négyzet középpontját D_4-nek mind a nyolc eleme fixen hagyja, vagyis a stabilizátor maga D_4. Azok a pontok, amelyeknek összesen négy képe van D_4 elemeinél, 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 D_4 elemei közül. Így egy pont képeinek száma szorozva a pontot helyben hagyó transzformációk számával mindig nyolcat ad, tehát D_4 elemszámát.

4.5.10. 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 $\{B, C\}$ pálya 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 $2n$.

4.5.11. 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 minden permutáció cserék szorzata, ezért S_4 mindegyik eleme megkapható egy alkalmas egybevágósági transzformációval.

4.5.13. 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.

4.5.16. 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.

4.5.17. Legyen $ABCD$ egy olyan téglalap, ami nem négyzet. Négy szimmetria biztosan van: az identitáson kívül a két oldalfelező merőlegesre való tükrözés, illetve a középpontos tükrözés. Ezek együtt a csúcsok halmazán tranzitívak. Az A csúcstól a másik három csúcs csupa különböző távolságra van, hiszen ez a téglalap nem négyzet. Ezért ha az A csúcs 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 az $(AB)(CD)$ permutáció a csúcsok halmazán. 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 4.4.25. Gyakorlatban.

4.5.20. 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. Az elemeket ugyanúgy jelöljük,

mint a 4.1.23. Állításban: $f = (1234)$, $f^2 = (13)(24)$, $f^3 = (1432)$, $t = (12)(34)$, $tf = (24)$, $tf^2 = (14)(23)$, $tf^3 = (13)$.

D_4	id	f	f^2	f^3	t	tf	tf^2	tf^3
id	id	f	f^2	f^3	t	tf	tf^2	tf^3
f	f	f^2	f^3	id	tf^3	t	tf	tf^2
f^2	f^2	f^3	id	f	tf^2	tf^3	t	tf
f^3	f^3	id	f	f^2	tf	tf^2	tf^3	t
t	t	tf	tf^2	tf^3	id	f	f^2	f^3
tf	tf	tf^2	tf^3	t	f^3	id	f	f^2
tf^2	tf^2	tf^3	t	tf	f^2	f^3	id	f
tf^3	tf^3	t	tf	tf^2	f	f^2	f^3	id

4.5.21. Elegendő az I^2, J^2, K^2, illetve az IJ, JI, IK, KI, JK, KJ mátrixszorzásokat elvégezni.

4.5.22. 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.

4.5.23. Jelölje C a φ értékkészletét. Ha $h_1, h_2 \in C$, akkor van olyan $g_i \in G$, melyre $\varphi(g_i) = h_i$ (ahol $i = 1, 2$). Mivel φ művelettartó, $\varphi(g_1 g_2) = h_1 h_2$, ezért $h_1 h_2$ benne van C-ben. Tudjuk, hogy minden csoporthomomorfizmus megőrzi az egységelemet és az inverzet is (2.2.44. Feladat). Ezért $1_H = \varphi(1_G) \in C$, és $h_1^{-1} = \varphi(g_1^{-1}) \in C$, azaz C tényleg részcsoport.

4.5.25. Az izomorfiaosztályok: $\{\mathbb{Z}_2^+, \mathbb{Z}_3^\times, \mathbb{Z}_6^\times, S_2\}$, $\{\mathbb{Z}_3^+, A_3\}$, $\{\mathbb{Z}_4^+, \mathbb{Z}_5^\times\}$, $\{\mathbb{Z}_8^\times, \mathbb{Z}_{12}^\times\}$, $\{S_3, D_3, \mathrm{GL}(2, \mathbb{Z}_2)\}$, $\{D_4\}$, $\{Q\}$, $\{\mathbb{Z}_8^+\}$. 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 $\mathrm{GL}(2, \mathbb{Z}_2)$ esetén pedig a $\mathbb{Z}_2$ fölötti kétdimenziós vektortér összesen három, nem nulla vektora (hiszen a hat mátrixhoz tartozó hat lineáris transzformáció nyilván csupa különböző permutációt ad ezen a három vektoron). Az utolsó három (nyolcadrendű) csoport közül semelyik kettő sem izomorf: egyetlen kommutatív van, a másik kettőben pedig nem ugyanaz a negyedrendű elemek száma (lásd 4.5.22. Feladat).

4.5.26. A legtöbb esetben csak az eredményt adjuk meg, a könnyű számolást az Olvasóra hagyjuk.

(1) Pályák: origó középpontú körök, illetve maga az origó. Stabilizátorok: kételeműek (az identitás és egy tengelyes tükrözés), kivéve az origót, melynek stabilizátora az egész csoport.

(2) Pályák: az x-tengellyel párhuzamos egyenesek. Stabilizátorok: egyeleműek.

(3) Már láttuk a 4.5.10. Gyakorlatban, hogy ez a csoport kételemű. Pályák: 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 pályákhoz az egész (kételemű) csoport, kételemű pályához egyelemű stabilizátor tartozik.

(4) Legyen A a kiválasztott csúcs, és jelölje B, C, D a három szomszédját. Mivel a kocka szimmetriacsoportja 48 elemű (4.5.9. Állítás), amely a csúcsokon tranzitív, az A csúcs G stabilizátora $48/8 = 6$ elemű. Ezeknél a szimmetriáknál nemcsak A, hanem a vele átellenes A' 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 pályája G-nél a háromelemű $\{B, C, D\}$ halmaz.

Jelölje a B, C, D csúcsokkal átellenes csúcsokat rendre B', C', D'. A G elemei ezeket „ugyanúgy” mozgatják, mint az eredeti csúcsokat (hiszen testátló testátlóba megy minden szimmetriánál). Például az AA' testátló körüli egyik 120 fokos forgatás a $\{B, C, D\}$ halmazon (BCD) cikluskén, a

$\{B', C', D'\}$ halmazon pedig $(B'C'D')$ ciklusként hat. Így $\{B', C', D'\}$ is pályája G-nek. Vagyis a G csoportnak két egyelemű és két háromelemű pályája van.

Az A és A' csúcsok G-beli stabilizátora maga $G \cong D_3$. 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. Ugyanígy a $\mathbb{Z}_2^+$ csoporttal izomorf a fennmaradó öt csúcs stabilizátora is.

(5) Tranzitív (vagyis $\{1, 2, 3, 4\}$ egyetlen pálya), az x pont stabilizátora az x-et nem tartalmazó két hármasciklus és az identitás, azaz egy háromelemű ciklikus csoport.

4.5.27. 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 téglalapnak négy szimmetriája van (4.5.17. Gyakorlat). A rombusznak is négy szimmetriája van: az átlókra tükrözés, a középpontos tükrözés, és az identitás, ezek is Klein-csoportot alkotnak. A négyzetnek nyolc szimmetriája van, ezek a D_4 diédercsoportot alkotják.

4.5.28. Az eredmények a következők.

(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 (a kocka és az oktaéder úgynevezett duális poliéderek), és így a kocka minden szimmetriája az oktaédernek is szimmetriája, és viszont . Így az oktaédernek is 48 szimmetriája van.

4.5.29. Az AB élet az AC élbe elviszi egy átlósíkra való tükrözés. Így sorban haladva minden él minden élbe elvihető, tehát G tényleg tranzitív az élek halmazán. 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 pontosan ennek a négyzetnek az egybevágóságai, vagyis 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.

♫ Ha a kockát négyzet alapú egyenes hasábnak képzeljük, és csak az ennek megfelelő szimmetriákat vesszük, akkor is egy 16 elemű részcsoportot kapunk (4.5.28. Gyakorlat (2)).

4.5.30. 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 pályáját, akkor az x stabilizátorának az elemszáma $|G|/|O|$. Amikor az x az O pályát befutja, akkor a (g, x) párok száma $|O||G|/|O| = |G|$ lesz. Így P elemszáma a pályák számának $|G|$-szerese.

4.5.31. 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 a pályák száma, és így a feladatban kérdezett szám a 23.

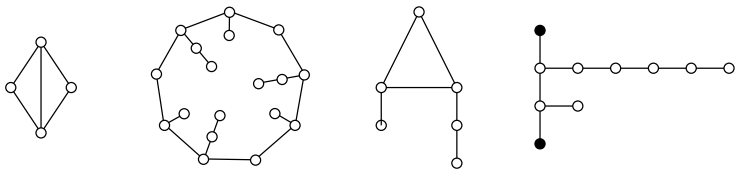
4.5.32. Alkalmazzuk a 4.5.30. Feladat állítását. A pályák száma 1, ezért a fixpontok átlagos száma is 1. De az egységelemnek ennél több fixpontja van, és így van olyan elem is, aminek 1-nél kevesebb fixpontja van, vagyis fixpontmentes.

Nem tranzitív csoportra az állítás nem igaz. Triviális ellenpéldát kapunk, ha egy pont stabilizátorát tekintjük például az S_n csoportban. A

$$G = \{id, (12)(34), (12)(56), (34)(56)\} \leq S_6$$

érdekesebb ellenpélda, mert ez egyik stabilizátornak sem részcsoportja.

4.5.33. 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.



4.5.34. 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 (lásd a fenti ábra utolsó gráfját). Annak megmutatásához, hogy a szimmetriák csoportja nem változott meg, az új gráf első- és másodfokú pontjait érdemes megvizsgálni.

4.5.35. 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.

4.5.36. Mivel g permutáció és X véges, ezért $g(Y) \subseteq Y$ ugyanazt jelenti, mint hogy $g(Y) = Y$. Két ilyen tulajdonságú elem szorzata és inverze is nyilván ilyen tulajdonságú, és ezért ezek részcsoportot alkotnak. Elegánsabb azonban a következő meggondolás. 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.

4.5.37. Mivel $g * x = y$, ezért

$$f * y = y \iff (fg) * x = g * x \iff (g^{-1}fg) * x = x\,.$$

De x stabilizátora H, ezért ez akkor igaz, ha $g^{-1}fg \in H$, azaz ha $f \in gHg^{-1}$.

4.5.38. A B pályája az AB-beli mellékosztályok halmaza, ennek hossza $|AB|/|B|$. A B stabilizátora azokból az $a \in A$ elemekből áll, melyekre $aB = B$, azaz $a \in B$, tehát a stabilizátor $A \cap B$. Így $|AB|/|B| = |A|/|A \cap B|$.

4.5.39. A Klein-csoport esetében $\{id, (12)(34), (13)(24), (14)(23)\}$, a D_3 diédercsoport esetében pedig

$$\{id, (123)(456), (132)(465), (14)(26)(35), (15)(24)(36), (16)(25)(34)\}\,.$$

4.6. Generált részcsoport

4.6.2. A 4.6.1. Állítás bizonyítása most is működik, csak egy apró módosítást kell tennünk. Amikor azt igazoljuk, hogy a megadott elemek részcsoportot alkotnak, problémát okozhat, hogy az $a = m_1g_1 + \ldots + m_ng_n$ elemhez egy $b = k_1g'_1 + \ldots + k_\ell g'_\ell$ 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.

4.6.5. 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 $H = K$. Hasonlóan igazolható, hogy legfeljebb egy legbővebb elem lehet.

Ha a halmazrendszerünk elemei pontosan az egész számok halmazának egyelemű részhalmazai, akkor itt minden elem egyszerre minimális és maximális elem is, legszűkebb és legbővebb elem pedig nincs. Aki most találkozik először a „legszűkebb" és „minimális" kifejezésekkel, annak érdemes megoldania a 4.6.10. Gyakorlatot is, ahol konkrét példákat láthat legszűkebb és minimális elemekre.

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. Ha M minimális elem, akkor $H \subseteq M$ (hiszen H legszűkebb elem), ezért M minimalitása miatt $H = M$. Tehát tényleg H az egyetlen minimális elem.

4.6.6. 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.

4.6.9. Tegyük föl, hogy ψ és φ is olyan 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 4.6.8. Tétel alkalmazásával is könnyen kihozhatnánk: a g elemet föl 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 tetszőleges (akár végtelen) X generátorrendszerre.

Tegyük föl, 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

$$\psi(k_1k_2) = \psi(k_1)\psi(k_2) = \varphi(k_1)\varphi(k_2) = \varphi(k_1k_2)\,,$$

vagyis $k_1k_2 \in K$. 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.

4.6.10.

(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.

4.6.11. Az eredmények a következők.

(1) A páros számok halmaza 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) fölírható $28x+34y$ 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 4.6.15. Feladatban. Megjegyezzük, hogy a fenti (1) állítást a 3.2.9. 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 4.2.28. Gyakorlat).

(4) A 4.2.29. 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 föl, hogy H az adott elemeket tartalmazó részcsoport, be kell látni, hogy A_4 minden eleme H-beli. Ezt meg lehetne úgy mutatni, hogy A_4 minden elemét kifejezzük (123) és (12)(34) segítségével. De mivel Lagrange tétele miatt $|H|$ osztója $|A_4| = 12$-nek, így 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-nek egész kitevős hatványa (a kitevő tehát nulla vagy negatív is lehet). 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 $M = KN^{n-1}$.

4.6.12. A 4.1.23. Állítás szerint D_n minden eleme fölírható 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, 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. 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.

A fenti megoldás megkülönbözteti azt az esetet, amikor t átlóra, illetve oldalfelező merőlegesre való tükrözés. Algebrailag ez annak felel meg, hogy az átlóra tükrözések is egymás konjugáltjai, és az oldalfelező merőlegesekre való tükrözések is (ez a tükrözések két darab háromelemű konjugáltosztálya, lásd 4.8.4. Definíció). Ugyanakkor D_6-nak van olyan automorfizmusa (önmagával való izomorfizmusa, lásd 4.8.12. Definíció), amely egy átlóra való tükrözést egy oldalfelező merőlegesre való tükrözésbe visz (lásd a 4.10.22. Feladat megoldását). Ezért amikor a D_6 csoportban a 4.1.23. Állítás szabályai szerint akarunk számolni, akkor t-nek bármelyik tengelyes tükrözést választhatjuk (ez egyébként a 4.1.23. Állítás bizonyításából is világos).

4.6.13. A $\langle g\rangle$ részcsoportnál az x és y elemek akkor és csak akkor vannak egy pályán, 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 $x, g(x), g^2(x), \ldots$ elemek vannak.

4.6.14. 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 és BA része K-nak. Ha viszont $AB = BA$ részcsoport, akkor 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 $K = AB = BA$.

♫ Az $AB = BA$ összefüggés *nem* azt jelenti, hogy $ab = ba$ minden $a \in A$ és $b \in B$ esetén, hanem csak azt, hogy minden ab fölírható $b'a'$ alakban, ahol $a' \in A$ és $b' \in B$ (és viszont). Példa erre az S_3 csoportban az $A = A_3$ (alternáló) részcsoport és a $B = \{id, (12)\}$ részcsoport.

4.6.15. 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 3.1.31. Gyakorlat miatt. Könnyen láthatóan u és v relatív prímek, és ezért $ux + vy$ alakban minden egész szám előáll. Így $\langle a/c, b/d\rangle = \langle (a, c)/[b, d]\rangle$.

4.6.16. Belátjuk, hogy $\mathbb{Q}^+$ egy X részhalmaza pontosan akkor generátorrendszer, ha minden q prímhatványhoz van olyan egyszerűsíthetetlen tört X-ben, melynek nevezője osztható q-val.

Tegyük föl először, hogy X generátorrendszer. Legyen $q = p^n$ ahol p prím, és írjuk föl 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 föl, hogy az X halmaz rendelkezik a fenti tulajdonsággal, jelölje H az X által generált részcsoportot. Ha a/b és c/d két egyszerűsíthetetlen tört X-ben, akkor az előző 4.6.15. Feladat miatt a szintén egyszerűsíthetetlen $(a, c)/[b, d]$ tört is H-beli. Így H tartalmaz akármilyen egésszel osztható nevezőjű egyszerűsíthetetlen törteket. Legyen $n \neq 0$ egész, belátjuk, hogy $1/n \in H$. Az előzőek szerint van olyan egyszerűsíthetetlen $a/b \in H$, melyre $n \mid b$, ehhez pedig olyan egyszerűsíthetetlen $c/d \in H$, hogy $a \mid d$. A 4.6.15. Feladat szerint $(a, c)/[b, d] \in H$, de most $(a, c) = 1$ (mert $a \mid d$ és $(c, d) = 1$), továbbá $n \mid [b, d]$ (mert $n \mid b$). Ezért $1/n$ egész többszöröse $1/[b, d] \in H$-nak. Ekkor pedig $m/n \in H$ tetszőleges m egészre, azaz $H = \mathbb{Q}$. 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. Tehát a feltétel a/b elhagyása után is teljesül.

Így $\mathbb{Q}^+$-nak nincs véges, sőt minimális generátorrendszere sem.

4.6.17. Elegendő megmutatni, hogy az Útmutatóban 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 föl $r'''h'''$ 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 $r^* = 1$.

4.6.18. Jelölje K az f^i és a tf^i alakú elemek halmazát, megmutatjuk, hogy ez a t és s által generált H részcsoport. A K elemei kifejezhetők t és s segítségével, és ezért $K \subseteq H$. Belátjuk, hogy K részcsoport.

Nyilván $f^{-1} = (ts)^{-1} = s^{-1}t^{-1} = st$. Ebből következik, hogy az f-nek a t-vel vett konjugáltja $t = t^{-1}$ miatt $tft = ttst = st = f^{-1}$. A t-vel való konjugálás szorzattartó, így $tf^it = f^{-i}$ minden i egészre, azaz $f^it = tf^{-i}$. Ebből megkapjuk a 4.1.23. Állítás végén fölírt képleteket (a kitevőben most nem mod n kell számolni), amiből látszik, hogy K zárt a szorzásra. Mivel $(tf^i)^{-1} = f^{-i}t = tf^i$, ezért K zárt az inverzképzésre is, azaz tényleg részcsoport. De K tartalmazza a t és $s = tf$ elemeket, és így $H \subseteq K$. Megmutattuk tehát, hogy $K = H$, azaz H elemei a kívánt alakban írhatók.

Ha $f = 1$, akkor $s = t$ és H a kételemű csoport. Ha $f \neq 1$, de $f^2 = 1$, akkor $H = \{1, s, t, st = ts = f\}$ a Klein-csoport. Ha egyik sem igaz, akkor megmutatjuk, hogy az f^i és a tf^j elemek páronként különbözőek. Tegyük föl, hogy $f^i = tf^j$, innen $t = f^{i-j}$, azaz t és f fölcserélhetők. Ezért $f^{-1} = tft = f$, vagyis $f^2 = 1$, és ezt az esetet már megvizsgáltuk.

Így ha f rendje $n \geq 3$, akkor a H rendje $2n$, és a 4.1.23. Állításban leírt képletek szerint kell benne szorozni. Ezért $H \cong D_n$.

4.6.19. Megmutatjuk, hogy E(2) véges részcsoportjai a következők.

(1) A véges ciklikus csoportok. Ezeket egy $2\pi/n$ szögű forgatás, illetve a másodrendű esetben egy tengelyes tükrözés is generálhatja.

(2) A D_n diédercsoport (egy szabályos n-szög szimmetriacsoportja), illetve a Klein-csoport (egy olyan téglalap vagy rombusz szimmetriacsoportja, ami nem négyzet).

Legyen G véges részcsoportja E(2)-nek. Ekkor G-ben nincs végtelen rendű elem, tehát eltolás és csúsztatva tükrözés, vagyis G elemei forgatások és tükrözések (4.1.13. Állítás). Ha G-ben minden forgatás az identitás, akkor G legfeljebb kételemű lehet. Valóban, ha $t \neq s$ nem identikus elemek G-ben, akkor tükrözések, de akkor ts nem identikus forgatás lenne, ami ellentmondás.

Ha tehát $|G| > 2$, akkor G-ben van egy $f \neq id$ forgatás, ennek centruma legyen P. Megmutatjuk, hogy G minden eleme fixálja P-t. Valóban, ha $g \in G$, de $g(P) = Q \neq P$, akkor a 4.1.18. Gyakorlat szerint gfg^{-1} egy Q körüli forgatás, melynek szöge f szöge, vagy annak ellentettje. Az első esetben a $gfg^{-1}f^{-1}$, a másodikban a $gfg^{-1}f$ elem nem identikus eltolás a 4.1.8. Állítás miatt, ami nem lehet. Tehát G elemei tényleg fixálják P-t.

Jelölje H a G-beli (P körüli) forgatásokból álló részcsoportot. A P körüli forgatások csoportja izomorf az 1 abszolút értékű komplex számok multiplikatív csoportjával. Így H izomorf a $\mathbb{C}^\times$ egy részcsoportjával, ami a 4.4.33. Feladat szerint ciklikus. Tehát H-t egy f forgatás generálja. Ha $G = H$, akkor készen vagyunk. Ha nem, akkor legyen t egy tükrözés G-ben. Tetszőleges másik s tükrözésre ts forgatás, azaz f^i alkalmas i-re. Ezért $s = tf^i$, azaz t és f generálja G-t. Így $G = \langle t, tf \rangle$, és a 4.6.18. Feladat miatt vagyunk készen.

♫ A megoldást úgy is be lehet fejezni, hogy tekintjük azt az egyenest, amire t tükröz, felveszünk ezen egy $R \neq P$ pontot, vesszük R képeit f hatványainál, és belátjuk, hogy G a kapott szabályos n-szög szimmetriacsoportja.

4.7. Homomorfizmusok és normálosztók

4.7.3. Legyen $K \leq H$, és tekintsük a K identikus leképezését. Ez nyilván homomorfizmus, melynek képe K.

4.7.5. Ha $g_1, g_2 \in \mathrm{Ker}(\varphi)$, akkor $\varphi(g_1) = \varphi(g_2) = 1$, és így φ művelettartása miatt $\varphi(g_1g_2) = \varphi(g_1^{-1}) = 1$. Ezért g_1g_2 és g_1^{-1} is benne van $\mathrm{Ker}(\varphi)$-ben. Benne van továbbá az egységelem is, és ezért részcsoport.

Tegyük föl, hogy $\mathrm{Ker}(\varphi) = \{1\}$. Ha $g_1, g_2 \in G$ és $\varphi(g_1) = \varphi(g_2)$, 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 föl, hogy φ injektív, és legyen $g \in \mathrm{Ker}(\varphi)$. Ekkor $\varphi(g) = 1 = \varphi(1)$, ahonnan φ injektivitása miatt $g = 1$. Tehát $\mathrm{Ker}(\varphi) = \{1\}$.

4.7.6. Ha $h \in \mathbb{Z}_n$, akkor $\varphi(g) = h$ akkor és csak akkor, ha g fölírható $nq + h$ alakban, vagyis ha $g \in h + n\,\mathbb{Z}$. Speciálisan $h = 0$ esetén $\mathrm{Ker}(\varphi) = n\,\mathbb{Z}$.

4.7.7. Érdekes, hogy több korábbi, nevezetesnek számító tétel is azt mondja ki, hogy egy-egy leképezés homomorfizmus.

(1) Ez a determinánsok szorzástétele (lásd E.5.1. Tétel). Kép: az egész $T^\times$, mag: 1 determinánsú mátrixok, vagyis $\mathrm{SL}(n, T)$.
(2) Ez a permutációk előjelének szorzástétele (4.2.14. Tétel). Kép: $\mathbb{Z}^\times = \{1, -1\}$, mag: A_n.
(3) Ez leolvasható a 4.1.23. Állításból, vagy abból, hogy forgatások szorzata forgatás, tengelyes tükrözések szorzata is forgatás, egy forgatás és egy tengelyes tükrözés szorzata pedig tengelyes tükrözés. (Harmadik megoldásként vehettük volna mindegyik transzformáció determinánsát is.) Kép: $\mathbb{Z}_2^+$, mag: forgatások.
(4) Az 1.3.10. Állítás szerint $|zw| = |z||w|$. Kép: pozitív valós számok, mag: az egységkörvonal, vagyis az 1 abszolút értékű komplex számok halmaza.
(5) 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.

4.7.8. $(12)N = N(12) = \{(12), (13), (23)\}$. Szó sincs azonban arról, hogy az (12) fölcserélhető az N elemeivel: $(12)(123) = (23)$ és $(12)(132) = (13)$, míg a jobbról szorzásnál fordítva van: $(123)(12) = (13)$ és $(132)(12) = (23)$.

4.7.9. Ha $gN = Ng'$, akkor $g = g1 \in gN = Ng'$ és $g = 1g \in Ng$. Tehát az Ng és Ng' jobb oldali mellékosztályoknak g közös eleme, és így ez a két mellékosztály megegyezik. Vagyis $gN = Ng' = Ng$.

4.7.13. Az asszociativitás teljesül, mert

$$(g_1Ng_2N)g_3N = \big((g_1g_2)g_3\big)N = \big(g_1(g_2g_3)\big)N = g_1N(g_2Ng_3N)\,.$$

4.7.14. A ψ leképezés homomorfizmus, mert

$$\psi(g_1)\psi(g_2) = (g_1N)(g_2N) = (g_1g_2)N = \psi(g_1g_2)\,,$$

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.

4.7.17. A homomorfizmustételt az alábbi φ homomorfizmusokra alkalmazzuk.

(1) A 4.7.7. Gyakorlat (4) pontjában szereplő homomorfizmus. A faktorcsoport elemei az origó körüli körök.
(2) $\varphi(x) = \cos(2\pi x) + i\sin(2\pi x)$ (vö. 2.2.43. Gyakorlat). A mag pontosan az egész számokból, a kép az 1 abszolút értékű komplex számokból áll.
(3) A 4.7.7. 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 4.7.6. Gyakorlatban szereplő homomorfizmus.

4.7.18. Minden $\{1\}$ szerinti mellékosztály egyelemű, és $g \mapsto \{g\}$ izomorfizmus G és $G/\{1\}$ között. A G/G az egyelemű csoporttal izomorf.

4.7.22. 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 műveletartása 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 $\mathrm{Ker}(\varphi) \subseteq K$.

4.7.23. A 4.6.14. Feladat miatt elég belátni, hogy $KN = NK$. De ez világos, hiszen $N \lhd G$, ezért $kN = Nk$ minden $k \in K$-ra.

4.7.27. A $\mathbb{Z}_{16}^{\times}$ csoport rendje 8, elemeit kényelmesebb ±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). Ezért ez a faktorcsoport a Klein-csoporttal izomorf (4.5.18. Tétel).

4.7.28. Ha van olyan α, hogy $\psi = \alpha \circ \varphi$, és $g \in \mathrm{Ker}(\varphi)$, akkor $\varphi(g) = 1$, és így $\psi(g) = \alpha\varphi(g) = \alpha(1) = 1$. Megfordítva, tegyük fel, hogy $\mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\psi)$. Definiáljuk az α leképezést a $\varphi(g) = h \implies \alpha(h) = \psi(g)$ képlettel. Mivel φ szürjektív, ez minden $h \in H$-ra értelmezi α-t (csak esetleg többértelműen). Ha azonban $h = \varphi(g_1) = \varphi(g_2)$, akkor $g_1g_2^{-1} \in \mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\psi)$, és így $\psi(g_1) = \psi(g_2)$. Tehát α jóldefiniált. A definícióból nyilvánvaló, hogy $\psi = \alpha \circ \varphi$.

Végül belátjuk, hogy α műveletartó. Ha $h_1, h_2 \in H$, akkor legyen $\varphi(g_1) = h_1$ és $\varphi(g_2) = h_2$. Ezért $\varphi(g_1g_2) = h_1h_2$, és így $\alpha(h_1h_2) = \psi(g_1g_2) = \psi(g_1)\psi(g_2) = \alpha(h_1)\alpha(h_2)$.

4.7.29. Tegyük föl, hogy X generátorrendszere a G csoportnak. A 4.6.9. Gyakorlat megoldásához hasonlóan most is kétféleképpen járhatunk el. Az első megoldásban a 4.6.8. 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, $L = H$.

4.7.30. 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 föl, 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 $k = hn \in H(N \cap K)$.

4.8. Hogyan keressünk normálosztót?

4.8.5. 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.

4.8.11. A centrum részcsoportja G-nek (ez közvetlen számolással is látható, vagy pedig abból következik, hogy $Z(G)$ az összes elem centralizátorainak a metszete). Nyilván $Z(G) \triangleleft G$, hiszen $Z(G)$ (egyelemű) konjugáltosztályok egyesítése. Hasonló okokból $Z(G)$ minden részcsoportja normálosztó G-ben.

4.8.13. Elsőként (2)-t igazoljuk. Mivel $\varphi_{gh}(x) = ghx(gh)^{-1} = g(hxh^{-1})g^{-1}$, ezért $\varphi_{gh} = \varphi_g \circ \varphi_h$, azaz tényleg homomorfizmust kaptunk. Ennek magja azokból a $g \in G$ elemekből áll, amelyekkel való konjugálás az identikus leképezés, vagyis $gxg^{-1} = x$ minden $x \in G$-re. Ezek tehát pontosan a centrum elemei. E homomorfizmus képe a φ_g alakú leképezések halmaza, ezek a belső automorfizmusok (amik így részcsoportot alkotnak). A homomorfizmustételből kapjuk, hogy $G/Z(G) \cong \mathrm{Inn}(G)$, azaz (3)-at is beláttuk.

Automorfizmusok kompozíciója és inverze is automorfizmus (4.3.6. Gyakorlat), azaz $\mathrm{Aut}(G)$ csoport. Ahhoz, hogy $\mathrm{Inn}(G)$ zárt a konjugálásra, elég belátni, 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

$$(\alpha \circ \varphi_g \circ \alpha^{-1})(x) = \alpha\big(g\alpha^{-1}(x)g^{-1}\big)\,.$$

Ezzel (1)-et is beláttuk. Végül (4) következik a 4.3.16. Gyakorlatból, hiszen izomorfizmusnál az elemek rendje nem változik.

4.8.14. Mivel a konjugálás szorzattartó, az állítást elég egy ciklusra megmutatni, vagyis 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 4.2.12. Lemma bizonyításához hasonlóan).

4.8.16. 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 konjugáltosztálya ugyanaz marad, mint S_4-ben.

Így tehát az A_4 csoportnak négy konjugáltosztálya 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 konjugáltosztály 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 V részcsoport (4.8.15. Állítás).

Be kell még látnunk, hogy ha $g \in A_n$, akkor g konjugáltjainak 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 izomorfizmustételből, mert $|S_n : A_n| = 2$ és

$$C_{A_n}(g) = C_{S_n}(g) \cap A_n\,.$$

Így megállapíthatjuk, hogy ha g fölcserélhető 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.

4.8.18. Az (1) állításban azt kell belátni, hogy ha K karakterisztikus részcsoport, akkor nemcsak $\alpha(K) \subseteq K$, hanem $\alpha(K) = K$ is teljesül minden α automorfizmusra. Ez azért igaz, mert α^{-1} is automorfizmus, és így $\alpha^{-1}(K) \subseteq K$, ahonnan α-t alkalmazva $K \subseteq \alpha(K)$ adódik.

A (2) bizonyításához tegyük föl, 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) 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 $\alpha(K) = K$.

4.8.19. Legyen N az N_i normálosztók metszete. Ez részcsoport (4.6.6. Gyakorlat), meg kell mutatni, hogy zárt a konjugálásra. Tegyük föl, 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 $gng^{-1} \in N$.

4.8.20. 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 föl. 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 φ_g^{-1}-re elmondva $H \subseteq \varphi_g^{-1}(H)$ adódik, ami azt jelenti, hogy $\varphi_g(H) \subseteq H$.

4.8.25. Tegyük föl, 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 innen $nk = kn$.

4.8.29. 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 $K \subseteq N_G(H)$.

4.8.31.

(1) Nyilván egy g elem akkor és csak akkor cserélhető föl X minden elemével, ha minden $x \in X$-nek benne van a centralizátorában.
(2) Hasson G a G összes részhalmazainak a halmazán konjugálással: legyen $g * X = gXg^{-1}$. 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 $C_G(X)$. (Az Olvasó gyakorlásul elvégezheti a bizonyítást közvetlen számolással is.)
(4) Ha X részcsoport, akkor a (3)-ban szereplő φ_g automorfizmusa X-nek, és így φ az $\mathrm{Aut}(X)$ csoportba képez. A homomorfizmustétel miatt tehát az állítás igaz.

4.8.32.

(1) Igen, mert $\mathbb{Z}^+$ Abel-csoport.
(2) Igen, a 4.1.23. 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 4.1.23. 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, része $\mathrm{GL}(n, \mathbb{R})$ centrumának, mert az egységmátrix skalárszorosai minden mátrixszal fölcserélhetők. Részcsoport is, így a 4.8.11. Gyakorlat miatt normálosztó. A 4.14.2. 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.

4.8.33. A D_3 és a $\mathrm{GL}(2, \mathbb{Z}_2)$ csoportok izomorfak az S_3 szimmetrikus csoporttal (lásd 4.5.25. Gyakorlat), amelynek már meghatároztuk a konjugáltosztályait 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 konjugáltosztálya egyelemű. Ugyanez mondható el f^2-ről is (ez a középpontos tükrözés). Valóban, a 4.1.23. 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 konjugáltosztályai $\{1\}$, $\{f^2\}$, $\{f, f^3\}$, $\{t, tf^2\}$, $\{tf, tf^3\}$. A normálosztók azok a részcsoportok, amik konjugáltosztályok 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 konjugáltosztálynak 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 konjugáltosztályai $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$, 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 konjugáltosztályai: az öt tükrözés együtt, továbbá minden forgatás az inverzével. Az egyetlen nemtriviális normálosztó a forgatásokból áll.

Az S_5 konjugáltosztályait a 4.8.14. Gyakorlatból kapjuk. Az eredmény:

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.

Ebből az A_5 konjugáltosztályait is megkaphatjuk a 4.8.16. Gyakorlat segítségével. Ennek megoldásában megállapítottuk, hogy ha egy $g \in A_n$ elem fölcserélhető S_n egy páratlan permutációjával 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. Ezért A_5-ben a hármasciklusok egyetlen húszelemű konjugáltosztályt, az $(ab)(cd)$ alakú permutációk pedig egy tizenötelemű konjugáltosztályt alkotnak (hiszen (123) fölcserélhető (45)-tel, (12)(34) pedig (12)-vel). Az ötösciklusok ugyanakkor két tizenkételemű osztályt kell, hogy alkossanak, hiszen a 24 nem osztója a 60-nak. Az A_5 konjugáltosztályai tehát rendre 1, 12, 12, 15, 20 eleműek.

Tegyük föl, hogy N nemtriviális normálosztója A_5-nek. Ekkor konjugáltosztályok egyesítése, az egységelemet tartalmazza, és rendje osztója A_5 rendjének. Ezért az 1, 12, 12, 15, 20 számok közül néhánynak az összege a 60 egy valódi osztója lesz úgy, hogy 1 is az összeadandók között van. Ez azonban ellentmondásra vezet. Valóban, az 1 mellé még legalább két számot be kell venni, mert $12+1$, $15+1$, $20+1$ nem osztói a 60-nak. Az $1+12+12$ és az $1+12+15$ sem osztói a 60-nak, az összes többi összeg pedig már meghaladja a 30-at. Ez az ellentmondás bizonyítja, hogy A_5 egyszerű csoport.

Az S_5 egyetlen nemtriviális normálosztója A_5. Ezt az előzőhöz hasonlóan lehet megmutatni. A 120 valódi osztói közül csak a $40 = 1+15+24$ és a $60 = 1+15+20+24$ kapható meg a konjugáltosztályok elemszámainak összegeként úgy, hogy az 1-et is felhasználjuk. Az első esetben az ötösciklusokat és az $(ab)(cd)$ alakú permutációkat választjuk az egységelem mellé, de ez nem részcsoport, mert $(12345)(12)(34) = (135)$. Hasonlóan láthatjuk, hogy a második esetben nem választhatjuk az $(abc)(de)$ alakú permutációkat 20 elemű osztálynak. Ha pedig az (abc) alakú permutációkat vesszük, akkor A_5 adódik.

♫ Az S_5 normálosztóit a 4.12.37. Gyakorlat (elemi) megoldásából is megkaphatjuk. Ebből ugyanis (A_5 már bizonyított egyszerűségét felhasználva) kiderül, hogy ha N nemtriviális normálosztó S_5-ben, akkor $N = A_5$.

4.8.34. Az A_4 rendje osztható hattal, de nincs benne hatelemű részcsoport, mert ez 2 indexű, azaz normálosztó lenne (4.7.19. Állítás), és ez ellentmond a 4.8.16. Gyakorlatban kapott felsorolásnak. Ugyanezt elmondhatjuk az A_5 csoportra is: ebben a 4.8.33. Gyakorlat miatt nincs 30 elemű részcsoport.

4.8.35. Az $(1, 2, \ldots, n)$ konjugáltjai az n hosszú ciklusok, vagyis $(n-1)!$ konjugáltja van. Így centralizátora $n!/(n-1)! = n$-elemű, az $(1, 2, \ldots, n)$ hatványaiból áll.

4.8.36. Ha A Abel, akkor centruma az egész csoport, kommutátor-részcsoportja pedig $\{1\}$. A Q kvaterniócsoportnak a 4.8.33. 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 g tetszőleges forgatás, akkor $tgt^{-1} = g^{-1}$. Ezért t pontosan akkor cserélhető föl g-vel, ha $g^2 = 1$. Ha n páratlan, akkor innen $g = 1$, ilyenkor D_n centruma egyelemű. Ha n páros, akkor D_n centruma az identitásból és a középpontos tükrözésből áll.

A fenti egyenlőséget átrendezve $tgt^{-1}g^{-1} = g^{-2}$ 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 nyilván normálosztó, és a rá vett faktor négyelemű, tehát ismét csak kommutatív.)

Az S_n szimmetrikus csoport $n = 2$-re Abel. Ha $n > 2$, akkor centruma $\{1\}$, kommutátor-részcsoportja A_n. Valóban, tegyük fel, hogy $f \in Z(S_n)$, akkor az előző 4.8.35. Gyakorlat szerint f az $(1, 2, \ldots, n)$ ciklus i-edik hatványa alkalmas i-re. De $(1, 2, \ldots, n)^i$-nel (12)-t konjugálva $(i +_n 1, i +_n 2)$ adódik. Ez $n > 2$ miatt csak akkor lehet $(12) = (21)$, ha $i = 0$. Ezért f az egységelem, és ezzel beláttuk, hogy $Z(S_n) = \{1\}$.

♫ A $Z(S_n) = \{1\}$ állítás kihozható a 4.8.14. Gyakorlatból is, hiszen a centrum elemei egyelemű konjugált osztályt alkotnak, egy adott ciklusszerkezetet azonban sokféleképpen „ki lehet tölteni” az $1, 2, \ldots, n$ számokkal, az egyetlen kivétel az identitáson kívül a kételemű halmazon az (ab). Apró gondot itt is a diszkusszió jelent, mert egy adott k hosszúságú ciklust k-féleképpen lehet fölírni, még a fenti esetben is $(12) = (21)$ kétféle kitöltés, amelynek eredménye ugyanaz.

Mivel S_n/A_n kételemű csoport, amely ciklikus, és így Abel-féle, ezért 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 (4.2.30. Gyakorlat), ezért $n > 2$ esetén $S_n' = A_n$.

Az A_4 csoportnak a 4.8.16. Gyakorlatban már meghatároztuk a konjugáltosztályait, és így látjuk, hogy centruma egyelemű. Belátjuk, hogy A_4' a négyelemű Klein-féle V normálosztó. Valóban, az eszerinti faktor háromelemű, és így kommutatív, ennél szűkebb normálosztó azonban csak az $\{1\}$ van, ami nem lehet A_4', mert ez nemkommutatív csoport.

♫ Ha $n \geq 5$, akkor A_n centruma $\{1\}$, kommutátor-részcsoportja önmaga, mert ilyenkor A_n nemkommutatív egyszerű csoport (4.12.30. Tétel).

4.8.37. Legyen G egy $2p$ rendű nemkommutatív csoport, ahol $p > 2$ prím. Ekkor G-ben nincs $2p$ rendű elem, különben ciklikus, és így kommutatív lenne. Nem lehet minden eleme másodrendű, mert kommutatív lenne (4.3.40. Feladat), ugyanakkor van benne másodrendű elem, mert rendje páros (4.4.32. Feladat). Így az elemrendek 1, 2 és p. Ha egy p rendű elem fölcserélhető lenne egy másodrendű elemmel, akkor a szorzatuk a 4.3.39. Gyakorlat miatt $2p$ rendű lenne, ami lehetetlen.

Ha f egy p rendű, t egy másodrendű elem, akkor ftf^{-1} is másodrendű, és mivel t és f nem cserélhetők föl, t-től különböző. A $H = \langle t, ftf^{-1}\rangle$ részcsoport rendje páros, és legalább háromelemű, ezért Lagrange tétele miatt csak maga G lehet. A 4.6.18. Feladat miatt $G \cong D_p$.

♫ Az előző bizonyítás végén „kiöntöttük a vizet a fazékból", amikor a csoportot két másodrendű elemmel generáltuk, hogy alkalmazni lehessen a 4.6.18. Feladatot. Ehelyett a $tft^{-1} = f^{-1}$ bebizonyításával, majd a 4.1.23. Állításra való hivatkozással is befejezhettük volna a megoldást. Ehhez azt kell észrevenni, hogy $\langle f\rangle$ egy 2 indexű részcsoport, és így $(ft)^2 \in \langle f\rangle$. Az $\langle f\rangle$ és az $\langle ft\rangle$ prímrendű részcsoportok viszont csak az egységelemben metszhetik egymást, és így ft-nek szükségképpen 2 a rendje, ahonnan $tft^{-1} = f^{-1}$ adódik.

4.8.38. Az $\{1, f^2\}$ normálosztó D_4-ben, sőt a 4.8.36. Gyakorlat szerint ez a 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.

♫ A 4.8.15. Állítás utáni apró betűs részben már láttunk egy geometriai bizonyítást a (3) állításra. Most egy algebrai gondolatmenet következik.

Legyen $V = \{id, (12)(34), (13)(24), (14)(23)\}$. Az S_4/V faktorcsoportban való számoláshoz legyen H az S_4-ben a 4 pont stabilizátora. Megmutatjuk, hogy ennek elemei reprezentánsrendszert alkotnak V szerint. Valóban, ha h_1 és h_2 ugyanabban a mellékosztályban lenne V szerint, akkor $h_1^{-1}h_2 \in V \cap H = \{1\}$, 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 $h \mapsto hV$ izomorfizmus H és S_4/V között. A H viszont az $\{1, 2, 3\}$ összes permutációiból áll, és így S_3-mal izomorf. Ezért $S_4/V \cong S_3$. Megjegyezzük, hogy ez az izomorfia az első izomorfizmustételből (4.7.25. Következmény) is adódik, hiszen $HV = S_4$, és így $S_4/V \cong H/(H \cap V)$.

♫ Az S_4/V faktorcsoport izomorfiatípusát a következőképpen is kiszámolhatjuk. Ennek a csoportnak az elemszáma $24/4 = 6$. Nincs hatodrendű eleme, mert S_4 minden eleme legfeljebb negyedrendű, és homomorf kép rendje osztója az eredeti elem rendjének. Tudjuk, hogy egy hatelemű csoport vagy ciklikus, vagy S_3-mal izomorf (4.8.37. Gyakorlat), és ezért S_4/V csakis S_3 lehet.

A $D_8/\{1, f^2, f^4, f^6\}$ faktor szintén négyelemű, és szintén a Klein-csoporttal izomorf, mert D_8 minden elemének négyzete benne van az $\{1, f^2, f^4, f^6\}$ normálosztóban.

4.8.39. Az eltolások nyilván egy N részcsoportot alkotnak. A 4.1.16. Gyakorlat miatt eltolás konjugáltja is eltolás, és így ez normálosztó. Rögzítsünk egy P pontot a síkon, és legyen $H \cong \mathrm{O}(2)$ ennek a stabilizátora az E(2) csoportban. Elég megmutatni, hogy H elemei reprezentánsrendszert alkotnak N szerint, azaz hogy tetszőleges Ng mellékosztályban H-nak egyetlen eleme van. De kg pontosan akkor van H-ban, ha $kg(P) = P$, és a síkon tényleg egyetlen olyan k eltolás van, ami $g(P)$-t P-be viszi.

4.8.40. Legyen $N = \{1, a\}$. Az $\{1\}$ mindig konjugáltosztálya G-nek, és mivel N a G konjugáltosztályainak egyesítése, $\{a\}$ is az. Tehát $a \in Z(G)$.

4.8.41. Az nyilvánvaló, hogy ha $H = \langle X \rangle$ kommutatív, akkor az $X \subseteq H$ elemei is egymással fölcserélhetőek. A megfordítást bizonyíthatnánk a 4.6.8. Tételre való hivatkozással is, hiszen ha X elemei páronként fölcserélhetők, akkor a belőlük és inverzeikből készített szorzatok is. Elegánsabb azonban a következő gondolatmenet.

Tegyük föl, hogy X elemei páronként fölcserélhetők. 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 fölcserélhetők $C_G(X)$ 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.

4.8.42. Ha $id \neq f \in \mathrm{E}(2)$ egy P pont körüli forgatás, akkor a 4.1.18. Gyakorlat szerint gfg^{-1} forgatás a $g(P)$ körül. Ha $gf = fg$, akkor $gfg^{-1} = f$, és így f fixálja $g(P)$-t. De f-nek csak egyetlen fixpontja van, és így $g(P) = P$. Ha g nem mozgás, akkor ugyanez a gyakorlat mutatja, hogy $gfg^{-1} = f^{-1}$. Ezért ekkor $f = f^{-1}$, azaz f a P-re tükrözés, amely minden P-t fixáló egybevágósággal fölcserélhető.

Összefoglalva: az identitás $\mathrm{E}(2)$ minden elemével fölcserélhető, a P-re tükrözés centralizátora a P stabilizátora (azaz $\mathrm{O}(2)$-vel izomorf), a többi P körüli forgatás centralizátora pedig a P körüli forgatásokból áll.

Legyen H a P körüli forgatások részcsoportja $\mathrm{E}(2)$-ben. A 4.1.18. Gyakorlat szerint $g \in \mathrm{E}(2)$ esetén gHg^{-1} a $g(P)$ körüli forgatások részcsoportja, és így H normalizátora a P pontot fixáló egybevágóságokból áll. Ezek a P körüli forgatások, és a P ponton átmenő egyenesekre tükrözések (4.1.13. Állítás).

4.8.43. Legyen $N > 1$ normálosztó $\mathrm{SO}(3)$-ban és $1 \neq f \in N$. A 4.1.29. Feladat szerint f egy α szögű forgatás egy e_1 egyenes körül, ahol $\alpha \neq 0$. Az f alkalmas hatványát véve feltehető, hogy $90^\circ \leq \alpha < 180^\circ$. Legyen e_3 egy olyan origón átmenő egyenes, mely e_1-re merőleges. Forgassuk át folytonosan e_1-et e_3-ba, és közben figyeljük, hogy milyen szöget zár be az f-nél vett képével. A kezdeti állapotban $f(e_1) = e_1$, azaz nulla fokos szöget zárnak be. A végállapotban $f(e_3)$ és e_3 szöge $\alpha \geq 90^\circ$. A forgatás során ez a szög is folytonosan változik, ezért létezik olyan e_2 egyenes, amely merőleges $f(e_2)$-re. Legyen g az e_2 körüli 180 fokos forgatás. Ekkor a $h = g^{-1}f^{-1}gf \in N$ transzformáció az e_2 egyenest tükrözi az origóra, és így csakis egy alkalmas egyenes körüli 180 fokos forgatás lehet. A 4.1.30. Gyakorlat szerint h konjugáltjaként megkapható az összes többi 180 fokos forgatás, és így azok is elemei N-nek. A 4.1.38. Gyakorlat szerint ilyen forgatások szorzataként minden forgatás megkapható.

4.8.44. 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 $\alpha(i) = ik$ (4.3.15. 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 4.8.13. Gyakorlat miatt $\mathrm{Inn}(S_3) \cong S_3/Z(S_3) \cong S_3$. Tehát minden automorfizmus belső, és $\mathrm{Aut}(S_3) \cong S_3$.

4.8.45. Tegyük föl, hogy 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 a G csoport 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 (4.4.32. Feladat). Megfordítva, páratlan rendű kommutatív csoportban az inverzképzés mindig szorzattartó, bijektív, és fixpontmentes.

4.8.46. Az n rendű elemek halmaza zárt minden automorfizmusra, így az általa generált részcsoportot minden automorfizmus önmagába viszi (a 4.7.29. Gyakorlat miatt).

4.8.47. Az alábbiakban α a G csoport egy automorfizmusát jelöli.

(1) A végtelen ciklikus csoportnak két automorfizmusa van, az identitás és az inverzképzés (4.8.44. Feladat), és ezek minden részcsoportot megőriznek. Ha H részcsoportja a G véges ciklikus csoportnak, akkor G-nek csak egyetlen $|H|$ elemszámú részcsoportja van (4.3.27. Állítás). Ezért ezt minden automorfizmus csak önmagába viheti.

(2) Mivel $g \in Z(G)$ fölcserélhető minden $h \in G$-vel, $\alpha(g)$ is fölcserélhető minden $\alpha(h)$-val, vagyis a csoport összes elemével, hiszen α szürjektív. 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 minden n egészre (4.3.15. Gyakorlat). Ezért a megadott részcsoportokat minden automorfizmus önmagába képzi.

4.8.48. 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 $L \subseteq LN$, így $[K, L] \subseteq [K, LN]$. Ugyanígy $[K, N] \subseteq [K, LN]$, azaz $[K, L][K, N] \subseteq [K, LN]$. A fordított tartalmazáshoz elég belátni, 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).

4.9. A direkt szorzat

4.9.1. Legyen $g = (\ldots, g_i, \ldots)$, $h = (\ldots, h_i, \ldots)$ és $k = (\ldots, k_i, \ldots)$. 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.

4.9.3. 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 föl 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.

4.9.10. Tegyük föl, hogy $\mathbb{Z}_k^\times$ ciklikus, és legyen $k = nm$, ahol n és m relatív prímek. Ekkor a 4.9.7. és a 4.9.9. 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.

4.9.13. A determinánsképzés homomorfizmus az $\{1,-1\}$ csoportba, melynek magja $\mathrm{SO}(3)$, így ez egy 2 indexű normálosztó. Jelölje g a középpontos tükrözést, ez minden origót fixáló egybevágósággal (sőt minden lineáris transzformációval) fölcserélhető, ezért benne van $\mathrm{O}(3)$ centrumában. Tehát $N = \{id, g\}$ normálosztó. A g nem mozgás, és így $N \cap \mathrm{SO}(3) = \{id\}$. Mivel $\mathrm{SO}(3)$ indexe 2, ezért $N\mathrm{SO}(3) = \mathrm{O}(3)$. Tehát teljesülnek a 4.9.12. Tétel feltételei.

4.9.14. 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 $G = G_1G_2G_3$, ahol $G_i \triangleleft G$, és mindegyik G_i csak az egységelemben metszi a másik kettő szorzatát. Ekkor a 4.9.12. Tétel miatt $G \cong G_1 \times (G_2G_3)$. Ezért elég megmutatni, hogy $G_2G_3 \cong G_2 \times G_3$. Ez ismét a 4.9.12. Tételből következik, azt kell csak belátni, hogy $G_2 \cap G_3 = \{1\}$. Ez következik a $G_2 \cap G_1G_3 = \{1\}$ feltételből, hiszen $G_3 \subseteq G_1G_3$.

♫ Igazából azt láttuk be, hogy $G \cong G_1 \times (G_2 \times G_3)$. Ez 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, műveletartó 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.

4.9.17. Az állítás következik az első izomorfizmustételből, amely szerint $NH/N \cong H/H \cap N$ (4.7.25. Következmény). Most $NH = G$ és $H \cap N = \{1\}$, tehát $G/N \cong H$ adódik.

4.9.18. A 4.8.13. Gyakorlat megoldásában már beláttuk, hogy $\varphi_{gh} = \varphi_g \circ \varphi_h$, azaz hogy φ homomorfizmus.

4.9.19. Az N elemeit azonosítsuk a sík pontjaival: az r eltolást $r(P)$-vel. Megmutatjuk, hogy a $h \in H$-val való konjugálás az N csoporton ugyanaz a leképezés, mint amit h, mint geometriai transzformáció, a síkon megad. Ehhez azt kell belátni, hogy tetszőleges $h \in H$ és $r \in N$ esetén az r-hez tartozó $r(P)$ pont képe h-nál éppen a hrh^{-1} eltoláshoz tartozó pontja a síknak, azaz $hrh^{-1}(P)$. De ez igaz, mert h^{-1} fixálja P-t.

4.9.21.

(1) Ahhoz, hogy a szorzás asszociatív 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 megmutatni, 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.
(4) Nyilván $(n, h) = (n, 1)(1, h)$.
(5) Ez a szorzás képletének közvetlen alkalmazásával adódik.
(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.
(6) Ha H^* normálosztó G-ben, akkor a 4.8.25. Gyakorlat szerint H^* minden eleme fölcserélhető N^* minden elemével. Az (5) képletéből ekkor $\big(\psi(h)\big)(n) = n$ adódik minden $n \in N$ és $H \in H$ esetén. Megfordítva, ha $\psi(h)$ mindig az identitás, akkor H^* minden eleme fölcserélhető N^* minden elemével, ezért H^* normalizátora tartalmazza N^*-ot (és H^*-ot is), vagyis az egész G. A 4.9.11. Állítás és a 4.9.12. Tétel szerint ebben és csak ebben az esetben kapunk direkt szorzatot.

4.9.22. (0, 1), (0, 3), (1, 1), (1, 3).

4.9.23. A másodrendű elemek száma az első csoportban 7, a másodikban csak 3.

4.9.24. Hányféleképpen bontható föl 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 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.

4.9.25. Olyan A és B normálosztókat keresünk, melyekre $A \cap B = \{e\}$ és $AB = G$. Abel-csoportban 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 4.3.27. 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 4.9.9. 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 4.8.16. és a 4.8.33. Gyakorlatokban, és ebből látszik, hogy mindegyik direkt felbonthatatlan. Végül legyen $A = \{1, f^2, f^4, t, tf^2, tf^4\} \lhd D_6$ és $B = \{1, f^3\} \lhd D_6$. Ezek a normálosztók mutatják, hogy $D_6 \cong D_3 \times \mathbb{Z}_2^+$.

4.9.26. Olyan A és B ötelemű részcsoportokat keresünk, amelyek különbözők. Ekkor ugyanis metszetük Lagrange tétele miatt egyelemű, 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).

4.9.27. Ha $g_1, g_2 \in G$, akkor $\big(g_1, \varphi(g_1)\big)\big(g_2, \varphi(g_2)\big) = \big(g_1 g_2, \varphi(g_1)\varphi(g_2)\big)$, mert a direkt szorzatban komponensenként szorzunk. Ez $\big(g_1 g_2, \varphi(g_1 g_2)\big) \in K$, hiszen φ szorzattartó. Így K zárt a szorzásra. Hasonlóan következik φ inverz-tartásából, hogy K az inverzképzésre is zárt.

Ha $\big(g, \varphi(g)\big) \in \{1\} \times H$, akkor $g = 1$, és így $\varphi(g) = 1$. Ezért K és $\{1\} \times H$ metszete csak az egységelemből áll. Tetszőleges $(g, h) \in G \times H$ fölírható $\big(1, h\varphi(g)^{-1}\big)\big(g, \varphi(g)\big)$ alakban, és így K tényleg komplementuma $\{1\} \times H$-nak.

Megfordítva, tegyük föl, hogy K komplementuma $\{1\} \times H$-nak. Ha (g, h_1) és (g, h_2) is eleme K-nak, akkor $(1, h_1 h_2^{-1}) \in K \cap \big(\{1\} \times H\big)$, így a feltétel szerint $h_1 h_2^{-1} = 1$. Ezért minden $g \in G$-hez legfeljebb egy olyan $h \in H$ van, melyre $(g, h) \in K$. De ilyen h létezik is, mert $(g, 1) \in G \times H = \big(\{1\} \times H\big)K$, és így $(g, 1) = (1, h)(g_1, h_1)$ alkalmas $h \in H$-ra és $(g_1, h_1) \in K$-ra. A szorzást elvégezve látjuk, hogy $g = g_1$ és ezért $(g, h_1) \in K$. Vagyis az a $\varphi : G \to H$ függvény, amely $(g, h) \in K$ esetén g-hez h-t rendeli, minden helyen egyértelműen definiált. Az, hogy homomorfizmus is, a megoldás első bekezdésében látottakhoz hasonlóan igazolható.

4.9.28. 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 $A \times C$. Így készen vagyunk a homomorfizmustétel miatt.

4.9.29. 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 fölcserélhető, azaz ha $(g, h) \in Z(G) \times Z(H)$.

Ha $x, y \in G$, akkor $[(x, 1), (y, 1)] = ([x, y], 1)$, így $G' \times \{1\} \subseteq (G \times H)'$. Ugyanígy $\{1\} \times H' \subseteq (G \times H)'$, és ezért 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.

♫ A bizonyítást 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. A megfordítás abból következik, hogy a kommutátorképzés „monoton”: $U \leq V$ esetén $U' \leq V'$. Emiatt $G' \times \{1\}$ és $\{1\} \times H'$ is része $(G \times H)'$-nek.

4.9.30. 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.

4.9.31. Legyen K egy 24 elemű részcsoport. Vizsgáljuk először azt az esetet, amikor $(id, 1) \notin K$. Ekkor $K \cap \big(\{id\} \times \mathbb{Z}_2^+\big)$ csak az egységelemből áll. Így $K\big(\{id\} \times \mathbb{Z}_2^+\big)$ rendje $24 \cdot 2/1 = 48$ (4.4.31. Gyakorlat), és ezért a K részcsoport komplementuma $\{id\} \times \mathbb{Z}_2^+$-nek. A 4.9.27. Gyakorlat miatt K egy $\varphi : S_4 \to \mathbb{Z}_2^+$ homomorfizmus gráfja. Ennek magja legfeljebb kettő indexű normálosztó S_4-ben, vagyis az S_4 vagy az A_4 (4.8.15. Állítás). Ha a mag S_4, akkor minden elem 0-ra képződik, és így $K = S_4 \times \{0\}$. Ha a mag A_4, akkor $K = \big(A_4 \times \{0\}\big) \cup \{(g, 1) : g \in S_4 - A_4\}$. Ez szintén S_4-gyel izomorf (4.9.17. Gyakorlat).

A másik eset az, amikor $(id, 1) \in K$, vagyis $\big(\{id\} \times \mathbb{Z}_2^+\big) \subseteq K$. Ekkor a moduláris szabály (4.7.30. Gyakorlat) szerint

$$K = \big(S_4 \times \{0\}\big)\big(\{id\} \times \mathbb{Z}_2^+\big) \cap K = \big((S_4 \times \{0\}) \cap K\big)\big(\{id\} \times \mathbb{Z}_2^+\big).$$

Azaz K az $\big(S_4 \times \{0\}\big) \cap K$ és az $\{id\} \times \mathbb{Z}_2^+$ normálosztóinak a direkt szorzata. Tehát az első tényező elemszáma 12, és ezért ez kettő indexű normálosztó $S_4 \times \{0\} \cong S_4$-ben. Így $\big(S_4 \times \{0\}\big) \cap K = A_4 \times \{0\}$.

4.9.32. 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 4.5.9. 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 H az identitásból és a középpontos tükrözésből álló részcsoport. Mivel a középpontos tükrözés G minden elemével fölcserélhető, H normálosztó, és így $G \cong N \times H$.

A 4.9.31. Gyakorlat szerint a G csoportban N-en kívül még egyetlen olyan K normálosztó van, amely S_4-gyel izomorf. Megmutatjuk, hogy ennek elemei pontosan a kocka mozgásai. Tekintsük azt a ψ homomorfizmust, amely G minden eleméhez annak determinánsát rendeli. Egy egybevágósági transzformáció determinánsa 1 vagy -1 lehet. A középpontos tükrözés determinánsa -1, ez nem mozgás. Ezért ψ magja egy 2 indexű, azaz 24 elemű normálosztó G-ben. Ez nem tartalmazza az előző bekezdésben leírt H normálosztót, és így a 4.9.31. Gyakorlat szerint S_4-gyel izomorf. Megmutatjuk, hogy K nem ugyanaz, mint az előző bekezdésben vizsgált N. Legyen e két szemközti lap középpontját összekötő egyenes. Ekkor az e körüli 90 fokos forgatás mozgás, de a két tetraédert megcseréli. Ezért ez eleme K-nak, de nem eleme N-nek. Természetesen G izomorf a K és H normálosztóinak direkt szorzatával is.

4.9.33. Legyen $X = \{i, j, k, -i, -j, -k\}$ az oktaéder csúcsainak halmaza. A 4.5.21. Gyakorlat előtti megjegyzés szerint az X halmaz elemei között a kvaternió-szorzás a négyzetre emeléstől eltekintve a vektoriális szorzat. Ha tehát A az oktaéder mozgása, akkor az Útmutatóban leírt megjegyzés szerint tartja a vektoriális szorzást, és így csoportautomorfizmushoz vezet (ha még az $A(1) = 1$ és $A(-1) = -1$ szabályokat hozzátesszük). Megfordítva, egy csoportautomorfizmus az X halmazon egy olyan leképezést ad, amely a vektoriális szorzatot tartja. Ezért ez a térnek egy olyan egybevágóságát indukálja, amely mozgás. Tehát $\mathrm{Aut}(Q)$ izomorf az oktaéder mozgáscsoportjával. Az oktaéder mozgásai (és szimmetriái is) ugyanazok, mint annak a kockának a mozgásai (szimmetriái), amelynek lapközéppontjai éppen az X-beli csúcsok. Ezért az oktaéder és a kocka mozgáscsoportja izomorf, vagyis a 4.9.32. Feladat megoldása szerint S_4.

4.9.34. Az Útmutatóbeli 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 2.2.20. 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 föl 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 feladat állítását a 7.3.16. Gyakorlatban általánosítjuk, Abel-csoportok helyett modulusokra.

4.9.35. A $\mathbb{Z}_p^n$, mint vektortér invertálható lineáris leképezéseinek csoportja nyilván $\mathrm{GL}(n, \mathbb{Z}_p)$-vel izomorf. Belátjuk, hogy ezek ugyanazok, mint a $(\mathbb{Z}_p^+)^n$ direkt hatvány összegtartó invertálható leképezései, vagyis

hogy minden összegtartó α leképezés skalárszorostartó 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 (4.3.15. Gyakorlat).

4.9.36. 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 e hatványok 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 4.9.8. 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.

♫ A véges Abel-csoportok alaptétele nélkül is beláthatjuk a most bizonyított állítást. Legyen g maximális rendű elem A-ban. Ha van olyan h elem, amelynek rendje nem osztója $e = o(g)$-nek, akkor van olyan p^m prímhatvány, amely h rendjét osztja, de e-t nem. A h-t egy alkalmas hatványával helyettesítve feltehető, hogy $o(h) = p^m$. Legyen $q \neq p$ prímosztója e-nek és $[e, p^m]$ az e és p^m legkisebb közös többszöröse. A gh elemet $[e, p^m]/q$-adik hatványra emelve nem kapunk 1-et, és így gh rendjében minden prím legalább akkora hatványon szerepel, mint e-ben, a p azonban nagyobb hatványon szerepel (hiszen $(gh)^e \neq 1$), ami ellentmond g választásának.

Hasonló bizonyítást gyárthatunk a 4.3.34. és a 4.3.39. Gyakorlatok felhasználásával is, megmutatva, hogy bármely g és h elemekhez van olyan elem A-ban, melynek rendje g és h rendjének legkisebb közös többszöröse.

Tegyük föl, 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.

4.9.37. A $G = \mathrm{AGL}(n, T)$ 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 $N \cap H = \{1\}$.

4.9.38.

(1) Ez a D_n diédercsoport lesz, az N-ben a forgatások vannak.
(2) Ez egy 21 elemű nemkommutatív csoport. Be kell látni, 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 $\mathbb{Z}_7^+$ automorfizmus-csoportja a 4.8.44. Feladat szerint izomorf $\mathbb{Z}_7^\times$-tel, ez pedig a 4.3.22. 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 4.3.29. 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 $D_6 \cong D_3 \times \mathbb{Z}_2^+$ (ezeknek 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.

4.9.39. 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 $B = A/M$ és $b = a + M$. A b elem rendje p^n a 4.7.20. Állítás miatt. Mivel faktorizálásnál az elemrend nem nőhet, a b maximális rendű a B csoport p-hatványrendű elemei között is. A 4.7.24. Tétel (1) pontja szerint $\langle a\rangle + M$ a $\langle b\rangle$ teljes inverz képe A-ban, ezért 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 föl indirekt, hogy $\langle b\rangle \neq B$. Megmutatjuk, hogy B minden elemének a rendje p-hatvány. Valóban, ha $g \in B$, akkor g rendje fölírható $p^m t$ 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 feltétel szerint tehát $\langle p^m g\rangle$ 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 fölírható 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 prímhatvány-rendű ciklikus csoportok direkt szorzatára, hiszen sorban leválaszthatunk ilyen direkt tényezőket, amíg el nem fogy a csoport.

4.10. Szabad csoportok és definiáló relációk

4.10.7. 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 (a természetes homomorfizmusnál) 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 a 0 és az 1 a skalárok, tehát egy vektorrendszer pontosan akkor 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 nincs benne az N normálosztóban.

Legyen $x_1, \ldots, x_k \in X$, 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 számossága ugyanaz, mint X számossága Azonban az Olvasó eltűnődhet azon, hogy egy $\mathbb{R}$ fölötti végtelen dimenziós vektortérnek miért nem lehet egy megszámlálható és egy ennél nagyobb elemszámú bázisa is egyszerre.

4.10.8. 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 föl, 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.

4.10.11. Az $tf = f^k t$ összefüggés lehetővé teszi, hogy a t betűket a szavak végére (vagy az elejére) vigyük. A későbbiek megértéséhez azonban hasznosabb egy kicsit másképp nézni erre a csoportra. Legyen N az f által generált részcsoport. Azt tudjuk, hogy t az f elemet a k-adik hatványába konjugálja. Mivel a konjugálás automorfizmus, a t az f minden hatványát is a k-adik hatványába konjugálja, ami N-beli. Ezért az N normalizátorában benne van a t, 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 4.7.29. 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 $f^u t^v$ alakban is fölírható.

4.10.18. A 4.3.40. 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 fölírni. 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 $|B(k, 2)| \leq 2^k$, ezért ez a homomorfizmus izomorfizmus lesz.

4.10.19. 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 fölcserélhető.

Ez azt jelenti, hogy a g elem által generált N normálosztó kommutatív. Valóban, (a 4.8.20. Gyakorlat miatt) a g elem által generált normálosztó a g konjugáltjai által generált részcsoport, és mivel ezek páronként fölcserélhetők, (a 4.8.41. Gyakorlat szerint) N Abel-csoport.

Megmutatjuk, hogy $B(k, 3)$ 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 (4.7.29. Gyakorlat), de a g_1 mellékosztálya az egységelem, ezért már a $g_2N, \ldots, g_kN$ elemek is generátorrendszert alkotnak. A $B(k, 3)/N$ faktorban 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

$$|B(k,3)| = 3^{k+\binom{k}{2}+\binom{k}{3}}.$$

4.10.21. 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 $a^2 = 1$ következik, és innen $1 = a^5 = a^2a^2a = a$.

(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) $\langle a, b \mid a^2 = 1,\ b^7 = 1,\ aba^{-1} = b^{-1}\rangle \cong D_7$ (4.10.10. 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, mely a 4.9.38. Gyakorlat (2) pontjában megadott G csoporttal izomorf. Valóban, a 4.10.11. 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 lesz, amely a 4.9.38. Gyakorlat (6) pontjában megadott G csoporttal izomorf. Valóban, a 4.10.11. 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 a D_3 diédercsoport 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 ezt összevetni a 4.6.12. Gyakorlattal.

(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 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. Megmutatjuk, hogy N normálosztó. Persze $a = u^2 \in N$, így elég belátni, 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 fölcserélhető elem generálja, melyek legfeljebb másodrendűek, ezért N kommutatív (4.8.41. 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 szerinte 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.

4.10.22. Adjuk meg a D_4 csoportot a 4.10.15. Példában szereplő definiáló relációkkal. Ezeket a D_4 csoport tetszőleges 90 fokos F forgatása, és tetszőleges T tengelyes tükrözése kielégíti a 4.1.23. Állítás miatt. Ezért a 4.10.13. Tétel szerint van olyan $\alpha : D_4 \to D_4$ szürjektív homomorfizmus, hogy $\alpha(f) = F$ és $\alpha(t) = T$. Ez persze izomorfizmus, azaz D_4-nek automorfizmusa. Ezért legalább $2 \cdot 4 = 8$ automorfizmus van.

♫ Ha csak az automorfizmusok számát akarjuk meghatározni, akkor a következőképpen járhatunk el. Egy tetszőleges automorfizmusnál f csak negyedrendű elembe, tehát f-be vagy f^3-be mehet. A t képe másodrendű, de f^2 nem lehet, mert az centrumelem, t meg nem. Ezért t csak a négy tengelyes tükrözésbe mehet. Ez összesen legfeljebb $2 \cdot 4 = 8$ lehetőség. Mivel D_4-et generálja t és f, ezzel az automorfizmust is meghatároztuk.

Minden α automorfizmushoz rendeljük hozzá azt a permutációt, amelyet α a tengelyes tükrözések négyelemű halmazán hoz létre. Mivel D_4-et generálják a tengelyes tükrözések, minden automorfizmust egyértelműen meghatároznak e négyelemű halmazon felvett értékei. Rajzoljuk rá ezt a négy tükrözést egy négyzet négy csúcsára úgy, hogy t és tf^2 átellenes csúcsokba kerüljön. Elég megmutatni, hogy ennek a négyzetnek minden α automorfizmus szimmetriája lesz. Tudjuk, hogy t és tf^2, továbbá tf és tf^3 is konjugált elempárok D_4-ben, tehát az α-nál vett képeik is konjugáltak. Ezért a négyzet átlója átlóba kell, hogy menjen.

4.10.23. Meg kell mutatni, hogy az Útmutatóban definiált $\psi : F \to G$ homomorfizmusra $\varphi = \alpha \circ \psi$. Ezt elegendő az X generátorrendszeren ellenőrizni (4.6.9. Gyakorlat). De ha $x \in X$, akkor $\alpha\big(\psi(x)\big) = \varphi(x)$, hiszen pontosan így választottuk a $\psi(x)$ ősképet.

4.10.24. 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 kommutátor-részcsoportja 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.

4.11. Prímhatványrendű csoportok, Sylow tételei

4.11.4. 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 fölcserélhetők, hiszen ha $a, b \in Z(G)$, akkor $(g^na)(g^mb) = (g^mb)(g^na)$. Így G kommutatív.

4.11.7. Tegyük föl, hogy $H \leq G$ indexe a p prím. Legyen $H \leq K \leq G$. A 4.4.28. 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 $K = H$.

4.11.10. Legyen G ilyen csoport. Ebben nem lehet minden elem négyzete az egységelem, mert akkor kommutatív lenne (4.3.40. Feladat). Nem lehet benne nyolcadrendű elem sem, mert akkor ciklikus lenne. Ezért minden egységtől különböző eleme másod- vagy negyedrendű. Legyen f egy negyedrendű elem. Az f által generált N részcsoport indexe 2, és ezért normálosztó. Ha $t \in G - N$, akkor $g = t^{-1}ft$ negyedrendű, mert f-nek konjugáltja, és $g \in N$, hiszen N normálosztó. Ha $g = f$, akkor $tf = ft$, és mivel t és f generálják G-t, a csoport kommutatív lenne, ami lehetetlen. Az $N \cong \mathbb{Z}_4^+$ másik negyedrendű eleme f^{-1}. Tehát $ft = tf^{-1}$.

Tegyük föl először, hogy van N-en kívül egy másodrendű elem, válasszuk ezt t-nek. Ekkor G kielégíti a D_4 csoport definiáló relációit (4.10.15. Példa), és így D_4-nek homomorf képe. Mivel G nyolcelemű, ezért $G \cong D_4$.

A másik eset az, hogy minden N-en kívüli elem negyedrendű, legyen t most egy ilyen elem. Ekkor t^2 másodrendű, tehát N-beli, és így csak f^2 lehet. Ekkor viszont a kvaterniócsoport 4.10.15. Példabeli definiáló relációi teljesülnek.

4.11.12. Az UT(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 csupa nulla áll). Mátrixszorzással könnyű ellenőrizni, hogy $N^3 = 0$ (és így $p > 2$ miatt $N^p = 0$). Az E és az N fölcserélhetők, 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 3.3.22. Feladatban látottak miatt) tagonként lehet p-edik hatványra emelni. Ekkor pedig $(E + N)^p = E^p + N^p = E$. Vagyis UT(3, p) minden egységtől különböző eleme p rendű.

Szintén mátrixszorzással igazolható, hogy UT(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 UT(3, p) csoport két elemmel generálható, bármely két olyan eleme generálja, amelyek nem fölcserélhetők. Ha ugyanis két ilyen elem valódi részcsoportot generálna, akkor annak rendje legfeljebb p^2 lehetne, és így kommutatív lenne.

Tegyük föl, hogy $p = 2$. Négyzetre emeléssel meggyőződhetünk róla, hogy a csoportban csak két negyedrendű elem van, és így a D_4 diédercsoportot kapjuk.

4.11.13. A 4.8.44. Feladat szerint $\mathbb{Z}_{p^2}^+$ automorfizmus-csoportja $\mathbb{Z}_{p^2}^\times$, 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 nemkommutatív, 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 4.10.11. Gyakorlat miatt ennek a definiáló relációkkal megadott csoportnak a rendje legfeljebb p^3, tehát a most konstruált szemidirekt szorzattal izomorf.

4.11.21. Az N a P konjugáltosztályainak egyesítése, Ezek 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 konjugáltosztálynak. Ez része P centrumának.

4.11.22. Mivel $H < P$, választhatunk olyan $H < K$ részcsoportot, amely tartalmazásra minimális. Ekkor H maximális részcsoportja K-nak, és így a 4.11.8. Tétel miatt $H \lhd K$.

4.11.23. Az első izomorfizmustétel miatt $(PN)/N \cong P/(P \cap N)$, így $(PN)/N$ 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.

4.11.24. Egy p^3 rendű G csoportnak minden valódi részcsoportja legfeljebb p^2 rendű, és így kommutatív (4.11.3. Következmény). Ha $G \cong A \times B$ nemtriviális direkt felbontás, akkor tehát A és B is kommutatív, de akkor G is kommutatív lenne.

4.11.25. 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 $\mathrm{UT}(n, T)$. A homomorfizmustétel tehát pont az állítást adja.

4.11.26. Ezek a prímhatványrendű ciklikus csoportok. Tegyük föl, hogy a G 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 mivel G véges, része lenne G egy maximális részcsoportjának, ami nem lehet M. Tehát G ciklikus. Mivel $\mathbb{Z}^+$-nak nem csak egy maximális részcsoportja van (hanem minden p prímre $p\,\mathbb{Z}$ maximális részcsoport), ezért G véges. 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.

4.11.27. A D_4 diédercsoporttal izomorf. 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).

A kocka szimmetriacsoportjának 2-Sylowja $D_4 \times \mathbb{Z}_2^+$, hiszen a 4.9.32. Feladat szerint a kocka szimmetriacsoportja $S_4 \times \mathbb{Z}_2^+$. Ezt a 16 elemű részcsoportot megadtuk a 4.5.29. Feladatban.

4.11.28. 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.

4.11.29. 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.

4.11.30. Mivel a p-Sylow részcsoportok konjugáltak, ezért minden p prímhez csak egy darab p-Sylow részcsoport van. Így véges sok nemtriviális normálosztót kapunk, jelölje ezeket $P_1, \ldots, P_k$. Az Útmutatóban megadott ötlet miatt $P_1P_2 \ldots P_k$ rendje G rendjével egyenlő, azaz $P_1P_2 \ldots P_k = G$. Ha egy kivételével szorozzuk őket össze, akkor az Útmutatóbeli ötlet miatt a szorzat rendje relatív prím lesz a kimaradó részcsoport rendjéhez, és így metszetük Lagrange tétele miatt csak az egységelemből áll. Ezek a Sylow-részcsoportok tehát teljesítik a 4.9.14. Gyakorlatban megadott feltételt.

4.11.31. Az S_3 csoportnak az összes részcsoportját leírtuk a 4.4.25. 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 4.11.28. Gyakorlat szerint $8/2 = 4$. 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 4.8.33. 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 V normálosztó. A V 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.

♫ Kiszámítjuk a Sylowok normalizátorait is. 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. (De mondhatnánk azt is, hogy A_5-ben nincs tizedrendű elem, és így egy tízelemű részcsoport csakis D_5 lehet a 4.8.37. Gyakorlat szerint.) Hasonlóképpen a 3-Sylowok normalizátora S_3-mal izomorf.

A D_n diédercsoportban $p > 2$ esetén csak egyetlen p-Sylow van. Valóban, legyen k a p kitevője n-ben. Ekkor $p > 2$ miatt minden p-Sylow rendje p^k. Egy ilyen részcsoportban nem lehet tükrözés, hiszen az másodrendű, és $2 \nmid p^k$. Ezért minden p-Sylow része a forgatásokból álló normálosztónak, ami ciklikus, és így egyetlen p^k rendű részcsoportja van (4.3.27. Állítás).

Legyen $n = 2^k m$, ahol m páratlan. Belátjuk, hogy a 2-Sylowok száma m. Ha egy szabályos n-szög valamelyik csúcsától m-esével lépdelve körbeindulunk, akkor egy szabályos 2^k-szöget kapunk. Az n-szög m darab ilyen 2^k-szögnek az uniója (melyek csúcshalmazai páronként diszjunktak). A D_n csoport azon elemei, amelyek egy ilyen 2^k-szöget fixen hagynak, egy D_{2^k}-val izomorf részcsoportot alkotnak D_n-ben. Ennek rendje 2^{k+1}, és így egy 2-Sylow részcsoportot kaptunk. Az m darab 2^k-szöghöz páronként különböző részcsoportok tartoznak (sőt könnyen láthatóan minden D_n-beli tengelyes tükrözés pontosan egy részcsoportban van benne ezek közül). Ezért találtunk m darab 2-Sylow részcsoportot. Ennél több nincs, mert egy 2-Sylow részcsoport indexe m, és ennek a 2-Sylowok száma osztója (4.11.18. Tétel (5) pont).

♫ Ha az előző gondolatmenetben $k = 1$, akkor „kétszögek" keletkeznek (az n-szög átlói). Ebben az esetben a D_2 csoport helyett arról a csoportról kell beszélni, amelynek elemei az identitás és a középpontos tükrözés mellett a kérdéses átló egyenesére, illetve az arra merőleges egyenesre való tükrözés. Ha pedig $k = 0$, akkor „egyszögek" keletkeznek (ami egyetlen csúcs). Ekkor D_1 helyett azt a csoportot kell tekinteni, amelynek egyetlen nem identikus eleme az adott csúcson átmenő átló egyenesére való tükrözés. Általában is igaz, hogy D_n bármely két 2-Sylowjának metszete a 2-hatvány rendű forgatásokból álló 2^k rendű részcsoport.

4.11.32. 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 4.11.28. 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.

4.11.33. Tegyük föl, 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 4.11.28. 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.

4.11.34. 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 föl, hogy bármely két p-Sylow metszete csak az egységelemből áll. Mindegyik p-Sylowban $p^2 - 1$ olyan elem van, melynek rendje 1-nél nagyobb p-hatvány. Ez összesen $q(p^2-1) = |G| - q$. A kimaradó q elem közül egy az egységelem, tehát csak $q-1$ darab q 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.

♫ A most látott gondolatmenet haszna, hogy bemutatja a következő, 4.11.35. Feladat megoldásának fő gondolatát. Lássunk vázlatosan egy második megoldást is. Ha egyik Sylow sem normálosztó, akkor a p-Sylowok száma q, és $q \equiv 1\ (p)$, azaz $q > p$. A q-Sylowok száma p vagy p^2 lehet, de $q > p$ miatt p nem kongruens 1-gyel mod q, ezért p^2 darab q-Sylow van. A fenti első bekezdéshez hasonló számolás ekkor azt mutatja, hogy p-hatvány rendű elemből legfeljebb p^2 lehet, azaz csak egy p-Sylow fér el. Ebből a megoldásból láthatjuk, hogy egy p^2q rendű csoportban valamelyik Sylow részcsoport biztosan normálosztó.

4.11.35. Ha csak egy p-Sylow van G-ben, akkor ez normálosztó. Tegyük föl, 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 föl, hogy $|D| > 1$, belátjuk, hogy $D \triangleleft G$ (és így G nem egyszerű). A 4.11.22. 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 legnagyobb elemszámú két p-Sylow metszetei között. Így $N_G(D)$ nem p-csoport, vagyis tartalmazza G egy Q q-Sylow részcsoportját. Bármely P p-Sylow részcsoportra igaz, hogy $PQ = G$, hiszen a 4.4.31. 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.

4.11.36. 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 $P \triangleleft P_1$ (hiszen N normálosztó). Ekkor pedig $P_1 \subseteq N_G(P)$.

4.11.37. A P részcsoport p-Sylowja K-nak is, így a Frattini-elvet a $K \lhd N_G(K)$ normálosztóra alkalmazva kapjuk, hogy $N_G(K) = K N_G(P)$, 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 G-ben $|G : N_G(P)|$). Így mindkét index kongruens 1-gyel mod p. De $N_K(P) = K \cap N_G(P) = N_G(P)$, és ezért

$$|G : N_G(P)| = |G : K| \cdot |K : N_G(P)| = |G : K| \cdot |K : N_K(P)| .$$

Tehát $|G : K|$ is 1-gyel kongruens mod p.

4.11.38. 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 (4.3.24. 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.

4.12. Permutációcsoportok

4.12.3. 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 homomorfizmustétel 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.

4.12.5. 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.

4.12.7. 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 $1H$ pályája 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 4.12.3. 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.

4.12.8. 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 föl, 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 tranzitíven hat X-en, az α szürjektív. Belátjuk, hogy injektív is. 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.

4.12.10. 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.

4.12.12. 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 4.12.11. 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 4.12.11. Állítás miatt a G csoport k-tranzitív. Tegyük föl, 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 $g_1 = g_2$.

4.12.14. Legyen $G = \mathrm{AGL}(n, T)$. 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 4.12.11. Állítás miatt G már 2-tranzitív a V halmazon.

Az $\mathrm{AGL}(n, T)$ 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 $\mathrm{AGL}(n, T)$ csoportok közül pontosan $\mathrm{AGL}(1, \mathbb{Z}_3) \cong S_3$ és $\mathrm{AGL}(n, \mathbb{Z}_2)$ lesz 3-tranzitív. Az első szigorúan 3-tranzitív is, a második akkor szigorúan 3-tranzitív (és egyben 4-tranzitív), ha $n = 2$ (ez az $\mathrm{AGL}(2, \mathbb{Z}_2) \cong S_4$ csoport szokásos hatása a négyelemű halmazon).

Valóban, tegyük föl, hogy az $\mathrm{AGL}(n, T)$ 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 $\mathrm{AGL}(1, \mathbb{Z}_3) \cong S_3$ csoport szigorúan 3-tranzitív hatását kapjuk a háromelemű halmazon. A második esetben kapott $\mathrm{AGL}(n, \mathbb{Z}_2)$ 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).

4.12.17. Az állítás a 4.12.12. Gyakorlat gondolatmenetével adódik (amikor $k = 1$). Ha az x pont stabilizátora egyelemű, akkor a pályájának a hossza G rendjével egyenlő. Ha G tranzitív is, akkor ez a pontok száma, vagyis a csoport foka.

4.12.19. A Cayley-tételben a g elemhez tartozó permutáció a g elemmel való balszorzás. Minden stabilizátor egyelemű, mert 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 4.12.8. Feladat miatt.

4.12.21. A pályákról tudjuk, hogy ekvivalenciarelációt alkotnak. Ha x és y egy pályán van, akkor $g \in G$ esetén $g*x$ és $g*y$ is egy pályán van: az x-et és y-t tartalmazó pályán. Így kongruenciát kaptunk. A csoport pontosan akkor tranzitív, ha az egész X egyetlen pálya, vagyis ha ez az 1_X kongruencia.

4.12.22. 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.

4.12.23. Csak a két triviális kongruencia van. Tegyük föl, hogy a $P \neq Q$ pontok kongruensek egy $\sim$ kongruenciánál. Jelölje Y a P pont osztályát a $\sim$ kongruenciánál, be kell látni, hogy Y az egész sík. A 4.1.34. Gyakorlat szerint az egyforma hosszú szakaszok mozgással egymásba vihetők, és így bármely két olyan pont $\sim$-relációban áll, melyek távolsága ugyanaz, mint P és Q távolsága. Ezért elegendő megmutatni azt, hogy a kongruens pontpárok között minden pozitív valós távolság előfordul.

A P körüli Q-t tartalmazó körvonal minden pontja benne van Y-ban, tehát ezek egymással is kongruensek. Ha tehát e kör sugara r, akkor megkaptuk a 0 és $2r$ közötti összes távolságot. Egy $2r$ távolságú pontpárból kiindulva a 0 és $4r$ közötti távolságokat is megkapjuk, és így tovább.

4.12.24. 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.

4.12.25. 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.

4.12.31. 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 1-től különböző 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).

4.12.34. Ha $G \leq S_X$ Frobenius-csoport, akkor $H \neq \{1\}$ (mert G nem reguláris), és $H \neq G$ (mert G tranzitív). A 4.5.37. 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 4.12.7. 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 azok az elemek vannak az egységelemen kívül, melyeknek nincs fixpontja, tehát amelyek H egyetlen konjugáltjában sincsenek benne. Az N tehát konjugáltosztályok egyesítése, és így ha részcsoport, akkor normálosztó is. A H-ra kirótt feltétel miatt $N_G(H) = H$, így H-nak n konjugáltja van. Ezek páronként diszjunktak (az egységelemet leszámítva), és ezért a mag elemszáma $|G| - n(|H| - 1) = n$, hiszen $n = |G : H|$. Nyilván $H \cap N = \{1\}$, és így $|NH| = |N||H| = n|H| = |G|$. Ezért $NH = G$.

4.12.35. 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} 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 az $\mathrm{AGL}(1, T)$ a T testen hat, a mag az $x + b$ alakú leképezésekből, vagyis az eltolásokból áll, a komplementumok a $T^\times$ csoporttal izomorfak.

4.12.36. 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 4.11.20. Következmény 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 $q \mid p - 1$).

4.12.37. Tegyük föl, 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 (4.11.7. Gyakorlat), tehát N csak A_n vagy S_n lehet.

Az első esetben $N \cap A_n = \{1\}$, így N minden eleme fölcserélhető A_n minden elemével (4.8.25. 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 (4.8.36. Gyakorlat). Ezért S_n-nek a triviálisakon kívül csak A_n lehet normálosztója.

♫ Az $N \cap A_n = \{1\}$ esetben a következőképpen is érvelhetünk. Az első izomorfizmustétel (4.7.25. Következmény) miatt $S_n/A_n \cong N/(N \cap A_n)$, azaz N elemszáma 2. A 4.8.40. Gyakorlat miatt $N \leq Z(S_n)$.

4.12.38. 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 pálya, 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 $|G| = |Y|$.

4.12.39. Elég belátni, hogy a stabilizátorok egyeleműek. Tranzitív csoportban a stabilizátorok egymás konjugáltjai (4.5.37. Gyakorlat), és mivel A Abel-féle, egyenlők. Tehát egy pont stabilizátorának elemei az összes pontot fixálják, és így minden stabilizátor egyelemű.

4.12.40. Egy kongruencia osztályai ugyanannyi elemből állnak (4.12.24. Gyakorlat), ez az elemszám tehát osztója a csoport fokának, ami prím. Így vagy minden osztály egyelemű, vagy csak egyetlen osztály van.

4.12.41. 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. 4.12.22. 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).

♫ Az utolsó két bekezdésben is felhasználhattuk volna a 4.12.27. Következményt. Például egy lap stabilizátora a kocka szimmetriacsoportjában nyolcelemű, és így a Sylow-tétel miatt nem lehet maximális részcsoportja egy $48 = 16 \cdot 3$ elemű csoportnak.

4.12.42. 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 föl, hogy $|G : H| = 3$, és hogy $|G|$ páratlan.

Tekintsük G hatását a H részcsoport szerinti bal mellékosztályok halmazán. A 4.12.7. 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 $H = N$.

4.12.43. Az $\mathrm{Aut}(G)$ akkor és csak akkor hat tranzitívan G egységtől különböző elemeinek a halmazán, ha $G \cong (\mathbb{Z}_p^+)^n$ alkalmas p prímre, azaz ha G egy elemi Abel-féle p-csoport. Valóban, ha a hatás tranzitív, akkor G minden 1-től különböző elemének a rendje ugyanaz. Mivel minden nemtriviális véges 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 elvihető, és így $Z(G) = G$, vagyis G Abel-csoport. Az alaptétel miatt $G \cong (\mathbb{Z}_p^+)^n$. Ezt a csoportot a 4.9.35. Gyakorlat szerint egy $\mathbb{Z}_p$ fölötti V vektortérnek tekinthetjük, melynek automorfizmus-csoportja $\mathrm{GL}(n, \mathbb{Z}_p)$. A lineáris algebra előírhatósági tétele miatt bármely nem nulla vektor bármely másikba elvihető egy lineáris transzformációval, és így a $(\mathbb{Z}_p^+)^n$ csoportok megfelelők.

Az $\mathrm{Aut}(G)$ akkor primitív a $G - \{1\}$ halmazon, ha $G \cong \mathbb{Z}_3^+$, vagy $G \cong (\mathbb{Z}_2^+)^n$. Valóban, az előző bekezdés szerint ilyenkor G egy n-dimenziós V vektortérnek tekinthető $\mathbb{Z}_p$ fölött. Ha a hatás primitív, 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 (4.12.14. Gyakorlat).

4.12.44. A pályák kongruenciát alkotnak, tehát ha csak triviális kongruencia van, 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.

4.12.45. 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 az $L \cap N$ normalizátora tartalmazza N-et, hiszen N Abel, de tartalmazza L-et is, hiszen $N \lhd G$ miatt $L \cap N \lhd L$. Így $N_G(L \cap N)$ tartalmazza $NL \geq NH = G$-t is, vagyis $L \cap N \lhd G$. 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 4.7.30. Gyakorlat miatt). Könnyű meggondolni, hogy a fenti megoldás valójában a most mutatott gondolatmenetnek a „visszafordítása" a permutációcsoportok nyelvére.

4.12.46. Tekintsük a 4.2.33. 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 pálya, $|G|$ 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 4.2.28. Gyakorlat miatt készen vagyunk.

4.12.47. 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 pályája nyolcelemű.

4.12.48. Legyen H egy k indexű részcsoport, a $k > 1$ feltétel azt jelenti, hogy $H < G$. Tekintsük G hatását a H szerinti bal mellékosztályokon. Ennek magja nem G (hiszen a mag a H konjugáltjainak a metszete a 4.12.7. Gyakorlat miatt, és $H < G$). Mivel G egyszerű, ez a mag csak az egységelemből áll, és így a 4.12.7. Gyakorlat szerint G beágyazható S_k-ba.

Speciálisan ha H egy k indexű valódi részcsoport A_n-ben, akkor A_n beágyazható S_k-ba. Ezért $n!/2 \leq k!$. Innen könnyű belátni, hogy $n \leq k$ (a kivétel csak az, hogy $2!/2 \leq 1!$, de tudjuk, hogy $k > 1$). Ezért A_n-ben minden valódi részcsoport legalább n indexű. Ilyenek persze vannak is, például a pontok stabilizátorai.

Legyen most H egy k indexű valódi részcsoport S_n-ben. Ha a H bal oldali mellékosztályain való hatás N magja csak az egységelemből áll, akkor $n! \leq k!$, azaz $n \leq k$. Ha nem, akkor N nemtriviális normálosztó. Ha $n \geq 5$, akkor ez csak A_n lehet (4.12.37. Gyakorlat), és $N \leq H < G$ miatt ekkor $H = A_n$. Vagyis $n \geq 5$ esetén az A_n-en kívül S_n minden valódi részcsoportjának az indexe legalább n. Most is minden pont stabilizátora n indexű.

Ugyanez a gondolatmenet $n = 3$ esetében is érvényes, mert a 4.8.15. Állítás miatt S_3 egyetlen nemtriviális normálosztója A_3. Az S_4 csoportban viszont van három indexű részcsoport is, például a négyzet szimmetriacsoportja (azaz D_4).

4.12.49. 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 pontosan akkor páratlan permutáció, ha g rendje páros, de $|G|/o(g)$ páratlan, vagyis ha ($|G|$ páros és) $o(g)$ 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 $A_G \lhd S_G$ alternáló csoport egy valódi normálosztóban metszi, aminek az indexe az első izomorfizmustétel miatt 2 lesz. Ha G egyszerű, és van 2 indexű normálosztója, akkor G a kételemű ciklikus csoport.

4.12.50. 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 4.12.48. 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 4.12.48. Feladat miatt G beágyazható S_6-ba, sőt a 4.12.49. 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 4.12.48. Feladat miatt lehetetlen, hiszen A_6 is egyszerű.

Végül tegyük föl, 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 4.12.33. Frobenius-tételt, akkor készen lennénk. Ugyanis az 5-Sylow normalizátora önmaga, és így a 4.12.36. 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.

4.12.51. Mivel G tranzitív, az X elemszáma osztja G rendjét, azaz $|G|$ páros. Tegyük föl, hogy $|G| = 4k+2$. Ekkor a 4.12.49. 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.

4.12.52. Tranzitív hatásban a stabilizátorok konjugáltak (4.5.37. 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 4.12.7. Gyakorlat miatt) K is stabilizátor a H mellékosztályain való hatásban. A 4.12.8. Feladat miatt minden tranzitív hatás ekvivalens egy tetszőleges stabilizátor szerinti mellékosztályokon való hatással. Tehát a H szerinti mellékosztályokon való hatás ekvivalens a K szerintivel.

4.12.53. A feltétel az, hogy minden $1 \neq h \in H$ esetén $\psi(h)$ fixpontmentes automorfizmusa legyen N-nek (azaz csak az egységelemet fixálja).

Valóban, 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. 4.12.34. Gyakorlat).

Megfordítva, tegyük föl, hogy tetszőleges $h \neq 1$ 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 az $nhn^{-1} \neq 1$ elemet, ahol $h \in H$, akkor $nhn^{-1}h^{-1} \in H \cap N$, mert N normálosztó. Ezért ez az egységelem, ahonnan $nh = hn$, tehát a h-val való konjugálás fixálja az n elemet.

♫ Könnyű megmutatni, hogy egy Frobenius-csoport „természetes” (vagy ami ezzel ekvivalens, a H komplementum mellékosztályain való) hatása ekvivalens a csoportnak az N magon való azon hatásával, amelynél N elemei balszorzással, H elemei konjugálással hatnak. (Ezt lényegében be is láttuk a 4.12.30. Tétel bizonyításában.) Ennek az észrevételnek a felhasználásával a fenti számolás némileg rövidebbé és természetesebbé tehető.

4.12.54. Tekintsük H hatását konjugálással az N egységtől különböző elemein. Minden $n \in N$ stabilizátora egyelemű, hiszen a 4.12.53. Gyakorlat miatt H elemei fixpontmentesen hatnak. Ezért minden pálya elemszáma $|H|$.

4.13. Feloldható és nilpotens csoportok

4.13.6. Ha egy csoportnak van olyan kompozíciólánca, amelyben a faktorok prímrendű ciklikusak, akkor mivel ezek kommutatívak, a csoport feloldható. Megfordítva, tegyük föl, hogy a G véges csoportnak van olyan normállánca, amelyben a faktorok kommutatívak. Ha ezt elkezdjük finomítani, akkor ez azt jelenti, hogy az $N \triangleleft K$ közé betoldunk egy M-et, melyre $N \triangleleft M \triangleleft K$. A második izomorfizmustétel 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 4.7.24. 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 kompozíciólánccá finomíthatjuk. Ebben szintén minden faktor kommutatív lesz, de egyúttal egyszerű csoport is. A kommutatív egyszerű csoportok azonban a prímrendű ciklikusak (4.8.3. Következmény).

Ha G egyszerű, akkor az egyetlen kompozíciófaktora maga G, ennek kell prímrendű ciklikusnak lennie ahhoz, hogy G feloldható legyen.

4.13.7. Az S_2 prímrendű ciklikus. Az S_3-ban $\{id\} \triangleleft \{id, (123), (132)\} \triangleleft S_3$ olyan kompozíciólánc, amelyben minden faktor Abel-féle. Az S_4 esetén

$$\{id\} \triangleleft \{id, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4 \triangleleft S_4$$

olyan normállánc, amelynek faktorai Abel-csoportok (hiszen a 4.8. szakaszban meghatároztuk S_4 összes normálosztóit, és láttuk, hogy a fenti négyelemű normálosztó a Klein-csoporttal izomorf).

Az E(2) csoport a 4.9.19. Gyakorlat szerint az eltolásokból álló N normálosztónak és egy tetszőleges P pont stabilizátorának a szemidirekt szorzata. Ez a stabilizátor a P körüli forgatásokból áll, és az SO(2)-vel izomorf kommutatív csoport, ami G/N-nel izomorf. Tehát az $\{id\} \triangleleft N \triangleleft \mathrm{E}(2)$ normállánc mutatja, hogy E(2) feloldható.

4.13.8. 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 4.9.28. 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.

4.13.16. 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 4.8.23. 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

$$\{1\} = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_{n-2} \triangleleft N_{n-1} \triangleleft N_n = G\,.$$

normállánca, amelyben a faktorok kommutatívak, akkor indukcióval azonnal láthatjuk, hogy $G^{(i)} \leq N_{n-i}$ 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 4.8.47. Gyakorlat miatt a kommutátor-részcsoport karakterisztikus. Tudjuk, hogy karakterisztikus részcsoport karakterisztikus részcsoportja is karakterisztikus (4.8.18. Gyakorlat), ezért a kommutátorlánc minden eleme karakterisztikus, speciálisan normálosztó.

4.13.17. Legyen H részcsoport a G feloldható csoportban. Indukcióval azonnal látjuk, hogy $H^{(i)} \subseteq G^{(i)}$ (ezt a jelölést az előző feladat megoldásában definiáltuk). Mivel G feloldható, van olyan n egész, hogy $G^{(n)} = \{1\}$. De akkor $H^{(n)} = \{1\}$, vagyis H is feloldható.

Ha N normálosztó a G feloldható csoportban, akkor a 4.8.48. 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 izomorfizmustétel miatt a $G^{(i)}N/N$ normálosztók olyan normálláncát képezik a G/N faktorcsoportnak, melynek faktorai kommutatívak.

♫ Az Olvasónak javasoljuk, hogy a feladat állításait próbálja meg kommutátor-részcsoport felhasználása nélkül kihozni az izomorfizmustételekből.

4.13.18. 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 izomorfizmustétel 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.

4.13.25. Az Útmutatóban szereplő állítások egyszerű mátrixszorzással igazolhatók, és következik belőlük, hogy $\mathrm{UT}(n, T)$ nilpotens. Álljon ugyanis N_i az $E + K$ alakú mátrixokból, ahol $K \in U_{n-i}$. Ekkor $N_{n-1} = \mathrm{UT}(n, T)$, és $[N_{n-1}, N_i] \subseteq N_{i-1}$ az Útmutatóbeli (3) összefüggés miatt, vagyis ez egy centrális lánca $\mathrm{UT}(n, T)$-nek. A 4.11.25. Gyakorlat miatt $\mathrm{T}(n, T)/\mathrm{UT}(n, T)$ Abel, és így $\mathrm{T}(n, T)$ feloldható.

4.13.26. Egy Abel-csoport minden kompozíciófaktora egyszerű Abel-csoport, azaz prímrendű ciklikus (lásd a 4.13.6. 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).

4.13.27. Ha a két prím egyenlő, akkor a csoport kommutatív (4.11.3. Következmény), és így feloldható. Ha a két prím különböző, akkor a 4.11.20. Tétel miatt a csoportban van prímrendű normálosztó. Ez kommutatív, és a rá vett faktor is prímrendű, tehát az is kommutatív.

4.13.28. Az E(3)-nak részcsoportja SO(3), ami nemkommutatív egyszerű csoport (4.8.43. Feladat). Ez tehát nem feloldható, és akkor a 4.13.17. Gyakorlat miatt E(3) sem lehet az.

4.13.29. 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 4.12.3. 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 4.13.18. Feladat miatt tehát G is feloldható.

Ha $p \neq 3$, akkor G/N az S_4 egy olyan részcsoportjával izomorf, amelynek rendje nem osztható hárommal, vagyis 2-hatvány. Ezért N indexe 2-hatvány, és így $N \subseteq P$ miatt csak $N = P$ lehetséges (különben N indexe p-vel osztható lenne). Ezért $p \neq 3$ esetén P normálosztó. Ha $p = 3$, akkor ez nem feltétlenül van így, az A_4 ellenpélda (4.8.16. Gyakorlat).

♫ Ha $p \neq 3$, akkor a Sylow-tételből is triviális, hogy a p-Sylow normálosztó, hiszen a a p-Sylowok száma osztója a 4-nek, és kongruens 1-gyel mod p. Persze a feloldhatóság is nyilvánvaló ilyenkor, hiszen a p-Sylow szerinti faktor négyelemű, azaz kommutatív.

4.13.30. Ha N minimális normálosztó G-ben, akkor feloldható (4.13.17. Feladat), és így (a 4.13.16. Feladat miatt) $N' < N$. De N' karakterisztikus részcsoport N-ben, ezért (a 4.8.18. 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 4.8.47. 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.

4.13.31. 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 4.7.24. 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 volt az indukció kezdő esete. Ezt a fajta indukciót már megismertük a 3.2.1. Tétel bizonyításában, 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.

Végül legyen G véges, feloldható, primitív permutációcsoport. Ebben minden pont stabilizátora maximális részcsoport (4.12.27. Következmény), amelynek az indexe az előzőek szerint prímhatvány. Ennek a stabilizátornak az indexe a csoport foka, hiszen minden primitív csoport tranzitív.

4.14. Véges egyszerű csoportok

4.14.1. Az egyetlen olyan 60-nál kisebb szám, aminek három különböző prímosztója is van, a 30. De egy 30 rendű csoport feloldható, a 4.11.33. Feladat miatt. A fennmaradó számok mindegyike $p^\alpha q$ vagy $4p^\alpha$ alakú, vagy prímhatvány. Így a 4.11.35, illetve a 4.13.29. Feladatok miatt készen vagyunk.

4.14.2. Elég belátni, hogy az $\mathrm{SL}(n, T)$ részcsoport centralizátora $\mathrm{GL}(n, T)$-ben éppen az egységmátrix nem nulla skalárszorosaiból áll. Jelölje $E^{i,j}$ $(i > j)$ azt a mátrixot, amelyben az i-edik sor j-edik eleme 1, és az összes többi elem nulla. Ekkor $E + E^{i,j}$ invertálható, és a determinánsa 1, tehát $\mathrm{SL}(n, T)$-ben van (érdemes ezt összevetni a 4.13.25. Feladatra adott útmutatásban szereplő állításokkal). Könnyű számolás mutatja, hogy ha egy mátrix az $E + E^{i,j}$ mátrixok mindegyikével fölcserélhető, akkor az az egységmátrix skalárszorosa.

Hasonló számolással kaphatjuk, hogy $|T| \geq 3$ esetén a H részcsoport normalizátora azokból a mátrixokból áll, amelyek minden sorában és oszlopában pontosan egy nem nulla elem van, centralizátora pedig a diagonális mátrixok csoportja. Ha $|T| = 2$, akkor persze H centralizátora $\mathrm{GL}(n.T)$.

4.14.4. Könnyű kiszámolni, hogy

$$\varphi : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \frac{ax+b}{cx+d}$$

művelettartó, és magja a skalármátrixokból (az egységmátrix skalárszorosaiból) áll. A homomorfizmustétel szerint $\mathrm{Im}(\varphi) = G \cong \mathrm{GL}(2, T)/\mathrm{Ker}(\varphi)$, ami definíció szerint $\mathrm{PGL}(2, T)$. (Azt, hogy a $T \cup \{\infty\}$ halmazon a hatás szigorúan 3-tranzitív, beláttuk a 245. oldal apró betűs részének a végén.)

4.14.7. Legyen $b_1, \ldots, b_n$ egy bázis a q elemű T test fölötti V vektortérben. 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 homomorfizmustétel 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 (4.3.22. Tétel), és így az ilyen elemek száma (a 4.3.24. Állítás szerint) éppen d.

4.14.10. 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 K/N faktorcsoportban az egész K/N 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.

4.14.11. Legyen G egy 200 rendű csoport, és $F = N/K$ ennek egy kompozíciófaktora. Ekkor F egyszerű csoport, melynek rendje 200-nak osztója. Ilyen nemkommutatív egyszerű csoport azonban a táblázat szerint nincs, mert a táblázatban csak két olyan csoport szerepel, amelynek rendje 200-nál nem nagyobb, de ezek a rendek (60 és 168) nem osztói 200-nak. Ezért F csak kommutatív (egyszerű) csoport lehet (azaz prímrendű ciklikus, a 4.8.3. Következmény szerint), és így G feloldható.

4.14.12. A kételemű test fölött 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 (4.9.35. Gyakorlat), ami a 4.8.44. Feladat miatt S_3.

A 4.14.4. Gyakorlat szerint a $\mathrm{PGL}(2, 3)$ csoport 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).

4.14.13. Tegyük föl, hogy a G egyszerű csoport rendje 60. A 4.12.48. 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 (mert ha 5, akkor ismét van 5 indexű részcsoport). 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.

4.14.14. Az $\mathrm{UT}(n, p)$ egy $p^{n(n-1)/2}$ rendű részcsoportja $\mathrm{GL}(n, p)$-nek. De $\mathrm{GL}(n, p)$-nek ismerjük a rendjét (4.14.7. Feladat). Könnyű kiszámolni, hogy ebben a rendben a p prím kitevője $n(n-1)/2$.

4.14.15. 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 $\mathrm{UT}(n, p)$-vel.

4.14.16. Legyen $N \lhd G \times G$ valódi normálosztó, $G_1 = G \times \{1\}$ és $G_2 = \{1\} \times G$. Ekkor $N \cap G_1$ normálosztó $G_1 \cong G$-ben, ami egyszerű csoport. Ezért ez a metszet vagy csak az egységelem, vagy pedig az egész G_1. Ez utóbbi esetben viszont N/G_1 normálosztó $(G \times G)/G_1 \cong G$-ben, ami egyszerű, és így N vagy az egész $G \times G$, vagy pedig $N = G_1$. Hasonlóan ha N különbözik G_2-től, akkor $N \cap G_2 = \{1\}$. De akkor N centralizálja G_1-et és G_2-t is a 4.8.25. Gyakorlat miatt. Ezért N benne van $G \times G$ centrumában, ami azonban egyelemű (4.9.29. Gyakorlat). Beláttuk tehát, hogy $G \times G$ valódi, nemtriviális normálosztói $G \times \{1\}$ és $\{1\} \times G$.

Ha G kommutatív, akkor mindig van másik normálosztó is $G \times G$-ben, például a (g, g) párok halmaza, ahol $g \in G$.

5. fejezet

Gyűrűk

5.1. Részgyűrű, ideál, direkt szorzat

5.1.7. A valós elemű 2×2-es mátrixok gyűrűjében álljon I azokból a mátrixokból, amelyek második oszlopa nulla. Mivel

$$\begin{bmatrix} x & u \\ y & v \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} xa+ub & 0 \\ ya+vb & 0 \end{bmatrix} \quad \text{és} \quad \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\begin{bmatrix} x & u \\ y & v \end{bmatrix} = \begin{bmatrix} ax & au \\ bx & bu \end{bmatrix},$$

ezért ez balideál, de nem jobbideál.

♫ A teljes mátrixgyűrű ideáljait az 5.3.3. és az 5.3.18. Feladatban, az egyoldali ideáljait a 8.7.10. és a 8.7.12. Feladatban írjuk majd le.

5.1.11. A $(18, 30)$ ideálban benne van a $30 - 18 = 12$, és így a $18 - 12 = 6$ is. Ezért $(6) \subseteq (18, 30)$. A (6) által generált ideálban viszont benne van a 6 minden többszöröse, vagyis a 18 és a 30 is. Ezért $(18, 30) \subseteq (6)$.

♫ Természetesen $(18, 30)$ elemei a $18x + 30y$ alakú számok, ahol $x, y \in \mathbb{Z}$. A lineáris diofantikus egyenlet megoldhatóságáról szóló számelméleti tétel szerint ezek pontosan a 18 és 30 legnagyobb közös osztójának, vagyis a 6-nak a többszörösei. Ennek az észrevételnek fontos szerepe lesz majd a legnagyobb közös osztó fogalmának ideálok segítségével történő megközelítésében, amit az 5.5. szakaszban tárgyalunk. Érdemes összevetni mindezt a 4.6.11. Gyakorlat (1) pontjának megoldásával, és az azt követő megjegyzésekkel is.

5.1.13. Az $IJ = \{a_1b_1 + \ldots + a_nb_n \ : \ a_k \in I, b_k \in J\}$ halmaz nyilván zárt az összeadásra. Zárt az ellentettképzésre is, mert

$$-(a_1b_1 + \ldots + a_nb_n) = (-a_1)b_1 + \ldots + (-a_n)b_n\,,$$

és mivel I ideál, $-a_1, \ldots, -a_n \in I$. Ugyanígy

$$r(a_1b_1 + \ldots + a_nb_n) = (ra_1)b_1 + \ldots + (ra_n)b_n \in IJ$$

tetszőleges $r \in R$ esetén. De $ra_1, \ldots, ra_n \in I$, hiszen I (bal)ideál, és ezért IJ is balideál. Hasonlóan látható, hogy IJ jobbideál is.

Az $I + J$ részcsoport, hiszen két részcsoport komplexusösszege. Az, hogy zárt az R elemeivel való bal- és jobbszorzásra, ugyanúgy látható be, mint IJ esetében.

A disztributivitáshoz belátjuk, hogy $(A + B)C$ is és $AC + BC$ is az ac és a bc alakú elemek véges összegeinek a H halmaza lesz, ahol $a \in A$, $b \in B$, $c \in C$. Az $AC + BC = H$ összefüggés világos, megmutatjuk, hogy $(A + B)C = H$. Az $A + B$ az $a + b$ alakú elemek halmaza, ahol $a \in A$ és $b \in B$. Ezért $(a + b)c = ac + bc \in H$ minden $c \in C$-re, vagyis $(A + B)C \subseteq H$. Megfordítva, $(A + B)C$ tartalmazza az ac és bc alakú elemeket, és zárt az összeadásra a komplexusszorzás definíciója miatt, tehát tartalmazza H minden elemét.

Az asszociativitás igazolásához azt kell belátni, hogy $(AB)C$-t és $A(BC)$-t is az $(ab)c = a(bc)$ elemek generálják az összeadásra, ahol $a \in A$, $b \in B$, $c \in C$. Ez az előző bizonyításhoz hasonlóan történhet. (Legyünk óvatosak, A, B, C nem feltétlenül részcsoport, de a szorzatok már véges összegek halmazai, és ezt tekintetbe kell vennünk a bizonyításnál.)

5.1.14. Legyen $I = (s_1, \ldots, s_n)$, $J = (t_1, \ldots, t_m)$ és K az nm darab s_it_j elem által generált ideál. Be kell látnunk, hogy IJ és K tartalmazzák egymást. Nyilván $s_it_j \in IJ$, és így az IJ ideál tartalmazza

K generátorelemeit, vagyis $K \subseteq IJ$. Megfordítva, IJ az ab alakú elemek véges összegeiből áll, ahol $a \in I$ és $b \in J$, és ezért az $IJ \subseteq K$ tartalmazáshoz elegendő megmutatni, hogy $ab \in K$. Az 5.1.9. Állítás miatt $a = u_1s_1 + \ldots + u_ns_n$ és $b = v_1t_1 + \ldots + v_mt_m$ alkalmas $u_i, v_j \in R$ elemekre. De akkor ab az $u_is_iv_jt_j$ alakú elemek összege, ahol $1 \leq i \leq n$ és $1 \leq j \leq m$. Az $u_is_iv_jt_j$ elem azonban s_it_j többszöröse, hiszen R kommutatív, és ezért K-ban van.

5.1.15. Az $m_1s_1+\ldots+m_ns_n+r_1s_1+\ldots+r_ns_n$ elem benne van minden X-et tartalmazó balideálban, hiszen az zárt az összeadásra, az ellentettképzésre (így az egész számokkal való szorzásra), és az R elemeivel való balszorzásra is. Megfordítva, az ilyen alakú elemek egy X-et tartalmazó balideált alkotnak: az összeadásra, kivonásra és az R elemeivel való balszorzásra való zártság könnyen látható, az $s_i \in X$ pedig azért van benne, mert (egytagú összegként) $1 \cdot s_i$ alakban írható, ahol $1 \in \mathbb{Z}$. Ezért ez a legszűkebb, X-et tartalmazó balideál. (Ha $n = 0$, vagyis X üres, akkor üres összegként csak R nullelemét kapjuk.)

Ha $X \subseteq R$ egy végtelen részhalmaz, akkor az összes olyan $m_1s_1 + \ldots + m_ns_n + r_1s_1 + \ldots + r_ns_n$ alakú (véges) összegek halmazát kell venni, ahol $s_i \in X$, $r_i \in R$, $m_i \in \mathbb{Z}$ és n pozitív egész.

5.1.16. Az ilyen alakú összegek nyilván X-et tartalmazó ideált alkotnak, mert $x = 1 \cdot x \cdot 1$, ahol 1 az R egységeleme, és nyilván ez a legszűkebb X-et tartalmazó ideál. Ha R nem egységelemes, akkor az olyan véges összegeket kell venni, melyek tagjai rxs, rx, xs és nx alakúak, ahol $x \in X$, $r, s \in R$ és $n \in \mathbb{Z}$.

5.1.20. A 2.4.29. Feladat megoldásában megadtunk egy olyan S gyűrűt, és egy olyan R nem nulla részgyűrűjét, melynek egységeleme nem ugyanaz, mint az S egységeleme. Ekkor R identikus beágyazása S-be a kívánt φ homomorfizmust adja. Másik példa, amikor S a 2×2-es valós mátrixok gyűrűje, R pedig az

$$\begin{bmatrix} r & 0 \\ 0 & 0 \end{bmatrix}$$

alakú mátrixok részgyűrűje, ahol $r \in \mathbb{R}$.

Ha $\varphi : R \to S$ gyűrűhomomorfizmus, és 1 jelöli az R egységelemét, akkor $r \cdot 1 = r = 1 \cdot r$, és így $\varphi(r) \cdot \varphi(1) = \varphi(r) = \varphi(1) \cdot \varphi(r)$, vagyis $\varphi(1)$ egységeleme $\mathrm{Im}(\varphi)$-nek. Így ha φ szürjektív, akkor az egységelem képe egységelem lesz.

Végül tegyük föl, hogy S nullosztómentes. A 2.4.29. Feladat megoldásában beláttuk, hogy S minden nem nulla részgyűrűjének egységeleme egyúttal az egész S-nek is egységeleme. Mivel $\varphi(1)$ egységeleme $\mathrm{Im}(\varphi) \leq S$-nek, ezért ha $\varphi \neq 0$, akkor $\varphi(1)$ egységeleme S-nek is. (Ezt a gondolatmenetet érdemes összevetni az 5.3.4. Lemma állításával.)

5.1.21. A 2.2.44. Feladat szerint minden csoporthomomorfizmus tartja az egységelemet és az inverzet is. Alkalmazzuk ezt a test additív és multiplikatív csoportjára.

5.1.22. Pontosan akkor, ha az egyik tényező a nullgyűrű, a másik pedig nullosztómentes. Ha ugyanis $0 \neq r \in R$ és $0 \neq s \in S$, akkor $(r, 0)(0, s) = (0, 0)$, de egyik tényező sem nulla. Ezért ha $R \times S$ nullosztómentes, akkor valamelyik tényező a nullgyűrű, és a direkt szorzat a másik tényezővel izomorf.

5.1.23. Legyen $k \in \mathbb{Z}_{nm}$ esetén $\varphi(k) = k(1, 1) \in \mathbb{Z}_n \times \mathbb{Z}_m$. Ez a megfeleltetés nyilván összeg- és szorzattartó a többszörös tulajdonságai miatt (2.2.20. Gyakorlat), hiszen $(1, 1)^2 = (1, 1)$ a $\mathbb{Z}_n \times \mathbb{Z}_m$ gyűrű egységeleme. A φ jóldefiniált és kölcsönösen egyértelmű, mert az $(1, 1)$ elem rendje az összeadásra nm (valójában ez az egyik izomorfizmus, ami a 4.9.8. Következményben szerepel).

5.1.24. Ezekben az R gyűrűkben minden elem az egységelem egész számszorosa. Ha G részcsoport és $g \in G$, továbbá $r \in R$, akkor $r = n \cdot 1$ alkalmas n egészre, de akkor $rg = n \cdot 1 \cdot g = ng \in G$. Ezért G ideál (és így részgyűrű).

5.1.25. A $\mathbb{Q}[x]$ esetében megfelelő lesz a $\mathbb{Z}[x]$ részgyűrű. A $\mathbb{Z}[x]$ esetében tekintsük azoknak a polinomoknak az S halmazát, melyeknek a konstans tagja tetszőleges, a többi együtthatója viszont páros szám. Ez nem ideál, mert az 1 köztük van, de az $x \cdot 1$ nincs. Ugyanakkor részgyűrűt kapunk. Ez közvetlen számolással is világos. Egyszerűbb azonban azt mondani, hogy ha tekintjük azt a $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$ homomorfizmust,

amely minden polinom együtthatóit redukálja mod 2 (2.3.8. Gyakorlat), akkor S pontosan a $\{0,1\} \leq \mathbb{Z}_2[x]$ részgyűrű teljes inverz képe lesz.

5.1.26. Tekintsük a 2.4.30. Gyakorlatban megadott

$$\varphi : f(x) = a_0 + a_1 x + \ldots + a_n x^n \mapsto f\big(p(x)\big) = a_0 + a_1 p(x) + \ldots + a_n p(x)^n$$

gyűrűhomomorfizmust. Ennek magja csak a nullából áll, hiszen ha $f \neq 0$, akkor $f\big(p(x)\big)$ foka f és p fokainak a szorzata (2.3.6. Gyakorlat). Ezért φ injektív, és így izomorfizmus $\mathbb{Z}[x]$ és $\mathrm{Im}(\varphi)$ között. De $\mathrm{Im}\,\varphi$ az 1 és p által generált részgyűrű az 5.1.2. Állítás miatt.

5.1.27. Mintaként megmutatjuk az egyik disztributív szabály ellenőrzését. Legyenek (r,n), (s,m) és (t,k) elemei az $R^1 = R^+ \times \mathbb{Z}^+$-nak. Ekkor

$$[(r,n)+(s,m)](t,k) = (r+s, n+m)(t,k) = \\ = \big((r+s)t + k(r+s) + (n+m)t, (n+m)k\big)\,,$$

és

$$(r,n)(t,k) + (s,m)(t,k) = (rt + kr + nt, nk) + (st + ks + mt, mk)\,.$$

Látható, hogy a kapott eredmény ugyanaz. Hasonlóan ellenőrizhetjük a többi gyűrűaxiómát is. A $(0,1)$ egységelem lesz, mert

$$(r,n)(0,1) = (r\cdot 0 + 1\cdot r + n\cdot 0, n\cdot 1) = (r,n)\,,$$

és hasonlóan $(0,1)(r,n) = (r,n)$. Végül az $(r,0)$ alakú elemek, ahol $r \in R$, az R-rel izomorf részgyűrűt alkotnak, mert az $r \mapsto (r,0)$ megfeleltetés könnyen láthatóan kölcsönösen egyértelmű és művelettartó.

♫ Megjegyezzük, hogy ha R már eredetileg is egységelemes volt, akkor a most konstruált gyűrű egységeleme nem egyezik meg az eredeti gyűrű egységelemével. Ilyenkor az új gyűrű biztosan nem is nullosztómentes: $(1,-1)(1,0) = (0,0)$.

5.1.28. Az $(1+1)(r+s)$ a disztributivitás miatt egyrészt

$$(1+1)r + (1+1)s = r + r + s + s\,,$$

másrészt

$$1(r+s) + 1(r+s) = r + s + r + s\,.$$

Balról $-r$-et, jobbról $-s$-et hozzáadva $r+s = s+r$ adódik.

5.1.29. Ha e balegység, akkor $e + r - re$ is az minden r esetén, mert $es = s$ miatt

$$(e + r - re)s = es + rs - res = s + rs - rs = s\,.$$

Ha csak egy balegység van, akkor $e + r - re = e$, vagyis $r = re$ minden r-re, tehát e jobb oldali egységelem is.

5.1.30. Ha s balinverze r-nek, akkor $s + 1 - rs$ is az, mert $sr = 1$ miatt

$$(s + 1 - rs)r = sr + r - rsr = 1 + r - r = 1\,.$$

Ha r-nek csak egy balinverze van, akkor $s + 1 - rs = s$, vagyis $1 = rs$.

5.1.31. Ha $1 \in R$ és $1 \in S$ is egységelem, akkor $(1,1)$ nyilván egységeleme $R \times S$-nek. Megfordítva, ha $R \times S$ egységelemes, akkor R és S is, mert ezek $R \times S$ homomorf képei a (szürjektív) projekcióknál.

Legyen K ideálja $R \times S$-nek és I azon $r \in R$ elemek halmaza, melyekre $(r,0) \in K$. Ez nyilván ideál R-ben (hiszen $t \in R$ esetén $(t,0)(r,0) \in K$, és így $tr \in I$, és hasonlóan $rt \in I$). Ugyanígy azon $s \in S$ elemek J halmaza, melyekre $(0,s) \in K$ az S-nek ideálja. Belátjuk, hogy $K = I \times J$.

Nyilván $r \in I$ és $s \in J$ esetén $(r,s) = (r,0) + (0,s) \in K$, és így $I \times J \subseteq K$. Megfordítva, ha $(r,s) \in K$, akkor mivel K ideál, $(r,0) = (r,s)(1,0) \in K$, tehát $r \in I$. Hasonlóan $s \in J$, és ezért $(r,s) \in I \times J$.

5.1.32. Legyen $1-ab$ inverze r. Ekkor $r-rab=1$, és így

$$(1+bra)(1-ba)=1-ba+bra-braba=$$
$$=1-ba+b(r-rab)a=1-ba+ba=1,$$

és hasonlóan $(1-ba)(1+bra)=1$. Ezért $1+bra$ kétoldali inverze $1-ba$-nak.

5.2. Faktorgyűrű

5.2.3. Csak a szorzási tulajdonságot igazoljuk (az összeadás egyszerűbb). Tudjuk, hogy $a-b\in I$ és $c-d\in I$. Ezért

$$ac-bd=a(c-d)+(a-b)d\in I\,.$$

Láthatjuk, hogy az 5.1.5. Tétel bizonyításának második felét másoltuk le. Ezért e számolás helyett a következőt is mondhattuk volna. Az a és a b ugyanannak a maradékosztálynak a reprezentánselemei, és hasonlóan c és d is. Mivel a faktorgyűrűben a szorzás jóldefiniált, ac és bd is ugyanabba az osztályba tartoznak, tehát kongruensek modulo I.

5.2.4. Az R/I faktorgyűrű nulleleme $0+I=I$, egységeleme $1+I$ lesz, ahol 1 az R egységeleme. Valóban, $(1+I)(r+I)=1\cdot r+I=r+I$, tehát $1+I$ bal oldali egységelem, és hasonlóan jobb oldali egységelem is. Végül ha R kommutatív, akkor a faktorgyűrű is az, mert

$$(r+I)(s+I)=rs+I=sr+I=(s+I)(r+I)\,.$$

E számolások helyett hivatkozhattunk volna arra is, hogy R/I az R képe a szürjektív természetes homomorfizmusnál (vö. 5.1.20. Gyakorlat).

5.2.7. A képek rendre $i+1,\ i^2=-1,\ i^3+3i+7=7+2i,\ bi+a$.

5.2.8. Legyen $\varphi:\mathbb{Q}[x]\to\mathbb{R}$ a „$\sqrt[3]{2}$ behelyettesítése" nevű homomorfizmus, vagyis az, amely az f polinomhoz az $f(\sqrt[3]{2})$ valós számot rendeli. Meg kell határozni φ képét és magját, majd alkalmazni a homomorfizmustételt. A kép meghatározásához osszuk el az f polinomot maradékosan x^3-2-vel. Ekkor a maradék legfeljebb másodfokú (vagy nulla) lesz, ezért

$$f(x)=(x^3-2)g(x)+(cx^2+bx+a)\,,$$

ahol $a,b,c\in\mathbb{Q}$. Ide $\sqrt[3]{2}$-t helyettesítve $\varphi(f)=a+b\sqrt[3]{2}+c\sqrt[3]{4}$ adódik. Ezért a kép tényleg a gyakorlat állításában leírt halmaz.

A φ magja azokból a racionális együtthatós polinomokból áll, melyeknek gyöke a $\sqrt[3]{2}$. Megmutatjuk, hogy ezek pontosan az x^3-2 többszörösei. Az x^3-2 többszörösei nyilván megfelelők. A megfordításhoz a 3.5.18. Feladat megoldásában látott ötletet alkalmazzuk. Tegyük föl, hogy az $f\in\mathbb{Q}[x]$-nek gyöke a $\sqrt[3]{2}$. Ekkor f-nek és $g(x)=x^3-2$-nek $\sqrt[3]{2}$ közös valós gyöke, továbbá x^3-2 a Schönemann–Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött. Ezért a 3.2.21. Gyakorlat miatt x^3-2 osztója $f(x)$-nek $\mathbb{Q}[x]$-ben.

5.2.10. Legyen $I=(x^2+x+1)$, $O=0+I$, $E=1+I$, $A=x+I$, $B=(x+1)+I$. Ezek a faktor összes elemei, mert az x^2+x+1-gyel való osztási maradék legfeljebb elsőfokú, vagy nulla. A műveleti táblák a következők.

$+$	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

$*$	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Mintaként számítsuk ki az AB szorzatot. Az x és $x+1$ reprezentánsok szorzata x^2+x, amit x^2+x+1-gyel maradékosan osztva 1-et kapunk (hiszen $\mathbb{Z}_2$ test fölött dolgozunk, és itt $x^2+x=1+x^2+x+1$). Így AB az $1+I=E$ osztály.

A táblázatból azonnal leolvasható, hogy a 0 nullelem, az E egységelem, A és B egymás inverzei, továbbá E az önmaga inverze. Ezért minden nem nulla elem invertálható, vagyis tényleg testet kaptunk. Az additív csoport a Klein-csoport, hiszen minden elem kétszerese nulla. A multiplikatív csoport persze a háromelemű ciklikus csoport, már csak a rendje miatt is. Az $\{O, E\}$ nyilván a $\mathbb{Z}_2$-vel izomorf résztest.

Végül megmutatjuk, hogy az $Ex^2 + Ex + E$ polinom gyökei A és B. Például az A-t behelyettesítve, és a táblázatok alapján számolva $EA^2 = EB = B$ és $B + A + E = E + E = 0$ adódik. Valójában beszorzással könnyen ellenőrizhető, hogy $Ex^2 + Ex + E = (Ex - A)(Ex - B)$.

5.2.14. Legyen $I = \{0, 4\} \lhd \mathbb{Z}_8$, ekkor 0, 1, 2, 3 reprezentánsrendszert alkot. Jelölje $\bar{i}$ az $i + I$ maradékosztályt ($0 \le i < 4$). Ekkor $\mathbb{Z}_8 / \{0, 4\}$ műveleti táblái a következők.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$*$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Látható, hogy a $\mathbb{Z}_4$-gyel izomorf gyűrűt kaptunk, hiszen az $i \leftrightarrow \bar{i}$ megfeleltetés művelettartó bijekció. Ha $J = \{0, 4, 12, 16\} \lhd \mathbb{Z}_{16}$, akkor 0, 1, 2, 3 szintén reprezentánsrendszert alkot, jelölje $\overline{j}$ a $j + J$ maradékosztályt ($0 \le j < 4$). Ekkor pontosan a fenti táblázatokat kapjuk, tehát $\mathbb{Z}_{16} / \{0, 4, 8, 12\}$ is izomorf $\mathbb{Z}_4$-gyel. Ugyanígy az (1), (6) és (8) esetekben is $\mathbb{Z}_4$-gyel izomorf gyűrűt kapunk. Külön kielemezzük a (8)-ban szereplő $\mathbb{Z}[x]/(4, x)$ faktorgyűrűt.

A $(4, x)$ ideálban a $4p(x) + xq(x)$ alakú polinomok vannak, ahol $p, q \in \mathbb{Z}[x]$. Ha x helyére nullát helyettesítünk, akkor $4p(0)$ adódik, tehát e polinom konstans tagja néggyel osztható. Megfordítva, ha egy $f \in \mathbb{Z}[x]$ polinom konstans tagja néggyel osztható, például $f(x) = 4a_0 + a_1x + \ldots + a_nx^n$, akkor benne van a $(4, x)$ ideálban, hiszen $4a_0 + xg(x)$ alakban írható. Ezért a 0, 1, 2, 3 jó reprezentánsrendszer lesz, és a fenti táblázatokat kapjuk.

♫ A második izomorfizmustétel szerint $\mathbb{Z}[x]/(4, x)$ izomorf a $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ gyűrű $(4, x)/(x)$ ideálja szerinti faktorával. A $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ izomorfizmust úgy kapjuk, hogy a homomorfizmustételt alkalmazzuk az $f \mapsto f(0)$ homomorfizmusra. Ezért ennél a izomorfizmusnál $(4, x)/(x)$ képe (4) lesz. Ez magyarázza, hogy miért kapjuk most is a $\mathbb{Z}_4$ faktorgyűrűt („a számlálóból és a nevezőből is elvesszük az x-et”).

Ha most $I = (8) \lhd 2\mathbb{Z}_{16}$, akkor 0, 2, 4, 6 alkotnak jó reprezentánsrendszert. Az $\bar{i} = i + I$ jelöléssel a következő táblázatokat kapjuk.

$+$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

$*$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{6}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$

Az (5) pontban szereplő $2\mathbb{Z}_{16}/(8)$ gyűrű tehát már nem izomorf $\mathbb{Z}_4$-gyel, mert például nem egységelemes. Ugyanakkor izomorf lesz a (4) pontban található $2\mathbb{Z}/(8)$ gyűrűvel.

Végül a $4\mathbb{Z}/(16)$ gyűrűben a reprezentánsrendszer 0, 4, 8, 12, a táblázatok

$+$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\overline{12}$
$\bar{0}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\overline{12}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\overline{12}$	$\bar{0}$
$\bar{8}$	$\bar{8}$	$\overline{12}$	$\bar{0}$	$\bar{4}$
$\overline{12}$	$\overline{12}$	$\bar{0}$	$\bar{4}$	$\bar{8}$

$*$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\overline{12}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{4}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{8}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\overline{12}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$

Ez a gyűrű egyik előzővel sem izomorf, mert zérógyűrű: minden szorzat nulla.

5.2.15. A reprezentánselemek $a+bx$ alakúak, ahol $a, b \in \mathbb{Q}$. Az kell, hogy $(a+bx)+I$ és $x+I$ szorzata $1+I$ legyen, ahol $I=(x^2+x+1)$. A szorzást elvégezve

$$x(a+bx) = bx^2+ax = b(x^2+x+1)+(a-b)x-b$$

miatt $(a-b)x-b+I$ adódik, ennek kell $1+I$-vel egyenlőnek lennie. Ez akkor igaz, ha $a-b=0$ és $b=-1$. Tehát a keresett inverz a $(-x-1)+I$ maradékosztály.

5.2.16. Tekintsük azt a sokszor használt φ homomorfizmust, amely egy polinomot együtthatónként „mod m" vesz (2.3.8. Gyakorlat). Ennek képe $\mathbb{Z}_m[x]$, magja pedig (m), és így a homomorfizmustétel a kívánt izomorfizmust adja.

5.2.17. Az Útmutatóban leírtakat folytatjuk. Ha $a \neq 0$, akkor $(a+bu+cv)u/a = u$, és ezért u benne van az $a+bu+cv$ által generált ideálban. Ugyanígy benne van v is, így $a=(a+bu+cv)-bu-cv$ is, és ezért ez az egész R. Vagyis minden valódi ideál része a $bu+cv$ alakú elemek M halmazának. Könnyű meggondolni, hogy M minden olyan részcsoportja ideál, ami zárt az $\mathbb{R}$ elemeivel való szorzásra. Ezek száma végtelen (egy kétdimenziós, $\mathbb{R}$ fölötti vektortér altereiről, másképp fogalmazva a sík egyeneseiről van szó).

5.2.18. Az (1)-ben a válasz igenlő, a homomorfizmustételt arra a $\varphi : \mathbb{R}[x] \to \mathbb{C}$ homomorfizmusra kell alkalmazni, melynél $\varphi(f) = f(\sqrt{2}i)$. Ennek képe az egész $\mathbb{C}$, mert $a+b\sqrt{2}i$ alakban minden komplex szám előáll (ahol $a, b \in \mathbb{R}$). Magja (x^2+2), mert ha egy valós együtthatós polinomnak gyöke a $\sqrt{2}i$, akkor a konjugáltja is, és ezért osztható $(x-\sqrt{2}i)(x+\sqrt{2}i) = x^2+2$-vel.

A (2)-beli izomorfizmus hamis, mert a bal oldal nem nullosztómentes. Valóban, legyen $I=(x^2-1)$, ekkor $(x-1)+I$ és $(x+1)+I$ egyike sem nulla, de a szorzatuk igen.

A (3)-beli izomorfizmus igaz. Legyen $\varphi : \mathbb{R}[x] \to \mathbb{R}\times\mathbb{R}$ az a leképezés, amely az $f \in \mathbb{R}[x]$ polinomhoz az $\big(f(1), f(-1)\big) \in \mathbb{R}\times\mathbb{R}$ párt rendeli. Ez könnyen láthatóan homomorfizmus, melynek magja $\big((x-1)(x+1)\big) = (x^2-1)$. Az $ax+b$ polinom képe $(a+b, a-b)$, és ilyen alakban $\mathbb{R}\times\mathbb{R}$ minden eleme előáll (a (c,d) párt $a=(c+d)/2$, $b=(c-d)/2$ szolgáltatja).

A (4)-beli izomorfizmus is igaz. Legyen $\varphi(a+bi) = (\overline{a+2b}, \overline{a-2b})$, ahol a fölülvonás modulo 5 maradékképzést jelent. Most azt is ellenőrizni kell, hogy φ művelettartó.

$$\varphi\big((a+bi)(c+di)\big) = \big(\overline{(ac-bd)+2(ad+bc)}, \overline{(ac-bd)-2(ad+bc)}\big)\,.$$

Ugyanakkor

$$\varphi(a+bi)\varphi(c+di) = \big(\overline{(ac+4bd)+2(ad+bc)}, \overline{(ac+4bd)-2(ad+bc)}\big)\,.$$

A kapott két eredmény egyenlő, mert a különbség mindkét komponensben $5bd$, ami eltűnik a modulo 5 maradékképzés során.

♫ Valójában arról van szó, hogy az i helyére ± 2-t helyettesítettünk, és ez azért van rendben, mert az $i^2+1=0$ összefüggés a $(\pm 2)^2+1 \equiv 0$ (5) összefüggésbe megy át, ami teljesül.

Ha $a+bi \in \mathrm{Ker}(\varphi)$, akkor $a+2b$ és $a-2b$ is osztható öttel. Így a kettő összege is, azaz $5 \mid 2a$, és mivel $(2,5)=1$, innen $5 \mid a$. Hasonlóan adódik, hogy $5 \mid b$. Ezért φ magjában tényleg az öttel osztható Gauss-egészek vannak. Végül belátjuk, hogy φ szürjektív. Tekintsük azokat az $a+bi$ alakú számokat, ahol $0 \leq a, b < 5$. Semelyik kettő különbsége nem osztható öttel, és így a képeik páronként különböznek. Ezért φ képe legalább 25 elemű, és így csak az egész $\mathbb{Z}_5\times\mathbb{Z}_5$ lehet.

Az (5) esetében is igaz az izomorfizmus, ez a gyűrű valójában a kilenc elemű test. Most is meg kell gondolni, hogy az Útmutatóban megadott φ művelettartó, a fentihez hasonló számolás most azért működik, mert i gyöke az x^2+1 polinomnak. A részletek kidolgozását az Olvasóra hagyjuk.

A (6) esetében a φ a nulla behelyettesítése $\mathbb{C}[x,y]$ elemeiben x helyére. Ez nyilván művelettartó, képe $\mathbb{C}[y]$, magja pedig azokból a polinomokból áll, amelyek mindegyik tagjában szerepel az x.

5.2.19. Az Útmutatóbeli $3\,\mathbb{Z}\,/(6)$ faktorgyűrűben $3+I$ egységelem lesz: $(3+I)(3n+I) = 9n+I = 3n+I$, hiszen $9n-3n=6n$ benne van az I ideálban. Valójában ez a faktorgyűrű a kételemű test. A $\mathbb{Z}$ nullosztómentes, de $\mathbb{Z}\,/6\,\mathbb{Z} \cong \mathbb{Z}_6$ nem az. Végül $\mathbb{Z}_4$ nem nullosztómentes, de $\mathbb{Z}_4\,/\{0,2\} \cong \mathbb{Z}_2$ az.

5.3. Egyszerű gyűrűk

5.3.3. 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. Hasonlóképpen az $ME^{i,j}$ mátrixban a j-edik oszlop megegyezik az M mátrix i-edik oszlopával, a többi oszlop pedig nulla. Így ha $M = ((m_{i,j}))$ tetszőleges mátrix, akkor $E^{i,j}ME^{k,\ell}$ az a mátrix, amelyben az i-edik sor ℓ-edik eleme $m_{j,k}$, a mátrix többi eleme pedig nulla.

Tegyük föl, hogy I ideál $T^{n\times n}$-ben, amely nem csak a nullmátrixból áll, vagyis van olyan $M \in I$, hogy $m = m_{j,k} \neq 0$. Ekkor az előző bekezdésben leírtak miatt I-ben benne van az a mátrix, amelyben az i-edik sor ℓ-edik eleme m, a többi elem nulla. Ezt még az egységmátrix b/m-szeresével megszorozva az m elem b-re változik. Ilyen mátrixok összegeként azonban minden mátrix előáll, tehát $I = T^{n\times n}$.

5.3.14. Az olyan $x \in \mathbb{Z}_{24}$ elemeket keressük, melyekre $18 *_{24} x = 0$, vagyis $24 \mid 18x$. Itt $(24, 18) = 6$-tal egyszerűsítve $4 \mid 3x$, és $(4, 3) = 1$ miatt $4 \mid x$. A keresett annullátor tehát a 4 többszöröseiből álló, hatelemű ideál. Hasonló számolás mutatja, hogy $\mathbb{Z}_m$-ben n annullátora az $m/(n, m)$ többszöröseiből álló, (n, m) elemű ideál.

5.3.15. Ha $ra = 0$, ahol $a \neq 0$, akkor $sra = 0$, és itt $sr \neq 0 \neq a$. A második állítás nem igaz. Például $\mathbb{Z}_6$-ban 2 és 3 is bal oldali nullosztó, de az összegük nem az.

5.3.16. A 2.2.32. Feladat szerint a $\mathbb{Z}_m$ gyűrűben egy elem pontosan akkor nullosztó vagy nulla, ha nem invertálható, azaz ha nem relatív prím m-hez. Megmutatjuk, hogy ezek akkor és csak akkor alkotnak ideált, ha m prímhatvány.

Valóban, ha $m = p^k$, ahol p prím, akkor $r \in \mathbb{Z}_m$ akkor és csak akkor nem relatív prím m-hez, ha $p \mid r$. De a p-vel osztható elemek nyilván ideált alkotnak. Ha viszont p és q különböző prímosztói m-nek, akkor $(p, q) = 1$ miatt van olyan $x, y \in \mathbb{Z}$, hogy $px + qy = 1$. Ekkor px és qy nem relatív prímek m-hez, és így mod m vett maradékuk $\mathbb{Z}_m$-ben nullosztó vagy nulla. Összegük viszont 1, ami nem nullosztó $\mathbb{Z}_m$-ben. Ezért ebben az esetben nem kapunk ideált.

5.3.17. A szorzást elvégezve kapjuk, hogy a bal annullátor azokból a mátrixokból áll, ahol mindkét sor összege nulla, a jobb annullátor pedig azokból, ahol mindkét oszlop összege nulla. (Az előbbi tehát balideál, az utóbbi pedig jobbideál a teljes mátrixgyűrűben.)

5.3.18. Az Útmutatóban megadott jelöléseket használjuk. Az nyilvánvaló, hogy $I \subseteq J^{n\times n}$. Tegyük föl, hogy $m \in J$. Ekkor van olyan $M \in I$, hogy $m = m_{j,k}$ alkalmas j-re és k-ra. Az 5.3.3. Feladat megoldása alapján látjuk, hogy I-ben benne van az a mátrix, amelyben az i-edik sor ℓ-edik eleme m, a többi elem nulla. (Felhasználtuk, hogy R egységelemes, ezért $E^{i,j} \in R^{n\times n}$.) Ilyenek összegeként minden $J^{n\times n}$-beli mátrix előáll, tehát $J^{n\times n} \subseteq I$.

Be kell még látni, hogy J ideál R-ben. A fentiek szerint J minden eleme megjelenik egy I-beli mátrix első sorának első elemeként. De akkor J két tetszőleges elemének összege (és különbsége) megjelenik a megfelelő két mátrix összegében (illetve különbségében), és mivel I zárt az összeadásra és a kivonásra, ezért J is. A nullmátrix eleme I-nek, ezért $0 \in J$. Végül ha $m \in J$ a fenti elem, akkor szorozzuk meg az M mátrixot az egységmátrix r-szeresével balról, illetve jobbról. A kapott rM illetve Mr mátrix I-ben van, és eleme lesz rm, illetve mr. Ezért J kétoldali ideál.

5.3.19. Tekintsük azt a $\varphi : R \to T^n$ leképezést, amely egy M felső háromszögmátrixhoz a főátlójában álló elemek sorozatát rendeli. Ez könnyen láthatóan szürjektív gyűrűhomomorfizmus (vö. 4.11.25. Gyakorlat), melynek magja pontosan a szigorú felső háromszögmátrixokból áll. Ezért ezek ideált alkotnak. A homomorfizmustétel miatt a szerinte vett faktor T^n-nel izomorf.

5.4. Láncfeltételek

5.4.2. Tegyük föl, hogy az állítás nem igaz. Ekkor alkalmas $g_1, \ldots, g_n \in \mathbb{Q}[x_1, x_2, \ldots]$ polinomokra $x_{n+1} = x_1g_1 + \ldots + x_ng_n$ teljesül a generált ideál képlete (5.1.9. Állítás) szerint. Ebbe az egyenletbe $x_1, \ldots, x_n$ helyébe nullát, x_{n+1} helyébe 1-et helyettesítve ellentmondást kapunk.

5.4.5. Igen, ugyanis minden balideál altér is, ha ezt a mátrixgyűrűt $\mathbb{R}$ fölötti vektortérnek tekintjük. Valóban, ha J balideál, $M \in J$ és $r \in \mathbb{R}$, akkor $(rE)M = rM \in J$ (itt E az egységmátrix), és így J zárt a skalárokkal való szorzásra. Nagyobb balideálhoz nagyobb dimenziójú altér tartozik. Mivel a teljes mátrixgyűrű n^2 dimenziós, minden balideálokból álló, szigorúan növő, vagy szigorúan fogyó lánc maximum $n^2 + 1$ tagból állhat.

5.4.6. A $(2, x)$ ideál elemei azok a polinomok, melyek konstans tagja páros. Valóban, ebben az ideálban (az 5.1.9. Állítás miatt) a $2p(x) + xq(x)$ alakú polinomok vannak, ahol $p, q \in \mathbb{Z}[x]$. Ezek konstans tagja páros (helyettesítsünk x helyére nullát, mint a 3.2.4. Gyakorlat megoldásában), és megfordítva, ha egy egész együtthatós polinom konstans tagja páros, az már $2n+xq(x)$ alakban is fölírható, ahol $n \in \mathbb{Z}$ és $q \in \mathbb{Z}[x]$. Ez azt jelenti, hogy $(2, x)$ szerint két mellékosztály van: $(2, x)$ és $1 + (2, x)$, ez utóbbi azokból a polinomokból áll, melyek konstans tagja páratlan. Így $\mathbb{Z}[x]/(2, x)$ izomorf a $\mathbb{Z}_2$ gyűrűvel (a 0 és 1 reprezentánsokkal így kell számolni). Ez test, tehát $(2, x)$ maximális ideál.

Az $(x, y) \triangleleft \mathbb{C}[x, y]$ ideál azokból a polinomokból áll, melyek konstans tagja nulla. Valóban, ennek elemei az $xp(x, y) + yq(x, y)$ alakú polinomok. Ebbe $(0, 0)$-t (vagyis $x = y = 0$-t) helyettesítve nulla adódik, tehát a konstans tag nulla. Megfordítva, ha egy polinom konstans tagja nulla, akkor az x-et tartalmazó tagokból x kiemelhető, ami pedig megmarad, az y-t tartalmazza, és ezekből y emelhető ki, tehát a polinom $xp(x, y) + yq(x, y)$ alakú, vagyis az (x, y) ideálban van.

Tekintsük azt a $\varphi : \mathbb{C}[x, y] \to \mathbb{C}$ homomorfizmust, amelyre $\varphi(p) = p(0, 0)$. Most mutattuk meg, hogy magja (x, y). A képe (már a konstans polinomok miatt is) az egész $\mathbb{C}$. Így a homomorfizmustétel miatt $\mathbb{C}[x, y]/(x, y) \cong \mathbb{C}$. Ez is test, és így (x, y) maximális ideál.

5.4.7. A Krull-tétel bizonyítását kell szó szerint követni, csak ideál helyett mindenütt balideált mondani..

5.4.8. Legyen $\mathcal{X}$ az R azon J ideáljainak a halmaza, melyekre $I \cap J = \{0\}$ teljesül. Az $\mathcal{X}$ halmaz nem üres, mert $\{0\}$ benne van. Vegyük $\mathcal{X}$ elemeinek egy nem üres $\mathcal{L}$ láncát, és legyen U az $\mathcal{L}$ elemeinek uniója. Ez ideál (5.4.4. Lemma), és nyilván $I \cap U = \{0\}$, vagyis $U \in \mathcal{X}$. Így a Zorn-lemma feltétele teljesül $\mathcal{X}$-re, vagyis van benne maximális elem.

5.4.9. Megmutatjuk, hogy ha $L \neq 0$ balideál R-ben, akkor $L = R$. Ebből az 5.3.8. Tétel miatt már következik az állítás, hiszen a nullosztómentesség miatt R nem prímrendű zérógyűrű. Tegyük föl, hogy $0 \neq a \in L$. Tekintsük $k = 1, 2, \ldots$ esetén az Ra^k balideálokat. Ezek nyilván fogyó sorozatot alkotnak, és így a minimumfeltétel miatt ez valamikor megszakad, azaz $Ra^k = Ra^{k+1}$ teljesül alkalmas $k > 0$ egészre. Legyen $s \in R$ tetszőleges. Ekkor $sa^k = ra^{k+1}$ alkalmas $r \in R$ elemre, és mivel R nullosztómentes, a nem nulla a^k elemmel egyszerűsíthetünk. Ezért $s = ra$. Ez azt jelenti, hogy $s \in L$, és mivel s tetszőleges volt, beláttuk, hogy $L = R$.

5.4.10. Tegyük föl, hogy a G csoportot $g_1, \ldots, g_n$ generálja. Azt kell megmutatni, hogy a valódi (vagyis G-től különböző) részcsoportok teljesítik a Zorn-lemma feltételét. Valóban, ezek halmaza nem üres, mert az egyelemű részcsoport köztük van. Vegyük G valódi részcsoportjainak egy $\mathcal{L}$ láncát, és legyen U ennek uniója. Ez az 5.4.4. Lemma csoportelméleti megfelelője miatt részcsoport G-ben, belátjuk, hogy valódi részcsoport. Ha $U = G$ teljesülne, akkor mindegyik g_i benne lenne valamilyen $G_i \in \mathcal{L}$ részcsoportban. Mivel $\mathcal{L}$ lánc, a véges sok G_i részcsoport között van „legnagyobb”, amely tehát tartalmazza a többit, és így az összes g_i elemet is. De akkor ez maga G, ami ellentmondás, hiszen $\mathcal{L}$ elemei valódi részcsoportok. Ezért a Zorn-lemma feltétele teljesül, és így van maximális részcsoport. Azt is láthatjuk ugyanezzel a gondolatmenettel, hogy G minden valódi részcsoportja része egy maximális részcsoportnak.

Most belátjuk, hogy a $\mathbb{Q}^+$ csoportnak nincs maximális részcsoportja. Az Útmutatóban leírtakat folytatva a $(q/p) + M \in \mathbb{Q}^+/M$ elem p-szerese nulla, hiszen $\mathbb{Q}^+/M$ rendje p. Ezért $q = p(q/p) \in M$, ami ellentmond annak, hogy $q \notin M$.

♫ Az előző gondolatmenet valójában azon múlik, hogy $\mathbb{Q}^+$ osztható csoport (7.7.13. Definíció), és így minden homomorf képe is osztható csoport, a $\mathbb{Z}_p$ viszont nem az, mert p-vel nem lehet osztani benne.

5.4.11. Az 5.1.13. Gyakorlat szerint a komplexusműveletekre igaz az asszociativitás és a disztributivitás is. Belátjuk, hogy $\overline{J} = J + RJ + JR + RJR$ ideál R-ben. A komplexusszorzás definíciója miatt részcsoport, és

$$R(J + RJ + JR + RJR) = RJ + RRJ + RJR + RRJR = RJ + RJR \subseteq \overline{J}\,.$$

Ezért $\overline{J}$ balideál, és a szimmetria miatt jobbideál is. Emeljük köbre először csak az összeg utolsó tagját. Mivel $I \triangleleft R$, ezért $RJR \subseteq I$, és mivel $J \triangleleft I$, ezért $IJI \subseteq J$. Tehát

$$(RJR)^3 = RJRRJRRJR = (RJRR)J(RRJR) \subseteq IJI \subseteq J\,.$$

Hasonló számolással látható, hogy $\overline{J}^3 \subseteq J$. Ekkor egy négytagú összeget emelünk köbre, és így 4^3 darab 3 tényezős szorzatot kell lekezelnünk. Ezek azonban mind hasonlóak az $(RJR)^3$ szorzathoz, csak néhány R betű hiányzik. Így a gondolatmenet mindegyik esetben ugyanaz lesz.

♫ A lényeg az, hogy három J betű szerepel a szorzatban, az első és az utolsó begyűjti a körülötte lévő R betűket, és közben I-re változik. A bonyolult képletek elkerülése végett érdemes az R helyett az R^1 gyűrűben számolni, ahol R^1 az R-nek az 5.1.27. Gyakorlatban leírt bővítése. Ebben I szintén ideál, de most a J által generált R-beli balideál $J + RJ$ helyett R^1J, a fenti $\overline{J}$ pedig R^1JR^1 lesz, és így a 4^3 tag helyett csak egyet kell kezelni.

Ha I minimális ideál R-ben, és nem egyszerű, akkor van egy $J \triangleleft I$ nemtriviális ideálja. Ekkor $J \subseteq \overline{J} \subseteq I$, és $\overline{J}$ is ideál R-ben, tehát I minimalitása miatt $\overline{J} = I$. Az imént bizonyítottak miatt $I^3 = \overline{J}^3 \subseteq J \neq I$. De I^3 is ideál R-ben, és ezért I minimalitása miatt $I^3 = 0$. Továbbá $I^2 \triangleleft R$, és ezért I^2 vagy I, vagy 0. Előbbi nem lehet, mert akkor $0 = I^3 = I^2I = I \cdot I = I$ teljesülne. Ezért $I^2 = 0$, azaz I zérógyűrű.

Az állítás csoportelméleti analogonja nem igaz. Legyen G véges egyszerű csoport. Ekkor $G \times G$-nek az $(a, b) \mapsto (b, a)$ másodrendű automorfizmusa. Készítsük el azt a $(G \times G) \rtimes \mathbb{Z}_2^+$ szemidirekt szorzatot, ahol $\mathbb{Z}_2$ másodrendű eleme ezen automorfizmus szerint hat. Könnyű meggondolni, hogy ebben $G \times G$ minimális normálosztó lesz (vö. 4.14.16. Gyakorlat), ami azonban nem is kommutatív, és nem is egyszerű csoport.

♫ A feladat első állításának csoportelméleti analogonja az, hogy ha $M \triangleleft N \triangleleft G$, és $\overline{M}$ az M által generált G-beli normálosztó, akkor az $[[\overline{M}, \overline{M}], \overline{M}]$ kölcsönös kommutátor-részcsoport része M-nek. Az előbb konstruált példa mutatja, hogy ez az állítás sem igaz.

5.5. A számelmélet alaptétele

5.5.11. A két generátort kivonva $(x+1, x+2) = (1)$ adódik, tehát az első esetben főideált kapunk. Belátjuk, hogy $(2x + 2, x + 4)$ nem főideál. Ha az lenne, akkor az 5.5.7. Következmény bizonyításához hasonlóan csakis (1) lehetne, hiszen a szereplő két polinom relatív prím (maga $x + 4$ is felbonthatatlan). De ez nem igaz, mert $(2x + 2, x + 4) \subseteq (2, x) \neq (1)$.

5.5.12. Az $R/(p)$ nullosztómentessége azt jelenti, hogy $r, s \in R$ esetén az $\big(r + (p)\big)\big(s + (p)\big) = rs + (p)$ szorzat csak akkor lehet nulla, ha valamelyik tényezője nulla. De $r + (p)$ akkor és csak akkor nulla, ha $r \in (p)$, azaz ha $p \mid r$. Hasonló állítás igaz s-re és rs-re is, tehát a faktorgyűrű nullosztómentessége pontosan p prímtulajdonságára „fordul le”. Az, hogy p nem egység, azzal ekvivalens, hogy $(p) \neq R$, vagyis hogy $R/(p)$ nem egyelemű gyűrű. Ezzel az első állítást beláttuk.

A $\mathbb{Z}[x]$ gyűrűben 2 prím az első Gauss-lemma miatt, de a szerinte vett faktor nem lesz test. Például az $x + (2)$ maradékosztálynak nincs inverze, hiszen ha $f(x) + (2)$ az lenne, akkor $xf(x) - 1 \in (2)$ teljesülne, márpedig az $xf(x) - 1$ polinom nem osztható kettővel, hiszen konstans tagja -1, azaz páratlan.

♫ Valójában $\mathbb{Z}[x]/(2) \cong \mathbb{Z}_2[x]$ teljesül az 5.2.16. Gyakorlat miatt. Ebből is következik az állítás, hiszen $\mathbb{Z}_2[x]$ nem test (az egységek a nem nulla konstans polinomok, vagyis az 1).

5.5.13. A $(b)(c)$ elemei az $(rb)(sc)$ alakú elemek véges összegei, ahol $r, s \in R$, és ezek pontosan bc többszörösei (hivatkozhattunk volna az 5.1.14. Gyakorlatra is). A $(b) + (c)$ elemei $rb + sc$ alakban írhatók, ahol $r, s \in R$, ezek pedig pontosan (b, c) elemei. Végül $r \in (b) \cap (c)$ akkor és csak akkor, ha $b \mid r$ és $c \mid r$. Ha t kitüntetett közös többszöröse b-nek és c-nek, akkor ez azzal ekvivalens, hogy $t \mid r$, vagyis hogy $r \in (t)$. Ezért $(b) \cap (c) = (t)$.

5.5.14. Az (I, J) nyilván $I + J$-vel egyenlő, hiszen ez az $I \cup J$ által generált ideál. Ezért az első szabály a disztributivitás, amit már beláttunk az 5.1.13. Gyakorlatban. Ha $I = (r)$, $J = (s)$ és $K = (t)$, akkor az előző 5.5.13. Gyakorlat szerint az $I(J + K) = IJ + IK$ azonosság az $(r)(s, t) = (rs, rt)$ összefüggésbe megy át. Tudjuk az 5.5.5. Lemmából, hogy (r, s) az r és s kitüntetett közös osztója, (rt, st) pedig az rt és st kitüntetett közös osztója által generált ideál. Ezért a disztributív szabályt főideálokra alkalmazva pontosan a kitüntetett közös osztó kiemelési tulajdonságát kapjuk.

A disztributivitás miatt

$$(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ + JI\,.$$

Az ennek megfelelő számelméleti állítás az, hogy $rs \mid (r, s)[r, s]$ (ahol (r, s) kitüntetett közös osztót, $[r, s]$ kitüntetett közös többszöröst jelöl).

♫ Mivel R főideálgyűrű, így alaptételes, és ezért valójában $(r, s)[r, s]$ az rs asszociáltja (3.1.31. Gyakorlat).

5.5.15. Az $R = \mathbb{Q}[x_1, x_2, \ldots]$ végtelen sok határozatlanú polinomgyűrű alaptételes, hiszen bármely polinom az osztóival együtt benne van a $\mathbb{Q}[x_1, x_2, \ldots, x_n]$ gyűrűk valamelyikében, ami alaptételes a 3.4.12. Következmény miatt. Ezért minden polinom felbomlik irreducibilisek szorzatára, és ha lenne két, lényegesen különböző felbontása, akkor az összes tényező benne lenne ebben a részgyűrűben, ami lehetetlen, hiszen itt egyértelmű a felbontás. Ezért R maximumfeltételes a főideálokra az 5.5.8. Tétel miatt, de nem maximumfeltételes az ideálokra, ezt láttuk be az 5.4.2. Gyakorlatban.

5.5.16. Az Útmutató jelöléseit használjuk, belátjuk, hogy az I_n ideál nem generálható n elemmel. Ehhez elég megmutatni, hogy az $R = \mathbb{Z}[x]/I_{n+1}$ gyűrű $I = I_n/I_{n+1}$ ideálja nem generálható n elemmel. Az I_n generátorait x-szel, vagy 2-vel szorozva I_{n+1}-be jutunk. Ezért az I faktorgyűrű minden elemének kétszerese nulla, azaz vektortérnek tekinthető a $\mathbb{Z}_2$ fölött (vö. 4.9.34. Gyakorlat), és ha $\varphi(f) \in \mathbb{Z}_2$ jelöli az $f \in \mathbb{Z}[x]$ polinom konstans tagjának 2-vel való osztási maradékát, akkor az I tetszőleges elemét $f + I_{n+1}$-gyel szorozva ugyanazt kapjuk, mint ha $\varphi(f)$-fel szoroznánk. Ezért ha $g_1, \ldots, g_k$ generálja az I ideált, akkor I minden eleme $\lambda_1 g_1 + \ldots + \lambda_k g_k$ alakban írható, ahol $\lambda_i \in \mathbb{Z}_2$. Más szóval az I-t mint $\mathbb{Z}_2$ fölötti vektorteret is generálják a $g_1, \ldots, g_k$ elemek. Tudjuk lineáris algebrából, hogy minden generátorrendszer elemszáma legalább akkora, mint egy tetszőleges független rendszer elemszáma. Ezért elég belátni, hogy az I-t generáló $n + 1$ darab $2^j x^{n-j} + I_{n+1}$ elem független ebben a vektortérben.

Tegyük föl, hogy $\lambda_0 2^n + \lambda_1 2^{n-1} x + \ldots + \lambda_n x^n \in I_{n+1}$, ahol $\lambda_j \in \mathbb{Z}_2$. Az I_{n+1} ideál elemei könnyen láthatóan az olyan $a_0 + a_1 x + \ldots + a_m x^m \in \mathbb{Z}[x]$ polinomok, amelyekben az a_j együttható osztható 2^{n+1-j}-vel minden $0 \le j \le n$ esetén (és m tetszőleges). Ezért $2^{n+1-j} \mid \lambda_j 2^{n-j}$, és így mindegyik λ_j páros, azaz $\mathbb{Z}_2$ nulleleme. Így a fenti lineáris kombináció triviális.

5.6. A polinomgyűrű ideáljai

5.6.1. A nullapolinom gyökeinek halmaza maga $\mathbb{C}$. Ha viszont $f \in \mathbb{C}[x]$ nem nulla polinom, akkor gyökeinek halmaza véges, és $\mathbb{C}$ minden véges részhalmaza nyilván előáll ilyen módon. Véges halmazok metszete is véges, tehát a $\mathbb{C}$-beli algebrai halmazok a $\mathbb{C}$-n kívül a $\mathbb{C}$ véges részhalmazai.

Ha $V = \mathbb{C}$, akkor azoknak a polinomoknak a halmaza, amelyek V minden elemén eltűnnek, csak a nullából áll. Ha $V = \{z_1, \ldots, z_n\}$, akkor egy polinom pontosan akkor tűnik el V minden elemén, ha $f(x) = (x - z_1) \ldots (x - z_n)$-nek többszöröse. A V-hez tartozó ideál tehát az f által generált (f) főideál.

5.6.4. Legyen $I \lhd R$. Tegyük föl, hogy $r \in R$ és $s \in \sqrt{I}$, Ekkor van olyan k, hogy $s^k \in I$. Tudjuk, hogy $(rs)^k = r^k s^k$, mert R kommutatív. Továbbá $r^k s^k \in I$, hiszen I ideál. Ezért $rs \in \sqrt{I}$. Vagyis $\sqrt{I}$ zárt az R elemeivel való szorzásra.

Tegyük föl, hogy $s, t \in \sqrt{I}$. Ekkor s és t is behatványozható I-be, mondjuk $s^n, t^m \in I$. A binomiális tétel alkalmazható, mert R kommutatív, és így

$$(s + t)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n + m - 1}{i} s^{n+m-1-i} t^i\,.$$

Ennek az összegnek minden tagja I-beli. Valóban, ha $i \geq n$, akkor $t^i \in I$. Ha viszont $i \leq n-1$, akkor $n+m-1-i \geq m$, és ezért $s^{n+m-1-i} \in I$. Beláttuk tehát, hogy $(s+t)^{n+m-1} \in I$, vagyis $s+t \in \sqrt{I}$. Nyilván $\sqrt{I}$ zárt az ellentettképzésre is, és ezért tényleg ideál. Az nyilvánvaló, hogy $I \subseteq \sqrt{I}$, hiszen I minden elemének már az első hatványa I-ben van.

Az $\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$ összefüggés belátásához azt kell meggondolni, hogy ha egy elem I_1-be és I_2-be is behatványozható, akkor a két kitevő közül a nem kisebbet véve a kapott hatvány már eleme lesz $I_1 \cap I_2$-nek is.

5.6.5. Mivel $360 = 2^3 \cdot 3^2 \cdot 5$, ezért $30 = 2 \cdot 3 \cdot 5$ köbe már többszöröse 360-nak. Ezért $30 \in \sqrt{(360)}$. Megfordítva, ha $360 \mid n^k$, akkor 360 mindegyik prímosztója, és így a 30 is osztója n-nek. Ezért $\sqrt{(360)} = (30)$.

Legyen most R alaptételes (tehát szokásos) gyűrű és $r \in R$. Ha $r = 0$, akkor R nullosztómentessége miatt (r) radikálja is csak a nullából áll. Ha $r \neq 0$, akkor az imént látott gondolatmenethez hasonlóan láthatjuk, hogy ahhoz, hogy $s^k \in (r)$, vagyis $r \mid s^k$ teljesüljön alkalmas k-ra, az szükséges és elégséges, hogy r minden prímosztója szerepeljen s-ben, azaz hogy r prímosztóinak szorzata ossza s-et. Speciálisan ha r egység, akkor (r) és a radikálja is maga R.

5.6.7. Ha $r \in R$, akkor az R/I faktorgyűrű $r+I$ eleme akkor és csak akkor nilpotens, ha van olyan $k > 0$ egész, hogy $(r+I)^k$ e faktorgyűrű nulleleme, vagyis I. Mivel a faktorgyűrűben reprezentánsokkal számolunk, ez azzal ekvivalens, hogy $r^k \in I$. Tehát $r+I$ akkor és csak akkor nilpotens, ha $r \in \sqrt{I}$, más szóval ha $r+I \in \sqrt{I}/I$.

5.6.8. Legyen I ideál R-ben és $J = \sqrt{I}$ az I radikálja. A feltétel szerint a J ideál végesen generált, azaz $J = (s_1, \ldots, s_n)$ alkalmas elemekre. Mindegyik s_i generátor behatványozható I-be, mondjuk $s_i^{k_i} \in I$. Legyen N a k_i kitevők maximuma, megmutatjuk, hogy $J^{nN} \subseteq I$ (valójában már $J^{k_1+\ldots+k_n-n+1} \subseteq I$). A J^{nN} ideál definíció szerint úgy kapható, hogy J-ből veszünk nN elemet, ezeket összeszorozzuk, majd az összes ilyen típusú szorzatokból véges összegeket képezünk. Ezért elegendő megmutatni, hogy ha $b_1, \ldots, b_{nN} \in J$, akkor a szorzatuk I-ben van.

A b_j elem fölírható $r_{1j}s_1 + \ldots + r_{nj}s_n$ alakban, ahol $r_{ij} \in R$. Végezzük el a beszorzást a $b = b_1 \ldots b_{nN}$ szorzatban a 2.1.10. Gyakorlat megoldásában lefektetett elvek szerint. Azt kapjuk, hogy b olyan nN tényezős szorzatok összege, amelyek tényezői az $r_{ij}s_i$ elemek közül kerülnek ki. Minden ilyen szorzatban kell lennie olyan s_i-nek, amelyik legalább N-szer szerepel (hiszen n-féle s_i van és nN tényező). Mivel R kommutatív, a szorzat tényezői átrendezhetők úgy, hogy a N darab s_i egymás mellé kerüljön. Tudjuk, hogy $s_i^N \in I$, és ezért a teljes szorzat is I-ben van. Beláttuk tehát, hogy $b \in I$, amiből az állítás is következik.

5.6.12. Tegyük föl, hogy $I_1 \subsetneq I_2 \subsetneq \ldots$ az R ideáljainak egy végtelen, szigorúan növő lánca. Álljon J_k az $R[x]$ azon polinomjaiból, amelyek mindegyik együtthatója I_k-beli. Könnyű ellenőrizni, hogy J_k ideál $R[x]$-ben, a konstans polinomok miatt pedig $J_k \neq J_{k+1}$. Ezért $J_1 \subsetneq J_2 \subsetneq \ldots$ az $R[x]$ ideáljainak egy végtelen, szigorúan növő lánca lenne.

5.6.14. Ha $J \cap K = \{0\}$, de J és K nem nulla, akkor legyen $0 \neq a \in J$ és $0 \neq b \in K$. Az ab szorzat eleme J-nek is és K-nak is, hiszen ezek ideálok. Ezért $ab \in J \cap K = \{0\}$. Ez ellentmond R nullosztómentességének.

5.6.15. Legyen R főideálgyűrű, ekkor tehát R szokásos gyűrű, és az 5.5.9. Következmény szerint alaptételes. Legyen $0 \neq r \in R$. Ha r felbontható a relatív prím $b, c \in R$ elemek szorzatára, akkor az 5.5.13. Gyakorlat szerint $(b) \cap (c)$ a b és c legkisebb közös többszöröse, vagyis a bc által generált ideál. Ez $(r) = (bc)$-nek akkor lesz nemtriviális metszetre bontása, ha b és c valódi osztója r-nek. Ha tehát r kanonikus alakjában legalább két (nem egység) prímhatvány szerepel, akkor (r) nem lesz metszetirreducibilis.

Ha viszont $r = p^k$ prímhatvány, akkor az R-et tartalmazó ideálokat r osztói generálják az 5.5.4. Lemma miatt. Ezért (p^{k-1}) része minden (r)-et valódi módon tartalmazó ideálnak, és így (r) csak triviálisan bontható metszetre. Végül az 5.6.5. Gyakorlat szerint ha p prím és $k \geq 1$, akkor a (p^k) ideál radikálja (p). Ezért (p^k) akkor egyezik meg a radikáljával, ha egy prím elemmel generálható.

5.6.16. Nyilván $bc \in P = (p)$ akkor és csak akkor, ha $p \mid bc$, továbbá $b \in P$ akkor és csak akkor ha $p \mid b$ és $c \in P$ akkor és csak akkor ha $p \mid c$. Ezért p prímtulajdonsága tényleg pontosan a gyakorlatban szereplő feltételt jelenti.

5.6.18. Az R/P faktorgyűrű $b + P$ és $c + P$ elemeinek szorzata $bc + P$. Ez akkor és csak akkor lesz az R/P nulleleme, azaz P, ha $bc \in P$. Továbbá $b + P$ akkor és csak akkor nulla, ha $b \in P$, és $c + P$ akkor és csak akkor nulla, ha $c \in P$. Ezért az R/P faktorgyűrű nullosztómentessége tényleg azzal ekvivalens, hogy P prímideál.

5.6.19. Az 5.3.12. Következmény miatt ha M maximális ideál, akkor R/M test, és így nullosztómentes (2.2.29. Tétel). Ezért az 5.6.18. Gyakorlat miatt M prímideál.

5.6.20. Tegyük föl, hogy $q = p^k$, ahol p prím. Belátjuk, hogy ez a k kielégíti a gyakorlatban szereplő feltételt. Mivel $bc \in Q = (q)$, ezért $q \mid bc$. De $b \notin Q$, ezért $p^k = q \nmid b$. Vagyis a p prím kitevője b-ben k-nál kisebb, bc-ben viszont legalább k. Ezért p osztója c-nek. De akkor $q = p^k \mid c^k$, vagyis $c^k \in Q$.

Tegyük most föl, hogy q nem prímhatvány asszociáltja, vagyis $q = p^m c$, ahol p prím, $m > 0$, és c egységtől különböző elem, ami már nem osztható p-vel. Legyen $b = p^m$. Ekkor $q \mid bc$ (tehát $bc \in Q$), továbbá $q \nmid b$ (azaz $b \notin Q$), de c nem hatványozható be a Q ideálba, mert c^k soha nem lesz már p-vel sem osztható. Ezért a gyakorlatban szereplő feltétel sem teljesül.

5.6.22. Az R/Q faktorgyűrű $b + Q$ és $c + Q$ elemeinek szorzata $bc + Q$. Ez akkor és csak akkor lesz az R/Q nulleleme, azaz Q, ha $bc \in Q$. Továbbá $b + Q$ akkor és csak akkor nulla, ha $b \in Q$. Végül $c + Q$ akkor és csak akkor nilpotens, ha van olyan $k > 0$ egész, hogy $(c + Q)^k = Q$, vagyis ha $c^k \in Q$. Ezért az R/Q faktorgyűrűre a gyakorlatban kirótt feltétel azzal ekvivalens, hogy Q primér.

5.6.23. A $\mathbb{Z}[x]$ gyűrű $I = (4, 2x)$ ideáljában azok a polinomok vannak, amelyek mindegyik együtthatója páros, és a konstans tag néggyel osztható. Ez nem primér, mert $2x$ benne van, 2 nincs benne, és x egyik hatványa sincs benne. Ugyanakkor I teljesíti a feladatban kiszabott feltételt. Ha ugyanis $f(x)g(x) \in I$, ahol $f, g \in \mathbb{Z}[x]$, akkor $2 \mid fg$. De 2 prím $\mathbb{Z}[x]$-ben a 3.4.3. Első Gauss-lemma miatt, ezért $2 \mid f$ vagy $2 \mid g$. Az első esetben f^2, a másodikban g^2 osztható néggyel, és így I-ben van.

5.6.24. Az (1) állítás bizonyításához tegyük föl, hogy $bc \in \sqrt{I} = P$, de $b \notin P$. Ekkor van olyan k, hogy $b^k c^k = (bc)^k \in I$. Mivel $b \notin P$, ezért $b^k \notin I$. De I primér, és ezért c^k behatványozható I-be. De akkor $c \in \sqrt{I} = P$. Ezért P prímideál.

A (2) állításra ellenpélda $\mathbb{Z}[x]$ gyűrűben az $I = (4, 2x)$ ideál. Valóban, az 5.6.23. Gyakorlat megoldásában már láttuk, hogy I nem primér. Belátjuk, hogy I radikálja (2). Valóban, 2 behatványozható I-be, hiszen $4 \in I$, ezért $2 \in \sqrt{I}$. Másfelől ha $f(x)^k \in I$, akkor $2 \mid f^k$, és mivel 2 prím $\mathbb{Z}[x]$-ben, ezért $2 \mid f$, azaz $f \in (2)$. Tehát tényleg $\sqrt{(4, 2x)} = (2)$. De a (2) prímideál, hiszen 2 prímtulajdonságú $\mathbb{Z}[x]$-ben a 3.4.3. Első Gauss-lemma miatt.

Végül a (3) állítás bizonyításához az Útmutatóban megadott jelöléseket használjuk. Az $m + rc$ alakú elemek, ahol $m \in M$ és $r \in R$ nyilván R-nek egy M-et és c-t tartalmazó ideálját alkotják. (Ez akár közvetlen számolással, akár az R/M faktorgyűrű vizsgálatával adódik.) Ez az ideál bővebb M-nél, mert $c \notin M$, ezért csakis az egész R lehet, és így 1 tényleg előáll $m + rc$ alakban. Mivel $m \in M = \sqrt{I}$, van olyan k, hogy $m^k \in I$. De a binomiális tétel miatt

$$m^k = (1 - rc)^k = 1 + \sum_{i=1}^{k} \binom{k}{i} (-rc)^i \,.$$

Ezért $m^k \in I$ valóban $1 + sc$ alakban írható. De akkor $b + s(bc) = b(1 + sc) \in I$, és mivel $bc \in I$, ezért $b \in I$.

5.6.26. Legyen $I = (2, x)^2 = (4, 2x, x^2)$ (az egyenlőség az 5.1.14. Gyakorlat következménye). Az I ideál radikálja tartalmazza a 2 és x polinomokat, tehát az $M = (2, x)$ ideált is. Ez azonban maximális ideál $\mathbb{Z}[x]$-ben az 5.4.6. Gyakorlat miatt. Mivel 1 nincs a radikálban, a radikál M lesz. Az 5.6.24. Feladat

(3) pontjában láttuk, hogy ha I radikálja maximális ideál, akkor I primér. Ezért $(4, 2x, x^2)$ tényleg primér ideál $\mathbb{Z}[x]$-ben.

A $(4, 2x, x^2)$ ideálban azok a polinomok vannak, amelyek konstans tagja 4-gyel osztható, az x-es tag együtthatója pedig páros. A $(4, x)$ elemei azok, ahol a konstans tag néggyel osztható, a $(2, x^2)$ elemei pedig azok, melyek konstans tagja, és az x-es tag együtthatója is páros. Ezért $(4, x) \cap (2, x^2) = (4, 2x, x^2)$ tényleg igaz. Ez nemtriviális metszetfelbontás, mert $x \in (4, x)$ és $2 \in (2, x^2)$, de $x, 2 \notin (4, 2x, x^2)$.

5.6.27. Ha r felbontható a relatív prím $b, c \in R$ elemek szorzatára, akkor az 5.5.13. Gyakorlat szerint $(b) \cap (c)$ a b és c legkisebb közös többszöröse, vagyis a bc által generált ideál. Így $(r) = (q_1) \cap \ldots \cap (q_n)$ adódik. Itt a tényezőket prímhatvány generálja, ezért az 5.6.20. Gyakorlat miatt primérek.

5.6.29. Az (1) bizonyításához használjuk föl a $\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$ összefüggést (amit az 5.6.4. Gyakorlatban bizonyítottunk). Ebből látjuk, hogy I radikálja is P. Tegyük föl, hogy $bc \in I$ de $b \notin I$. Ekkor van olyan i, hogy $b \notin Q_i$. Persze $bc \in Q_i$, és mivel Q_i primér, c behatványozható Q_i-be, azaz $c \in \sqrt{Q_i} = P$. De I radikálja is P, ezért c behatványozható I-be is, azaz I primér.

A (2) belátásához az Útmutatóban leírtakat folytatjuk. Legyen c_0 olyan elem, ami P_1-ben benne van, de P_2-ben nincs. Ekkor alkalmas k-ra $c = c_0^k \in Q_1$, de $c \notin P_2$, mert P_2 prímideál. Az I-t előállító metszet rövidíthetetlensége miatt $Q_2 \cap \ldots \cap Q_n$ valódi módon tartalmazza az I ideált, tehát létezik olyan $b \in Q_2 \cap \ldots \cap Q_n$, amely nem eleme I-nek. Ekkor tehát $b \notin Q_1$. Persze $bc \in I$, hiszen $bc \in Q_i$ minden $i \geq 2$-re b miatt, és $bc \in Q_1$ a c miatt. Mivel $b \notin I$, ha I primér lenne, akkor c benne lenne I radikáljában. Ez azonban nem igaz, hiszen P_2 tartalmazza I radikálját, és $c \notin P_2$.

5.6.33. Tegyük föl, hogy P prímideál, és a B, C ideálok egyike sem része P-nek. Legyen $b \in B - P$ és $c \in C - P$. Ekkor $bc \in BC$, de mivel P prímideál, $bc \notin P$. Ezért BC sem része P-nek.

Megfordítva, tegyük föl, hogy P-re teljesül a gyakorlatban megfogalmazott feltétel. Ha $bc \in P$ (ahol $b, c \in R$), akkor legyen $B = (b)$ és $C = (c)$. Ekkor $BC = (bc) \subseteq P$. A feltétel szerint B vagy C része P-nek. Az első esetben $b \in P$, a másodikban $c \in P$. Ezért P prímideál.

5.6.34. Legyen $P_1 = (x)$ és $P_2 = (x, y)$ a $\mathbb{C}[x, y]$ gyűrűben. Nyilván $P_1 \subsetneq P_2$. A P_2 maximális ideál (5.4.6. Gyakorlat), ezért prímideál is (5.6.19. Gyakorlat). A $P_1 = (x)$ azért prímideál, mert az x prímtulajdonságú elem generálja (5.6.16. Gyakorlat).

♫ Ehelyett mondhattuk volna azt is, hogy $\mathbb{C}[x, y]/(x) \cong \mathbb{C}[y]$ nullosztómentes (lásd 5.2.18. Feladat, (6) pont), és így (x) prímideál. A gondolatmenet általánosítható, például mutatja, hogy (x, y) prímideál $\mathbb{C}[x, y, z]$-ben is.

Miért igaz, hogy x prím $\mathbb{C}[x, y]$-ban? Ez közvetlenül is ellenőrizhető, például annak felhasználásával, hogy egy polinom akkor és csak akkor osztható x-szel, ha x helyére nullát helyettesítve a nullapolinomot kapjuk. De felhasználhatjuk azt is, hogy $\mathbb{C}[x, y]$ alaptételes, és ezért minden irreducibilis eleme prím.

5.6.35. Az (x^2, y) radikálja (x, y), hiszen az x és y polinomokat tartalmazza, de (x, y) már maximális ideál (5.4.6. Gyakorlat). Ezért (x^2, y) primér (5.6.24. Feladat, (3) pont). Az (x^2, y)-ban az $x^2 f(x, y) + yg(x, y)$ alakú polinomok vannak, ezek könnyen láthatóan azok, amelyekben nem szerepel konstans tag és x-es tag. Speciálisan $x \notin (x^2, y)$ és így (x^2, y) nem egyenlő a radikáljának az első hatványával. A radikál többi hatványa viszont nem tartalmazza az y polinomot, hiszen olyan polinomokból áll, melyek minden tagja legalább másodfokú (az 5.1.14. Gyakorlat miatt).

5.6.36. A főideálok primér-felbontását az 5.6.27. Gyakorlatból, a radikálokat pedig az 5.6.5. Gyakorlatból kaphatjuk. Ebből az (1) és (2) esetben adódik a megoldás.

(1): $(x^2 + y^2)$ primér felbontása $(x + iy) \cap (x - iy)$, a metszet mindkét tényezőjének radikálja saját maga, és $(x^2 + y^2)$ radikálja is saját maga, ami nem prímideál.

(2): (xy^2) primér felbontása $(x) \cap (y^2)$, itt $\sqrt{(x)} = (x)$, $\sqrt{(y^2)} = (y)$ és $\sqrt{(xy^2)} = (xy)$, ez sem prímideál.

(3): Az (x^2, xy) nagyon hasonlít az 5.6.23. Feladatban szereplő $(2^2, 2x)$ ideálhoz, és így a primér felbontást is ugyanúgy kapjuk: $(x^2, y) \cap (x)$, a tényezők radikáljai (x, y), illetve (x). Indoklás: tekintsük $\mathbb{C}[x, y]$ elemeit y polinomjainak. Ekkor (x^2, xy) azokból a polinomokból áll, melyek konstans tagja x^2-tel, a többi

együtthatója x-szel osztható. Az (x^2, y) elemei azok, melyek konstans tagja x^2-tel osztható, az (x) elemei azok, melyekben minden együttható x-szel osztható. Ezért (x^2, y) tényleg e két ideál metszete. Az (x^2, y) primér, mert radikálja (x, y), ami maximális ideál (5.6.24. Feladat, (3) pont). Az (x) is primér, mert prímideál. Az (x^2, xy) radikálja az 5.6.4. Gyakorlat miatt $(x, y) \cap (x) = (x)$, ami prímideál.

(4): Az (x^3, x^2y^2, xy^3) primér felbontása $(x^3, x^2y^2, y^3) \cap (x)$, radikálja (x), ami prímideál, a tényezők radikáljai (x, y), illetve (x). Az indoklás hasonló a (3)-belihez.

5.6.37. Mivel $\mathbb{C}[x_1, \ldots, x_n]$ Noether-gyűrű az 5.6.11. Tétel (Hilbert bázistétele) miatt, az I ideál véges sok $f_1, \ldots, f_n$ polinommal generálható. Ha ezeknek nincs közös gyöke, akkor a közös gyökeik halmaza üres, és ezen a halmazon a konstans 1 polinom is eltűnik. Ezért a Nullahelytétel miatt 1^k benne van az I ideálban, azaz I nem valódi ideál.

5.6.38. Az $I = (xy, z)$ ideál azokból a polinomokból áll, amelyek mindegyik tagjában szerepel vagy z, vagy pedig x is és y is (más szóval nincs bennük x^k-os és y^k-os tag, a konstans tagot is ide sorolva). Az I nem primér, hiszen xy eleme, de nincs benne x, és y egyetlen hatványa sem. Ugyanakkor a fenti megjegyzés miatt $(xy, z) = (x, z) \cap (y, z)$, ahol a tényezők már primérek (sőt maximális ideálok).

Tegyük föl, hogy I előáll primér ideálok szorzataként. A tényezők száma minden ilyen felbontásban legalább kettő, és egyik tényező sem egyenlő I-vel, hiszen I nem primér. Válasszuk a tényezők számát minimálisnak, ami azt jelenti, hogy mindegyik rész-szorzat valódi módon tartalmazza I-t. Összevonásokkal elérhetjük, hogy $(xy, z) = I_1 \cdot I_2$ legyen, ahol I_1 és I_2 is valódi módon tartalmazza I-t (persze I_1 és I_2 már nem feltétlenül primér). Legyen $f \in I_1$, belátjuk, hogy f konstans tagja nulla.

Tegyük föl, hogy ez nem igaz, jelölje c az f konstans tagját. Legyen $g \in I_2$. Ha a g polinomban szerepel dx^k alakú tag, ahol $0 \neq d \in \mathbb{C}$, akkor válasszuk ki ezek közül azt, amelyre k a legkisebb (lehet $k = 0$ is). Ekkor $fg \in I$-nek cdx^k tagja lesz (hiszen x^k-os tag az fg szorzatban csak ezen az egy módon keletkezhet). Ez ellentmond annak, ahogy I elemeit leírtuk a megoldás első bekezdésében. Tehát dx^k alakú tag nem szerepelhet g-ben. Hasonlóképpen látjuk, hogy dy^k alakú tag sem szerepelhet. Ezért $g \in (xy, z) = I$. Ez minden $g \in I_2$-re igaz, tehát $I_2 \subseteq I$. Ez ellentmondás, tehát f konstans tagja tényleg nulla.

Hasonlóan láthatjuk, hogy I_2 minden elemének nulla a konstans tagja. Ez azonban azt jelenti, hogy $I_1 I_2$-ben csupa olyan polinom található, amelyben minden tag legalább másodfokú. Ez ellentmond annak, hogy $z \in (xy, z) = I_1 I_2$.

5.6.39. A $(G_1, \ldots, G_m)$ elemei a $h_1 G_1 + \ldots + h_m G_m$ alakú polinomok, ahol $h_1, \ldots, h_m \in \mathbb{C}[x_1, \ldots, x_n]$ (5.1.9. Állítás). A $h_i G_i$ minden tagja osztható G_i-vel. Ezért az összeadás elvégzésekor keletkező tagok mindegyike osztható valamelyik G_i-vel. Ha az eredmény (az összevonások után) F, akkor tehát F is osztható valamelyik G_i-vel.

5.6.40. Legyen F egy $f \in I$ polinom főtagja, G_i pedig a g_i főtagja. Ekkor $F \in (G_1, \ldots, G_m)$, ezért az előző 5.6.39. Gyakorlat miatt valamelyik G_i osztója F-nek. Azt kell még megmutatni, hogy $g_1, \ldots, g_m$ generálja I-t. Legyen $f \in I$ és végezzük el a „maradékos osztást" $g_1, \ldots, g_m$-mel (5.6.31. Definíció). Ekkor a kapott r maradék I-beli, és ha nem lenne nulla, akkor a már bebizonyított állítás szerint r főtagja osztható lenne valamelyik G_i-vel. Ez lehetetlen, mert akkor az osztási eljárást tovább folytathatnánk. Ezért $r = 0$, és így f benne van a $(g_1, \ldots, g_m)$ ideálban.

5.6.41. Jelölje J az I-beli polinomok főtagjai által generált ideált. Ez végesen generált az 5.6.11. Hilbert-féle bázistétel szerint, legyen $J = (h_1, \ldots, h_k)$. Mindegyik $h_i \in J$ polinomot I-beli polinomok főtagjai generálják, és ebben a generálásban csak véges sok polinom vesz részt (5.1.15. Gyakorlat). Minden egyes h_i-hoz egy ilyen véges rendszert kiválasztva, és ezeket egyesítve azt kapjuk, hogy $J = (G_1, \ldots, G_m)$, ahol mindegyik G_i egy $g_i \in I$ főtagja. Ekkor $g_1, \ldots, g_m$ teljesíti az 5.6.40. Feladat feltételét, és így Gröbner-bázis.

5.6.42. Az Útmutatóban leírtakat folytatva tekintsük az x_j kitevőjét G_1-ben és G_2-ben, jelölje k_j ezeknek a minimumát, H pedig az $x_1^{k_1} \ldots x_n^{k_n}$ polinomot. Így H a G_1 és G_2 (egyik) kitüntetett közös osztója. Mivel

P_1G_1 és P_2G_2 asszociáltak, ezért asszociáltság erejéig

$$P_1H = (P_1G_1,\, P_1G_2) = (P_2G_2,\, P_1G_2) = (P_2,\, P_1)G_2\,,$$

vagyis G_2 osztója P_1H-nak, legyen $Q = P_1H/G_2$. Az S-polinom definíciója szerint

$$s = S(g_1, g_2) = \frac{G_2}{H}g_1 - \frac{G_1}{H}g_2\,.$$

A feltétel szerint az s-et a $g_1, \ldots, g_m$ rendszerrel elosztva a maradék nulla. Ezért $s = q_1g_1 + \ldots + q_mg_m$, ahol mindegyik q_ig_i főtagja lexikografikusan nem nagyobb, mint s főtagja. Az s főtagja viszont lexikografikusan kisebb, mint G_1G_2/H, hiszen a kivonásnál ez a tag kiesik a polinomból. Alakítsuk át f-et a következőképpen:

$$f = f - Q\big(s - (q_1g_1 + \ldots + q_mg_m)\big) = r_1g_1 + \ldots + r_mg_m\,,$$

ahol

$$r_1 = p_1 - \frac{QG_2}{H} + Qq_1\,, \quad r_2 = p_2 + \frac{QG_1}{H} + Qq_2\,, \quad r_i = p_i + Qq_i \quad (i \geq 3)\,.$$

Úgy kapunk ellentmondást, hogy megmutatjuk: az $f = r_1g_1 + \ldots + r_mg_m$ előállításban mindegyik r_ig_i főtagja lexikografikusan nem nagyobb, mint P_1G_1, de a P_1G_1 konstansszorosa kevesebbszer fordul elő, mint az $f = p_1g_1 + \ldots + p_mg_m$ előállítás esetében. (Az is előfordulhat, hogy az új előállításban P_1G_1 konstansszorosa már egyáltalán nem szerepel, ekkor viszont mindegyik főtag kisebb P_1G_1-nél, ami szintén ellentmond $p_1, \ldots, p_m$ választásának.)

Beláttuk, hogy q_ig_i főtagja kisebb, mint G_1G_2/H. Ezért Qq_ig_i főtagja kisebb, mint $QG_1G_2/H = P_1G_1$. Vagyis az r_i polinomok utolsó, Qq_i tagjai csak P_1G_1-nél kisebb tagokat hozhatnak be, ezekkel nem kell törődnünk. Az r_i polinom első tagja, azaz p_i, szintén nem hozhat be P_1G_1-nél nagyobb tagot, hiszen p_ig_i főtagja $P_iG_i \preceq P_1G_1$. Ebből következik, hogy $i \geq 3$ esetén r_ig_i főtagja csak akkor lehet P_1G_1 konstansszorosa, ha P_iG_i a P_1G_1 konstansszorosa volt, egyébként pedig r_ig_i főtagja kisebb, mint P_1G_1.

Az r_2-ben $QG_1/H = P_1G_1/G_2$, ez konstansszorosa $P_2G_2/G_2 = P_2$-nek. Ezért r_2g_2 főtagja szintén P_1G_1 konstansszorosa lehet csak, vagy annál kisebb. Végül az r_1 polinomban a $QG_2/H = P_1$ kiejti p_1 főtagját, és így r_1g_1 főtagja kisebb, mint P_1G_1. Emiatt azon főtagok száma, amelyek P_1G_1 konstansszorosai, biztosan legalább eggyel csökkent a $p_1, \ldots, p_m$ rendszerhez képest.

5.6.43. Tekintsük az f_i polinomok főtagjai által generált J ideált. Ha valamelyik r_{ij} polinom nem nulla, akkor az R főtagja egyik f_i főtagjával sem osztható. Az 5.6.39. Gyakorlat szerint R nincs benne J-ben. Ezért az eljárás következő lépésénél a bővebb generátorrendszer főtagjai által generált ideál valódi módon tartalmazza J-t. Mivel $\mathbb{C}[x_1, \ldots, x_n]$ Noether-gyűrű, ez az ideálsorozat stabilizálódik, és ezért az algoritmus is véget ér.

5.7. Hányadostest

5.7.3. Az 5.7.2. Tétel bizonyítását kell módosítani. A P halmaz most azokból az (a, b) párokból áll, melyekben $b \in F$. Mivel F zárt a szorzásra, e párok összegét és szorzatát ugyanazzal a képlettel értelmezhetjük. A számolásokban szükséges egyszerűsítések elvégezhetők, hiszen egy gyűrűben minden olyan elemmel szabad egyszerűsíteni, amely nem nulla, és nem nullosztó. Természetesen csak azon (a, b) párok osztályának konstruáltunk inverzet, melyekre $a \in F$.

5.7.6. A páros számok gyűrűjének a racionális számok $\mathbb{Q}$ teste hányadosteste lesz. Valóban, ebben részgyűrűt alkotnak a páros számok, és a p/q racionális szám előáll $2p/2q$ alakban, vagyis két páros szám hányadosaként is. A hányadostest egyértelműsége (5.7.4. Tétel) miatt „másképp" nem is lehet hányadostestet csinálni a páros számok gyűrűjéhez.

A $\mathbb{Z}[x]$ hányadosteste ugyanaz, mint $\mathbb{Q}[x]$ hányadosteste, tehát az $f(x)/g(x)$ racionális törtfüggvények teste, ahol $f, g \in \mathbb{Q}[x]$. Valóban, egy ilyen hányadost a nevezőkkel bővítve két egész együtthatós polinom hányadosát kapjuk. Végül a Gauss-egészek gyűrűjének hányadosteste az $a + bi$ számokból álló test lesz,

ahol $a, b \in \mathbb{Q}$. Ez tényleg test a 2.2.35. Gyakorlat szerint, és minden eleme valójában egy Gauss-egész és egy közönséges egész hányadosa.

5.7.7. Legyen b nem nulla eleme I-nek. Ekkor R hányadostestének minden r/s eleme fölírható $(rb)/(sb)$ alakban is. A számláló és a nevező így már I-nek elemei, és ezért R hányadosteste egyben I-nek is hányadosteste lesz.

5.7.8. Mivel P prímideál, az F szorzásra zárt. Jelölje M azoknak az $a/b \in S$ törteknek a halmazát, melyekre $a \in P$. Könnyű számolás mutatja, hogy ezek ideált alkotnak. Ha a c/d tört nincs M-ben, akkor $d/c \in S$, azaz c/d invertálható, és így egyetlen valódi ideálban sincs benne. Ezért M tartalmazza S minden valódi ideálját.

5.7.9. Az általánosítás a következő. Legyen R alaptételes (szokásos) gyűrű és $f \in R[x]$ egy nem konstans polinom. Ha létezik olyan $p \in R$ prím, 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 P hányadosteste fölött.

A bizonyítás ugyanaz, mint az $R = \mathbb{Z}$ esetében, ezért azt az Olvasóra hagyjuk. Megjegyezzük azonban, hogy ennek elmondásához $\mathbb{Z}[x]$ számelméletének alapjait, például a Gauss-lemmákat is általánosítani kell alaptételes gyűrű fölött polinomokra. Ebben semmi nehézség nincsen, itt az állítások megfogalmazását is az Olvasóra hagyjuk.

5.7.10. Legyen I ideálja S-nek és $J = I \cap R$. A feltétel szerint $J = (a)$ alkalmas $a \in R$ elemre. Megmutatjuk, hogy az S gyűrűben az a elem által generált főideál I. Mivel $a \in I$, ez a főideál része I-nek. Megfordítva, tegyük föl, hogy $r/s \in I$, ahol $r, s \in R$. Az 5.5.9. Következmény miatt R alaptételes, így feltehető, hogy r és s relatív prímek. Az 5.5.5. Lemma szerint $1 = rx + sy$ alkalmas $x, y \in R$ elemekre. Így $1/s = x(r/s) + y \in S$. Nyilván $r = s(r/s) \in J$, vagyis van olyan $b \in R$, hogy $ab = r$. Így $r/s = a(b/s)$. De $1/s \in S$ miatt $b/s \in S$, tehát r/s benne van az a által S-ben generált főideálban.

5.7.11. Tegyük föl, hogy R teljesíti a feladatban kirótt feltételt. Könnyű ellenőrizni, hogy az Útmutatóban definiált S tényleg R-et tartalmazó részgyűrűje T-nek, és benne az (a/b^k) főideálok növő láncot alkotnak. Mivel S alaptételes, ez a lánc az 5.5.8. Tétel miatt stabilizálódik, vagyis van olyan $m \geq 1$ egész és $t = r + (sa/b^k) \in S$, hogy $t(a/b^m) = a/b^{m+1}$. Innen $t = 1/b$, ahonnan $b^{k-1} = b^k r + sa$. Ezért $b^{k-1} \mid sa$, de b^{k-1} relatív prím a-hoz, és így (a 3.1.24. Gyakorlat szerint) $b^{k-1} \mid s$. Ezért $1 = br + s'a$, ahol $s' = s/b^{k-1} \in R$. Tehát az 1 benne van az (a, b) ideálban.

Legyen most $a', b' \in R$, belátjuk, hogy (a', b') főideál. Ha a' és b' valamelyike nulla, akkor ez nyilvánvaló. Ha nem, akkor legyen d a legnagyobb közös osztójuk. Az $a = a'/d$ és $b = b'/d$ elemekre az előző bekezdés eredményét alkalmazva azt kapjuk, hogy $d \in (a', b')$, vagyis $(d) = (a', b')$.

Legyen I ideálja R-nek. Mivel R alaptételes, az 5.5.8. Tétel miatt az R gyűrű I által tartalmazott főideáljai között van egy (a') maximális. Ha $(a') \neq I$ lenne, akkor létezne olyan $b' \in I$, amelyre $b' \notin (a')$. Az előző bekezdésben igazoltak miatt (a', b') főideál, ami része I-nek, és (a')-t valódi módon tartalmazza. Ez az ellentmondás mutatja, hogy $I = (a')$, vagyis R főideálgyűrű.

5.8. Karakterisztika és prímtest

5.8.6. A nullosztómentesség miatt $r^p - s^p = (r - s)^p$ csak akkor lehet nulla, ha $r = s$. Ugyanez a Frobenius-endomorfizmus hatványaira is elmondható, hiszen injektív leképezések kompozíciója is injektív.

5.8.8. Nyilván $ne, \ell e \neq 0$ akkor és csak akkor, ha $n, \ell \neq 0$, hiszen a karakterisztika nulla. Továbbá $(me)/(ne) = (ke)/(\ell e)$ akkor és csak akkor, ha $(m\ell - nk)e = 0$. A nulla karakterisztika azt jelenti, hogy ez az $m\ell - nk = 0$, vagyis az $m/n = k/\ell$ összefüggéssel ekvivalens. A φ összegtartó, hiszen

$$\varphi\left(\frac{m}{n} + \frac{k}{\ell}\right) = \varphi\left(\frac{m\ell + nk}{n\ell}\right) = \frac{(m\ell + nk)e}{(n\ell)e} = \frac{me}{ne} + \frac{ke}{\ell e} = \varphi\left(\frac{m}{n}\right) + \varphi\left(\frac{k}{\ell}\right).$$

Hasonlóan látható a szorzattartás is. A φ injektív, mert a magja nulla: ha $\varphi(m/n) = 0$, azaz $(me)/(ne) = 0$, akkor $me = 0$, és a nulla karakterisztika miatt $m = 0$. Végül tekintsük az $\mathrm{Im}(\varphi) \subseteq T$ halmazt. Ez résztest (hiszen test homomorf képe), ami az e egységelemet tartalmazza. Így az e által generált P résztest része $\mathrm{Im}(\varphi)$-nek. Másrészt $(me)/(ne)$ nyilván eleme P-nek, hiszen P résztest, és így $\mathrm{Im}(\varphi) \subseteq P$.

5.8.10. A φ injektív, hiszen testnek csak triviális ideáljai vannak. Emiatt ha $0 \neq t \in T$, akkor $\varphi(t) \neq 0$, és $\varphi(nt) = n\varphi(t)$ miatt $nt = 0$ akkor és csak akkor, ha $n\varphi(t) = 0$. Ezért t és $\varphi(t)$ rendje az összeadásra ugyanaz, és ez már meghatározza a karakterisztikát.

5.8.11. Legyen S azon $t \in T$ elemek halmaza, melyekre $\varphi(t) = t$. Könnyű számolással láthatjuk, hogy S zárt a négy alapműveletre (vö. 6.5.10. Gyakorlat). Ha $\varphi(t) \neq 0$, akkor $\varphi(1t) = \varphi(1)\varphi(t)$, ahonnan $\varphi(t)$-vel egyszerűsítve $\varphi(1) = 1$, tehát $1 \in S$. Így S résztest lesz, és ezért tartalmazza T prímtestét.

5.8.12. Ha T karakterisztikája nem 2, akkor a $2 = 1+1$ elem nem nulla T-ben, és így oszthatunk vele (vagyis T minden elemének „van fele"). Ekkor pedig az 1.2.1. Gyakorlatban leírt teljes négyzetté való kiegészítés eljárása működik, és a másodfokú egyenlet szokásos megoldóképletéhez vezet. Ezért az (1) állítás igaz.

Egy kettő karakterisztikájú testben nem működik a teljes négyzetté való kiegészítés eljárása. Valóban, $T[x]$-ben tagonként lehet négyzetre emelni, és így

$$a(y+w)^2 + b(y+w) + c = ay^2 + by + (aw^2 + bw + c)\,.$$

Vagyis hiába toljuk el a polinomot, az elsőfokú tag együtthatója nem változik, és így nem is lehet eltüntetni. A megoldóképlet is értelmetlen, mert a nevezőben $1+1 = 0$ szerepel. Ha $T = \mathbb{Z}_2$ és $f(x) = x^2+x \in T[x]$, akkor ennek gyökei 0 és 1, de egyik sem kapható meg a megoldóképletből. Ezzel (2)-t is megoldottuk.

Végül a (3) állítás 2-től különböző karakterisztikájú testben nyilván igaz (1) miatt, $T = \mathbb{Z}_2$ fölött viszont nem. Valóban, T minden eleméből vonható négyzetgyök T-ben, hiszen mindegyik elem négyzetgyöke önmaga. Mégis van T fölött másodfokú irreducibilis polinom, az $x^2 + x + 1$ (hiszen ennek nincs gyöke T-ben).

♫ Ha α_1 és α_2 az $f(x) = ax^2 + bx + c$ két gyöke, akkor $a^2(\alpha_1 - \alpha_2)^2 = b^2 - 4ac$ igaz 2 karakterisztikában is (3.7.9. Gyakorlat). Ezért ha T-ben minden elemből vonható négyzetgyök, akkor $\alpha_1 - \alpha_2 \in T$. Továbbá a gyökök és együtthatók összefüggése miatt $\alpha_1 + \alpha_2 = -b/a \in T$. De ebből a két egyenletből mégsem kapható meg α_1 és α_2, mert ez valójában csak egyetlen egyenlet: a 2 karakterisztika miatt $\alpha_1 - \alpha_2 = \alpha_1 + \alpha_2$. Minden más karakterisztika esetén ennek az egyenletrendszernek a megoldása a szokásos megoldóképlethez vezet.

5.8.13. Az $x^n - 1$ deriváltja nx^{n-1}. Ha $p \nmid n$, akkor ez nem a nullapolinom, és így csak a 0 lehet gyöke, ami azonban nem gyöke $x^n - 1$-nek. Ezért az 5.8.3. Tétel miatt $x^n - 1$-nek nincs többszörös gyöke.

5.8.14. Tegyük föl, hogy $\varepsilon \in T$ gyöke Φ_n-nek, és legyen ℓ az ε rendje a T 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 föl indirekt, hogy $\ell < n$. Ekkor ε gyöke már az $x^\ell - 1 \in T[x]$-nek is. De $x^\ell - 1 = \prod_{d\mid\ell} \Phi_d(x)$, vagyis van olyan $m \mid \ell$, hogy $\Phi_m(\varepsilon) = 0$. Tehát az $x - \varepsilon$ gyöktényező kiemelhető a Φ_n és a Φ_m polinomokból. Persze $m \mid n$ és $m \neq n$, azaz ekkor ε legalább kétszeres gyöke $\Phi_m(x)\,\Phi_n(x) \mid x^n - 1$-nek. Az $x^n - 1$ polinomnak azonban nincs többszörös gyöke T-ben az 5.8.13. Gyakorlat miatt. Ez az ellentmondás bizonyítja, hogy ε rendje tényleg n.

Ha ε egy n-edrendű eleme T-nek, akkor ε gyöke $x^n - 1 = \prod_{d\mid n} \Phi_d(x)$-nek, tehát valamelyik Φ_d-nek is, és így $\Phi_d(x) \mid x^d - 1$ miatt $\varepsilon^d = 1$ teljesül. Mivel ε rendje n, csakis $d = n$ lehetséges.

5.8.15. Tegyük föl, hogy a p prím osztja $\Phi_n(nN)$-et (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 $\mathbb{Z}_p^\times$ 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 föl (2.4.9. Gyakorlat), és így van olyan N, amikor a $\Phi_n(nN)$ érték 1-től és -1-től is különbözik.

5.8.16. Belátjuk, hogy ha $p \mid n$, akkor $p^2 \mid \Phi_n(c)$ csak akkor lehetséges, ha $p = n = 2$. Ebben az esetben persze $4 \mid \Phi_2(c) = c + 1$ akkor és csak akkor, ha $c \equiv -1$ (4).

Tegyük föl, hogy $p^2 \mid \Phi_n(c)$, ahol $n = pm$. Először megvizsgáljuk a $c = \pm 1$ esetet. A 3.9.19. és 3.9.20. Feladatok szerint $\Phi_n(\pm 1)$ prím vagy ± 1, így nem osztható p^2-tel, kivéve a $\Phi_1(1) = \Phi_2(-1) = 0$ eseteket. Mivel $p \mid n$, nekünk csak a $p = n = 2$ felel meg.

Ha $c \neq \pm 1$, akkor a körosztási polinomok rekurziós képlete miatt $\Phi_{pm}(x) \mid (x^{pm} - 1)/(x^m - 1)$, és így $\mathbb{Z}_p$ fölött

$$\Phi_{pm}(x) \;\Big|\; \frac{x^{pm} - 1}{x^m - 1} = \frac{(x^m - 1)^p}{x^m - 1} = (x^m - 1)^{p-1}\,.$$

Innen $p \mid \Phi_n(c)$ miatt azt kapjuk, hogy $p \mid (c^m - 1)^{p-1}$, azaz c^m fölírható $ap + 1$ alakban, ahol $a \in \mathbb{Z}$. Ezt behelyettesítve, a binomiális tétel szerint (immár $\mathbb{Z}$-ben számolva, $c^m \neq 1$ azaz $c \neq \pm 1$ esetén)

$$\frac{c^{pm} - 1}{c^m - 1} = \frac{\left(\sum_{j=0}^{p} \binom{p}{j}(ap)^j\right) - 1}{ap + 1 - 1} =$$

$$= (ap)^{p-1} + \binom{p}{p-1}(ap)^{p-2} + \cdots + \binom{p}{2}ap + \binom{p}{1}\,,$$

hiszen az 1 a számlálóban is kiesik. Ha $p > 2$, akkor az itt fellépő tagok mindegyike osztható p^2-tel, kivéve az utolsót, hiszen ekkor $p \mid \binom{p}{2}$, és $\binom{p}{1} = p$. Ez ellentmondás, mert az összegről tudjuk, hogy osztható $\Phi_n(c)$-vel, és így p^2-tel is.

A $p = 2$ esetben az a feladat feltevése, hogy $4 \mid \Phi_n(c)$. Ha c páros, akkor $\Phi_n(c) \mid c^n - 1$ páratlan szám, ez nem lehet. Ha viszont c páratlan, akkor $c \equiv \pm 1$ (4), és így $4 \mid \Phi_n(1)$ vagy $4 \mid \Phi_n(-1)$. Ezeket az eseteket már elintéztük a megoldás legelején.

5.8.17. Ebben a megoldásban az $o_n(b)$ jelölést használjuk a b számnak a mod n vett rendjére (lásd 25. oldal). Megmutatjuk, hogy $\big(\Phi_m(c), \Phi_n(c)\big)$ vagy 1, vagy pedig egy p prímszám. Ez utóbbi pontosan akkor teljesül, ha $m = p^\alpha k$ és $n = p^\beta k$ alkalmas $\alpha, \beta \geq 0$ és $k \geq 1$ egészekkel, melyekre $k \mid p - 1$.

Tegyük föl először, hogy $\big(\Phi_m(c), \Phi_n(c)\big) \neq 1$. Ekkor van olyan p prímszám, ami a $\Phi_m(c)$, $\Phi_n(c)$ számokat osztja. Legyen $m = p^\alpha k$ és $n = p^\beta \ell$, ahol már $p \nmid k$ és $p \nmid \ell$ (itt α és β nulla is lehet). A 3.9.23. Feladat miatt $\mathbb{Z}_p$ fölött $\Phi_n = \Phi_k^{\varphi(p^\alpha)}$, és ezért $p \mid \Phi_k(c)$. Az 5.8.14. Feladat miatt $o_p(c) = k$ (és innen $k \mid p - 1$). Ugyanígy $o_p(c) = \ell$, tehát $k = \ell$.

Megfordítva, tegyük föl, hogy m és n ilyen alakú. Legyen c egy olyan egész szám, melyre $o_p(c) = k$. Ilyen szám létezik, hiszen a $\mathbb{Z}_p$ test multiplikatív csoportja ciklikus (4.3.22. Tétel). Az 5.8.14. Feladat miatt c gyöke $\mathbb{Z}_p[x]$-ben $\Phi_k(x)$-nek. Az előző bekezdésben írtak miatt tehát $p \mid \big(\Phi_m(c), \Phi_n(c)\big)$.

Hátra van még annak bizonyítása, hogy $\big(\Phi_m(c), \Phi_n(c)\big)$ értéke, ha nem 1, akkor prímszám. Tegyük föl, hogy van egy közös p prímosztó. Ez egyértelműen meghatározott, hiszen az eddig bizonyítottak szerint m és n kanonikus alakjában csak egy kitevőben van eltérés. Azt kell megmutatni, hogy p^2 nem közös osztó. Ha az lenne, akkor az 5.8.16. Feladat miatt $p = 2$, és az n, m számok közül amelyik páros, az kettővel egyenlő. Ezért n és m egyike kettő, a másik 1. Azaz $4 \mid \big(\Phi_1(c), \Phi_2(c)\big) = (c - 1, c + 1)$, ami lehetetlen.

5.9. Rendezett gyűrűk és testek

5.9.4. Legyen $d = -c$. A $c \leq 0$-hoz d-t adva $0 \leq d$ adódik, és ezért $ad \leq bd$, azaz $-ac \leq -bc$. Ehhez $ac + bc$-t adva az első állítást kapjuk.

A második állítás igazolásához adjunk $a \geq 0$-hoz b-t. Ekkor $0 = a + b \geq b$ adódik, ahonnan $b \geq 0$, és a rendezés antiszimmetriája miatt $b = 0$. De akkor $a = -b = 0$.

5.9.6. Az világos a részben rendezésre vonatkozó szabályokból, hogy a pozitivitástartomány zárt a szorzásra (a nullosztómentesség miatt), és nem tartalmazza a nullát. Az összeadásra való zártság a 5.9.4. Gyakorlatból következik.

Megfordítva, legyen $P \subseteq R$ összeadásra és szorzásra zárt, a nullát nem tartalmazó részhalmaz. Definiáljuk a részben rendezést az $a < b \iff b - a \in P$ képlettel. Ekkor a $\leq$ reláció tranzitív, mert P zárt az összeadásra, továbbá nyilván reflexív. Ha $a \leq b$ és $b \leq a$, de $a \neq b$, akkor $a-b$ és $b-a$ is P-ben van, tehát az összegük is, ami ellentmondás, mert $0 \notin P$. Ezért részben rendezést kaptunk, amely könnyen láthatóan teljesíti az 5.9.3. Definícióban megadott (1) és (2) feltételeket. Például a (2) igazolása a következőképpen fest. Ha $c = 0$ vagy $a = b$, akkor az állítás nyilvánvaló. Különben $b - a \in P$ és $c \in P$, ezért a szorzásra zártság miatt $(b-a)c \in P$, ahonnan $bc < ac$.

Ha $\leq$ elrendezés, akkor tetszőleges $r \neq 0$ esetén $r > 0$ vagy $r < 0$. Utóbbi esetben mindkét oldalhoz $-r$-et adva $-r \geq 0$. Itt egyenlőség nem állhat, mert $r \neq 0$, és így $-r \in P$. Megfordítva, ha P rendelkezik a megadott tulajdonsággal, akkor $a \neq b \in R$ esetén $a - b \in P$ vagy $-(a-b) \in P$. Az első esetben $a > b$, a másodikban $a < b$. Ezért $\leq$ elrendezés.

5.9.9. Tegyük föl, hogy $\leq$ elrendezése a hányadostestnek, ami R rendezésének kiterjesztése, és $a, b \in R$, ahol $b \neq 0$. Megmutatjuk, hogy a/b akkor és csak akkor pozitív, ha $a > 0$ és $b > 0$, vagy $a < 0$ és $b < 0$.

Ha $a/b > 0$, akkor b-vel szorozva $b > 0$ esetén $a \geq 0$, ha pedig $b < 0$, akkor az 5.9.4. Gyakorlat szerint $a \leq 0$ adódik. Egyenlőség egyik esetben sem állhat, mert ha $a = 0$, akkor a/b is nulla. Megfordítva, ha $a > 0$ és $b > 0$, akkor $a/b < 0$ nem lehet, mert innen b-vel szorozva $a \leq 0$ adódna. Mivel elrendezésről van szó, és mivel $a \neq 0$ miatt $a/b \neq 0$, csakis $a/b > 0$ lehetséges. Ha $a < 0$ és $b < 0$, akkor $a/b = (-a)/(-b)$, és így az előző gondolatmenet szerint $a/b > 0$.

Ezért az R gyűrű rendezése egyértelműen meghatározza a hányadostest pozitivitástartományát, és így a rendezését is. Megfordítva, legyen P azon a/b törtek halmaza, ahol a és b is pozitív. Belátjuk, hogy ez pozitivitástartomány lesz egy alkalmas rendezésre. Ehhez az 5.9.6. Gyakorlatot használjuk. Nyilván $0 \notin P$, és P zárt a szorzásra. Tegyük föl, hogy a/b és $c/d \in P$, be kell látni, hogy $(a/b) + (b/d) \in P$, vagyis hogy $ad + bc$ és bd is pozitív. Ez nyilvánvaló, hiszen a, b, c, d pozitív.

5.9.10. Két eset van: $\sqrt{2}$ vagy pozitív, vagy negatív. Megmutatjuk, hogy mindkettő lehetséges, és egyértelműen meghatározza a rendezést. Ezért a feladatbeli $\mathbb{Q}(\sqrt{2})$ gyűrűnek két elrendezése van.

Tegyük föl, hogy a $\leq$ elrendezésnél $\sqrt{2} > 0$ és legyen $a, b \in \mathbb{Q}$. Meg kell mutatnunk, hogy $a + b\sqrt{2}$ előjele egyértelműen meghatározott. Ha $b = 0$, akkor ezt tudjuk, hiszen a racionális számokon a rendezés egyértelmű az 5.9.8. Következmény miatt. Tegyük föl, hogy $b > 0$. Ha $a \geq 0$, akkor persze $a + b\sqrt{2} > 0$. Ha $a < 0$, akkor

$$(a + b\sqrt{2})(-a + b\sqrt{2}) = -a^2 + 2b^2 \in \mathbb{Q} \ .$$

Itt $-a + b\sqrt{2} > 0$, és $-a^2 + 2b^2$ előjelét is ismerjük, hiszen ez nem nulla racionális szám. Ezért $-a + b\sqrt{2}$ előjele is egyértelműen meg van határozva. Végül ha $b < 0$, akkor a $-a - b\sqrt{2}$ előjelét az előzőek szerint ismerjük, és így $a + b\sqrt{2}$ előjelét is.

Beláttuk tehát, hogy legfeljebb egy olyan rendezés van, ahol $\sqrt{2} > 0$. Persze ilyen létezik is, az, amit a valós számok szokásos rendezéséből kapunk.

Ha $\sqrt{2} < 0$, akkor a fenti számolás megismétlése helyett egyszerűbb a következőt mondani. Tekintsük a $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$ képlettel definiált leképezést. Ez könnyen láthatóan $\mathbb{Q}(\sqrt{2})$-nek önmagával való izomorfizmusa. Az imént beláttuk, hogy egyetlen olyan pozitivitástartomány van, amelynek $\sqrt{2}$ eleme. Ezért φ-t alkalmazva látjuk, hogy egyetlen olyan van, aminek $\varphi(\sqrt{2}) = -\sqrt{2}$ eleme.

5.9.11. A P nyilván zárt az összeadásra és a szorzásra, és nincs benne a nullapolinom, tehát ez pozitivitástartomány. Elrendezést kapunk, hiszen egyik nem nulla racionális együtthatós polinomnak sem gyöke az π, és így a polinom vagy az ellentettje pozitív lesz (5.9.6. Gyakorlat). Ugyanez a módszer nem működik $\mathbb{R}[x]$ esetén, mert $x - \pi$ se nem pozitív, se nem negatív (vagyis rendezést kapunk, de ez nem elrendezés).

5.9.12. Az Útmutatóban megadott pozitivitástartomány könnyen ellenőrizhetően elrendezést ad (5.9.6. Gyakorlat). A kapott elrendezésnél az x „végtelenül kicsi pozitív" mennyiségnek képzelhető: a nullánál nagyobb, de minden pozitív számnál kisebb. Ha a konstrukciót úgy végezzük, hogy $x - b$ polinomjaival

dolgozunk, akkor $0 + 1(x - b)$ pozitív, de $-\varepsilon + 1(x - b)$ negatív lesz minden pozitív ε számra. Ebben az esetben x csak „végtelenül picit" nagyobb b-nél. Ezért minden b-re más rendezést kapunk.

5.9.13. Legyen T az R hányadosteste. Először az Útmutatóban kimondott állításokat igazoljuk. A nem nulla T-beli elemek négyzetösszegeinek P_0 halmaza nyilván zárt az összeadásra és a szorzásra, továbbá az R-re tett feltétel miatt nem tartalmazza a nullát. Ezért az 5.9.6. Gyakorlat miatt P_0 pozitivitástartomány. Ha $P \supseteq P_0$ pozitivitástartomány és $0 \neq r \in T$, akkor legyen P_1 a $pr+q$ alakú elemek halmaza, ahol $p, q \in P$. Ekkor P_1 zárt az összeadásra, de zárt a szorzásra is, mert

$$(p_1r + q_1)(p_2r + q_2) = (p_1p_2r^2 + q_1q_2) + (p_1q_2 + p_2q_1)r\,.$$

Nyilván $p_1q_2 + p_2q_1 \in P$, de $p_1p_2r^2 + q_1q_2 \in P$ is teljesül, hiszen $r^2 \in P_0 \subseteq P$. Ezért P_1 tényleg zárt a szorzásra. Ha $-r$ nem írható föl p/q alakban, ahol $p, q \in P$, akkor P_1 nem tartalmazza a nullát, és így pozitivitástartomány.

A Zorn-lemma feltétele alkalmazható a P_0-t tartalmazó pozitivitástartományok halmazára, mert egy lánc uniója is zárt az összeadásra, szorzásra, és nem tartalmazza a nullát. Ezért létezik ezek között egy P maximális elem. Megmutatjuk, hogy ez T elrendezését adja. Ha $0 \neq r \in T$, de sem r, sem $-r$ nincs P-ben, akkor mivel P maximális, nem bővíthető r-rel a fenti módon, és ezért $-r = p_1/q_1$ alkalmas $p_1, q_1 \in P$-re. De P nem bővíthető $-r$-rel sem, ezért $r = p_2/q_2$ alkalmas $p_2, q_2 \in P$-re. Ekkor azonban $p_1q_2 + p_2q_1 = 0$, ami ellentmond annak, hogy P pozitivitástartomány.

5.10. Minimálpolinom algebrákban

5.10.2. Legyen $u = \sqrt[3]{7 + 5\sqrt{2}}$ és $v = \sqrt[3]{7 - 5\sqrt{2}}$. Ekkor $z = u + v$, ezt köbre emelve

$$z^3 = u^3 + v^3 + 3uv(u + v) = 14 + 3uvz\,.$$

De $uv = \sqrt[3]{49 - 50} = -1$, ezért $z^3 + 3z - 14 = 0$ teljesül. Vagyis z gyöke a megadott polinomnak. De ez nem irreducibilis $\mathbb{Q}$ fölött, hiszen gyöke a 2. A gyöktényezőt kiemelve $x^3 + 3x - 14 = (x - 2)(x^2 + 2x + 7)$. Ez utóbbi polinomnak nincs valós gyöke, viszont z valós szám. Ezért $z = 2$, minimálpolinomja $x - 2$.

♫ A z kifejezést úgy kapjuk, hogy az $x^3 + 3x - 14$ polinomra a Cardano-képletet alkalmazzuk.

5.10.4. Ha T tartalmazza R egységelemét, akkor T és R egységeleme ugyanaz (például az 5.3.4. Lemma miatt). Az összeadásra R Abel-csoport, tehát csak a skalárral szorzás négy axiómáját kell ellenőrizni. Ezek következnek abból, hogy R-ben érvényes a kétoldali disztributivitás és a szorzás asszociativitása, továbbá hogy T és R egységeleme ugyanaz. Példaként belátjuk, hogy $(\lambda + \mu)r = \lambda r + \mu r$ (itt $\lambda, \mu \in T$, $r \in R$, az egymás mellé írás skalárral szorzást jelöl). A skalárral való szorzás definíciója miatt $\lambda r = \lambda * r$, $\mu r = \mu * r$ és $(\lambda + \mu)r = (\lambda + \mu) * r$. Ezért ez az azonosság tényleg az R-beli disztributivitás egy speciális esete. Ezzel (1)-et beláttuk.

Ahhoz, hogy algebrát kapjunk, a gyűrű- és vektortér-tulajdonságokon kívül még arra van szükség, hogy $\lambda \in T$ és $r, s \in R$ esetén $\lambda(r * s) = (\lambda r) * s = r * (\lambda s)$ teljesüljön. Az s helyébe az egységelemet írva $\lambda * r = r * \lambda$ adódik. Megfordítva, ha ez teljesül, akkor algebrát kapunk, hiszen R-ben a művelet asszociatív.

5.10.5. A $\varphi : \lambda \to \lambda e$ leképezésről könnyű belátni, hogy összeg- és szorzattartó. Példaként a szorzattartást igazoljuk.

$$\varphi(\lambda)\varphi(\mu) = (\lambda e)(\mu e) = \lambda\big(e(\mu e)\big) = \lambda(\mu e^2) = (\lambda\mu)e = \varphi(\lambda\mu)$$

(itt többször is használtuk a $\lambda(rs) = (\lambda r)s = r(\lambda s)$ algebra-tulajdonságot, és a vektortér-axiómákat is). Ha $1 \in T$ az egységelem, akkor a vektortér-axiómák miatt $\varphi(1) = e$. Ezért φ nem azonosan nulla, és mivel magja ideál a T testben, a φ injektív. Így T izomorf $\varphi(T) \leq A$-val, ami tehát részteste A-nak. Ez a résztest benne van A centrumában, hiszen ha $r \in A$ és $\lambda \in T$, akkor az algebra-tulajdonság miatt

$$r(\lambda e) = \lambda(re) = \lambda(er) = (\lambda e)r\,.$$

Végül ha $\lambda, \mu \in T$, akkor $\lambda(\mu e) = (\lambda\mu)e$ a vektortér-axiómák miatt, és így $\varphi(T)$ altér is.

♫ Absztrakt algebrai vizsgálatokban azonosítani szokás a λ és λe elemeket, és így felteszik, hogy egységelemes algebrában az alaptest valójában az algebra részteste, és a két egységelem is ugyanaz. Ez azonban néha nem praktikus, például lineáris algebrában nem azonosítjuk a 3 skalárt és a $3E$ mátrixot.

5.10.7. A 2.4.30. Gyakorlat megoldásának mintájára járunk el, a szorzattartást ugyanazon a speciális eseten vizsgáljuk meg. Legyen A egységeleme e, továbbá $f(x) = \alpha + \beta x$ és $g(x) = \gamma + \delta x$. Ekkor

$$f(x)g(x) = (\alpha + \beta x)(\gamma + \delta x) = \alpha\gamma + (\alpha\delta + \beta\gamma)x + \beta\delta x^2 .$$

Ezért azt kell belátni, hogy az A algebrában

$$(\alpha e + \beta a)(\gamma e + \delta a) = \alpha\gamma e + (\alpha\delta + \beta\gamma)a + \beta\delta a^2 .$$

A bal oldalon a szorzást elvégezve a disztributivitás miatt

$$(\alpha e)(\gamma e) + (\alpha e)(\delta a) + (\beta a)(\gamma e) + (\beta a)(\delta a)$$

adódik. Az algebra-axiómák miatt $\lambda(rs) = (\lambda r)s = r(\lambda s)$, ahol r és s algebra-elemek, λ pedig T-beli skalár. Ezért a fenti összeg

$$(\alpha\gamma)e^2 + (\alpha\delta)(ea) + (\beta\gamma)(ae) + (\beta\delta)a^2$$

alakban írható. Mivel e egységelem, a kívánt eredményt kapjuk. Az általános számolás ugyanígy működik, csak a képletek bonyolultabbak, a részletek kidolgozását az Olvasóra hagyjuk.

♫ Fontos észrevenni, hogy a hatványai egymással és az egységelemmel is fölcserélhetők. Még fontosabb azonban, hogy itt valójában az a elemet a skalárokkal cseréltük föl. Ennek így szó szerint persze nincs értelme, hiszen a skalárokkal csak balról szorzunk, de a fenti számolásból mégis ezt érezhetjük ki. Ezért fontos az 5.10.5. Gyakorlat megoldásában megvizsgált $\lambda = \lambda e$ azonosítás. Ha ugyanis a skalárokat A centrumelemeivé tesszük, akkor a fenti számolás is érthetőbbé válik: nem kell annyit zárójelezni, és mindig figyelni arra, hogy mi az algebra eleme, és mi skalár, továbbá az e betűk is eltűnnek a képletekből.

5.10.13. Az állítás bonyolult közvetlen számítással is igazolható, ha a polinomot általános alakban írjuk föl, és behelyettesítünk. Egyszerűbb azonban a következőt mondani. Tekintsük az

$$s(x) = \big(x - (1 + \sqrt{2})\big)\big(x - (1 - \sqrt{2})\big) = x^2 - 2x - 1$$

polinomot. Ez irreducibilis $\mathbb{Q}$ fölött, hiszen másodfokú, és nincs racionális gyöke. Tehát az 5.10.12. Tétel miatt ez lesz $1+\sqrt{2}$ minimálpolinomja. Ha az $f \in \mathbb{Q}[x]$ polinomnak gyöke $1+\sqrt{2}$, akkor az 5.10.10. Tétel miatt $s \mid f$, és így $1 - \sqrt{2}$ is gyöke f-nek.

♫ Az állítás hasonlít ahhoz, amikor azt bizonyítottuk, hogy ha egy valós együtthatós polinomnak gyöke az $a + bi$, akkor a konjugáltja, $a - bi$ is gyöke (lásd 3.3.6. Lemma). Abban a bizonyításban nem a minimálpolinomról esett szó, hanem azt használtuk ki, hogy a komplex konjugálás művelettartó, és a valós számokat fixálja. Hasonlóan tekinthetjük azt a φ leképezést, amely az $a + b\sqrt{2}$ számhoz $a - b\sqrt{2}$-t rendel ($a, b \in \mathbb{Q}$). Ez izomorfizmusa az $a + b\sqrt{2}$ alakú számok testének önmagával, amely minden racionális számot saját magába visz. Arra biztatjuk az Olvasót, hogy ennek segítségével adjon új bizonyítást a fenti állításra, a 3.3.6. Lemma bizonyítása alapján. A „megfejtés" elolvasható a 6.5. szakasz elején (valójában a 6.5.3. Állítás bizonyításában).

5.10.14. Az 5.10.13. Gyakorlat megoldásához hasonlóan járunk el. Az $1 + \sqrt[3]{2}$ gyöke az $(x-1)^3 - 2$ polinomnak, ami az $x^3 - 2$ eltoltja, és így irreducibilis $\mathbb{Q}$ fölött. Ezért ez $1 + \sqrt[3]{2}$ minimálpolinomja, és így minden olyan racionális együtthatós polinomnak, amelynek az $1 + \sqrt[3]{2}$ gyöke, az $1 + \varepsilon\sqrt[3]{2}$ számok is gyökei lesznek, ahol ε harmadik egységgyök.

5.10.15. Az (1) esetben az eredmény $x^2 - 2x + 2$. Legyen $z = 1 + i$, ekkor $i = z - 1$, négyzetre emelve és rendezve $z^2 - 2z + 2 = 0$. Az $x^2 - 2x + 2$ polinomnak tehát gyöke az $1+i$, és ez akkor lesz a minimálpolinom, ha irreducibilis $\mathbb{Q}$ fölött. Ez látszik abból, hogy másodfokú, és nincs gyöke $\mathbb{Q}$-ban.

A (2) esetben az eredmény $x^4 - 2x^2 + 9$. Ha $z = \sqrt{2} + i$, akkor $(z - i)^2 = 2$, azaz $z^2 - 3 = 2iz$, még egyszer négyzetre emelve és rendezve $z^4 - 2z^2 + 9 = 0$. A kapott $x^4 - 2x^2 + 9$ polinom gyökei $\pm\sqrt{2} \pm i$, ezért

$$x^4 - 2x^2 + 9 = (x^2 - 2\sqrt{2}x + 3)(x^2 + 2\sqrt{2}x + 3)$$

a felbontása $\mathbb{R}$ fölött irreducibilisek szorzatára (hiszen valós gyök nincs). Mivel a tényezők normáltak, de nem racionális együtthatósak, ezért a 3.3.12. Példában látottakhoz hasonlóan a polinom irreducibilis $\mathbb{Q}$ fölött.

A (3) esetben hasonló számolással $x^6 - 4x^3 + 2$ adódik, ami a Schönemann–Eisenstein-kritérium miatt irreducibilis.

A (4) esetben az eredmény $\Phi_{18}(x) = x^6 - x^3 + 1$, az (5) esetben pedig $\Phi_n(x)$, hiszen minden körosztási polinom irreducibilis $\mathbb{Q}$ fölött (3.9.9. Tétel), és normált.

A (6) esetben az eredmény $x^3 - (3/4)x - (1/8)$. A $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ azonosságból kapjuk, hogy $\cos 20^\circ$ gyöke a ennek a polinomnak. Az irreducibilitás a racionális gyökteszt segítségével ellenőrizhető, hiszen harmadfokú polinomról van szó.

5.10.16. A számolás hasonló az 5.1.2. Állítás bizonyításához. A különbség az, hogy a generált részalgebra altér is, és ezért minden elemének a skalárszorosait is tartalmazza. Ezért a polinomok most nem egész együtthatósak, hanem T-beli együtthatósak lesznek (és az 5.10.7. Gyakorlat állítását kell menet közben alkalmazni). Az $a_1, \dots, a_n$ által generált részalgebra elemei a $p(a_1, \dots, a_n)$ alakú elemek lesznek, ahol $p \in T[x_1, \dots, x_n]$ és $p(0, \dots, 0) = 0$.

5.10.17. A 4.14.2. Gyakorlat megoldásához hasonlóan jelölje $E^{i,j}$ $(i > j)$ azt a mátrixot, amelyben az i-edik sor j-edik eleme 1, és az összes többi elem nulla. Könnyű számolás mutatja, hogy ha egy mátrix az $E^{i,j}$ mátrixok mindegyikével fölcserélhető, akkor az az egységmátrix skalárszorosa. Továbbá a λE akkor és csak akkor cserélhető föl az összes μE alakú mátrixszal, ha λ benne van D centrumában.

5.11. A számfogalom lezárása

5.11.1. A $p_1 + q_1 i + r_1 j + s_1 k$ és $p_2 + q_2 i + r_2 j + s_2 k$ kvaterniók szorzata

$$(p_1p_2 - q_1q_2 - r_1r_2 - s_1s_2) + (p_1q_2 + q_1p_2 + r_1s_2 - s_1r_2)i + \\ + (p_1r_2 - q_1s_2 + r_1p_2 + s_1q_2)j + (p_1s_2 + q_1r_2 - r_1q_2 + s_1p_2)k\,.$$

Ennek alapján φ szorzattartása mátrixszorzással ellenőrizhető (az összegtartás, és φ injektivitása nyilvánvaló, továbbá az is, hogy φ tartja a valós skalárokkal való szorzást is, tehát algebrahomomorfizmus).

♫ A φ összeg- és skalárszorostartása miatt a szorzattartás valójában következik a 4.5.21. Gyakorlat állításából.

5.11.3. A $z\overline{z} = p^2+q^2+r^2+s^2$ és $\overline{z \cdot w} = \overline{w} \cdot \overline{z}$ összefüggések közvetlenül adódnak a kvaterniószorzásnak az előző, 5.11.1. Gyakorlatban megadott képletéből. Ezért

$$N(z \cdot w) = z \cdot w \cdot \overline{z \cdot w} = z \cdot w \cdot \overline{w} \cdot \overline{z} = z \cdot N(w) \cdot \overline{z} = z \cdot \overline{z} \cdot N(w) = N(z) \cdot N(w)\,,$$

hiszen az $N(w) \in \mathbb{R}$ skalár minden kvaternióval fölcserélhető. Ha $N(z) = 0$, akkor z is nulla, hiszen valós számok négyzetösszege csak akkor nulla, ha minden tag nulla. Emiatt minden nem nulla z kvaterniónak $\overline{z}/N(z)$ inverze lesz (kvaterniót valós számmal persze tagonként, pontosabban együtthatónként kell elosztani).

Ha $i(p + qi + rj + sk) = (p + qi + rj + sk)i$, akkor a műveleteket elvégezve $rk - sj = -rk + sj$, ahonnan $r = s = 0$. Tehát az i centralizátora csak a $p + qi$ alakú kvaterniókból áll. Ugyanezt j-re fölírva kapjuk, hogy a kvaterniók ferdetestének centruma csak a valós számokból áll.

5.11.11. Az (1) esetben megfelel az $\mathbb{R}[x]$, a (2) esetben pedig az $\mathbb{R}^{2\times 2}$ teljes mátrixgyűrű.

5.11.12. Az $i + j$ négyzete -2, normája 2, inverze $-(1/2)i - (1/2)j$, minimálpolinomja $x^2 + 2$ (hiszen ez irreducibilis $\mathbb{R}$ fölött; elsőfokú minimálpolinomja nyilván pontosan $\mathbb{R}$ elemeinek van). Az $i + j + k$ négyzete -3, inverze $-(1/3)i - (1/3)j - (1/3)k$, minimálpolinomja $x^2 + 3$.

5.11.13. Ha $z_1 = p_1 + q_1 i + r_1 j + s_1 k$ nem valós kvaternió, akkor az 5.11.7. Állítás szerint a z és az 1 által generált részalgebra $\mathbb{C}$-vel izomorf. Ezt a részalgebrát már z_1 is generálja, hiszen ha z nem valós komplex szám, akkor z és z^2 nem párhuzamosak (hiszen $z^2/z = z$ nem valós).

Legyen

$$w_1 = \frac{q_1 i + r_1 j + s_1 k}{\sqrt{q_1^2 + r_1^2 + s_1^2}}\,.$$

Ez ugyanazt a részalgebrát generálja, mint z_1. De $w_1^2 = -1$ az 5.11.5. Következmény miatt. Készítsük el w_2-t analóg módon $z_2 = p_2 + q_2 i + r_2 j + s_2 k$-ból. Ha z_1 és z_2 ugyanazt a részalgebrát generálja, akkor w_1 és w_2 is, de mivel ez $\mathbb{C}$-vel izomorf, benne az $x^2 + 1$ polinomnak csak két gyöke van. Ezért $w_1 = \pm w_2$, azaz a (q_1, r_1, s_1) és a (q_2, r_2, s_2) vektorok párhuzamosak. Megfordítva, ha ezek a vektorok párhuzamosak, akkor w_1 és w_2 egymás valós számszorosai, és így z_1 és z_2 is ugyanazt a részalgebrát generálják.

5.11.14. Ha $z = w^2$, akkor w és z fölcserélhetők, ezért az 5.11.8. Állítás miatt w benne van a z által generált részalgebrában, amely az 5.11.7. Állítás miatt $\mathbb{C}$-vel izomorf, és így ebben z-nek tényleg két négyzetgyöke van.

5.11.15. Ha $z^n = 1$, akkor tekintsük a z (és az 1) által generált részalgebrát $\mathbb{K}$-ban. Az 5.11.7. Állítás szerint ez $\mathbb{C}$-vel izomorf, jelölje w az i-nek megfelelő elemet. Az 5.11.5. Következmény miatt $w = qi + rj + sk$, ahol $q^2 + r^2 + s^2 = 1$. Ezért a megoldások

$$z = \cos(m2\pi/n) + iq\sin(m2\pi/n) + jr\sin(m2\pi/n) + ks\sin(m2\pi/n)\,,$$

ahol $0 \le m < n$ és $q^2 + r^2 + s^2 = 1$.

6. fejezet

Galois-elmélet

6.1. Testbővítések

6.1.2. Az $\bigl(a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4}\bigr)\bigl(a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4}\bigr)$ szorzás eredménye

$$(a_1a_2 + 2b_1c_2 + 2c_1b_2) + (a_1b_2 + b_1a_2 + 2c_1c_2)\sqrt[3]{2} + (a_1c_2 + b_1b_2 + c_1a_2)\sqrt[3]{4}\,.$$

6.1.3. A lineáris egyenletrendszert megoldva az eredmény $1 - (1/2)\sqrt[3]{4}$.

6.1.6. Jelölje M az L azon elemeinek a halmazát, amelyek $\alpha_1, \ldots, \alpha_n$-ből és K elemeiből előállnak a négy alapművelet véges sokszori alkalmazásával. Ez a halmaz részteste L-nek, hiszen ha γ és δ előáll a kívánt módon, akkor $\gamma \pm \delta$ és $\gamma\delta$, továbbá $\gamma \neq 0$ esetén $1/\gamma$ is előáll így. Továbbá M tartalmazza K-t és az $\alpha_1, \ldots, \alpha_n$ elemeket. Mivel $K(\alpha_1, \ldots, \alpha_n)$ a legszűkebb olyan részteste L-nek, amely tartalmazza K-t és az $\alpha_1, \ldots, \alpha_n$ elemeket, ezért $K(\alpha_1, \ldots, \alpha_n) \subseteq M$. Megfordítva, ha α előáll $\alpha_1, \ldots, \alpha_n$-ből és K elemeiből a négy alapművelet véges sokszori alkalmazásával, akkor $\alpha \in K(\alpha_1, \ldots, \alpha_n)$, hiszen ez egy résztest, amely tartalmazza K-t és az $\alpha_1, \ldots, \alpha_n$ elemeket. Vagyis $M \subseteq K(\alpha_1, \ldots, \alpha_n)$, és így $M = K(\alpha_1, \ldots, \alpha_n)$. Ezzel (1)-et beláttuk.

A (2) igazolásához az (1)-et használjuk. Ha $\beta_1, \ldots, \beta_m$ előáll $\alpha_1, \ldots, \alpha_n$-ből és K elemeiből a négy alapművelet segítségével, akkor $\beta_j \in K(\alpha_1, \ldots, \alpha_n)$ minden $1 \leq j \leq m$ esetén. Így a $K(\alpha_1, \ldots, \alpha_n)$ test tartalmazza K-t és a $\beta_1, \ldots, \beta_m$ elemeket. De $K(\beta_1, \ldots, \beta_m)$ a legszűkebb ilyen tulajdonságú részteste L-nek, és ezért $K(\beta_1, \ldots, \beta_m) \subseteq K(\alpha_1, \ldots, \alpha_n)$. Megfordítva, ha $K(\beta_1, \ldots, \beta_m) \subseteq K(\alpha_1, \ldots, \alpha_n)$, akkor mindegyik $\beta_j \in K(\alpha_1, \ldots, \alpha_n)$, és ezért (1) miatt fölírhatók a kívánt alakban.

A (3) nyilvánvalóan következik (2)-ből. Végtelen sok generátor esetén az állítások érvényben maradnak, azonban természetesen egy-egy kifejezésben véges sok generátorelemet használhatunk csak föl.

6.1.7. Az 6.1.6. Gyakorlat miatt azt kell belátni, hogy $\sqrt{6}$ kifejezhető racionális számokkal, $\sqrt{3}$-mal, valamint $\sqrt{2} + \sqrt{3} + 1$-gyel, a négy alapműveletet felhasználva. Például $\sqrt{6} = \sqrt{3}\bigl((\sqrt{2} + \sqrt{3} + 1) - 1\bigr)$ egy ilyen előállítás.

A második állítás igazolásához (a 6.1.6. Gyakorlat (3) miatt) elég észrevenni, hogy $\sqrt{2} = \bigl(\sqrt[6]{2}\bigr)^3$, $\sqrt[3]{2} = \bigl(\sqrt[6]{2}\bigr)^2$, végül $\sqrt[6]{2} = \sqrt{2}\big/\sqrt[3]{2}$.

6.1.8. A (2) és (3) következik a 6.1.6. Gyakorlat (3) állításából. Az (1) bizonyításához elég belátni, hogy $\bigl(K(\alpha)\bigr)(\beta) = K(\alpha, \beta)$. Mivel α, β elemei, K pedig része $\bigl(K(\alpha)\bigr)(\beta)$-nak, ezért $K(\alpha, \beta) \subseteq \bigl(K(\alpha)\bigr)(\beta)$. Megfordítva, $K(\alpha)$ része a $K(\alpha, \beta)$ testnek, β pedig eleme, és így $\bigl(K(\alpha)\bigr)(\beta) \subseteq K(\alpha, \beta)$.

6.1.10. Azt kell meggondolni, hogy az ilyen p/q alakú törtek testet alkotnak, amely az összes α_i elemet és K-t is tartalmazza, továbbá hogy ha egy $M \leq L$ test tartalmazza K-t és az összes α_i elemet, akkor a szóban forgó p/q törteket is.

6.1.15. Az α szám $\mathbb{Q}$ fölötti minimálpolinomja $x^3 + 3x + 1$. Ehhez a 6.1.13. Tétel miatt elég belátni, hogy ez a polinom irreducibilis $\mathbb{Q}$ fölött. Ez következik abból, hogy a polinom harmadfokú, és a racionális gyökteszt (3.3.10. Tétel) miatt nincs racionális gyöke (3.3.4. Állítás).

Mivel $\alpha^3 + 3\alpha + 1 = 0$, innen α^2-tel szorozva $\alpha^5 + 3\alpha^3 + \alpha^2 = 0$. Ebből kifejezhetjük α^5-t, és így $\alpha^5 + 2\alpha^3 = -3\alpha^3 - \alpha^2 + 2\alpha^3 = -\alpha^3 - \alpha^2$. Az $\alpha^3 + 3\alpha + 1 = 0$ összefüggésből α^3 is kifejezhető, és így

a végeredmény $\alpha^5 + 2\alpha^3 = -\alpha^2 + 3\alpha + 1$. Látható, hogy α valamennyi polinomja redukálható legfeljebb másodfokúvá úgy, hogy a legmagasabb fokú tagot mindig alacsonyabb fokúakkal fejezzük ki.

Az $\alpha/(\alpha - 3)$ kiszámítása a 6.1.3. Gyakorlathoz hasonló: az eredményt $a + b\alpha + c\alpha^2$ alakban keressük, keresztbe szorzunk, nullára redukálunk, az α kapott polinomját redukáljuk legfeljebb másodfokúvá az előző bekezdésben látott módszerrel, majd az együtthatókat nullává tesszük, és a kapott lineáris egyenletrendszert megoldjuk a, b, c-re. Az eredmény:

$$\alpha/(\alpha - 3) = (1/37) - (9/37)\alpha - (3/37)\alpha^2 .$$

Számítógéppel kiszámolható, hogy α közelítőleg $-0{,}322185$. A `Maple` programban az

```
evalf(solve(x^3+3*x+1=0, x));
```

parancsot érdemes használni. Így a fenti eredmények e szám behelyettesítésével (közelítőleg) ellenőrizhetők.

6.1.19. Ha $K = L$, akkor L-ben például az 1 elem bázist alkot K fölött, tehát a bővítés foka 1. Megfordítva, ha az L dimenziója K fölött 1, akkor van egy elemből álló $\{\alpha\}$ bázisa. Ekkor $k\alpha$ alakban (ahol $k \in K$) előáll L minden eleme, speciálisan az 1 is. De $k\alpha = 1$-ből $\alpha \in K$ következik, és így α minden K-beli többszöröse K-ban van. Tehát $L = K$.

Ha $\alpha \in L$ elsőfokú K fölött, akkor minimálpolinomja $x - k$ alakú alkalmas $k \in K$-ra. Ennek α gyöke, és így $\alpha = k \in K$. Megfordítva, ha $\alpha \in K$, akkor a K fölötti minimálpolinomja $x - \alpha \in K[x]$ (mert ez irreducibilis), tehát α elsőfokú.

6.1.21. A hányadostest konstrukciója (vagyis az 5.7.2. Tétel bizonyítása) alapján azt kell belátni, hogy $f(x)/g(x) = u(x)/v(x)$ pontosan akkor igaz, ha $f(\alpha)/g(\alpha) = u(\alpha)/v(\alpha)$ tetszőleges $f, g, u, v \in K[x]$ esetén, ahol $g, v \neq 0$. (Ekkor $g(\alpha)$ és $v(\alpha)$ sem nulla, mert α transzcendens, tehát e törtek értelmesek.) Keresztbe szorozva a bizonyítandó állítás az, hogy $f(x)v(x) - u(x)g(x) = 0$ akkor és csak akkor, ha $f(\alpha)v(\alpha) - u(\alpha)g(\alpha) = 0$. Ez nyilvánvaló, hiszen α transzcendens, és így csak akkor lehet gyöke az $fv - ug$ polinomnak, ha az a nullapolinom.

♫ Az állítást kihozhatjuk a hányadostest egyértelműségét leíró 5.7.4. Tételből is. Csak azt kell belátni, hogy az $f(x) \leftrightarrow f(\alpha)$ megfeleltetés izomorfizmus $K[x]$ és az L test megfelelő részgyűrűje között. Ez következik a homomorfizmustételből, ha azt az „α behelyettesítése" nevű homomorfizmusra alkalmazzuk (5.10.7. Gyakorlat), hiszen α transzcendenciája azt fejezi ki, hogy ennek a magja nulla.

6.1.22. Az állítást n szerinti indukcióval bizonyítjuk (az $n = 0$ eset nyilvánvaló). A 6.1.8. Gyakorlathoz hasonlóan láthatjuk, hogy $K(\alpha_1, \ldots, \alpha_n) = M(\alpha_n)$, ahol $M = K(\alpha_1, \ldots, \alpha_{n-1})$. Az α_n algebrai M fölött is (hiszen K fölötti minimálpolinomja M-beli együtthatós). Ezért a 6.1.16. Tétel miatt $M(\alpha_n)$ elemei az α_n szám M-beli együtthatós polinomjai. Ezek az M-beli együtthatók az indukciós föltevés alapján az $\alpha_1, \ldots, \alpha_{n-1}$ elemek K-beli együtthatós polinomjai.

Végtelen sok generátor esetén az állítás érvényben marad, ekkor a generátorok összes K-beli együtthatós polinomjait kell tekinteni, de persze mindegyik polinomban csak véges sok generátor szerepelhet.

6.1.23. Ha $\alpha \cdot 1 + \beta \cdot i + \gamma \cdot (\sqrt{2} + 3i) = 0$, ahol $\alpha, \beta, \gamma \in \mathbb{Q}$, akkor e szám valós és képzetes része is nulla kell, hogy legyen, azaz $\alpha + \gamma\sqrt{2} = 0$ és $\beta + 3\gamma = 0$. Az első összefüggés csakis $\gamma = 0$ esetén állhat fenn, mert különben $\sqrt{2} = -\alpha/\gamma$ racionális szám lenne. Innen persze $\alpha = 0$, és a második egyenletből $\beta = 0$. Az (1) pontban megadott rendszer tehát független $\mathbb{Q}$ fölött.

Ugyanez a halmaz $\mathbb{R}$ fölött garantáltan nem független, hiszen $\mathbb{C}$ dimenziója $\mathbb{R}$ fölött 2, és így három független elem nem létezik. A (2) esetben tehát nemleges a válasz.

Végül a (3)-ban megadott rendszer is független. Ha $\alpha \cdot 1 + \beta \cdot \pi + \gamma \cdot (1/\pi) = 0$, akkor π-vel szorozva $\beta\pi^2 + \alpha\pi + \gamma = 0$. Ez racionális α, β, γ esetén csak úgy lehet, ha mindhárom nulla, mert különben π gyöke lenne a $\beta x^2 + \alpha x + \gamma \in \mathbb{Q}[x]$ nem nulla polinomnak, és így nem lenne transzcendens szám.

6.1.24. Tudjuk elemi számelméletből, hogy $\sqrt{2}$, $\sqrt{3}$ és $\sqrt{6}$ irracionális számok. De tudjuk onnan is, hogy például a $\sqrt{2}$ másodfokú $\mathbb{Q}$ fölött (hiszen a minimálpolinomja $x^2 - 2$), és ezért a $\mathbb{Q}(\sqrt{2})$ elemei egyértelműen állnak elő $u + v\sqrt{2}$ alakban, ahol $u, v \in \mathbb{Q}$ (és így persze $\sqrt{2} \notin \mathbb{Q}$). Tegyük föl, hogy $\sqrt{3} = u + v\sqrt{2}$ teljesül. Négyzetre emelve $3 = u^2 + 2v^2 + 2uv\sqrt{2}$. Innen $uv\sqrt{2} \in \mathbb{Q}$. Ha tehát u és v egyike sem nulla,

akkor $\sqrt{2} \in \mathbb{Q}$, ami nem igaz. Ha $v = 0$, akkor $\sqrt{3} = u \in \mathbb{Q}$, szintén ellentmondás. Végül ha $u = 0$, akkor $\sqrt{3} = v\sqrt{2}$, ahonnan $\sqrt{2}$-vel szorozva $\sqrt{6} = 2v \in \mathbb{Q}$, ami úgyszintén lehetetlen. Ezért $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. A most látott gondolatmenetet a 6.1.26. Feladatban általánosítjuk.

6.1.25. A $c = \sqrt{2} + \sqrt{3}$ megfelelő. Nyilván $c \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, kérdés, hogy $\sqrt{2}$ és $\sqrt{3}$ kifejezhető-e c-vel és racionális számokkal. Mivel $c^2 = 5 + 2\sqrt{6}$, ezért $\sqrt{6} \in \mathbb{Q}(c)$. Továbbá $c^3 = 2\sqrt{2} + 3\sqrt{3} + 3\sqrt{6}c$, ezért innen $d = 2\sqrt{2} + 3\sqrt{3} \in \mathbb{Q}(c)$. De akkor $\sqrt{3} = d - 2c \in \mathbb{Q}(c)$, és így $\sqrt{2} = c - \sqrt{3} \in \mathbb{Q}(c)$.

♫ Az előzőnél egyszerűbb megoldás is van:

$$\frac{1}{c} = \frac{1}{\sqrt{3} + \sqrt{2}} = \frac{\sqrt{3} - \sqrt{2}}{\sqrt{3}^2 - \sqrt{2}^2} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}(c)\,.$$

De $\sqrt{3} + \sqrt{2}$ és $\sqrt{3} - \sqrt{2}$ segítségével nyilván kifejezhető $\sqrt{2}$ és $\sqrt{3}$ is. Ez persze véletlen szerencse, a fenti módszer általánosabb. Megjegyezzük, hogy a $\sqrt{2} + k\sqrt{3}$ számok, ahol $k \in \mathbb{Q}$, véges sok kivétellel mind generálják a bővítést (lásd a 6.3.8. Tétel bizonyítását). Sőt, a Galois-elmélet főtételéből az is következik, hogy valójában $k = 0$ az egyetlen kivétel (6.5.15. Gyakorlat).

6.1.26. A $K(\sqrt{c})$ elemei $u + v\sqrt{c}$ alakúak, ahol $u, v \in K$. (Ez akkor is igaz, ha $\sqrt{c} \in K$, csak akkor ez az előállítás nem egyértelmű.) Speciálisan $\sqrt{b} = u + v\sqrt{c}$, négyzetre emelve $b = u^2 + cv^2 + 2uv\sqrt{c}$. Innen $uv\sqrt{c} \in K$. Ha tehát u és v egyike sem nulla, akkor $\sqrt{c} \in K$, de akkor $\sqrt{b} \in K$ is teljesül. Ha $v = 0$, akkor $\sqrt{b} = u \in K$. Végül ha $u = 0$, akkor $\sqrt{b} = v\sqrt{c}$, ahonnan $\sqrt{c}$-vel szorozva $\sqrt{bc} = vc \in K$.

6.1.27. Az (1)-et n szerinti indukcióval bizonyítjuk. Ha $n = 0$, akkor $\sqrt{b} \in \mathbb{Q}$. Elemi számelméletből tudjuk, hogy ez csak $b = 1$ esetén lehetséges (hiszen egy egyszerűsíthetetlen tört akkor és csak akkor egy racionális szám négyzete, ha pozitív, és a számlálójában és a nevezőjében is minden prímszám páros kitevőn szerepel). Tehát $n = 0$ esetén (1) igaz.

Tegyük föl, hogy az állítás igaz $n-1$-re. Legyen $K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. Ekkor $\sqrt{b} \in K(\sqrt{p_n})$, tehát a 6.1.26. Feladat miatt vagy $\sqrt{b} \in K$, vagy $\sqrt{bp_n} \in K$. Ha $\sqrt{b} \in K$, akkor az indukciós föltevés miatt készen vagyunk. Tegyük föl, hogy $\sqrt{bp_n} \in K$. Ha a bp_n szám négyzetmentes, akkor erre az indukciós föltevést alkalmazva azt kapjuk, hogy csak $p_1, \ldots, p_{n-1}$ szerepelhet benne. De akkor b is fölírható a $p_1, \ldots, p_n$ prímek segítségével. Ha bp_n nem négyzetmentes, akkor b számlálójában szerepel a p_n prím. Ebben az esetben b/p_n négyzetmentes, és $\sqrt{b/p_n} = \sqrt{bp_n}/p_n \in K$. Ezért az indukciós feltevést most a b/p_n számra alkalmazhatjuk. Ezzel az (1) állítást beláttuk.

Ebből (2) azonnal következik, ha (1)-et n helyett $n-1$-re és $b = p_n$-re alkalmazzuk.

Végül (3) igazolásához tegyük föl, hogy $q_1\sqrt{p_1} + \ldots + q_n\sqrt{p_n} = 0$ alkalmas q_i racionális számokra. Ha ez a lineáris kombináció nemtriviális, akkor a prímeket átindexelve feltehető, hogy $q_n \neq 0$. De akkor $\sqrt{p_n} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$, ami ellentmond a (2) állításnak.

6.2. A szorzástétel és következményei

6.2.1. Az $\mathbb{R}$ fölötti függetlenség bizonyításához tegyük föl, hogy

$$c_1b_1 + d_1ib_1 + c_2b_2 + d_2ib_2 + \ldots + c_nb_n + d_nib_n = 0\,,$$

ahol $c_1, \ldots, c_n, d_1, \ldots, d_n \in \mathbb{R}$. Ez az összefüggés a $z_j = c_j + id_j$ jelöléssel a $z_1b_1 + \ldots + z_nb_n = 0$ alakban írható. A $\mathbb{C}$ fölötti függetlenség miatt innen mindegyik $z_j = 0$. Tehát z_j valós és képzetes része, azaz c_j és d_j is nulla, és így a függetlenséget beláttuk.

Most megmutatjuk, hogy $\mathbb{R}$ fölött generátorrendszert kaptunk. Tetszőleges $v \in V$ vektor fölírható $v = z_1b_1 + \ldots + z_nb_n$ alakban, ahol $z_j \in \mathbb{C}$. Legyen $z_j = c_j + id_j$, ahol $c_j, d_j \in \mathbb{R}$. Az előző bekezdésbeli átalakítást fordított irányban végezve

$$v = c_1b_1 + d_1ib_1 + c_2b_2 + d_2ib_2 + \ldots + c_nb_n + d_nib_n$$

adódik.

6.2.6. Ha $f(\alpha) = 0$, ahol $f \in K[x]$, akkor α minimálpolinomja osztója f-nek (6.1.13. Tétel), és így foka, ami az α foka is egyben, legfeljebb akkora, mint az f foka. Oszthatóság viszont általában nem áll fenn, hiszen α minimálpolinomját bármilyen polinommal megszorozva olyan polinomhoz jutunk, amelynek α gyöke. Például az $\alpha = \sqrt[3]{2}$ elemről már láttuk, hogy minimálpolinomja $x^3 - 2$, de persze gyöke az $(x^3 - 2)(x - 79)$ negyedfokú racionális együtthatós polinomnak is, és $3 \nmid 4$.

6.2.7. A $\sqrt[4]{2}$ foka $\mathbb{Q}$ fölött 4, hiszen gyöke az $x^4 - 2$ polinomnak, ami a Schönemann–Eisenstein-kritérium (3.5.2. Tétel) miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a minimálpolinom (a 6.1.13. Tétel (4) állítása miatt). Ugyanez a gondolatmenet mutatja, hogy $\sqrt{2}$ foka $\mathbb{Q}$ fölött 2, és így a $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$ bővítés foka is 2 (a 6.1.20. Következmény szerint).

A $\sqrt[4]{2}$ gyöke az $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ polinomnak is, és így foka $\mathbb{Q}(\sqrt{2})$ fölött legfeljebb 2 lehet (az előző 6.2.6. Gyakorlat miatt). Ennél kevesebb nem lehet, mert ha 1 lenne, akkor $\sqrt[4]{2} \in \mathbb{Q}(\sqrt{2})$ teljesülne (6.1.19. Gyakorlat). Ez lehetetlen: a $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$ bővítés másodfokú, nem lehet negyedfokú eleme, mert elem foka osztója a bővítés fokának (6.2.4. Állítás).

6.2.9. Legyen ε primitív harmadik egységgyök. Az $\alpha = \varepsilon\sqrt[3]{2}$ szám gyöke az $x^3 - 2$ polinomnak, amely irreducibilis $\mathbb{Q}$ fölött, ezért α foka $K = \mathbb{Q}$ fölött 3. Ha $L = \mathbb{Q}(\sqrt[3]{2})$, akkor $x^3 - 2$ felbomlik L fölött a következőképpen:

$$x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}\right).$$

Az α a másodfokú tényezőnek lesz gyöke, és így foka L fölött legfeljebb 2. De ez a fok nem 1, mert L elemei valós számok, α pedig nem valós komplex szám, tehát $\alpha \notin L$. Ezért α foka L fölött 2. Így ez jó példa, hiszen $2 \nmid 3$.

6.2.11. A 6.1.8. Gyakorlat szerint $K(\alpha, \beta) = K(\alpha)(\beta)$, jelölje k ennek a testnek a K fölötti fokát. A 6.2.10. 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

$$|K(\alpha, \beta) : K(\alpha)| = \frac{|K(\alpha, \beta) : K|}{|K(\alpha) : K|} = \frac{mn}{m} = n\,.$$

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.

6.2.14. Az ilyen alakú számok a $\mathbb{Q}$ fölött harmadfokú $\mathbb{Q}(\sqrt[3]{2})$ testet alkotják. E bővítés minden elemének foka osztója háromnak. De a $\sqrt[6]{2}$ foka $\mathbb{Q}$ fölött 6, mert a Schönemann–Eisenstein miatt $x^6 - 2$ polinom irreducibilis $\mathbb{Q}$ fölött. Tehát sem ez a szám, sem a másodfokú $\sqrt{2}$ nem írható föl a kívánt alakban.

♫ Jegyezzük meg, hogy sok harmadfokú szám van, ami szintén nem írható föl ilyen alakban, ilyen például az $x^3 - 2$ polinom két nem valós gyöke.

6.2.15.

(1) Tekintsük a $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ testláncot. Megmutatjuk, hogy mindkét bővítés foka 2, és így az eredmény 4 lesz. Valóban, $\mathrm{gr}_{\mathbb{Q}}(\sqrt{2}) = 2$, hiszen $x^2 - 2$ irreducibilis $\mathbb{Q}$ fölött. A második bővítés esetében azt kell megvizsgálnunk, hogy $x^2 - 3$ irreducibilis-e $\mathbb{Q}(\sqrt{2})$ fölött. Ha nem lenne az, akkor másodfokú lévén mindkét gyöke benne lenne $\mathbb{Q}(\sqrt{2})$-ben. Ez azonban ellentmond a 6.1.24. Gyakorlatnak.

♫ Hiába tudjuk a 6.1.25. Feladatból, hogy $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, ez nem segít a fokszám meghatározásában. Ahhoz ugyanis, hogy $\sqrt{2} + \sqrt{3}$ negyedfokú, az $x^4 - 10x^2 + 1$ irreducibilitását kellene ellenőriznünk (3.3.24. Feladat).

(2) A 6.2.11. Gyakorlat miatt a válasz $2 \cdot 3 = 6$, mert $\mathrm{gr}_{\mathbb{Q}}(\sqrt{2}) = 2$ és $\mathrm{gr}_{\mathbb{Q}}(\sqrt[3]{2}) = 3$ relatív prímek. A $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$ összefüggést is felhasználhattuk volna (6.1.7. Gyakorlat).

(3) A bővítés foka legfeljebb 6, hiszen $\mathbb{Q}(\sqrt{2}\sqrt[3]{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, és ez utóbbi a 6.2.11. Gyakorlat miatt hatodfokú $\mathbb{Q}$ fölött, hiszen $(2, 3) = 1$. Ugyanakkor ha $\alpha = \sqrt{2}\sqrt[3]{3}$, akkor $\alpha^3 = 6\sqrt{2} \in \mathbb{Q}(\alpha)$, és $\alpha^4 = 12\sqrt[3]{3} \in \mathbb{Q}(\alpha)$, ezért a $\mathbb{Q}(\alpha)$ bővítésnek van másod- és harmadfokú eleme is, azaz $[2, 3] = 6$ osztója $|\,\mathbb{Q}(\alpha) : \mathbb{Q}\,|$-nak, és így a végeredmény 6. Menet közben beláttuk, hogy $\mathbb{Q}(\sqrt{2}\sqrt[3]{3}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$

(4) Az eredmény 4 a 6.2.11. Gyakorlat (2) pontja miatt, mert $(3, 4) = 1$.

(5) A 6.2.7. Gyakorlatban láttuk, hogy $\sqrt[4]{2}$ foka $\mathbb{Q}(\sqrt{2})$ fölött 2. De $\sqrt{8} = 2\sqrt{2}$ miatt $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{8})$, és így a válasz a 2.

(6) Az i nem eleme a $\mathbb{Q}(\sqrt[4]{2})$ testnek, mert ez valós számokból áll, az i pedig nem valós. Ezért az i foka $\mathbb{Q}(\sqrt[4]{2})$ fölött legalább kettő (6.1.19. Gyakorlat). Másrészt i gyöke a másodfokú $x^2+1 \in \mathbb{Q}(\sqrt[4]{2})[x]$ polinomnak, és így foka legfeljebb kettő. Ezért a válasz a kérdésre 2.

(7) Alkalmazzuk a $\mathbb{Q} \leq \mathbb{Q}(\sqrt[4]{2}) \leq \mathbb{Q}(\sqrt[4]{2}, i)$ testláncra a (6)-ra adott választ és a szorzástételt. Azt kapjuk, hogy $\mathbb{Q}(\sqrt[4]{2}, i)$ a $\mathbb{Q}$-nak nyolcadfokú bővítése. De akkor, ismét a szorzástétel miatt, $\sqrt[4]{2}$ foka 4 lesz $\mathbb{Q}(i)$ fölött, csak most a $\mathbb{Q} \leq \mathbb{Q}(i) \leq \mathbb{Q}(\sqrt[4]{2}, i)$ testláncot kell tekinteni.

(8) Vegyük észre, hogy $\mathbb{Q}(\sqrt{2})(\sqrt{2}+\sqrt[4]{2}) = \mathbb{Q}(\sqrt{2})(\sqrt[4]{2})$ (6.1.8. Gyakorlat). Ezért az eredmény ebben az esetben is 2.

(9) Legyen $\alpha = \sqrt{2}+\sqrt[4]{2}$. A $\sqrt{2}$-t a túloldalra átvíve és négyzetre emelve $\alpha^2 - 2\sqrt{2}\alpha + 2 = \sqrt{2}$. Innen $\alpha^2+2 = \sqrt{2}(2\alpha+1)$. Ismét négyzetre emelve $\alpha^4-4\alpha^2-8\alpha+2 = 0$, ami a Schönemann–Eisenstein miatt irreducibilis. Ezért α negyedfokú $\mathbb{Q}$ fölött.

(10) Az eredmény 2. Nyilván $\sqrt{\pi}$ gyöke az $x^2 - \pi \in \mathbb{Q}(\pi)$ polinomnak, azt kell belátni, hogy $\sqrt{\pi} \notin \mathbb{Q}(\pi)$. Tegyük föl az ellenkezőjét, akkor $\sqrt{\pi}\,g(\pi) = f(\pi)$ teljesül alkalmas $f, g \in \mathbb{Q}[x]$ nem nulla polinomokra a 6.1.9. Tétel miatt. Négyzetre emelve kapjuk, hogy az $f^2(x) - xg^2(x) \in \mathbb{Q}[x]$ polinomnak gyöke a π. Ez nem a nullapolinom, hiszen $f^2(x)$ foka páros, $xg^2(x)$ foka páratlan, ami ellentmond annak, hogy π transzcendens szám.

♫ Azt, hogy $x^2 - \pi$ irreducibilis $\mathbb{Q}(\pi)$ fölött, a Schönemann–Eisenstein általánosított változatából is megkaphatjuk (5.7.9. Gyakorlat). Csak azt kell észrevenni, hogy $\mathbb{Q}(\pi)$ izomorf a $\mathbb{Q}[x]$ hányadostestével (6.1.21. Gyakorlat), és hogy $\mathbb{Q}[x]$-ben az x prím.

6.2.16. A 6.1.27. Feladat (2) pontja szerint $\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$, és így $\sqrt{p_n}$ foka e test fölött csak 2 lehet. Ezért n szerinti indukcióval, a szorzástételt alkalmazva látjuk, hogy az eredmény 2^n.

6.2.17. Mivel i algebrai, ha a és b algebrai, akkor $a + bi$ is az, hiszen az algebrai számok testet alkotnak (6.2.12. Tétel). Megfordítva, tegyük föl, hogy $z = a+bi$ algebrai. Ekkor z gyöke egy racionális együtthatós nem nulla f polinomnak. Ennek $\overline{z} = a - bi$ is gyöke (a 3.3.6. Lemma miatt, hiszen f valós együtthatós). De a és b kifejezhető $a + bi$-vel, $a - bi$-vel és i-vel: $a = (z + \overline{z})/2$ és $b = (z - \overline{z})/2i$, és ezért a és b algebrai számok.

6.2.18. Ha $\alpha = \pi + 3$ algebrai lenne, akkor $\alpha - 3 = \pi$ is az lenne, hiszen az algebrai számok testet alkotnak, ami ellentmondás. Hasonlóan látható, hogy $5\pi + 6$ és $\pi + \sqrt{2}$ sem lehet algebrai. Ha $\sqrt{\pi}$ algebrai lenne, akkor négyzete is, ez sem lehet. Végül belátjuk, hogy π semmilyen racionális együtthatós, nem konstans polinomja sem lehet algebrai. Ha ugyanis $g(\pi)$ algebrai lenne, azaz gyöke lenne egy racionális együtthatós $f \neq 0$ polinomnak, akkor $f\big(g(\pi)\big) = 0$, azaz π gyöke lenne a racionális együtthatós, nem nulla $f\big(g(x)\big)$ polinomnak.

6.2.19. Ha α algebrai és β transzcendens, akkor $\gamma = \alpha + \beta$ transzcendens, mert ha γ algebrai lenne, akkor $\gamma - \alpha = \beta$ is az lenne, hiszen az algebrai számok testet alkotnak. Hasonlóan látjuk, hogy egy nem nulla algebrai szám és egy transzcendens szám szorzata mindig transzcendens. Ugyanígy egy transzcendens szám

n-edik hatványa és n-edik gyöke is transzcendens, minden $n > 0$ egészre (hiszen egy algebrai szám gyökei és hatványai algebraiak, lásd 6.2.5. Állítás, 6.2.12. Tétel).

6.2.20. A $\mathbb{Q}$ minden algebrailag zárt L bővítése tartalmazza az $x^n - 2$ polinom egy gyökét. Ez a polinom irreducibilis $\mathbb{Q}$ fölött a Schönemann–Eisenstein-kritérium miatt, és így ez a gyök n-edfokú eleme L-nek. Emiatt a $K \leq L$ bővítés foka minden n egész számnál nagyobb vagy egyenlő, és így csakis végtelen lehet.

6.2.21. Ilyen a $\mathbb{Q} \leq \mathbb{A}$ bővítés (ahol $\mathbb{A}$ az algebrai számok teste).

6.2.22. Ha $K \leq L$ és $L \leq M$ algebrai bővítések és $\alpha \in M$, akkor bővítsük K-t az α elem L fölötti minimálpolinomjának együtthatóival. A kapott $N \leq L$ test véges bővítése K-nak, mert véges sok algebrai elemmel bővítettünk. De α algebrai N fölött, ezért $K \leq N(\alpha)$ véges, vagyis α algebrai K fölött.

6.3. Normális bővítések

6.3.1. A $\mathbb{Q}(\sqrt[3]{2}, \varepsilon\sqrt[3]{2}, \varepsilon^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ egyenlőség a 6.1.6. Gyakorlat miatt teljesül, hiszen a szereplő elemek egymással nyilvánvalóan kifejezhetők. A $\sqrt[3]{2}$ harmadfokú, az ε viszont másodfokú $\mathbb{Q}$ fölött, hiszen a minimálpolinomja a $\Phi_3(x) = x^2 + x + 1$ körosztási polinom. (Ennek irreducibilitásához nem kell használni a 3.9.9. Tételt, elegendő észrevenni, hogy $x^2 + x + 1$ másodfokú, de nincs valós gyöke.) Mivel 2 és 3 relatív prímek, a $|\,\mathbb{Q}(\sqrt[3]{2}, \varepsilon) : \mathbb{Q}\,|$ bővítés hatodfokú a 6.2.11. Gyakorlat miatt.

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, lásd 6.2.6. Gyakorlat). 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.

6.3.7. Az Útmutatóban bevezetett jelöléseket használjuk. Mivel s_i irreducibilis K fölött, $K \leq L$ pedig normális bővítés, mindegyik s_i polinom összes gyöke L-ben van. Ezért f is gyöktényezőkre bomlik L fölött. Az f gyökei között szerepel mindegyik α_i, és ezek már generálják L-et K fölött. Tehát f összes gyöke is az L testet generálja.

6.3.12. Az $x^4 - 2$ gyökeit úgy kapjuk, hogy a $\sqrt[4]{2}$-t végigszorozzuk a negyedik egységgyökökkel (1.5.4 Tétel), azaz ± 1-gyel és $\pm i$-vel. Így $x^4 - 2$ felbontási teste $\mathbb{Q}$ fölött $\mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$ a 6.1.6. Gyakorlat miatt. Ez nyolcadfokú $\mathbb{Q}$ fölött (lásd 6.2.15. Gyakorlat, (6) és (7) kérdés).

6.3.13. Legyen ε egy n-edik primitív egységgyök, ez gyöke az $x^n - 1$ és a $\Phi_n(x)$ polinomoknak. A 3.9.9. Tétel miatt a $\Phi_n(x)$ körosztási polinom irreducibilis $\mathbb{Q}$ fölött, és így ez az ε minimálpolinomja. Tehát a $\mathbb{Q} \leq \mathbb{Q}(\varepsilon)$ bővítés foka $\varphi(n)$. Az $x^n - 1$ és a $\Phi_n(x)$ gyökei ε-nak hatványai, és ezért benne vannak a $\mathbb{Q}(\varepsilon)$ bővítésben. Így $\mathbb{Q}(\varepsilon)$ e polinomok közös felbontási teste $\mathbb{Q}$ fölött.

6.3.14. Az eredmények a következők.

(1) A felbontási test a 6.3.12. Gyakorlathoz hasonlóan $\mathbb{Q}(\sqrt[6]{2}, \eta)$, ahol η primitív hatodik egységgyök. Ennek foka 2 lesz $\mathbb{Q}(\sqrt[6]{2})$ fölött, mert gyöke a másodfokú $\Phi_6(x) = x^2 - x + 1$ polinomnak, de nem valós szám, és így nem elsőfokú e test fölött. Ezért a keresett fokszám fokszám $6 \cdot 2 = 12$.

(2) A felbontási test $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, hiszen $(x^2 - 2)(x^2 - 3)$ gyökei $\pm\sqrt{2}$ és $\pm\sqrt{3}$. A 6.2.15. Gyakorlat (1) pontja szerint ez $\mathbb{Q}$-nak negyedfokú bővítése.

(3) A felbontási test $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \varepsilon)$, ahol ε primitív harmadik egységgyök. Ez $\mathbb{Q}$-nak 12 fokú bővítése, hiszen $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$ hatodfokú. Megjegyezzük, hogy ugyanazt a testet kaptuk, mint az (1) pontban, hiszen a harmadik és a hatodik primitív egységgyökök egymás ellentettjei, tehát ugyanazt a bővítést generálják.

6.3.15. Tegyük föl, hogy $K \leq L$ és $|L : K| = 2$. Legyen $\alpha \in L - K$. Ekkor α másodfokú K fölött, jelölje s a minimálpolinomját. Az s egyik gyöke L-ben van, ezért ez a minimálpolinom két elsőfokú tényezőre bomlik L fölött. Tehát L a felbontási teste s-nek K fölött, és így normális bővítése K-nak. Ezzel az első állítást beláttuk.

(Ha s másik L-beli gyöke β, akkor a gyökök és együtthatók összefüggése miatt $\alpha+\beta \in K$, és így $\beta \in L$. Ez a fenti gondolatmenet egy módosítása.)

♫ Megjegyezzük, hogy a 6.3.4. Tétel állítása másodfokú bővítés esetén nyilvánvaló. Valóban, ha f irreducibilis K fölött, és van L-ben egy α gyöke, akkor f az α minimálpolinomjának konstansszorosa, és az előbbi gondolatmenetek bármelyike szerint f másik gyöke is L-beli.

Tegyük most föl, hogy K karakterisztikája nem 2, és (a fenti jelöléseket használva) $s(x) = x^2 + bx + c$. A 3.7.9. Gyakorlat szerint $(\alpha-\beta)^2 = b^2 - 4c \in K$. Ha d jelöli a b^2-4c elemet (ami az s diszkriminánsa), akkor $\sqrt{d} = \alpha - \beta \in L$. Annak igazolásához, hogy $K(\sqrt{d}) = L$, elég belátni, hogy $\sqrt{d} \notin K$. Ez világos az 5.8.12. Gyakorlatból, hiszen a karakterisztika nem 2, és ezért a másodfokú egyenlet gyökei a gyökképletből megkaphatók ($\alpha, \beta = (-b \pm \sqrt{d})/2 \in L$). Márpedig α-ról föltettük, hogy nem eleme K-nak, és ezért $\sqrt{d}$ sem lehet eleme.

6.3.16. A 6.3.7. Feladat szerint minden véges normális bővítés egy alkalmas polinom felbontási teste. Így van olyan $f \in K[x]$ polinom, hogy M az f felbontási teste K fölött. De akkor az M az f-nek felbontási teste L fölött is, és így az $L \leq M$ bővítés is normális. Megjegyezzük, hogy az állítás igaz akkor is, ha nem tesszük föl a bővítések végességét (lásd 6.4.21. Feladat).

6.3.17. Legyenek f összes gyökei $\alpha_1, \ldots, \alpha_m$, ekkor tehát $M = L(\alpha_1, \ldots, \alpha_m)$. A 6.3.7. Feladat szerint minden véges normális bővítés egy alkalmas polinom felbontási teste, azaz van olyan $g \in K[x]$ polinom, hogy L a g felbontási teste K fölött. Ekkor M az fg felbontási teste K fölött, hiszen fg gyökei az f és g gyökei együttvéve, a g gyökei K fölött az L-et generálják, és az f gyökeit még hozzávéve M-et kapjuk. Ezért M felbontási test K fölött, és így normális bővítése K-nak.

Két normális bővítés egymásutánja általában nem lesz normális. Például a $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt[4]{2})$ bővítésláncban a két közbülső bővítés másodfokú, és így normális (6.3.15. Feladat). A nagy bővítés mégsem normális, mert a $\mathbb{Q}$ fölött irreducibilis x^4-2 polinomnak csak két gyökét tartalmazza (a $\pm\sqrt[4]{2}$ számokat igen, a másik két gyököt, azaz $\pm i\sqrt[4]{2}$-t viszont nem, mert ezek nem valósak).

6.4. Testbővítések konstrukciója

6.4.2. Az 5.2. szakaszban leírt reprezentánsrendszer az $a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ alakú polinomokból áll, ahol n az s foka és $a_0, \ldots, a_{n-1} \in K$. Mivel minden (s) szerinti mellékosztályban egyetlen ilyen polinom van, ezért a 6.4.1. Tételbeli izomorfizmus kölcsönösen egyértelmű megfeleltetést létesít e polinomok halmaza, és $K(\alpha)$ elemei között, ahol a fenti polinomnak $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ felel meg (hiszen a φ leképezés az $x \mapsto \alpha$ helyettesítés). Ez pedig pontosan azt jelenti, hogy $K(\alpha)$ elemei egyértelműen fölírhatók ebben az alakban.

6.4.11. Fogjuk föl az $L = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ testet $\mathbb{Q}(\sqrt[3]{2})(\varepsilon\sqrt[3]{2})$ alakúnak. Mivel $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ hatodfokú bővítése $\mathbb{Q}$-nak, a $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}\varepsilon)$ bővítés foka a szorzástétel miatt $6/3 = 2$. De

$$f(x) = x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}),$$

ezért $\varepsilon\sqrt[3]{2}$ gyöke az $s(x) = x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$ polinomnak. Sőt, s az $\varepsilon\sqrt[3]{2}$ minimálpolinomja $\mathbb{Q}(\sqrt[3]{2})$ fölött, hiszen az imént láttuk, hogy $\varepsilon\sqrt[3]{2}$ foka $\mathbb{Q}(\sqrt[3]{2})$ fölött 2, és s is másodfokú. Ezért $L = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ elemei egyértelműen írhatók $u + v\varepsilon\sqrt[3]{2}$ alakban, ahol $u, v \in \mathbb{Q}(\sqrt[3]{2})$.

Fogjuk most föl az $L = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ testet $\mathbb{Q}(\varepsilon\sqrt[3]{2})(\sqrt[3]{2})$ alakúnak. Az előbbi gondolatmenettel azt kapjuk, hogy $\sqrt[3]{2}$ másodfokú $\mathbb{Q}(\varepsilon\sqrt[3]{2})$ fölött, és minimálpolinomja

$$t(x) = x^2 + \varepsilon\sqrt[3]{2}x + \varepsilon^2\sqrt[3]{4}.$$

Ezért $L = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ elemei egyértelműen írhatók $u' + v'\sqrt[3]{2}$ alakban, ahol $u, v \in \mathbb{Q}(\varepsilon\sqrt[3]{2})$.

Mivel $\sqrt[3]{2}$ és $\varepsilon\sqrt[3]{2}$ közös $\mathbb{Q}$ fölötti minimálpolinomja x^3-2, a

$$\psi : a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + b\varepsilon\sqrt[3]{2} + c\varepsilon^2\sqrt[3]{4}$$

megfeleltetés izomorfizmus a $\mathbb{Q}(\sqrt[3]{2})$ és a $\mathbb{Q}(\varepsilon\sqrt[3]{2})$ testek között a 6.4.7. Állítás miatt (valójában pontosan ezt a konkrét izomorfizmust számoltuk ki példaként a 6.4.7. Állítás előtt). Természetesen $\psi(\sqrt[3]{2}) = \varepsilon\sqrt[3]{2}$. A feladatunk tehát csak annyi, hogy ezt a ψ leképezést kiterjesszük egy $\varphi : L \to L$ izomorfizmussá. A tervünk az, hogy ez a leképezés

$$\varphi : u + v\varepsilon\sqrt[3]{2} \mapsto \psi(u) + \psi(v)\sqrt[3]{2}$$

legyen, ahol $u, v \in \mathbb{Q}(\sqrt[3]{2})$. Hogyan ellenőrizhetnénk (számolás nélkül), hogy ez izomorfizmus lesz?

A megoldás kulcsa a következő. Ha ψ-t (együtthatónként) kiterjesztjük egy $\mathbb{Q}(\sqrt[3]{2})[x] \to \mathbb{Q}(\varepsilon\sqrt[3]{2})[x]$ izomorfizmussá, akkor az $s(x)$ polinom képe $t(x)$ lesz. Ez a 6.4.8. Izomorfizmuskiterjesztési tételben leírt szituáció, arról van szó, hogy $g + (s) \mapsto \psi(g) + (t)$ izomorfizmus a $\mathbb{Q}(\sqrt[3]{2})[x]/(s)$ és a $\mathbb{Q}(\varepsilon\sqrt[3]{2})[x]/(t)$ faktorgyűrűk között. Az első faktor $L = \mathbb{Q}(\sqrt[3]{2})(\varepsilon\sqrt[3]{2})$-vel, a második pedig $L = \mathbb{Q}(\varepsilon\sqrt[3]{2})(\sqrt[3]{2})$-vel izomorf a 6.4.1. Tételben megadott módon. Ezeket az izomorfizmusokat komponálva a kívánt φ leképezés adódik.

6.4.15. Tegyük föl, hogy K algebrailag zárt és $K \leq L$ algebrai bővítés. Legyen $\alpha \in L$ és s az α minimálpolinomja K fölött. Ekkor s irreducibilis K fölött, és mivel K algebrailag zárt, az s elsőfokú. Tehát $\alpha \in K$ (6.1.19. Gyakorlat), és így $K = L$. Beláttuk tehát, hogy L elsőfokú bővítése K-nak.

Megfordítva, tegyük föl, hogy K minden algebrai bővítése elsőfokú. Legyen $f \in K[x]$ irreducibilis polinom. Ekkor a 6.4.3. Tétel szerint létezik olyan $K \leq M$ bővítés, amelyben f-nek van egy α gyöke. Az $L = K(\alpha) \leq M$ egy algebrai bővítés, és így a feltétel szerint elsőfokú, azaz $\alpha \in K$. Ezért f maga is elsőfokú, és így K algebrailag zárt.

6.4.16. Mivel $K \leq L$ véges bővítés, generálható véges sok $\alpha_1, \ldots, \alpha_m$ algebrai elemmel. Legyen f ezen elemek K fölötti minimálpolinomjainak szorzata. Az f polinomnak L fölött létezik egy M felbontási teste a 6.4.5. Következmény miatt. A 6.3.17. Gyakorlat miatt $K \leq M$ is normális bővítés, ami nyilván véges.

6.4.17. A 6.3.8. Tétel bizonyítását kell általánosítani. Csak azt a két pontot emeljük ki, ahol külön meggondolnivaló van.

A bizonyításban szereplő $s(x)$ és $t(x)$ polinomokat gyöktényezők szorzatára bontottuk $\mathbb{C}$-ben. Most $\mathbb{C}$ helyett egy olyan $L \leq M$ testet kell használni, amelyre a $K \leq M$ bővítés normális, ilyen létezik a 6.4.16. Gyakorlat miatt.

Másodszor, szükségünk volt arra, hogy az irreducibilis t polinomnak nincs többszörös gyöke a $K \leq M$ bővítésben. Ez abból következik, hogy K tökéletes.

6.4.18. A 6.4.15. Gyakorlat szerint elég belátni, hogy L minden M algebrai bővítése elsőfokú. Mivel $K \leq L$ és $L \leq M$ algebrai, ezért a 6.2.22. Feladat miatt $K \leq M$ is algebrai. Legyen $\alpha \in M$, ekkor az α elem K fölötti minimálpolinomja gyöktényezők szorzatára bomlik L fölött a feltétel miatt. Ezért $\alpha \in L$, vagyis $L = M$.

6.4.19. Tegyük föl, hogy $K \leq M$ és M algebrailag zárt. Legyen L az M testben a K fölött algebrai elemek halmaza. Ez résztest a 6.2.12. Tétel miatt, és algebrai bővítése K-nak. Ha $f \in K[x]$ irreducibilis polinom, akkor M algebrai zártsága miatt f gyöktényezőkre bomlik M fölött, és persze a gyökök mind L-beliek. Ezért $K \leq L$ teljesíti a 6.4.18. Feladat feltételét, és így algebrailag zárt.

6.4.20. Az Útmutatóban leírtakat folytatjuk. Ha f szerepel h tényezői között, akkor N tartalmazza f gyökeit, legyenek ezek $\alpha_1, \ldots, \alpha_n$. Helyettesítsünk x_j^f helyébe α_j-t, így egy $\varphi : S \to N$ homomorfizmust kapunk. Ennél az I ideál $g_1, \ldots, g_k$ generátorai nullába mennek, hiszen ezek a generátorok éppen az f polinomok gyökei és együtthatói közötti összefüggéseket fejezik ki. A K minden elemét φ saját magába képzi, speciálisan az egységelemet is. A kapott $1 = 0$ ellentmondás bizonyítja, hogy I tényleg valódi ideál.

Az $M = R/J$ faktorgyűrű test az 5.3.12. Következmény miatt, megmutatjuk, hogy a $k + J$ mellékosztályok, ahol $k \in K$, a K-val izomorf résztestet alkotnak M-ben. Az világos, hogy $k \mapsto k + J$ egy $K \to M$ homomorfizmus, melyben az 1 elem képe nem nulla. Ezért ennek magja valódi ideálja K-nak. De a K test egyszerű gyűrű (5.3.2. Állítás), és így ez az ideál csak a nullából áll, vagyis K-t tényleg beágyaztuk M-be.

Ha $f \in K[x]$ normált, n-edfokú, irreducibilis polinom, akkor az Útmutató első bekezdésében írtak szerint az M test fölött az f gyökténye zők szorzatára bomlik, gyökei az $x_j^f + J$ elemek lesznek.

♫ Ez az utolsó mondat picit pontatlan. Valójában arról van szó, hogy f-et át kell vinnünk $M[x]$-be azzal az izomorfizmussal, amely a $k \in K$-hoz $k + J$-t rendeli. Ezen a fajta nehézségen azonban már úrrá lettünk a 6.4.3. Tétel bizonyításában, ezért most több részletet nem írunk, hanem K-t azonosítjuk az M megfelelő résztestével, ugyanúgy, mint akkor.

A megoldást a 6.4.18. Feladatra való hivatkozással fejezhetjük be, ehhez csak azt kell meggondolni, hogy a $K \leq M$ bővítés algebrai. Legyen L az M-ben a K fölött algebrai elemekből álló résztest. Az $x_j^f + J \in M$ elem gyöke f-nek, és így L-beli. De ezek generálják M-et K fölött (hiszen az R gyűrűt generálják K elemeivel együtt az x_j^f határozatlanok). Ezért $L = M$.

6.4.21. Tegyük föl, hogy az N testet az f_i polinomok gyökei generálják K fölött (ahol $N \leq L$ és $i \in I$). Legyen $f \in K[x]$ irreducibilis polinom, melynek egy α gyöke N-ben van. Ekkor α kifejezhető véges sok, mondjuk az $f_1, \ldots, f_m$ polinomok gyökeivel. Az $f_1 \ldots f_m$ szorzat felbontási teste része N-nek, és persze K-nak normális bővítése. Tartalmazza az α gyököt, és így az irreducibilis f többi gyökét is. Ezért f összes gyöke N-beli, azaz $K \leq N$ normális.

Megfordítva, ha $K \leq N$ normális, akkor vegyük minden $\alpha \in N$ esetén α minimálpolinomját K fölött. E polinomok összes gyökei N-beliek (hiszen mindegyik irreducibilis K fölött), és együttvéve az N testet generálják K fölött. Ezért tényleg minden normális bővítés egy polinomhalmaz felbontási teste lesz.

Végül ha $K \leq M$ normális bővítés és $K \leq L \leq M$, akkor az előzőek szerint M egy alkalmas polinomhalmaz felbontási teste K fölött. Ugyanennek a polinomhalmaznak M felbontási teste L fölött is, és így $L \leq M$ is normális bővítés.

6.4.22. A 3.6.15. Feladat megoldásának első bekezdése minden test fölött igaz, azaz ha $f \in K[x]$ irreducibilis, és f-nek van többszörös gyöke K egy bővítésében, akkor $f' = 0$. Legyen $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, ekkor $j a_j = 0$ teljesül minden $1 \leq j \leq n$ esetén. Ez nulla karakterisztikában lehetetlen, mert f irreducibilis lévén nem konstans, és $n > 0$ fokú polinom esetén a nem nulla főegyüttható n-szerese nem lehet nulla. Ha a karakterisztika egy p prímszám, akkor $j a_j = 0$ azt jelenti, hogy $p \mid j$ vagy $a_j = 0$ minden j-re, ami az állítás első felét bizonyítja.

Most tegyük föl, hogy $f(x) = g(x^p)$ alkalmas $g \in K[x]$ polinomra. Bővítsük K-t az f egy α gyökével. Ekkor $g(\alpha^p) = 0$. A gyöktényezőt kiemelve $g(x) = (x - \alpha^p)h(x)$ alkalmas h polinomra. De akkor

$$f(x) = g(x^p) = (x^p - \alpha^p)h(x^p) = (x - \alpha)^p h(x^p)\,,$$

hiszen p karakterisztikában tagonként lehet p-edik hatványra emelni (5.8.4. Tétel). Így pedig α többszörös gyöke f-nek.

6.4.23. A Schönemann–Eisenstein-kritériumnak az 5.7.9. Gyakorlatban megadott általánosítását alkalmazzuk. Legyen $R = \mathbb{Z}_p[z]$, ez test fölötti polinomgyűrű, és így alaptételes (5.5.9. Következmény). A z ebben felbonthatatlan elem (hiszen elsőfokú polinom), és ezért prím. Így az $x^p - z$ polinomra teljesül a Schönemann–Eisenstein-kritérium feltétele, és ezért irreducibilis az $R = \mathbb{Z}_p[z]$ gyűrű K hányadosteste fölött. Ez a hányadostest a 6.1.21. Gyakorlat szerint izomorf a $\mathbb{Z}_p(\alpha)$ testtel, ahol α transzcendens elem $\mathbb{Z}_p$ fölött, és az izomorfizmusnál z az α-nak felel meg. Tehát $x^p - \alpha$ tényleg irreducibilis $\mathbb{Z}_p(\alpha)$ fölött, és mivel x^p-nek polinomja, a 6.4.22. Feladat szerint alkalmas bővítésben van többszörös gyöke. Megjegyezzük, hogy $x^p - \alpha$ irreducibilitását másképp is igazolhatjuk, lásd a 6.4.24. Feladat megoldása utáni megjegyzést.

6.4.24. Tegyük föl, hogy a K test $p \neq 0$ karakterisztikájú, és minden eleméből vonható K-ban p-edik gyök. Legyen $f \in K[x]$ irreducibilis polinom, és tegyük föl, hogy ennek van többszörös gyöke K egy bővítésében (azaz inszeparábilis). A 6.4.22. Feladat szerint $f(x) = g(x^p)$ alkalmas $g \in K[x]$ polinomra. A feltétel szerint g minden együtthatójából vonható K-ban p-edik gyök. Mivel p karakterisztikában tagonként lehet p-edik gyököt vonni, azt kapjuk, hogy $f(x) = g(x^p) = h(x)^p$ alkalmas $h \in K[x]$ polinomra. Ez ellentmond annak, hogy f irreducibilis K fölött.

Most tegyük föl, hogy K tökéletes test, melynek karakterisztikája $p \neq 0$. Legyen $\alpha \in K$ és $g(x)$ az $x^p - \alpha$ polinomnak egy K fölött irreducibilis tényezője. Ha β gyöke g-nek K egy bővítésében, akkor $\beta^p = \alpha$, és ezért $x^p - \alpha = (x - \beta)^p$. Ennek g osztója. De K tökéletes, és így g-nek nem lehet többszörös gyöke ebben a bővítésben. Ez csak úgy lehetséges, hogy g elsőfokú, azaz $\beta \in K$. Ezért K-ban az α elemből vonható p-edik gyök.

♫ Minden $p \neq 0$ karakterisztikájú K test esetén $x^p - \alpha$ vagy irreducibilis K fölött, vagy $\sqrt[p]{\alpha}$ egyetlen értéke (a fenti β) eleme K-nak. Valóban, $g(x)$-et normáltnak feltételezve $g(x) = (x - \beta)^n$, és így konstans tagja, azaz $\beta^n \in K$. De $\beta^p = \alpha \in K$, és e két elemből kifejezhető β, mert $(n, p) = 1$, és így megoldható az $nu + pv = 1$ diofantikus egyenlet $\mathbb{Z}$-ben. Ezt a gondolatmenetet nulla karakterisztikában is elmondhatjuk, de ott kissé bonyolultabb lesz, lásd a 6.9.1. Lemma bizonyítását. A most leírt érvelés második megoldást ad a 6.4.23. Feladatra.

6.4.25. Az Útmutatóban leírtakat folytatva legyen g az α minimálpolinomja K fölött. Ekkor $g(\alpha) = 0$ miatt $f \mid g$. Mivel K tökéletes, g-nek nincsenek többszörös gyökei, de akkor egyetlen osztójának sem lehetnek.

♫ Az állítás azt az érdekes következményt vonja maga után a 6.4.24. Feladatban adott jellemzés miatt, hogy ha K egy $p \neq 0$ karakterisztikájú test, amelynek minden eleméből vonható p-edik gyök, akkor ez az algebrai bővítéseiben is teljesül.

6.4.26. Minden véges test karakterisztikája egy p prím (hiszen az összeadásra nézve nem lehet benne végtelen rendű elem). A Frobenius-endomorfizmus minden kommutatív, $p \neq 0$ karakterisztikájú gyűrűben művelettartó (5.8.4. Tétel), és nullosztómentes gyűrűben injektív, hiszen a magja csak a nullelemből áll. Véges gyűrűben emiatt szürjektív is, és így minden p karakterisztikájú véges testben minden elemből vonható p-edik gyök. A 6.4.24. Feladatbeli jellemzés szerint tehát a véges testek tökéletesek.

6.4.27. Jelölje P azoknak az L-beli elemeknek a halmazát, amelyeket elég sokszor p-edik hatványra emelve K-ba jutunk. Ha α és β ilyen elemek, mert $\alpha^{p^n} \in K$ és $\beta^{p^m} \in K$, akkor az $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén az α/β elemeket $p^{\max(m,n)}$-edik hatványra emelve K elemét kapjuk, hiszen ez a hatványozás művelettartó. Ezért P részteste L-nek. A P zárt a p-edik gyökvonás műveletére is, hiszen L tökéletes, és így a 6.4.24. Feladat miatt zárt erre a műveletre. Ezért P is tökéletes test. Megjegyezzük, hogy P a legszűkebb K-t tartalmazó tökéletes test, néha a K tökéletes *burkának* is hívják.

6.5. Szimmetriák és közbülső testek

6.5.4. Legyen s az α minimálpolinomja K fölött. Ekkor $\beta = \varphi(\alpha)$ is gyöke s-nek a 6.5.3. Állítás miatt. Mivel K tökéletes test, s-nek α és β is egyszeres gyöke. Tudjuk, hogy asszociáltság erejéig s az egyetlen K fölött irreducibilis polinom, melynek α, illetve β gyöke (6.1.13. Tétel). Ezért ha f-et $K[x]$-beli kanonikus alakban írjuk fel, és ebben s az m-edik hatványon szerepel, akkor α is és β is pontosan m-szeres gyöke f-nek. Vagyis β ugyanannyiszoros gyöke f-nek, mint α.

6.5.6. Tegyük föl, hogy ψ is relatív automorfizmus, és $\psi(\alpha_i) = \varphi(\alpha_i)$ mindegyik i-re. Tekintsük azon $\beta \in L$ elemek M halmazát, melyre $\psi(\beta) = \varphi(\beta)$. Mivel ψ és φ is tartja az összeadást, kivonást, szorzást és osztást, az M részteste L-nek. Mivel ψ és φ fixálja K elemeit, ezért $K \subseteq M$. Végül $\alpha_1, \ldots, \alpha_m \in M$ a feltétel szerint. Tehát M egy olyan K-t tartalmazó résztest, amely az $\alpha_1, \ldots, \alpha_m$ elemeket tartalmazza. De $L = K(\alpha_1, \ldots, \alpha_m)$ a legszűkebb ilyen résztest, és ezért $L \subseteq M$. Ez azt jelenti, hogy $\psi = \varphi$.

6.5.10. Ha $\alpha, \beta \in T$, akkor $\varphi(\alpha) = \alpha$ és $\varphi(\beta) = \beta$. De φ összegtartó, így $\varphi(\alpha+\beta) = \varphi(\alpha)+\varphi(\beta) = \alpha+\beta$, azaz $\alpha + \beta \in T$. Hasonlóan kapjuk, hogy $\alpha - \beta$, $\alpha\beta$, és $\beta \neq 0$ esetén α/β is T-beli. Végül $K \subseteq T$, hiszen φ relatív automorfizmus, és így fixálja K elemeit.

6.5.13. A számolások és az eredmények ugyanazok, csak a gyökjelek alatt 2 helyett 5-öt kell írni. Azonban amíg $\gamma = \sqrt[4]{2} + i\sqrt[4]{2}$ negyedik hatványa -8, vagyis az $x^4 + 8$ polinomnak gyöke, amely irreducibilitásának igazolására trükközésre kényszerültünk, addig a $\sqrt[4]{5} + i\sqrt[4]{5}$ elem negyedik hatványa -20, és az $x^4 + 20$ polinom a Schönemann–Eisenstein-kritérium miatt irreducibilis (ha a prímszámot a kritériumban 5-nek vesszük). Ez tehát némiképp egyszerűsíti a bizonyítást.

♫ Ha általában az $x^4 - p$ felbontási testét vizsgáljuk, ahol p pozitív prímszám, akkor is hasonló a számolás, a fenti $x^4 + 20$ helyett $x^4 + 4p$ adódik $\sqrt[4]{p} + i\sqrt[4]{p}$ minimálpolinomjára. Ebből érezhetjük, hogy az $x^4 - 2$ példájában a 2 prímszám „kettős szerepet játszik”, hiszen a 2 tetszőleges p esetén „bejön”. Ennek oka az, hogy $(1+i)^2 = 2i$ (és az i, mint negyedik egységgyök, benne van a vizsgált bővítésben). A következő gyakorlatban tovább taglaljuk a $p = 2$ egybeesés következményeit.

6.5.14. 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 $\mathbb{Q}(\sqrt[4]{2}, i)$ 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.

6.5.15. A bővítés negyedfokú a 6.2.15. Gyakorlat miatt. Válasszuk benne az $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ bázist. Nyilván $\sqrt{d}$ képe csak $\pm\sqrt{d}$ lehet minden racionális d számra, hiszen az $x^2 - d$ polinom gyökei permutálódnak. Ez négy lehetőséget hagy meg szimmetriára aszerint, hogy $\sqrt{2}$ képe $\sqrt{2}$-e vagy $-\sqrt{2}$, és ettől függetlenül, hogy $\sqrt{3}$ képe $\sqrt{3}$-e vagy $-\sqrt{3}$. Ez a négy szimmetria Klein-csoportot alkot a kompozícióra, és így ez a Galois-csoport. Ha például a

$$\varphi : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

automorfizmust vesszük, akkor ennek fixpontjai a $\mathbb{Q}(\sqrt{6})$ testet alkotják. A másik két nemtriviális közbülső test a $\mathbb{Q}(\sqrt{2})$ és a $\mathbb{Q}(\sqrt{3})$, és így a $\mathbb{Q}$-val és a $\mathbb{Q}(\sqrt{2}, \sqrt{3})$-mal együtt összesen 5 közbülső test van.

6.6. A Galois-elmélet főtétele

6.6.6. Tegyük föl, hogy $T_1 \leq T_2$ és $\varphi \in T_2^\sharp$. Ekkor φ fixálja T_2 elemeit, és így T_1 elemeit is. Ezért $\varphi \in T_1^\sharp$. A másik állítás hasonlóan igazolható.

6.6.11. A 6.3.1. Gyakorlat szerint $x^3 - 2$ felbontási teste $L = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, amely $\mathbb{Q}$-nak hatodfokú bővítése. Így a főtétel miatt a Galois-csoport is hatelemű. Másfelől a Galois-csoport elemei permutálják $x^3 - 2$ gyökeinek halmazát, és egy-egy ilyen permutáció már egyértelműen meghatároz egy automorfizmust. Ezért a Galois-csoport részcsoportja az S_3 szimmetrikus csoportnak, és mivel hatelemű, csak maga S_3 lehet. A 4.4.25. Gyakorlatban meghatároztuk S_3 összes részcsoportját. Ezek a két triviális részcsoporton kívül az A_3 alternáló csoport, továbbá a három transzpozíció által generált kételemű részcsoportok. Ez utóbbiaknak a főtétel miatt $\mathbb{Q}$ harmadfokú bővítése kell, hogy megfeleljen, ezek tehát $x^3 - 2$ három gyökéből kaphatók: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\varepsilon\sqrt[3]{2})$, $\mathbb{Q}(\varepsilon^2\sqrt[3]{2})$. Például a $\mathbb{Q}(\sqrt[3]{2})$-höz tartozó részcsoport egységtől különböző eleme $x^3 - 2$ másik két gyökét cseréli ki (ez a komplex konjugálás). Végül az A_3 alternáló csoporthoz $\mathbb{Q}$ másodfokú bővítése tartozik, ez tehát csak a $\mathbb{Q}(\varepsilon)$ lehet.

6.6.12. Az Útmutatóbeli jelölésekkel tegyük föl, hogy ψ eleme a $\mathbb{Q} \leq \mathbb{Q}(\varepsilon)$ bővítés G Galois-csoportjának. Ekkor $\psi(\varepsilon)$ 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. Ilyen szimmetria létezik is a 6.5.8. Állítás miatt, hiszen $\Phi_n(x)$ irreducibilis polinom, ezért ε minimálpolinomja, és így ε konjugáltjai pontosan a primitív n-edik egységgyökök. 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.

6.6.13. A 6.3.14. Gyakorlatban megmutattuk, hogy a szóban forgó két polinom felbontási teste ugyanaz: $\mathbb{Q}(\sqrt[6]{2}, \eta)$, ahol η primitív hatodik egységgyök. Azt is beláttuk, hogy ez $\mathbb{Q}$-nak 12 fokú bővítése. Ezért a

két polinom G Galois-csoportja is ugyanaz, és a rendje 12. A 6.5.12. Állítást (és az azt követő megjegyzést) alkalmazva a G csoportot felfoghatjuk úgy is, mint az $(x^2-2)(x^3-2)$ gyökein ható permutációcsoportot, melynek egy kételemű és háromelemű pályája van. Emiatt G tekinthető az $S_2 \times S_3$ direkt szorzat részcsoportjának. De ez a direkt szorzat 12 elemű, és így $G \cong S_2 \times S_3$.

♫ Megjegyezzük, hogy $S_2 \times S_3$ izomorf a D_6 diédercsoporttal (4.9.25. Gyakorlat). Ez a diédercsoport közvetlenül is adódott volna, ha x^6-2 Galois-csoportját a 6.5. szakaszban látott módon, az x^4-2-höz hasonlóan számítjuk ki.

6.6.14. A 6.5.13. Gyakorlat szerint x^4-5 felbontási teste $L = \mathbb{Q}(\sqrt[4]{5}, i)$, Galois-csoportja pedig D_4. Három $\mathbb{Q}$ fölött másodfokú résztest van, a $\mathbb{Q}(i)$, a $\mathbb{Q}(\sqrt{5})$ és a $\mathbb{Q}(i\sqrt{5})$ (vö. 6.1. ábra). Legyen $\eta = (1+i)/\sqrt{2}$ primitív nyolcadik egységgyök. Ha $\eta \in L$ teljesülne, akkor $i \in L$ miatt $\sqrt{2} \in L$ is igaz lenne, így $\mathbb{Q}(\sqrt{2})$ másodfokú részteste lenne L-nek. Ez a résztest azonban a felsorolt három másodfokú résztest egyikével sem egyenlő (a 6.1.26. Feladat miatt). Ebből az ellentmondásból már látszik, hogy x^4-5 és x^4+5 felbontási teste különböző, ha ugyanis megegyeznének, akkor x^4+5 mindegyik gyöke, speciálisan $\eta\sqrt[4]{5}$ is L-ben lenne, és így $\eta \in L$ is teljesülne. Ezzel az első állítást be is láttuk.

♫ Ha az x^4-5 helyett az x^4-2-t vizsgálnánk, akkor $\sqrt{2}$ benne lenne a bővítésben, hiszen megkapható $\sqrt[4]{2}$ négyzeteként, és így az előző bekezdésben látott módon nem jutnánk ellentmondásra. Ebben a felbontási testben persze η is benne van, amint azt a 6.5.14. Gyakorlat megoldásában láttuk.

Mivel $\eta^2 = 2i \in L$, az η foka L fölött 2, és így $L(\eta)$ a $\mathbb{Q}$-nak 16 fokú bővítése. Jelölje M az x^4+5 felbontási testét $\mathbb{Q}$ fölött. E polinom gyökei az $\alpha = \eta\sqrt[4]{5}$ szám negyedik egységgyökszörösei, vagyis $\pm\alpha$ és $\pm i\alpha$, és így $M = \mathbb{Q}(\eta\sqrt[4]{5}, i)$. Belátjuk, hogy ez is nyolcadfokú bővítése $\mathbb{Q}$-nak. A szorzástétel miatt nyilván legfeljebb nyolcadfokú. Ugyanakkor $\eta^2 = i \in M$ miatt $|M(\eta) : M| \leq 2$. Viszont $M(\eta) = L(\eta)$, és így $M(\eta)$ foka is 16, azaz M foka legalább nyolc. Tehát $|M : \mathbb{Q}| = 8$. Így x^4+5 Galois-csoportja is nyolcelemű. Mivel ennek gyökei is páronként nullát adnak összegül, a Galois-csoport részcsoportja D_4-nek (ugyanúgy, mint az x^4-2 esetében), és ezért csak D_4 lehet.

6.6.15. A polinom irreducibilis a Schönemann–Eisenstein-kritérium miatt, és így öt különböző komplex gyöke van. A diszkriminánsa $5 \cdot 10^4 - 4 \cdot 16^4 < 0$ (ez a megfelelő determináns kiszámításával adódik), és így a 3.7.8. Állítás miatt a nem valós gyökök száma nem osztható néggyel. Ez persze páros szám, hiszen ezek a gyökök konjugált párokban jelentkeznek, és így a polinomnak két nem valós, és három valós gyöke van.

♫ Azt, hogy három valós gyök van, az analízis módszereivel, függvényvizsgálattal is beláthatjuk, hiszen a polinom deriváltjának könnyű meghatározni a gyökeit.

A polinom Galois-csoportját a gyökök halmazán ható permutációcsoportnak fogva föl a komplex konjugálás egy transzpozíciót eredményez. Továbbá G tranzitív részcsoportja S_5-nek, hiszen a polinom irreducibilis (6.5.12. Állítás). A 4.12.46. Feladat szerint ha S_5 egy tranzitív részcsoportja tartalmaz transzpozíciót, akkor az csak az egész S_5 lehet.

6.6.16. Legyen $K = \mathbb{Z}_p(\alpha)$ és β gyöke az $x^p-\alpha$ polinomnak egy bővebb testben. Ekkor $\beta^p = \alpha$, és így $x^p - \alpha = (x-\beta)^p$ (hiszen p karakterisztikában tagonként lehet p-edik hatványra emelni). Vagyis a felbontási test $L = K(\beta)$. A $K \leq L$ bővítés Galois-csoportja egyelemű, mert minden relatív automorfizmus permutálja $x^p-\alpha$ gyökeit, és így β csak saját magába mehet.

♫ Megjegyezzük, hogy a $K \leq L$ bővítés foka p, hiszen a 6.4.23. Feladatban beláttuk, hogy $x^p-\alpha$ irreducibilis K fölött. A Galois-elmélet főtétele tehát itt nem érvényes, aminek oka az, hogy a K test nem tökéletes.

6.6.17. A 6.4.16. Gyakorlat miatt létezik olyan M test, hogy $K \leq L \leq M$ és M véges normális bővítése K-nak. Ennek Galois-csoportja is véges, és minden közbülső test különböző részcsoportnak felel meg a főtétel miatt, tehát ezek száma is véges.

6.6.18. A 6.4.16. Gyakorlat miatt létezik olyan M test, hogy $K \leq L \leq M$, és M véges normális bővítése K-nak. Legyen $G = G(M/K)$ és $H = G(M/L)$ az L közbülső testnek megfelelő részcsoportja G-nek. Ekkor a főtétel miatt $|G : H| = 4$, keressük a H-t tartalmazó valódi részcsoportokat. Ha ilyen legfeljebb

egy van, akkor készen vagyunk. Ha van két különböző, mondjuk H_1 és H_2, akkor mindkettő indexe G-ben kettő (hiszen 4-nek osztója), és így $H_1 \cap H_2$ csak H lehet. Ekkor $H \lhd G$ (mert a kettő indexű részcsoportok normálosztók, és így H két normálosztó metszete). Vagyis $K \leq L$ normális bővítés. A Galois-csoportja tehát vagy a Klein-csoport, ekkor öt közbülső test lesz, vagy ciklikus, és ekkor a közbülső testek száma három. (Felhasználtuk e két négyelemű csoport részcsoportjainak leírását.)

6.6.19. A $h(x)$ polinomra G bármely elemét alkalmazva csak a tényezők cserélődnek, a polinom nem változik. Ezért h együtthatói fixen maradnak G elemeinél, és így a 6.6.2. Állítás (vagy akár a főtétel) miatt $h \in K[x]$. Ha $t \in K[x]$ normált, irreducibilis polinom, amely h-nak osztója, akkor t-nek gyöke $\varphi(\alpha)$ alkalmas $\varphi \in G$-re, de akkor φ inverzét alkalmazva kapjuk, hogy α is gyöke t-nek, vagyis $t = s$ (az α minimálpolinomja). Tehát a h polinom $K[x]$-beli kanonikus alakjában csakis s szerepelhet tényezőként, és mivel h normált is, $h = s^m$ alkalmas m egészre. A fokszámok összehasonlításával adódik, hogy $m = |L : K|/\mathrm{gr}_k(\alpha)$, hiszen $|G| = |L : K|$. Ezzel (1)-et beláttuk.

Tegyük föl, hogy a (2)-beli f polinom $K[x]$-beli és irreducibilis. Mivel K tökéletes, a γ_i számok (mint az f irreducibilis polinom gyökei) páronként különbözők. Legyen $\alpha = \gamma_1$, ekkor f minimálpolinomja α-nak K fölött, hiszen normált, irreducibilis, és α gyöke. Ezért f gyökei az α konjugáltjai, vagyis α pályáját alkotják a G csoportnál. (Ez következik a 6.5.8. Állításból, de (1)-ből is, ha elkészítjük α-hoz a h polinomot, hiszen f az α minimálpolinomja, és így $f \mid h$.)

Most tegyük föl, hogy a γ_i számok páronként különbözők, és G-pályát alkotnak. Ekkor $f(x)$ nyilván G-invariáns, és így $K[x]$-beli. Ha s jelöli a γ_1 minimálpolinomját K fölött, akkor $s \mid f$. De s-nek gyöke $\varphi(\gamma_1)$ minden $\varphi \in G$-re, ezért $s = f$ (ugyanazok a gyöktényezőik), vagyis f is irreducibilis.

6.6.20. Az Útmutatóban leírt gondolatmenet hiányzó részeit pótoljuk, az ottani jelöléseket használva. Elsőként belátjuk, hogy G tranzitívan hat az (α_i, β_j) párok halmazán (G elemei komponensenként hatnak). Azt tudjuk (a 6.6.19. Gyakorlat miatt), hogy $\{\alpha_1, \ldots, \alpha_n\}$ és $\{\beta_1, \ldots, \beta_m\}$ is pályája G-nek. Legyen N az α_1 stabilizátora G-ben (a pálya hosszát leíró 4.5.8. Tétel miatt ennek indexe n), és M a β_1 stabilizátora G-ben (ennek indexe m). Ekkor az (α_1, β_1) pár stabilizátora $N \cap M$. Nyilván $N \cap M$ indexe osztható n-nel is és m-mel is, és mivel ezek relatív prímek, nm-mel is. Tehát (α_1, β_1) stabilizátorának indexe legalább nm, vagyis pályája legalább nm elemű, és így tényleg az összes párt tartalmazza.

Az Útmutatóban láttuk, hogy az $\alpha_1 + \beta_1$ összeg különbözik az összes többi $\alpha_i + \beta_j$ összegtől. Mivel G tranzitív az (α_i, β_j) párokon, tranzitív az $\alpha_i + \beta_j$ összegeken is. Vagyis $\alpha_1 + \beta_1$ bármelyik ilyen összegbe elvihető G egy elemével, és ezért ez is különbözni fog az összes többi összegtől. Vagyis a 6.6.19. Gyakorlat (2) pontjának feltételei teljesülnek az f polinomra.

6.7. Véges testek

6.7.4. Az állítás közvetlen számolással is igazolható, a műveleti táblából látszik, hogy az $A = x+(x^2+x+1)$ és a $B = (x+1)+(x^2+x+1)$ elemek egymás négyzetei. Egyszerűbb azonban azt mondani, hogy e K test $K^\times = K - \{0\}$ multiplikatív csoportja háromelemű, és így Lagrange tétele miatt minden nem nulla elem köbe az egységelem. De akkor az $x(x^3 - 1)$ polinomnak már minden elem gyöke, a 0 is. Ugyanez a fajta „javítás” szerepel a kis Fermat-tételben is az Euler-Fermat tételhez képest (hogy 0-ra is működjön).

6.7.6. Nem a 6.7.5. Tétel bizonyítása hibás, hanem az idézőjelbe tett mondat vége. Az $x^3 - x$ polinomnak ugyanis csak két gyöke van $\mathbb{Z}_2$ bármely bővítésében: a 0 és az 1, ezek közül az 1 kétszeres gyök. Ez a példa azt mutatja, hogy a 6.7.5. Tétel bizonyításának utolsó bekezdése (a deriváltat használó gondolatmenet) nem hagyható el. Persze az merő véletlen, hogy az $x^3 - x$ polinom gyökei résztestet alkotnak $\mathbb{Z}_2$-ben, a tipikus esetben ilyesmi csak akkor igaz, ha x kitevője a karakterisztika hatványa.

6.7.9. Ha f irreducibilis $K = \mathbb{F}_{p^m}$ fölött és n-edfokú, akkor már egy gyök hozzávétele is az $L = \mathbb{F}_{p^{mn}}$ testet generálja (hiszen n-edfokú bővítés keletkezik). Mivel véges test minden véges bővítése normális, ez egyben felbontási test is lesz. Ezért (1) igaz.

A 6.7.8. Tétel szerint $K = \mathbb{F}_{p^m}$ részteste $L = \mathbb{F}_{p^{mn}}$-nek (és a bővítés foka n). Ha α az L multiplikatív csoportjának generátoreleme, akkor $K(\alpha) = L$. Ezért α-nak a K fölötti minimálpolinomja n-edfokú és irreducibilis K fölött.

6.7.10. Legyen f egy d-edfokú irreducibilis polinom $\mathbb{Z}_p$ fölött. Ha f osztója az $x^{p^n} - x$ polinomnak, akkor f gyöktényezőkre bomlik az $\mathbb{F}_{p^n}$ test fölött (6.7.5. Tétel). Legyen α az f egyik gyöke, ekkor $K(\alpha) \leq \mathbb{F}_{p^n}$, és így α foka (ami f foka, vagyis d) osztja a bővítés fokát (ami n). Megfordítva, ha $d \mid n$ akkor a 6.7.8. Tétel miatt $\mathbb{F}_{p^d}$ részteste $\mathbb{F}_{p^n}$-nek. Az f egy gyökével $\mathbb{Z}_p$-t bővítve $\mathbb{F}_{p^d}$ adódik. Ezért f-nek van egy α gyöke $\mathbb{F}_{p^n}$-ben, és így f az α minimálpolinomja (asszociáltság erejéig). De α gyöke $x^{p^n} - x$-nek, ezért f osztója ennek a polinomnak. Mivel $x^{p^n} - x$-nek nincs többszörös gyöke, ezért minden ilyen f irreducibilis polinom csak egyszer szerepel benne tényezőként.

6.7.12. Az f gyökei konjugált elemek, és ezért egymásba test-automorfizmussal átvihetők (6.4.12. Következmény). Ez automorfizmusa a multiplikatív csoportnak is, és így a rendet megőrzi.

6.7.16. Az $\mathbb{F}_{27}$ multiplikatív csoportja a $\mathbb{Z}_{26}^+$ ciklikus csoport. Ebben azoknak az elemeknek a száma, melyek négyzete az egységelem, a 4.3.24. Állítás szerint 2. Ugyanakkor harmadrendű eleme nincs, mert $3 \nmid 26$. A $\mathbb{Z}_{26}^+$ csoportban a négyzetre emelés endomorfizmus, melynek magja a fentiek szerint kételemű. Ezért a képének az elemszáma $26/2 = 13$. Ez azt jelenti, hogy a négyzetelemek száma a nullával együtt 14. Ugyanakkor minden elem köbelem, ez hasonlóan számolható ki, de tudjuk onnan is, hogy 3 karakterisztikában a köbre emelés minden véges testnek test-automorfizmusa.

♫ Az ilyen típusú feladatokat számolással is megoldhatjuk. Például ha a négyzetelemeket keressük, és β a multiplikatív csoport egyik generátora, akkor a $\beta^k = x^2$ egyenlet megoldásához x-et β^y alakban írhatjuk. Ekkor a $2y \equiv k$ (26) kongruenciához jutunk.

Mivel $f(x) = x^4 + x^3 + x^2 + x + 1 = (x^5 - 1)/(x - 1)$, ezért az f gyökeinek ötödik hatványa 1. De $5 \nmid 26$, és ezért az egyetlen ilyen elem az 1, ami viszont f-nek nem gyöke. Ezért az f polinomnak nincs gyöke ebben a testben.

A $g(x) = x^2 - x + 1$ viszont az $x^6 - 1$ polinomnak osztója (hiszen g a hatodik körosztási polinom). Az eddigiekhez hasonlóan számolva az $x^6 = 1$ egyenletnek csak két gyöke van $\mathbb{F}_{27}$-ben, az 1 és a -1. Ezért g-nek egyetlen gyöke van ebben a testben, a -1 (ami kétszeres).

♫ Az $x^4 + x^3 + x^2 + x + 1 = \Phi_5(x)$ gyökei a multiplikatív csoport ötödrendű elemei az 5.8.14. Feladat miatt, de ilyen ebben a testben nincs. Továbbá 3 karakterisztikájú testben $\Phi_6(x) = \Phi_2(x)^2 = (x - 1)^2$ a 3.9.23. Feladat miatt. Így az eredményt számolás nélkül is megkaphattuk volna.

Hasonlóképpen 3 karakterisztikájú testben az $x^2 - x + 1$ polinomot is írhatjuk $x^2 + 2x + 1 = (x + 1)^2$ alakban, ahonnan látszik, hogy az egyetlen gyöke a -1.

6.7.17. Az $x^2 + 1$ polinomnak $\mathbb{Z}_{17}$-ben gyöke a ± 4, és így $x^2 + 1$ felbontási teste maga $\mathbb{Z}_{17}$. Az $x^2 - 3$ polinomnak nincs gyöke ebben a testben (ezt legegyszerűbben az elemek négyzetre emelésével láthatjuk be, de aki ismeri számelméletből a Legendre-szimbólumok elméletét, az gyorsabban is célhoz érhet). Ezért $x^2 - 3$ irreducibilis, és így egy gyökével bővítve másodfokú bővítést kapunk, vagyis az $\mathbb{F}_{17^2}$ testet. Ez felbontási teste lesz ennek a polinomnak (hiszen minden másodfokú bővítés normális a 6.3.15. Feladat miatt, vagy mert véges testek esetében minden véges bővítés normális a 6.7.8. Tétel miatt).

6.7.18. Az 5.8.14. Feladat szerint az $x^2 + x + 1 = \Phi_3(x)$ gyökei a test harmadrendű elemei, hiszen a karakterisztika egyik esetben sem három. (Ez persze most könnyen adódik az $x^2 + x + 1 = (x^3 - 1)/(x - 1)$ képletből.) Ilyen az $\mathbb{F}_{121}$ testben van, mert a multiplikatív csoport ciklikus, és rendje 120, ami hárommal osztható. Ezért ebben az esetben a felbontási test maga $\mathbb{F}_{121}$. Az $\mathbb{F}_{125}$ testben azonban nincs harmadrendű elem, mert 124 nem osztható hárommal. Ezért a másodfokú $x^2 + x + 1$ polinom irreducibilis, és így egy gyökével bővítve másodfokú bővítést kapunk, vagyis a felbontási test az $\mathbb{F}_{5^6}$.

♫ Az $x^2 + x + 1$ polinom gyökeinek megkeresését a másodfokú egyenlet megoldóképlete segítségével négyzetgyökvonásra vezethetnénk vissza, hiszen a karakterisztika nem 2 (lásd 5.8.12. Gyakorlat), ez azonban nem segítene sokat, hiszen nincs négyzetgyök-táblázatunk.

6.7.19. Legyen $L = \mathbb{F}_{2^m}$ a keresett felbontási test. Az Útmutatóban írtak miatt $11 \mid 2^m - 1$. Könnyű ellenőrizni, hogy a legkisebb ilyen tulajdonságú m szám a 10 (valójában arról van szó, hogy a 2 rendje 10 mod 11). Megfordítva, $\mathbb{F}_{2^{10}}$ multiplikatív csoportja ciklikus, ezért $\varphi(11) = 10$ darab 11 rendű eleme van. Ezért $x^{11} - 1$ gyöktényezőkre bomlik. A felbontási test $\mathbb{Z}_2$ fölött tehát $\mathbb{F}_{2^{10}}$.

Az 5.8.4. Tétel szerint 11 karakterisztikában tagonként lehet 11-edik hatványra emelni. Ezért $\mathbb{Z}_{11}$ fölött a felbontási test maga $\mathbb{Z}_{11}$, és $x^{11} - 1 = (x-1)^{11}$.

6.7.20. Ha a $\mathbb{F}_{p^m}$ multiplikatív csoportjának van n rendű eleme, akkor Lagrange tétele miatt n osztója a csoport rendjének, azaz $p^m - 1$-nek. Megfordítva, ha $n \mid p^m - 1$, akkor az $\mathbb{F}_{p^m}^{\times}$ csoportban van n rendű elem, hiszen ez ciklikus csoport (4.3.24. Állítás). De $n \mid p^m - 1$ azt jelenti, hogy m jó kitevője p-nek mod n, vagyis hogy $k = o_n(p) \mid m$. Ezzel az (1) állítást beláttuk.

Az (1) miatt az $\mathbb{F}_{p^k}$ testben is van n rendű elem. Ennek n különböző hatványa van, és így az $x^n - 1$ gyöktényezőkre bomlik ebben a testben. Persze akkor $\Phi_n(x) \mid x^n - 1$ is gyöktényezőkre bomlik. Az 5.8.14. Feladat szerint tehát $\mathbb{F}_{p^m}$ minden n rendű eleme benne van az $\mathbb{F}_{p^k}$ résztestben. Megmutatjuk, hogy minden n rendű α elem generálja is ezt a résztestet. Valóban, ha d jelöli az α fokát $\mathbb{Z}_p$ fölött, akkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^d}$, és így (1) miatt $k \mid d$. De $\alpha \in \mathbb{F}_{p^k}$ miatt $d \mid k$ (hiszen elem foka osztja a bővítés fokát), tehát $k = d$. Ezzel a (2) és (3) állításokat is beláttuk.

A Φ_n minden irreducibilis tényezője egy n rendű elem minimálpolinomja, tehát (2) miatt k-adfokú, és így (4) igaz.

A feladat utolsó kérdésére egy válasz: $p = 2$ és $n = 7$. Ekkor $k = 3$, $\Phi_7(x) = (x^3 + x^2 + 1)(x^3 + x + 1)$, és itt az összes harmadfokú, $\mathbb{Z}_2$ fölött irreducibilis polinom szerepel (3.3.21. Gyakorlat). A példa azért működik, mert az $\mathbb{F}_8$ test multiplikatív csoportjában minden 1-től különböző elem rendje 7, és így minden olyan elem, amely generálja a bővítést, hetedrendű, azaz gyöke Φ_7-nek.

6.7.21. Az (1) a hatvány rendjének képletéből (4.3.10. Gyakorlat) világos, hiszen α rendje $p^m - 1$. A (2) következik az előző 6.7.20. Feladat (2) pontjából.

Az, hogy β foka m, azt jelenti, hogy β az egész $\mathbb{F}_{p^m}$ testet generálja, azaz hogy nincsen benne egyetlen valódi résztestben sem. A 6.7.8. Tétel szerint a valódi résztestek elemszáma $\mathbb{F}_{p^d}$, ahol $d \mid m$, és ebben a résztestben β akkor és csak akkor van benne, ha $\beta^{p^d} = \beta$. Mivel $\beta = \alpha^j \neq 0$, ez azzal ekvivalens, hogy $\alpha^{jp^d - j} = 1$, azaz hogy $p^m - 1 \mid j(p^d - 1)$, ami pontosan a (3)-beli $(p^m - 1)/(p^d - 1) \mid j$ feltétel. Ezzel (3)-at is igazoltuk. Megjegyezzük, hogy (3) elemi számelméleti meggondolásokkal is azonnal adódik (2)-ből.

6.7.22. A 6.7.21. Feladatban $p = 2$, $m = 4$ és $j = 3$. Az $\mathbb{F}_{2^4}$ testben α rendje 15, ezért $\beta = \alpha^3$ ötödrendű, és foka a prímtest fölött 2 rendje modulo 5, vagyis 4.

♫ A β elem tehát nem generálja a multiplikatív csoportot, de az $\mathbb{F}_{2^4}$ testet igen. A négy ötödrendű elem minimálpolinomja valójában a Φ_5 körosztási polinom. Érdemes meggondolni, hogy (3) persze teljesül β esetében, hiszen $j = 3$ nem osztható sem 15-tel, sem 5-tel (de mégsem relatív prím 15-höz, és β ezért nem generálja a multiplikatív csoportot).

6.7.23. Bármelyik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ fölötti felbontási teste a 6.7.9. Gyakorlat szerint $\mathbb{F}_{p^n}$. Ezek a polinomok az $\mathbb{F}_{p^n}$ azon elemeinek minimálpolinomjai, amelyek nincsenek benne egyetlen valódi résztestben sem (hiszen egy elem foka akkor n, ha az egész bővítést generálja a prímtest fölött).

Ha $p = 2$ és $n = 8$, akkor a résztestek rendje 2^k, ahol $k \mid 8$ (a 6.7.8. Tétel szerint). Ezek egymást tartalmazzák, hiszen 8 osztói $1 \mid 2 \mid 4 \mid 8$. Vagyis a keresett elemek azok, amik kívül esnek az $\mathbb{F}_{2^4}$ résztesten, ez $2^8 - 2^4 = 240$ elem. Mindegyik minimálpolinomja tehát nyolcadfokú. Azonban mindegyik polinomot nyolcszor számoltuk, hiszen 8 gyöke van. (A véges testek tökéletesek a 6.4.26. Feladat miatt, tehát többszörös gyök nem lehet.) Ezért $240/8 = 30$ nyolcadfokú irreducibilis polinom van $\mathbb{Z}_2$ fölött.

Ezt általánosítva ha $q = r^n$, ahol r prím, akkor $\mathbb{Z}_p$ fölött a q-adfokú irreducibilis polinomok száma $\left(p^{r^n} - p^{r^{n-1}}\right)/r^n$. Ennek oka az, hogy $q = r^n$ egyetlen „maximális” valódi osztója r^{n-1}.

Végül ha $n = 12$, akkor hat résztest van. A maximális résztestek $\mathbb{F}_{2^4}$ és $\mathbb{F}_{2^6}$, ezek metszete csakis $\mathbb{F}_{2^2}$ lehet (hiszen 4 és 6 legnagyobb közös osztója 2). Ezért a keresett elemek száma $2^{12} - 2^6 - 2^4 + 2^2$, a 12-edfokú irreducibilis polinomok száma pedig ennek 12-edrésze, vagyis 335.

6.7.24. Az Útmutatóban megadott színezésről megmutatjuk, hogy megfelelő. Az $\mathbb{F}_{16}^\times$ csoport 15 elemű, benne $\mathbb{F}_4^\times$ egy háromelemű részcsoport. Ezért minden elem 5-ödik hatványa benne van ebben a részcsoportban, vagyis a színezés a megadott színekkel történik. Ha α, β, γ egyszínű háromszög, akkor legyen $\theta = (\alpha + \beta)/(\beta + \gamma)$. Ekkor $\theta^5 = 1$ és $(\theta + 1)^5 = (\alpha + \gamma)^5/(\beta + \gamma)^5 = 1$ (mert 2 karakterisztikában $2\beta = 0$). De $\mathbb{Z}_2$ fölött az $x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$ és $(x + 1)^5 - 1 = x(x^4 + x^3 + 1)$ polinomok relatív prímek (3.3.21. Gyakorlat), és így nem lehet közös gyökük semmilyen bővítésben. Ez az ellentmondás mutatja, hogy jó színezést konstruáltunk.

♫ Közvetlen számolás is célhoz vezetne: az $1 = (\theta + 1)^5 = \theta^5 + \theta^4 + \theta + 1$ egyenletből $\theta^4 + \theta^3 + 1 = 0$ (hiszen $\theta \neq 0$), viszont $\theta^5 = 1$ miatt ugyaninnen $\theta^4 + \theta + 1 = 0$, ahonnan $\theta^3 = \theta$, és így $\theta^2 = 1$, végül $\theta = 1$, ami nem jó.

Lényegében arról van szó, hogy $\Phi_5(x)$ irreducibilis $\mathbb{Z}_2$ fölött, és $\Phi_5(x + 1)$ is az, de tőle különböző. Ez nem minden prímre van így, például $\mathbb{Z}_2$ fölött $\Phi_3(x) = \Phi_3(x + 1)$.

Legyen most G egy 17 csúcsú teljes gráf, melynek éleit három színnel színeztük. Ha A egy csúcs, akkor ennek 16 szomszédja van, és így létezik olyan szín, mondjuk a piros, hogy A-ból legalább 6 piros él indul ki. Jelölje H az A-ból induló piros élek végpontjait. Ha ezek között megy piros él, akkor van piros háromszög. Ha nem megy, akkor legyen $B \in H$, ebből a H-beli pontokhoz legalább három egyforma színű, mondjuk fehér él indul. Ha ezek végpontjai között megy fehér él, akkor van fehér háromszög. Ha nem, akkor e szomszédok közötti összes él már csak a harmadik színű, mondjuk zöld lehet. De akkor találtunk egy zöld háromszöget.

6.8. Geometriai szerkeszthetőség

6.8.12. Az E.4.2. Tétel szerint ha n kanonikus alakja $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, ahol egyik α_i kitevő sem nulla, akkor

$$\varphi(n) = p_1^{\alpha_1 - 1} \dots p_1^{\alpha_k - 1}(p_1 - 1) \dots (p_k - 1)\,.$$

Ez pontosan akkor lesz 2-hatvány, ha mindegyik tényező az. Ezért $p_j \neq 2$ esetén $\alpha_j = 1$, továbbá $p_j - 1$ is 2-hatvány minden j-re. Ha $p_j = 2^m + 1$, akkor a $b + 1 \mid b^{2\ell+1} + 1$ összefüggés miatt könnyű belátni, hogy m maga is 2-hatvány (lásd [1], 1.4.4. Feladat).

6.8.17. Szerkesszünk egy $A_0, \dots, A_{n-1}$ csúcsú, O középpontú szabályos n-szöget, majd minden A_i csúcsból kiindulva egy olyan $B_{i,0}, \dots, B_{i,m-1}$ szabályos m-szöget, melynek középpontja szintén O, és első csúcsa, $B_{i,0} = A_i$. Belátjuk, hogy a kapott nm darab $B_{i,j}$ pont szabályos nm-szöget alkot. Az $A_0 O B_{i,j}$ szög

$$\frac{360^\circ i}{n} + \frac{360^\circ j}{m} = \frac{360^\circ}{nm}\big(mi + nj\big)\,.$$

Ha $0 \leq k < nm$, akkor $(n, m) = 1$ miatt az $mx + ny = k$ diofantikus egyenlet megoldható x-re és y-ra. Legyen i az x szám n-nel, j az y szám m-mel való osztási maradéka. Ekkor $mi + nj \equiv k\ (nm)$, és ezért a $B_{i,j}$-hez tartozó szög $k360^\circ/nm$. Így a szabályos nm-szög k-adik csúcsát megkaptuk minden k-ra.

6.8.18. Mivel $0 = \Phi_5(\varepsilon) = 1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4$, így

$$\eta_1 + \eta_2 = \eta_1\eta_2 = \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1\,.$$

Ezért η_1 és η_2 az $x^2 + x - 1$ polinom gyökei. De $\varepsilon^4 = \varepsilon^{-1}$ miatt $\varepsilon^2 - \eta_1\varepsilon + 1 = 0$. Így

$$\varepsilon,\, \varepsilon^4 = \frac{\frac{\sqrt{5}-1}{2} \pm \sqrt{\left(\frac{\sqrt{5}-1}{2}\right)^2 - 4}}{2} = \frac{\sqrt{5} - 1}{4} \pm i\frac{\sqrt{2(5 + \sqrt{5})}}{4}$$

(a valós rész $\cos 72^\circ$, a képzetes rész $\pm \sin 72^\circ$). Ugyanígy

$$\varepsilon^2, \varepsilon^3 = \frac{\frac{-\sqrt{5}-1}{2} \pm \sqrt{\left(\frac{-\sqrt{5}-1}{2}\right)^2 - 4}}{2} = \frac{-\sqrt{5}-1}{4} \pm i\frac{\sqrt{2(5-\sqrt{5})}}{4}$$

(a valós rész $\cos 144^\circ$, a képzetes rész $\pm \sin 144^\circ$).

6.8.19. Az (1) és (2) esetben, amikor csak az egységszakasz adott, az alaptest a $\mathbb{Q}$. Az $\sqrt[5]{2}$ nem szerkeszthető, mert ötödfokú, és az 5 nem 2-hatvány. A $\sqrt[4]{2}$ szerkeszthető. Ez látszik abból, hogy a minimálpolinomjának felbontási teste nyolcadfokú bővítése $\mathbb{Q}$-nak (6.3.12. Gyakorlat), és a 8 egy 2-hatvány (6.8.15. Tétel). De egyszerűbb azt mondani, hogy a szerkesztés nyilvánvalóan elvégezhető: előbb 2-ből, majd $\sqrt{2}$-ből szerkesszünk négyzetgyököt.

A (3) és (4) esetben az alaptest $\mathbb{Q}(\sqrt[3]{2})$. A $\sqrt[6]{2}$ egy négyzetgyökvonással megszerkeszthető. Az $\sqrt[5]{2}$ foka viszont a 6.2.11. Gyakorlat miatt efölött a test fölött is 5, hiszen 5 és 3 relatív prímek. Ezért $\sqrt[5]{2}$ a $\sqrt[3]{2}$ segítségével sem szerkeszthető.

Az (5) esetben az alaptest a $\mathbb{Q}(\pi)$. A környégyszögesítés a $\sqrt{\pi}$ szerkesztését jelenti, ami most elvégezhető egy négyzetgyökvonással. A 6.2.15. Gyakorlat (10) pontja szerint $\sqrt{\pi}$ másodfokú $\mathbb{Q}(\pi)$ fölött.

Végül a (6) esetben az alaptest $\mathbb{Q}(\cos 40^\circ)$, és $\cos 20^\circ$-ot kell szerkeszteni. Ez nyilván elvégezhető szögfelezéssel. Valójában ha a szabályos 9-szög csúcsait összekötjük a középpontjával, és az egyeneseket meghosszabbítjuk, akkor a körülírt körrel való metszéspontjaik pontosan a szabályos 18-szög hiányzó csúcsait jelölik ki.

A $\cos 2\gamma = 2\cos^2\gamma - 1$ összefüggés miatt $\cos 2\gamma \in \mathbb{Q}(\cos\gamma)$ minden γ szögre. Ezt kétszer alkalmazva $\cos 20^\circ = -\cos 160^\circ \in \mathbb{Q}(\cos 40^\circ)$ adódik. Ezért $\cos 20^\circ$ elsőfokú $\mathbb{Q}(\cos 40^\circ)$ fölött.

6.8.20. A koordinátarendszert csak úgy szabad fölvenni, hogy $(0, 0)$ és $(1, 0)$ adott, vagy szerkeszthető pont legyen. Ebben az esetben ez nem teljesül.

6.8.21. Az Útmutatóban javasolt $a = 1$, $b = 1$, $f_a = 1$ feltehető, hiszen ha ebben a speciális esetben nem szerkeszthető meg a (létező) háromszög, akkor az általános esetben sem. Ekkor $\beta = \alpha$ és $\gamma = 180^\circ - 2\alpha$, hiszen az ABC háromszög most egyenlő szárú. Jelölje T az A csúcsból induló szögfelező metszéspontját a BC oldallal. Ekkor CAT is egyenlő szárú háromszög, és így a CTA szög is γ. Ezért az ABT háromszögben a szögek összege $(\alpha/2) + \alpha + 2\alpha = 180^\circ$, ahonnan $\alpha = 360^\circ/7$. Tehát ha a háromszöget meg lehetne szerkeszteni, akkor szabályos hétszöget is lehetne szerkeszteni, ami ellentmond a 6.8.11. Tételnek.

♫ Van ilyen háromszög: például az $A_1 \ldots A_7$ szabályos hétszögben $A_1A_3A_6$, mert az A_1A_3 és az A_1A_6 átlók egyenlőek, és az $A_6A_1A_3$ szög $\gamma = 3 \cdot 180^\circ/7$.

6.8.22. Az Útmutató jelöléseivel a háromszög területe $\rho(x + b) = xm$, ahol az alaphoz tartozó m magasság Pitagorasz tétele szerint $\sqrt{b^2 - x^2}$. Az egyenletet négyzetre emelve, $\rho = 1$ miatt

$$(x + b)^2 = x^2(b^2 - x^2) = x^2(b + x)(b - x)\,.$$

Így egyszerűsíthetünk $x + b$-vel. Átrendezve $x^3 - bx^2 + x + b = 0$ adódik. Ha például $b = 5$, akkor a kapott polinom a racionális gyökteszt miatt irreducibilis a $\mathbb{Q}$ alaptest fölött. Ezért a kapott x érték harmadfokú, azaz nem szerkeszthető.

♫ Némi geometriai intuícióval elképzelhetjük, hogy hány megoldása van a feladatnak. A szárak A metszéspontját helyezzük az egységsugarú kör kerületén kívülre, de ahhoz nagyon közel, rajzoljuk meg A-ból a körhöz a két érintőt, és mérjük föl rájuk A-ból a b távolságot. A kapott pontokat jelölje B és C. Ekkor az A-nál lévő szög csaknem 180°, és a BC egyenes nagyon közel van az A ponthoz. Most kezdjük el A-t távolítani a kör középpontjától. Ekkor a BAC szög csökken, a BC egyenes pedig kezd átkerülni a kör túlsó oldalára. Egy idő után, feltéve, hogy b nem túl pici szám, a BC egyenes „átér", és megoldást kapunk. Tegyük föl, hogy b hatalmas szám. Ekkor a BAC szög még mindig közel 180°, és a kapott x érték csak picivel lesz kevesebb b-nél. Ha tovább távolítjuk az A pontot, akkor elérünk abba az állapotba, amikor A távolsága a kör középpontjától durván $b - 1$, és a BAC szög már csaknem nulla fok. Ekkor újabb megoldást kapunk, melyben x értéke csak icipicit nagyobb, mint 1.

Mindezt algebrailag is megközelíthetjük. Az $f(x) = x^3 - bx^2 + x + b$-nek mint x polinomjának mindenképp van egy negatív valós gyöke -1 és 0 között, hiszen $f(-1) = -2$ és $f(0) = b > 0$. A diszkriminánsa $4(b^4 - 11b^2 - 1)$, ennek egyetlen pozitív valós gyöke közelítőleg $b = 3{,}33$. Az ennél kisebb (pozitív) b értékekre f-nek csak egy valós gyöke van (hiszen a diszkriminánsa negatív), tehát ekkor a feladatnak nincs megoldása. Ha b nagyobb ennél az értéknél, akkor f másik két gyöke pozitív (hiszen a gyökök összege $b > 0$ és $f(0) > 0$). A fenti esetben, amikor $b = 5$, a két pozitív megoldás közelítőleg $x = 1{,}307$ és $x = 4{,}537$.

6.8.23. A 3°-os szög szerkeszthető, mert ez a szabályos 120-szög középpontjában szereplő szög, és az $n = 120 = 2^3 \cdot 3 \cdot 5$ kielégíti a 6.8.11. Tétel feltételeit. Emiatt persze szerkeszthető n fokos szög minden $3 \mid n$ esetén. Ha most n tetszőleges, akkor osszuk el maradékosan 3-mal: $n = 3q + r$. Az előző megjegyzés miatt a $3q$ fokos szög szerkeszthető, és így az r fokos is. Az r lehetséges értékei 0, 1 és 2. De 1 és 2 fokos szög nem szerkeszthető, mert akkor 20°-os szög (és így szabályos 18-szög) is szerkeszthető lenne. Vagyis pontosan a 3-mal osztható n-ek felelnek meg.

6.8.24. Tekintsük a $K = \mathbb{Q}\big(\cos(2\pi/n)\big)$ test fölött az $i\sin(2\pi/n)$ számot. Ennek négyzete K-ban van, és ezért első- vagy másodfokú bővítést generál. A 6.8.11. Tétel bizonyításának végén beláttuk, hogy

$$\mathbb{Q}\big(\cos(2\pi/n), i\sin(2\pi/n)\big) = \mathbb{Q}\big(\cos(2\pi/n) + i\sin(2\pi/n)\big),$$

és hogy ennek foka $\mathbb{Q}$ fölött $\varphi(n)$. Ez a test nem valós, ha $n > 2$, a K viszont igen. Ezért a bővítés másodfokú, és így a szorzástétel miatt $\cos(2\pi/n)$ foka $\mathbb{Q}$ fölött $\varphi(n)/2$, ha $n > 2$. Ha $n = 1$ vagy 2, akkor az eredmény 1.

6.9. Egyenletek gyökjelekkel való megoldhatósága

6.9.3. A 6.6.12. Feladat megoldását módosítjuk. A $K(\varepsilon)$ test fölött Φ_n nem biztos, hogy irreducibilis, de ε minimálpolinomja ennek osztója. Ezért ε konjugáltjai továbbra is ε bizonyos hatványai lesznek, ezek benne vannak $K(\varepsilon)$-ban, és így a bővítés normális. A relatív automorfizmusok a $\psi_j(\varepsilon) = \varepsilon^j$ képlettel megadott leképezések között lesznek (ahol $(j, n) = 1$), de nem feltétlenül az összes ilyen leképezést kapjuk meg. E leképezések kompozíciója azonban ugyanúgy számolható ki, mint a $K = \mathbb{Q}$ esetben, és így a Galois-csoport részcsoportja $\mathbb{Z}_n^\times$-nek.

6.9.13. Legyen ε egy n-edik primitív egységgyök, és β az α szám egyik n-edik gyöke (egy bővítésben). Ekkor az $x^n - \alpha$ felbontási teste K fölött $L = K(\varepsilon, \beta)$. Ha φ relatív automorfizmus, akkor $\varphi(\varepsilon) = \varepsilon^a$, ahol $(a, n) = 1$ és $1 \le a < n$, továbbá $\varphi(\beta) = \varepsilon^b\beta$, ahol $0 \le b < n$, hiszen φ permutálja $\Phi_n(x)$ és $x^n - \alpha$ gyökeit is. Az $a \in \mathbb{Z}_n^\times$ és $b \in \mathbb{Z}_n$ számok már egyértelműen meghatározzák a φ automorfizmust, mert $K(\varepsilon, \beta) = L$. Jelöljük ezt a φ automorfizmust $\varphi_{a,b}$-vel.

Rendeljük hozzá $\varphi_{a,b}$-hez az Útmutatóban leírt $A(a, b) : x \to ax + b$ permutációt a $\mathbb{Z}_n$ halmazon. Megmutatjuk, hogy ez tartja a kompozíciót. Valóban,

$$A(a, b) \circ A(c, d) : x \mapsto a(cx + d) + b = acx + (ad + b),$$

azaz $A(a, b) \circ A(c, d) = A(ac, ad + b)$. Ugyanakkor $\varphi_{a,b}\varphi_{c,d}(\varepsilon) = \varepsilon^{ac}$ (lásd a 6.6.12. Feladat megoldását), továbbá

$$\varphi_{a,b}\varphi_{c,d}(\beta) = \varphi_{a,b}(\varepsilon^d\beta) = \varphi_{a,b}(\varepsilon)^d\varphi_{a,b}(\beta) = \varepsilon^{ad}\varepsilon^b\beta = \varepsilon^{ad+b}\beta.$$

Ezért a $\varphi_{a,b} \mapsto A(a, b)$ megfeleltetés művelettartó, és így a keresett Galois-csoport részcsoportja az A csoportnak.

Végül az A feloldható, mert az $A(1, b)$ alakú elemek $\mathbb{Z}_n^+$-szal izomorf kommutatív normálosztót alkotnak benne, és az erre vett faktor $\mathbb{Z}_n^\times$ lesz, ami szintén kommutatív (vö. 4.9.37. Gyakorlat). Mivel feloldható csoport részcsoportja is feloldható (4.13.17. Feladat), a keresett Galois-csoport is feloldható.

♫ Ha azokat az $A(a, b)$ permutációkat tekintjük, ahol $a = \pm 1$, akkor a D_n diédercsoporttal izomorf részcsoportot kapunk A-ban ($n \ge 3$ esetén).

6.9.14. Legyen az A minimálpolinomja $m(x) = (x-\lambda)g(x)$. Itt g alacsonyabb fokú, mint m, így $g(A) \neq 0$. Ez azt jelenti, hogy alkalmas w vektorra $v = g(A)(w) \neq 0$. Tudjuk, hogy $0 = m(A) = (A-\lambda I)g(A)$, ahol I az identitás. Ezt w-re alkalmazva $(A-\lambda I)v = 0$ adódik. Ezért v sajátvektor és λ sajátérték.

6.9.15. A $\psi(\beta) = \varepsilon_j \beta$ összefüggés nyilvánvaló számolással adódik. Legyen S az (ε_j, γ) elemek összege, midőn j befutja az $1, 2, \ldots, p$ számokat, és γ rögzített. Elég belátni, hogy S nincs benne K-ban. Valóban, ekkor az összeg valamelyik tagja sincs benne K-ban, de ez nem lehet (ε_p, γ), mert ezt ψ saját magába viszi, azaz K-beli.

Az S összeget közvetlenül kiszámíthatjuk. A p-edik egységgyökök összege nulla, és így az $\varepsilon_j^{-\ell}$ számok összege $\ell \neq 0$ esetén 0, ha meg $\ell = 0$, akkor az összeg p. Ezért $S = p\gamma$. Ha tehát $\gamma \notin K$, akkor ez nincs K-ban (ehhez elég csak annyit föltenni, hogy K karakterisztikája nulla legyen, sőt, hogy ne legyen p).

A 6.9.9. Lemma bizonyításában ez a gondolatmenet azt a részt váltja ki, amikor belátjuk, hogy a ψ lineáris transzformációnak valamelyik 1-től különböző p-edik egységgyök sajátértéke.

6.10. A legfeljebb negyedfokú egyenletek

6.10.1. A $\mathbb{Q}(\varepsilon)$ Galois-csoportja $\mathbb{Z}_9^\times \cong \mathbb{Z}_6^+$ (6.6.12. Feladat). Ez kommutatív, tehát minden részcsoportja normálosztó, azaz minden közbülső test normális. A komplex konjugálás másodrendű, tehát fixpontjai, azaz $\mathbb{Q}(\varepsilon)$ valós elemei egy harmadfokú, normális L bővítését alkotják $\mathbb{Q}$-nak. A Galois-csoport elemeit $\varepsilon + \overline{\varepsilon} = 2\cos 40^\circ$-re alkalmazva $\varepsilon^2 + \overline{\varepsilon}^2 = 2\cos 80^\circ$ és $\varepsilon^4 + \overline{\varepsilon}^4 = 2\cos 160^\circ$ adódik. Ezek tehát irracionális számok, amelyek mindegyike L-et generálja. A közös minimálpolinomjuk

$$\big(x - (\varepsilon + \overline{\varepsilon})\big)\big(x - (\varepsilon^2 + \overline{\varepsilon}^2)\big)\big(x - (\varepsilon^4 + \overline{\varepsilon}^4)\big) = x^3 - 3x + 1$$

(ez beszorzással adódik, felhasználva, hogy $\Phi_9(x) = x^6 + x^3 + 1$ miatt a primitív kilencedik egységgyökök összege nulla, továbbá hogy $\varepsilon^3 + \varepsilon^6 = -1$, hiszen ezek a harmadik primitív egységgyökök).

♫ A fenti egyenlőségről úgy is meggyőződhetünk, hogy az $\varepsilon + \overline{\varepsilon}$ számot behelyettesítjük az $x^3 - 3x + 1$ polinomba. Ekkor 0 adódik, és így ez a polinom csak a minimálpolinom lehet, mert $\varepsilon + \overline{\varepsilon}$-ról tudjuk, hogy harmadfokú. De akkor a polinomnak gyöke lesz $\varepsilon + \overline{\varepsilon}$ két másik konjugáltja is, tehát a fenti gyöktényezős alakot kapjuk.

Megjegyezzük, hogy a $g(z) = z^2 - 2$ függvény körbepermutálja az $x^3 - 3x + 1$ polinom gyökeit. Ebből is látszik, hogy egyetlen gyök hozzávételekor a másik két gyök automatikusan bekerül, és így normális bővítést kapunk. E polinom gyökei között tehát ezek a „rejtett összefüggések", ami miatt a Galois-csoportja csak $\mathbb{Z}_3^+$, és nem a teljes S_3.

A Cardano-képletből $x^3 - 3x + 1$ gyökei

$$\sqrt[3]{-\frac{1}{2} + \frac{\sqrt{3}}{2}i} + \sqrt[3]{-\frac{1}{2} - \frac{\sqrt{3}}{2}i}$$

lesznek. Ezzel semmi újat nem tudtunk meg róluk, hiszen a köbgyök alatt a primitív harmadik egységgyökök állnak, és nem okoz meglepetést az, hogy ha η primitív harmadik egységgyök, akkor $\sqrt[3]{\eta}$ primitív kilencedik egységgyök. (Persze a köbgyökök 3-3 értékét úgy kell párosítani, hogy a szorzatuk 1 legyen.)

6.10.3. Az, hogy a $\mathbb{Z}_3$ test 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 sem lehet behelyettesíteni a nevezőben található 3 miatt, de a képlet levezetésének a módszere sem működik. Valóban, a 8. oldalon található (1.3) egyenletrendszer $3uv = -p$ egyenlete három karakterisztikában nyilván csak $p = 0$ esetén teljesülhet.

Ha veszünk egy harmadfokú irreducibilis polinomot, mondjuk $x^3 - x + 1$-et $\mathbb{Z}_3$ fölött, akkor ennek egyetlen β gyöke az $\mathbb{F}_{27}$ 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 lesznek gyökkifejezések $\mathbb{Z}_3$ fölött a 6.9.8. Definíció értelmében! Ha ugyanis β gyökkifejezés 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 itt 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 $x^3 - \alpha = (x - \gamma)^3$.

6.10.5. Elég belátni, hogy a felbontási test nem változik meg. Ez azért igaz, mert α akkor és csak akkor gyöke $f(cx + d)$-nek, ha $c\alpha + d$ gyöke $f(x)$-nek. De α és $c\alpha + d$ egymással kifejezhetők, és így ugyanazt a testet generálják.

6.10.6. Beszorzással $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = s - t$ és $(\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_3) = s + t + 2\alpha_1\alpha_2\alpha_3$. Tudjuk, hogy a gyökök összege nulla, ezért ez a szorzat valójában $-\alpha_3\alpha_3\alpha_1$, azaz $s + t = -3\alpha_1\alpha_2\alpha_3 = 3q$. Mivel $st = \big((s + t)^2 - (s - t)^2\big)/4$, innen (2) is leolvasható.

A G Galois-csoport másodrendű elemei transzpozíciót adnak a gyökök halmazán ahonnan (4) adódik. Hasonlóan a harmadrendű elemek hármasciklusok, és így az s és t elemeket fixálják. Ezért s és t benne van az A_3 részcsoporthoz tartozó M résztestben. Az f irreducibilitása miatt G tranzitív, és így vagy S_3, vagy A_3. Ez utóbbi esetben $M = K$, tehát $s, t \in K$. (Ekkor persze $s - t \in K$, vagyis a diszkrimináns négyzetelem K-ban.) Ha viszont $G = S_3$, akkor M másodfokú bővítése K-nak. Ezt generálja s is és t is, mert különben $s, t \in K$ teljesülne, ami (4)-nek ellentmond. (Ekkor $s - t$ sem lehet K-ban, mert különben $s + t \in K$ miatt $s, t \in K$ lenne, tehát a diszkrimináns nem négyzetelem K-ban.)

6.10.7. 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 (4.8.15. Állítás). Ha G rendje 8, akkor 2-Sylow, és így D_4-gyel izomorf (4.11.27. Gyakorlat). Végül ha G rendje 4, akkor vagy ciklikus, vagy a Klein-csoporttal izomorf (4.5.18. Tétel). Ezért más Galois-csoport nem fordulhat elő, mint amit a feladatban felsoroltunk.

A 3.8.8. 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 (6.10.4. 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 $u_1 = (\alpha_1\alpha_2 + \alpha_3\alpha_4)/2$ (3.8.8. 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 (4.8.15. Állítás). 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 a pálya hosszát megadó 4.5.8. 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.

6.10.8. A 3.8.11. 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 6.10.7. 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 6.10.7. Feladat (3) 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.

6.10.9. A 3.8.8. Feladatban bizonyított összefüggéseket és az Útmutatóban bevezetett jelöléseket is 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 3.8.8. Feladatból tudjuk, hogy ha az u gyök segítségével bontjuk föl 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: $L^2(x)=e^2x^2-cx+(u^2-d)$, és itt a főegyüttható nem nulla. Ezért L^2 egyetlen gyöke $c/2e^2$, ahonnan

$$f(x)=(x^2+u)^2-(ex-c/2e)^2=(x^2-ex+u-c/2e)(x^2+ex+u+c/2e)\,.$$

Az $x^2-ex+u-c/2e$ diszkriminánsa $(\alpha_1-\alpha_2)^2=e^2-4u+2c/e$, ugyanígy $(\alpha_3-\alpha_4)^2=e^2-4u-2c/e$. Az $e^2=2u-b=(\alpha_1+\alpha_2-\alpha_3-\alpha_4)^2/4$ összefüggést felhasználva az Útmutatóban fölírt képlet adódik.

Legyen G az f Galois-csoportja. A 6.10.7. 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.

6.10.10. A 6.8.15. 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 6.10.7. Feladat szerint viszont az f felbontási testének foka akkor és csak akkor 2-hatvány, ha a harmadfokú rezolvensnek van gyöke K-ban.

7. fejezet

Modulusok

7.1. Részmodulusok, homomorfizmusok

7.1.2. Lásd 2.2.20. Gyakorlat (ide kapcsolódik a 2.2.37. Gyakorlat is).

7.1.5. A 4.6.1. Állítás bizonyítása lényegében szó szerint átvihető.

7.1.7. Mivel φ csoporthomomorfizmus is, a magja részcsoport. Azért lesz részmodulus, mert ha $\varphi(m) = 0$, akkor $\varphi(rm) = r\varphi(m) = r0 = 0$. Az alábbiak elolvasása előtt érdemes átismételni a 4.7.12. Állítás bizonyítását. 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. Ugyanezek a tételek még általánosabban is beláthatók (lásd 8.2.20. Feladat).

A csoportelméleti 4.7.24. Tétel és a gyűrűelméleti 5.2.11. Tétel moduluselméleti változata a következő. Tegyük föl, hogy $\varphi : M \to K$ szürjektív modulushomomorfizmus, melynek magja N. Ekkor a következő állítások teljesülnek.

(1) Ha U 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 izomorfizmustétel 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 izomorfizmustétel azt mondja ki, hogy ha $K \leq N \leq M$ részmodulusok, akkor $(M/K)/(N/K) \cong M/N$. Végül a homomorfizmustétel állítása az, hogy ha $\varphi : M \to K$ modulushomomorfizmus, akkor $\mathrm{Im}(\varphi) \cong M/\operatorname{Ker}(\varphi)$.

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 fölcserélhetők). 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-nek osztója, és így A 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 7.3.16. 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, amelyre $Av = w$ (például a lineáris leképezések 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. Ha $w \in W$, akkor $A(w) \in W$, innen $A^2(w) = A(A(w)) \in W$, és így tovább, azaz $A^i(w) \in W$ minden i-re. Legyen $f(x) = t_0 + t_1x + \ldots + t_kx^k \in T[x]$. Ekkor

$$fw = \big(t_0I + t_1A + \ldots + t_kA^k\big)(w) = t_0w + t_1A(w) + \ldots + t_kA^k(w)\,.$$

Ez az elem W-ben van, hiszen W altér.

7.1.12. Nem izomorfak. Ha ugyanis lenne e két modulus között egy $\varphi : \mathbb{R} \to \mathbb{R}$ modulus-izomorfizmus, akkor minden $f \in \mathbb{R}[x]$ polinomra

$$\varphi\big(f(1)r\big) = \varphi(fr) = f\varphi(r) = f(2)\varphi(r)$$

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 1×1-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, 7.3.19. 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. Ahhoz, hogy a φ leképezés jóldefiniált, azt kell ellenőrizni, hogy ha $m_1 + N = m_2 + N$, akkor $\varphi_0(m_1) = \varphi_0(m_2)$. Ez világos, hiszen ilyenkor $m_1 - m_2 \in N \subseteq \mathrm{Ker}(\varphi_0)$. A kapott φ összegtartó és skalárszorostartó, ez utóbbit látjuk be. A faktormodulusban a műveletet a reprezentánsokkal végezzük, és ezért $r \in R$ esetén

$$\varphi\big(r(m + N)\big) = \varphi(rm + N) = \varphi_0(rm) = r\varphi_0(m) = r\varphi(m + N)\,.$$

Az összegtartás hasonlóan igazolható.

7.2. Direkt összeg és függetlenség

7.2.2. Csak a különbségeket mutatjuk meg a 4.9.14. 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 az $m = (\ldots, m_i, \ldots) \in M$ elemnek csak az első, hatodik és tizedik komponense nem nulla, akkor

$$m = (m_1, 0, \ldots) + (\ldots, 0, m_6, 0, \ldots) + (\ldots, 0, m_{10}, 0, \ldots)\,.$$

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 komponense nulla.

Most tegyük föl, hogy az M_i^* részmodulusokra teljesül az (1) és a (2). Tekintsük a

$$\varphi : (\ldots, m_i, \ldots) \mapsto \sum_{i \in I} m_i$$

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 $m_{i_1}, \ldots, m_{i_n}$, ekkor

$$\varphi(m) = m_{i_1} + \ldots + m_{i_n} = 0\,, \quad \text{azaz} \quad m_{i_1} = -m_{i_2} - \ldots - m_{i_n}\,.$$

Ez azonban azt jelentené, hogy a $0 \neq m_{i_1}$ 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 ugyanazt állítja, mint a (2), csak a (2) állítását az m_i helyett az $r_i m_i \in M_i$ elemekre kell alkalmazni.

7.2.5. Ha r invertálható eleme az R gyűrűnek, akkor $rm = 0$-ból $m = 0$ következik (az r inverzével kell balról szorozni, lásd a 2.2.29. Tétel, illetve az 1.3.7. Következmény bizonyítását). Speciálisan vektortérben (sőt, ferdetest fölötti modulusban is) igaz, hogy ha $rm = 0$, akkor $r = 0$ vagy $m = 0$. 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 rendszere sincs, hiszen minden b elemre $6b = 0$, de $6 \neq 0$.

7.2.7. A 6 nem tehető be $\mathbb{Z}_{12}^+$ egyetlen gyenge bázisába sem. Ha ugyanis $6 = b_1, b_2, \ldots, b_n$ gyenge bázis, akkor $3 = r_1 b_1 + \ldots + r_n b_n$ alkalmas $r_i \in \mathbb{Z}$ elemekre, 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 ez a rendszer 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 $r_1b_1 + \ldots + r_nb_n = 0$, 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, mert $A(v) = v \in \langle v \rangle$ 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 (1.5.9. Feladat) megoldását követjük. Az $O(rm)$ elemei azok a $t \in R$ elemek, melyekre $trm = 0$, vagyis $tr \in O(m)$. De

$$trm = 0 \iff o(m) \mid tr \iff \frac{o(m)}{(o(m), r)} \text{ osztója } t\text{-nek}$$

(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 többszöröse volna, és ilyenkor a modulus annullátora csak a $\{0\}$, vagyis az exponense is nulla.

7.3.9. 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 $\varphi : r \mapsto rm$ modulushomomorfizmus szürjektív ${}_RR$-ből $\langle m \rangle$-re, és így a homomorfizmustétel 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 generátora. Ekkor $sm_1 = m_2$ alkalmas $s \in R$ elemre. Ha $rm_1 = 0$, akkor $rm_2 = rsm_1 = srm_1 = s0 = 0$, hiszen R kommutatív. 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.

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 ${}_RR$ 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 generátor rendjének a hatvány rendjének képlete miatt, ezért (5) is igaz (hiszen a 7.3.7. Gyakorlat miatt az exponens az elemrendek legkisebb közös többszöröse).

7.3.10. Az alábbiak elolvasása előtt érdemes átismételni az analóg csoportelméleti állítások 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 $r_1v_1 + \ldots + r_kv_k = 1$. Ekkor

$$m = (r_1v_1 + \ldots + r_kv_k)m = r_1(v_1m) + \ldots + r_k(v_km)\,.$$

Ez azt jelenti, hogy $\langle m\rangle \subseteq \langle v_1m\rangle + \ldots + \langle v_km\rangle$. A fordított tartalmazás nyilvánvaló, hiszen $v_im \in \langle m\rangle$. Ezért már csak azt kell megmutatni, hogy a $v_1m, \ldots, v_km$ elemek gyengén függetlenek (a 7.2.8. Gyakorlat miatt). Tegyük föl, hogy $s_1v_1m + \ldots + s_kv_km = 0$. Ekkor $o(m) = u$ osztója $s_1v_1 + \ldots + s_kv_k$-nak. Mivel $u_i \mid v_j$ ha $j \neq i$, innen kapjuk, hogy $u_i \mid s_iv_i$. De u_i és v_i relatív prímek, ezért $u_i \mid s_i$. Ekkor viszont $u = u_iv_i \mid s_iv_i$, ahonnan $s_iv_im = 0$ (hiszen az m rendje u). Tehát a v_im elemek tényleg gyengén függetlenek. A hatvány rendjének képlete miatt $o(v_im) = u/v_i = u_i$, 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 $\pi_1 : (x, y) \mapsto x$ és $\pi_2 : (x, y) \mapsto y$ projekcióhomomorfizmusoknál 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.

7.3.12. 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, mert R nullosztómentes, 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.

A $\mathbb{Z}_6$ gyűrűt önmaga fölött modulusnak képzelve 2 és 3 torzióelemek, hiszen rendjük 3, illetve 2, de az összegük nem az, mert az 5 rendje nulla.

7.3.14. 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 4.3.24. 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 pedig $m\,\mathbb{Z}_n^+$. A homomorfizmustétel miatt $m\,\mathbb{Z}_n^+$ 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 $\mathbb{Z}_n^+ / m\,\mathbb{Z}_n^+ \cong \mathbb{Z}_{(m,n)}^+$.

7.3.15. A számolások nyilvánvalóak, az R kommutativitása ahhoz kell, hogy részmodulust kapjunk (és ne csak részcsoportot).

7.3.16. Ahhoz, hogy $\big(s + (r)\big)m = sm$ jóldefiniált, azt kell belátnunk, 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 4.9.34. 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.

7.3.17. 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 (4.4.27. 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.

7.3.18. Könnyű belátni, 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. 7.3.9. Feladat) melyik polinom.

Az A karakterisztikus polinomja $f(x) = -x(1-x)^2$ (hiszen felső háromszög-mátrixról van szó). 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 7.3.9. Gyakorlat (5) pontja miatt.

A 7.3.9. 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 3.1.22. Gyakorlat (2) pontja miatt) hat. Ha $g \mid x(x-1)^2$, akkor a hozzá tartozó részmodulus $\langle gu \rangle$ lesz, ez leolvasható a 7.3.9. Feladat megoldásából.

7.3.19. 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.

7.3.20. 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 $o(b)/p$.

7.3.21. 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 7.3.10. Gyakorlat (4) állításának speciális esete, amikor az u_i elemek az u elemnek a prímhatványosztói.

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. Az eredeti összefüggésből $m_1 = 0$.

7.3.22. Az állításokat már beláttuk a 7.3.9. Feladat megoldásában.

7.3.23. 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-ből M_j-re. Megjegyezzük, hogy az M_i modulusok izomorfiája a 7.9.22. Feladatból is következik.

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 rendszer is az, 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 tényleg független.

Gyenge függetlenségre ez a gondolatmenet nem működik: 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 $b_1' = 3 +_6 4 = 1$. De az 1 és a 3 nem gyengén függetlenek, hiszen $3\cdot 1 +_6 1\cdot 3 = 0$, 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 7.3.10. 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 (1) esetében a mátrix sorai olyan (u, v) egész számokból álló számpárok, 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 létezik egy olyan b_1, b_2 bázis, amelyre $\mathbb{Z}_6^+ \cong (\mathbb{Z}^+ \times \mathbb{Z}^+)/K$, 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 7.3.10. 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.

$$\begin{bmatrix} -x & 1 & 0 \\ 0 & -x & 0 \\ 0 & 0 & -x \end{bmatrix} \begin{bmatrix} 1 & -x & 0 \\ -x & 0 & 0 \\ 0 & 0 & -x \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -x & -x^2 & 0 \\ 0 & 0 & -x \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -x & 0 \\ 0 & 0 & -x^2 \end{bmatrix}.$$

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 aldeterminánsban lesz az oszlopok valamelyik sorrendjében. Ezért ebben a harmadik esetben két $i \times i$ méretű aldeterminánsban „helyet cserél" (és még az előjelük is megváltozhat). De ekkor az összes ilyen aldeterminánsban 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 $a = \det(v_1, v_2, \ldots, v_i)$ aldeterminánsban, ha ennek valamelyik, mondjuk az első oszlopához egy olyan u oszlop r-szeresét adtuk, ami ezen az aldeterminánson kívül van. Ekkor azonban szerepel a $\pm b = \det(u, v_2, \ldots, v_i)$ aldeterminánsban 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 aldeterminánsban értéke $s_1 s_2 \ldots s_i$. Ugyanakkor ha egy $i \times i$ méretű aldeterminánsban nem 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 ([2], 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 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 pontosan akkor nulla, ha sorai lineárisan összefüggenek. (Ezt testre bizonyítottuk, de az R szokásos gyűrűre is igaz: az R hányadostestére kell alkalmazni, majd a nevezőkkel fölszorozni.) 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 fölírni, 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 a 7.4.15. 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 maximumfeltétel. 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 maximumfeltétel 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 nyilvánvalóan generálják az $a_1 + T, \ldots, a_k + T$ elemei, azt kell megmutatni, hogy ezek 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 (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, $r_ip^{\alpha_i - 1}c_i = 0$, 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 belátásához, 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 $r_i = t_i p^{\alpha_i - 1}$ alkalmas t_i-re. De akkor

$$b = t_1 p^{\alpha_1 - 1} c_1 + \ldots + t_n p^{\alpha_n - 1} c_n + 0 + \ldots + 0 = t_1 c_1'' + \ldots + c_n''.$$

7.5.4. Nyilván $r_1c_1' + \ldots + r_nc_n' + s_1d_1' + \ldots + s_mc_m'$ akkor és csak akkor nulla az $M/M[p]$ faktormodulusban, 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 7.3.20. 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 $p^m v = 0$ alkalmas m egészre, és $p^m v = (A - \lambda E)^m(v)$.

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

$$r_1(b_1 + pM) + \ldots + r_k(b_k + pM) = (r_1b_1 + \ldots + r_kb_k) + pM$$

pontosan 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 következik, hogy a bázis elemszáma egyértelmű, feltéve, hogy R-ben van prím. Előfordulhat, hogy nincs prím, például ha R 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 7.3.21. 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 $p^mc = 0$ miatt p^m-nek valódi osztója), akkor $f \mid p^{m-1}$, azaz $c_m = p^{m-1}c = 0$ (és a nullvektor nem lehet benne független rendszerben).

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 $p^mc = 0$. 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 $L - xE$ 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).

$$\begin{bmatrix} 1 & 0 \\ 0 & -(x-1)^2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x(3-x) \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & (x^3-x^2)/2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1-x^3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \varepsilon_1 & 0 \\ 0 & 0 & \varepsilon_1 \end{bmatrix}$$

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.

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

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 T végtelen test, V egy k-dimenziós vektortér T fölött, A lineáris transzformációja V-nek 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 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 tartozhat, vagyis a tényezők páronként relatív prímek. Ezért M ciklikus modulus (7.3.10. Gyakorlat).

Megfordítva, ha M ciklikus, és egy u elem generálja, akkor a 7.3.9. Feladat miatt a részmodulusok kölcsönösen egyértelmű megfeleltetésben állnak az u rendjének osztóival (asszociált osztókat nem különböztetjük meg). Így véges sok invariáns altér van. Az u rendje a modulus exponense, vagyis az A minimálpolinomja. Egy konkrét ilyen példát elemeztünk a 7.3.18. Gyakorlatban.

Végül a 7.4.10. Gyakorlat miatt M pontosan akkor ciklikus, ha az A karakterisztikus mátrixának normálalakjában szereplő $s_1, \dots, s_k$ 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. Az invariáns alterek száma ilyenkor a minimálpolinom normált osztóinak a száma (hiszen a minimálpolinom a modulus exponense).

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 fölcserélhető R minden elemével.

7.7.5. Legyen $\varphi \in \mathrm{Hom}(\mathbb{Z}_m^+, \mathbb{Z}_n^+)$, és $\varphi(1)$ rendje d. Ekkor d osztója n-nek, mert $\varphi(1) \in \mathbb{Z}_n^+$, és d 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 oldjuk meg a 7.7.26. Gyakorlatot, majd alkalmazzuk a 7.3.14. Gyakorlatot.

7.7.10. Feleltessük meg a $b \in M$-nek 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 skalárszorostartó 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

$$\mathrm{Hom}_R\Big(\bigoplus_i M_i,\, K\Big) \cong \prod_i \mathrm{Hom}_R(M_i, K)\,,$$

legyen $(\ldots, \varphi_i, \ldots) \in \prod_i \mathrm{Hom}_R(M_i, K)$ képe $\varphi \in \mathrm{Hom}_R\left(\bigoplus_i M_i, K\right)$, ahol

$$\varphi(\ldots, m_i, \ldots) = \sum_i \varphi_i(m_i)\,.$$

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

$$\mathrm{Hom}_R\left(M, \prod_i K_i\right) \cong \prod_i \mathrm{Hom}_R(M, K_i)\,.$$

Legyen $(\ldots, \varphi_i, \ldots) \in \prod_i \mathrm{Hom}_R(M, K_i)$ képe $\varphi \in \mathrm{Hom}_R\left(M, \prod_i K_i\right)$, ahol

$$\varphi(m) = (\ldots, \varphi_i(m), \ldots)\,.$$

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

$$\bigoplus_i \mathrm{Hom}_R(M, K_i) \hookrightarrow \mathrm{Hom}_R\left(M, \bigoplus_i K_i\right) \hookrightarrow \prod_i \mathrm{Hom}_R(M, K_i)$$

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 a b által generált A részcsoportot, ennek rendje n, és elég belátni, hogy ebben b osztható minden n-hez relatív prím m számmal. Ezt kongruenciákkal azonnal láthatjuk, sőt már igazoltuk is a 4.3.35. 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 1.5.13. 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, elég belátni, 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, melynek rendje a lehető legnagyobb. Jelölje ezt a rendet n. Mivel A osztható, van olyan $b \in A$, melyre $nb = a$. A 4.3.36. 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 leképezés 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 skalárszorostartás 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 belátni, 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 homomorf képe véges rendű. Általában igaz, hogy $\mathrm{Hom}(A, B) = 0$, ha A torziócsoport, B pedig torziómentes.

(2) $\mathrm{Hom}(\mathbb{Q}^+, \mathbb{Z}^+) = \mathrm{Hom}(\mathbb{Q}^+, \mathbb{Z}_n^+) = 0$, mert $\mathbb{Q}^+$ osztható csoport, $\mathbb{Z}^+$-nek és $\mathbb{Z}_n^+$-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 azt kell végiggondolni, 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. 2.2.37. 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 kell ilyen részletesen indokolni a fentieket, akkor nézze meg a 2.2.43. Gyakorlat megoldását. Ide kapcsolódik a 7.3.16. 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.

Be kell még látni, hogy a $b \leftrightarrow \varphi_b$ leképezés izomorfizmus $\mathrm{Hom}(\mathbb{Z}_m^+, B)$ 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. Legyen $f \in \mathrm{Hom}(A, B)$, ekkor $\mathrm{Hom}(id_A, \varphi) : f \to f \circ \varphi$. De

$$(f \circ \varphi)(a) = f\big(\varphi(a)\big) = f(na) = nf(a)\,.$$

Ezért $f \circ \varphi = nf$. Hasonlóan látható, hogy a $\mathrm{Hom}(\varphi, id_A)$ leképezés, amely minden $f \in \mathrm{Hom}(B, A)$-hoz a $\varphi \circ f$-et rendeli, szintén az n-szerezés.

7.7.28. A pozitív valós számok csoportja a szorzásra osztható, hiszen minden pozitív valós számból vonható (pozitív) n-edik gyök minden n-re. Ez a csoport $\mathbb{R}^+$-szal izomorf a 4.3.3. Példa (4) pontja szerint. Osztható Abel-csoport nem lehet szabad, hiszen a szabad generátorokat csak 1-gyel és -1-gyel lehet elosztani egy szabad csoportban (miként $\mathbb{Z}^+$-ben is).

A pozitív racionális számok csoportja a szorzásra viszont szabad (és nem osztható). Szabad generátorrendszert alkotnak benne a prímszámok, hiszen minden pozitív racionális szám egyértelműen írható véges sok prímszám egész kitevős hatványának szorzataként. Ez a csoport a $\mathbb{Z}^+$ megszámlálható sok példányban vett direkt összegével izomorf.

7.7.29. A $\mathrm{Hom}(id_K, \varphi)$ injektivitása azt jelenti, hogy a magja nulla, vagyis ha $f \in \mathrm{Hom}_R(K, N)$, akkor $\varphi \circ f = 0$ esetén $f = 0$. Ez igaz, mert ha $f \neq 0$, akkor van olyan $k \in K$, hogy $f(k) \neq 0$, de akkor φ injektivitása miatt $(\varphi \circ f)(k) = \varphi\big(f(k)\big) \neq 0$. Ezért (1) igaz.

Legyen $N = \mathbb{Z}^+$, $M = \mathbb{Z}_n^+$, φ a mod n vett maradék képzése és $K = \mathbb{Z}_n^+$. Ekkor $\mathrm{Hom}(K, N) = 0$, hiszen $K = \mathbb{Z}_n^+$ torziócsoport, $N = \mathbb{Z}^+$ pedig torziómentes. Ezért az $f : K \to M$ identikus leképezés biztosan nem kapható meg $\mathrm{Hom}(K, N) = 0$ egy elemének képeként, vagyis $\mathrm{Hom}(id_K, \varphi)$ nem szürjektív. Ezért (2) hamis.

A $\mathrm{Hom}(\varphi, id_K)$ injektivitása azt jelenti, hogy ha $f \in \mathrm{Hom}_R(M, K)$, akkor $f \circ \varphi = 0$ esetén $f = 0$. Ez igaz, mert φ szürjektív, és így $f \circ \varphi = 0$ azt jelenti, hogy f a φ képén, azaz a teljes M-en nulla. Ezért (3) igaz.

Legyen $N = \mathbb{Z}^+$, $M = \mathbb{Q}^+$, $\varphi : \mathbb{Z}^+ \to \mathbb{Q}^+$ az identikus beágyazás és $K = \mathbb{Z}^+$. Ekkor $\mathrm{Hom}(M, K) = 0$ a 7.7.25. Gyakorlat (2) pontja miatt. Ezért az $f : N \to K$ identikus leképezés biztosan nem kapható meg $\mathrm{Hom}(M, K) = 0$ egy elemének képeként, vagyis $\mathrm{Hom}(\varphi, id_K)$ nem szürjektív. Ezért (4) hamis.

7.7.30. Az állítások rutinszerű ellenőrzését az Olvasóra hagyjuk.

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 skalárszorostartás az első változóban azt jelenti, hogy $(rx)y = r(xy)$, ez az R szorzásának az asszociativitásából következik. A skalárszorostartás a második változóban azt jelenti, hogy $x(ry) = r(xy)$. Ennek igazolásához R kommutativitását is föl 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. Be kell látni, hogy két bilineáris függvény összege is bilineáris, továbbá, hogy a pontonkénti összeadásra és skalárral való szorzásra teljesül az összes modulusaxióma. A 7.7.2. Gyakorlat megoldásához hasonlóan ezt is az Olvasóra hagyjuk.

7.8.5. A bihomomorfizmus-tulajdonságokat úgy 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 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 7.3.14. 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

$$\sum_i r_i(s_i \otimes b_i) = 1 \otimes \Big(\sum_i r_i s_i b_i \Big) .$$

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

$$\sum_i n_i(m_i \otimes b_i) = 1 \otimes \Big(\sum_i n_i m_i b_i \Big) .$$

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 $mB \subseteq \operatorname{Ker}(\varphi_0)$, 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. 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 $\varphi \circ \psi = id_{K_1}$.

7.8.22. 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

$$m = (\ldots, m_i, \ldots) \in \bigoplus_i M_i$$

és $k \in K$. Ekkor $f(m, k) = (\ldots, m_i \otimes k, \ldots)$ bihomomorfizmus, amely egy olyan

$$\varphi : \Big(\bigoplus_i M_i\Big) \otimes K \to \bigoplus_i (M_i \otimes K)$$

homomorfizmust eredményez, melyre $\varphi\big((\ldots, m_i, \ldots) \otimes k\big) = (\ldots, m_i \otimes k, \ldots)$. Ennek inverzét a következőképpen kapjuk meg. Legyen $m_i \in M_i$ esetén

$$f_i(m_i, k) = (\ldots, 0, m_i, 0, \ldots) \otimes k \in \Big(\bigoplus_i M_i\Big) \otimes K\,.$$

Ezt a tenzorszorzaton keresztülvezetve egy $\psi_i : M_i \otimes K \to \big(\bigoplus_i M_i\big) \otimes K$ homomorfizmust kapunk. Legyen

$$\psi(\ldots, x_i, \ldots) = \sum_i \varphi_i(x_i)$$

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.

7.8.23. 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 a 7.8.22. Feladat (3) pontjának megoldása miatt ez nem fordulhat elő.

7.8.24. Tudjuk, hogy

$$(\psi\otimes\chi)(a\otimes b)=\psi(a)\otimes\chi(b)=(na)\otimes(mb)=(nm)(a\otimes b)\,.$$

Vagyis $\psi\otimes\chi$ az $a\otimes b$ alakú elemeket nm-szerezi. Mivel ezek generátorrendszert alkotnak, ezért $\psi\otimes\chi$ az $A\otimes B$ minden elemét nm-szerezi.

7.8.25. Legyen $m\in M$ és $k\in K$. Mivel φ szürjektív, van olyan $n\in N$, hogy $\varphi(n)=m$. Ezért

$$(id_K\otimes\varphi)(k\otimes n)=id_K(k)\otimes\varphi(n)=k\otimes m\,.$$

Így $id_K\otimes\varphi$ képe tartalmazza a $k\otimes m$ alakú elemeket. Mivel ezek generátorrendszert alkotnak $K\otimes M$-ben, ezért $id_K\otimes\varphi$ szürjektív. Ezért (1) igaz.

Legyen $N=\mathbb{Z}^+$, $M=\mathbb{Q}^+$, $\varphi:\mathbb{Z}^+\to\mathbb{Q}^+$ az identikus beágyazás és $K=\mathbb{Z}^+_n$. Ekkor

$$(id_K\otimes\varphi)(1\otimes 1)=id_K(1)\otimes\varphi(1)=1\otimes 1=(n\cdot 1)\otimes(1/n)=0\otimes(1/n)=0\,.$$

Ugyanakkor az $1\otimes 1\in\mathbb{Z}^+_n\otimes\mathbb{Z}^+_n$ elem nem nulla, mert $f(x,y)=xy$ olyan bihomomorfizmus $\mathbb{Z}^+_n\times\mathbb{Z}^+_n$-ből $\mathbb{Z}^+_n$-ba, amelyre $f(1,1)\neq 0$ (ha $n>1$, lásd a 7.8.17. Gyakorlat (2) pontjának megoldását). Vagyis $id_K\otimes\varphi$ nem injektív, és így (2) hamis.

7.8.26. 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

$$(\varphi\otimes\varphi)(1\otimes 1)=2\otimes 2=2(1\otimes 2)=1\otimes(2\cdot 2)=1\otimes 0=0\,.$$

7.8.27. Legyen $s\in T$, és $f : T\times M\to T\otimes M$ az a bihomomorfizmus, 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

$$\varphi_{s_1+s_2}=\varphi_{s_1}+\varphi_{s_2}\quad\text{és}\quad\varphi_{s_1s_2}=\varphi_{s_1}\circ\varphi_{s_2}\,.$$

Ezért a most definiált szorzás modulussá teszi $T\otimes M$-et T fölött (ez lényegében következik a 7.7.30. 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 7.8.22. 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 $T \otimes M_i$ 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.

7.9. Nemkommutatív gyűrűk

7.9.3. Páros számlálójú tört alatt természetesen olyat értünk, amelynek a nevezője páratlan (hiszen különben minden törtet 2-vel bővítve páros számlálójú törtet kapnánk). Könnyű meggondolni, hogy az R gyűrű invertálható elemei a páratlan számlálójú törtek.

Ha b páratlan egész szám, akkor az $1 - (2a/b)$ invertálható R-ben, inverze $b/(b-2a)$ (hiszen $b-2a$ páratlan szám). Mivel $2a/b$ minden q többszöröse is páros számlálójú, ezért $1-q$ is invertálható. Így $J(R)$ tartalmazza a páros számlálójú törteket. Ha viszont c is, b is páratlan, akkor c/b nincs benne $J(R)$-ben, mert már $1 - c/b = (b-c)/b$ is páros számlálójú (nevezője pedig páratlan), és így nem invertálható. Ezzel az első állítást beláttuk.

A $\mathbb{Z}$ Jacobson-radikálja viszont csak a nullából áll. Valóban, $\mathbb{Z}$ invertálható elemei 1 és -1. Ha tehát $1 - ra$ minden $r \in \mathbb{Z}$-re invertálható, akkor $1 - ra = \pm 1$ minden r esetén. De itt végtelen sok számról van szó, kivéve, ha $a = 0$.

Megjegyezzük, hogy $\mathbb{Z}$-ben az $1 - 2 = -1$ invertálható, de a 2 még sincs benne a Jacobson-radikálban. Ez a példa mutatja, hogy a definícióban valóban minden r-re meg kell követelni $1 - ra$ invertálhatóságát.

7.9.5. Tegyük föl, hogy $e^2 = e \in J(R)$. Ekkor $1 - e$-nek létezik egy s balinverze, azaz $s(1-e) = 1$. Jobbról e-vel szorozva $e = s(1-e)e = s(e - e^2) = 0$.

7.9.16. Legyen $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ az n prímtényezős felbontása, ahol mindegyik $\alpha_i \geq 1$, és $m = p_1 \dots p_k$. Megmutatjuk, hogy $J(\mathbb{Z}_n) = (m)$.

Valóban, az m számot az α_i kitevők maximumára emelve n-nel osztható lesz, Ezért m nilpotens eleme $\mathbb{Z}_n$-nek, és így a 7.9.2. Állítás miatt benne van $J(\mathbb{Z}_n)$-ben. Ekkor persze m többszörösei is benne vannak. Más elem viszont nem lehet benne, mert a Wedderburn–Artin-tétel szerint $J(\mathbb{Z}_n)$ minden eleme nilpotens. Ha pedig $a \in \mathbb{Z}_m$ nilpotens, akkor $p_i \mid a^\ell$ alkalmas ℓ egészre, azaz $p_i \mid a$. Ez minden i-re igaz, és így $m \mid a$.

♫ Természetesen a Wedderburn–Artin-tétel felhasználása nélkül is kihozhattuk volna, hogy (m)-en kívül nincs eleme a radikálnak, akár az inverzek kiszámolásával, akár annak megmutatásával, hogy a $\mathbb{Z}_n$ maximális ideáljai a p_i által generált k darab főideál, és ezek metszete (m).

Tudjuk, hogy $\mathbb{Z}_n \cong \mathbb{Z}/(n)$, és az $(m) \lhd \mathbb{Z}_n$ ideálnak a teljes inverz képe $\mathbb{Z}$-ben (m) lesz. Így az 5.2.11. Tétel miatt $\mathbb{Z}_n/(m) \cong \mathbb{Z}_m$. Az 5.1.23. Gyakorlat szerint tehát $\mathbb{Z}_m/J(\mathbb{Z}_m)$ izomorf a $\mathbb{Z}_{p_1}, \dots, \mathbb{Z}_{p_k}$ testek direkt szorzatával.

7.9.17. Egy felső háromszögmátrix akkor és csak akkor invertálható, ha determinánsa nem nulla, azaz ha a főátlójában nem fordul elő a nulla. Ebből azonnal látszik, hogy ha M felső háromszögmátrix, és $E - (\lambda E)M$ minden λ skalár esetén invertálható, akkor M főátlójában csupa nulla kell, hogy szerepeljen. Így $J(R)$-ben csak szigorú felső háromszögmátrixok lehetnek (amelyek főátlója végig nulla).

Megmutatjuk, hogy a szigorú felső háromszögmátrixok mind benne vannak a radikálban. A 7.9.2. Gyakorlat miatt ehhez elég belátni, hogy nilpotensek, és ideált alkotnak R-ben. A nilpotencia közvetlen számolással kapható, az 5.3.19. Gyakorlat miatt pedig tényleg ideálról van szó, amely szerinti faktor T^n-nel izomorf.

♫ Természetesen könnyű „kézzel” is kiszámolni, hogy ha M szigorú felső háromszögmátrix és N felső háromszögmátrix, akkor NM is szigorú felső háromszögmátrix, és így $E - NM$ determinánsa 1, azaz invertálható. Tehát M benne van a radikálban. A radikál szerinti faktorizálásnál a mátrixokból „eltüntetjük” a főátló fölötti elemeket, tehát a faktorban csak a főátló elemei „számítanak”, és ezért lesz a faktor T^n-nel izomorf.

7.9.18. Az R gyűrűben nem lehet nullától különböző nilpotens elem. Valóban, ha $r^k = 0$, akkor r minden elég nagy kitevőjű hatványa is nulla. Márpedig az $r^n = r$ egyenletből következik, hogy $r^{1+\ell(n-1)} = r$ minden $\ell \geq 1$ esetén. Ez tényleg csak $r = 0$ esetén lehetséges.

Ebből a Wedderburn–Artin-tétel szerint következik, hogy $J(R) = \{0\}$ (hiszen a radikál minden eleme nilpotens). Adunk azonban erre az állításra egy másik bizonyítást is, ami végtelen R gyűrűre is működik. Legyen $e = r^{n-1}$, akkor $e^2 = r^{2n-2} = r^n r^{n-2} = rr^{n-2} = r^{n-1} = e$. Ha $r \in J(R)$, akkor tehát e idempotens eleme $J(R)$-nek, ami a 7.9.5. Gyakorlat szerint csak $e = 0$ esetén lehetséges. De akkor $r = r^n = er = 0$.

Tehát a Wedderburn–Artin-tétel szerint R teljes mátrixgyűrűk direkt szorzata. Egy teljes mátrixgyűrűben azonban mindig van szigorú felső háromszögmátrix, ami nilpotens, kivéve ha a mátrixgyűrű 1×1-es. Ezért R ferdetestek direkt szorzata. Ezek végesek, és így a 6.7.13. Wedderburn-tétel szerint kommutatívak. Ezért R is kommutatív.

7.9.19. 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 $N + K = M$.

7.9.20. 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 $N \cong M/K \cong M_i$.

7.9.21. A szabad R-modulusok teljesen reducibilisek, hiszen ezek ${}_R R$ diszkrét direkt hatványai, és ezek is előállnak az M_i modulusok példányainak direkt összegeként. De minden R-modulus egy szabadnak homomorf képe, ezért az előző 7.9.20. Gyakorlat miatt teljesen reducibilis. Ha ez a modulus egyszerű is, akkor az idézett gyakorlat (2) pontja miatt valamelyik M_i-vel izomorf.

7.9.22. Legyen $r \in R$, ekkor az r elemmel való jobbszorzás, vagyis az $s \mapsto sr$ leképezés egy ${}_R R \to {}_R R$ modulushomomorfizmus. Így ${}_R(Jr)$ vagy nulla, vagy izomorf ${}_R J$-vel. Másrészt $I = \sum\{Jr \,:\, r \in R\}$ kétoldali ideál, és így R egyszerűsége miatt $I = R$, azaz ${}_R R$ teljesen reducibilis. Mivel ${}_R R$ izomorf az ${}_R J$ példányainak összegével, ezért az előző 7.9.21. Gyakorlat miatt minden egyszerű R-modulus izomorf ${}_R J$-vel.

7.9.23. Legyen $R = A_1 \times \cdots \times A_k$ a teljes mátrixgyűrűk direkt szorzatára való felbontás. A 7.9.22. Feladat állítása minden ferdetest fölötti teljes mátrixgyűrűre vonatkozik, hiszen ezek egyszerűek (5.3.18. Feladat), és Artin-félék (mert véges dimenziós algebrák), tehát van minimális balideáljuk. (A minimális balideáljaik leírása a 8.7.10. és a 8.7.12. Feladatokban olvasható.) A 7.3.23. Feladatban láttuk, hogy hogyan lehet ezt a gyűrűt minimális balideálok direkt összegére bontani.

Legyen tehát J_i az A_i egy minimális balideálja, ekkor A_i előáll J_i példányainak (direkt) összegeként. 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 minimális balideáljainak (vagyis az ${}_R J_i$ balideáloknak) összegeként, akkor éppen k-féle izomorfiatípus fog szerepelni. A 7.9.21. Gyakorlat miatt minden egyszerű R-modulus izomorf valamelyik ${}_R J_i$-vel, és mindegyik R-modulus teljesen reducibilis.

7.9.24. Jelölje J az ${}_R R$ minimális balideáljainak összegét (ha nincs ilyen, akkor $J = 0$). A Krull-tétel bizonyításához (292. oldal) hasonlóan látjuk, hogy ha $J \neq R$, akkor J része egy K maximális balideálnak.

Ez direkt összeadandó, vagyis ${}_RR = K \oplus N$ alkalmas N balideálra. Mivel K maximális, ${}_RR/K \cong N$ egyszerű modulus, vagyis minimális balideál. Ezért $N \subseteq J \subseteq K$, ami ellentmondás, azt mutatja, hogy $J = R$, vagyis hogy ${}_RR$ teljesen reducibilis.

7.9.25. Tegyük föl, hogy $R = J(R) \oplus B$ egy B balideálra. Ekkor $1 = a + b$, ahol $a \in J(R)$ és $b \in B$. Legyen s inverze $1 - a$-nak, akkor $1 = s(1 - a) = sb \in B$, és így $B = R$, tehát $J(R) = \{0\}$.

7.9.26. Az 5.1.23. Gyakorlat szerint $\mathbb{Z}_n$ a $\mathbb{Z}_q$ gyűrűk direkt szorzata, ahol q befutja az n kanonikus alakjában szereplő prímhatványokat. A $\mathbb{Z}_q$-ban csak a 0 és az 1 idempotens, mert ha $p^\alpha = q \mid e^2 - e = e(e - 1)$, akkor p az e és $e - 1$ számok közül csak egynek lehet osztója, és ezért $q \mid e$ vagy $q \mid e - 1$. A direkt szorzatban egy elem akkor idempotens, ha minden komponense az, ezért $\mathbb{Z}_n$ idempotenseinek száma 2^k, ahol k az n prímosztóinak a száma.

7.9.27. Nyilván $r = re + r(1 - e)$, ezért $Re + R(1 - e) = R$. Tegyük föl, hogy $r \in Re \cap R(1 - e)$, akkor $r = se = t(1 - e)$. Jobbról e-vel szorozva $r = se = se^2 = t(1 - e)e = t(e - e^2) = 0$.

7.9.28. Ha e idempotens, r tetszőleges eleme R-nek, akkor $(er - ere)^2 = 0$. Ezért ha R-ben nincs nem nulla nilpotens elem, akkor $er = ere$. Ugyanígy $re = ere$, tehát $er = re$.

8. fejezet

Általános algebrák, hálók

8.1. Hálók

8.1.2. Ha $D \subseteq B$ és $D \subseteq C$, akkor D minden eleme benne van B-ban és C-ben is, tehát $B \cap C$-ben is. Ezért $D \subseteq B \cap C$. Részcsoportokra ugyanez a bizonyítás (csak hozzá kell tenni, hogy $H \cap K$, azaz H és K *halmazelméleti* metszete szintén részcsoport).

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 jobb oldali 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 e két elem legkisebb felső korlátja 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 E.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 $\equiv$ ekvivalenciareláció. 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 ekvivalenciareláció, 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 (484. oldal) 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.

8.1.28. 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 4.4.25. Gyakorlat miatt az S_3 részcsoporthálója a 8.3. ábrán (484. oldal) látható M_3 hálóhoz hasonlít, csak a középső sorban nem három, hanem négy elem van. A Q kvaterniócsoportnak minden

részcsoportja normálosztó (4.8.33. Gyakorlat), a normálosztóhálója izomorf a D_4 normálosztóhálójával (vö. 6.1. ábra, 374. oldal a könyvben), és a 8.5. ábrán is látható (488. oldal a könyvben).

Az A_4 alternáló csoportnak nincs hatelemű részcsoportja (mert az kettő indexű, és így normálosztó lenne, ami a 4.8.33. 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 8.5. ábrán látható.

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, $\varphi(h \vee k) = \varphi(h) \vee \varphi(k)$. Speciálisan ha $h \leq k$, akkor $h \vee k = k$, ezért $\varphi(k) = \varphi(h) \vee \varphi(k) \geq \varphi(h)$.

8.2.14. Jelölje a C_4 négyelemű lánc elemeit $0 < c < d < 1$, és tekintsük a 8.3. ábrán (484. oldal) látható C_2^2 hálót. 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 izomorfizmustétel: $B[\theta]/\theta \cong B/(B|_\theta)$.

Második izomorfizmustétel: $(A/\theta)/(\rho/\theta) \cong A/\rho$.

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 fölcserélhetők, akkor a 8.1.25. Feladat megoldásának mintájára csak azt kell megmutatni, hogy $\theta \circ \rho$ már maga is ekvivalenciareláció. A reflexivitás nyilvánvaló, a szimmetria azonnal látszik θ és ρ fölcserélhetőségéből. 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 értéket 4-féleképpen választhatjuk, a lehetőségek száma tehát $4^{16} = 4\,294\,967\,296$. Azaz több mint négymilliárd ilyen algebra van.

8.2.34. Csak az eredményeket adjuk meg, néhány mintabizonyítással és 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 $0 * x = x * 0 = 0$ 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) (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 kongruenciahálóját, 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 $\equiv$ ekvivalenciarelációra, 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 $a \equiv b$, így $a \vee b \equiv a \vee a = a$, tehát $a \vee b$, és hasonlóan $a \wedge b$ is eleme C-nek. Ezért C részháló. Tegyük föl, hogy $h \leq a \leq k$ és $h, k \in C$. Ekkor $h \equiv k$, ahonnan a-val egyesítve $a = a \vee h \equiv a \vee k = k$. Így $a \in C$.

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 (484. oldal) 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 $1 = 1 \wedge 1 \equiv b \wedge c = 0$. Így 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 könyvben, a 8.8. ábrán látható (495. oldal).

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 kongruenciahálója is ugyanaz, mint az N_5 kongruenciahálója, és a 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 (484. oldal) 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). 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 (484. oldal).

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. Tegyük föl, hogy $a_1, \ldots, a_N$ tetszőleges elemei az adott 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 $g_1(x_2, x_2) = g_1\big(\pi_2(x_1, x_2, x_3), \pi_2(x_1, x_2, x_3)\big)$, ezért változókat azonosíthatunk, továbbá $g_3(x_3, x_1) = g_3\big(\pi_3(x_1, x_2, x_3), \pi_1(x_1, x_2, x_3)\big)$, ami változók tetszőleges cserélgetését 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 az (egységelemes) R gyűrű fölött, akkor a kifejezésfüggvényei az $r_1 x_1 + \ldots + r_n x_n$ 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, és 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 a 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. Definíció kompatibilitási feltétele 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 az eredmény $\big(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\big)$. 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 ilyenkor $\big(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\big)$

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. Már láttuk, hogy minden kifejezésfüggvény monoton. A megfordításhoz 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 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 a függvényeknek az összeVAGYoltja megfelelő lesz.

8.3.18. Ha a 8.3.6. Gyakorlat képletében néhány x_i helyébe konstansokat írunk, akkor 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 $\equiv$ ekvivalenciarelációt 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 $f(b_1, x, a_3)$ 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 meghatározzák, lásd a 4.6.9. 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} (E.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. Egy 1 elemmel generált háló csak 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).

Megmutatjuk, hogy a 8.3. ábrán (484. oldal) 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 hálóhomomorfizmus.

8.3.30. Az Útmutatóban megadott gyűrűk azért szabadok, mert egy polinomba tetszőleges értékeket be szabad helyettesíteni, és ez a hozzárendelés homomorfizmus (lásd a 2.4.28. 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 a 2.4.30. Gyakorlat). Az egész együtthatókkal nincs probléma, hiszen gyűrűelem egész számszorosát definiáltuk a 2.2.19. 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 minimumfüggvényt 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 Útmutatóbeli $v(x, y)$ 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,

amiből világos a (kétténezős) 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 (mert $(1, 0) \cdot (0, 1) = (0, 0)$), 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) 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 szubdirekt irreducibilisek (sőt M_3 egyszerű is) a 8.2.37. Gyakorlat miatt: a 8.8. ábrán (megoldások, 495. oldal) $\theta \wedge \rho$-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 kongruenciahálója lánc (az ideálok a 2^k osztóinak felelnek meg a 4.3.27. Állítás miatt).

8.4.20. Ha p prím, akkor mind a $\mathbb{Z}_{p^k}^+$ ciklikus, mind a $\mathbb{Z}_{p^\infty}$ kváziciklikus csoport szubdirekt irreducibilis, hiszen az egyetlen p rendű részcsoportjukat minden nem nulla részcsoport tartalmazza a 4.3.27. Állítás,

illetve a 7.7.17. Gyakorlat miatt. 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 , ahol p alkalmas prímszám. Ez „elemien" is bizonyítható (4.9.39. 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, 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 nem nulla polinom, akkor alkalmas (egész) helyettesítésre az értéke nem nulla. Ez következik a 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. Adjuk meg a D_4 diédercsoportot az $\langle f, t \mid f^4 = t^2 = 1,\ ft = tf^{-1}\rangle$ definiáló relációkkal, és legyen $N = \{(1, 1), (f^2, f^2)\}$. Ez normálosztó a $D_4 \times D_4$ csoportban, a szerinte vett faktorcsoportnak $i = (f, t)N$ és $j = (1, f)N$ elemei, és az általuk generált csoport könnyen láthatóan Q-val izomorf (a 4.10.15. 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 $t = (j, j)K$ 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 fölcserélhető, 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 (4.3.40. 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 fölcserélhetők, 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 fölcserélhető N minden elemével, vagy pedig N minden elemét az inverzébe konjugálja. Ez valójában G minden elemére igaz, hiszen ha $g \in G$, akkor $g = g^3g^4$, 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 belátjuk, 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 fölcserélhető g^4-nel, és így $g = g^3g^4$ miatt elég belátni, hogy $st = ts$. A t fölcserélhető $(st)^4$-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 $g = g^3g^4$ 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 $g = g^4g^3$, 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 (4.10.15. 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-féle torziócsoport). Jelölje P a H csoportnak azt a 2-Sylow részcsoportját, ami a másodrendű t elemet tartalmazza. A P Abel, hiszen minden P-beli elem négyzete az egységelem az $x^6 = 1$ azonosság miatt. Továbbá P és N generálja H-t. A t viszont fölcserélhető 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 homomorfizmustétel 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 index-halmaz 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. Erre példa a $\mathbb{Z}_{p^\infty}$ kváziciklikus csoport, ahol az A_i egyre növekvő p-hatványrendű ciklikus csoportok.

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 feltevés 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 fölírt 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 metszettartást.

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 (3.1.22. 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 $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, 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 $(\beta_1, \ldots, \beta_n)$ egy eleme e láncok direkt szorzatának, akkor ő a $p_1^{\beta_1} \ldots p_k^{\beta_k} \mid n$ számnak felel meg. Röviden: minden szám osztóhálója láncok direkt szorzatával izomorf.

Az eddigiekből a ciklikus csoportok kongruenciahálóira (azaz részcsoporthálóira) 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 4.3.27. Állítás miatt. (A megfeleltetés a részcsoportok és a számok között mindkét irányban rendezéstartó, tehát háló-izomorfizmus.)

Ha R főideálgyűrű, akkor alaptételes (5.5.9. Következmény), és a kongruenciái főideáloknak felelnek meg. Két elem akkor és csak akkor generálja ugyanazt a főideált, ha asszociáltak. Ezért ha felsoroljuk asszociáltság erejéig az R-beli prímeket, és minden $r \in R$ elemhez hozzárendeljük a megfelelő kitevők sorozatát, akkor az R ideáljainak hálóját ugyanúgy beágyaztuk az N háló példányainak direkt szorzatába, mint a fenti megjegyzésben. Röviden: az egész számokra adott bizonyítás minden főideálgyűrűre működik.

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 $a \equiv b\ (\theta_I \wedge \rho_F)$. Ekkor alkalmas $c \in I$-re $a \vee c = b \vee c$, és alkalmas $f \in F$-re $a \wedge f = b \wedge f$. A feltétel miatt $c \leq f$, így

$$b = (b \vee c) \wedge b = (a \vee c) \wedge b = (a \wedge b) \vee (c \wedge b) \leq$$
$$\leq a \vee (f \wedge b) = a \vee (f \wedge a) = a$$

(az elnyelési tulajdonságot és a disztributivitást használtuk, továbbá azt, hogy a két hálóművelet monoton). Az a és b cseréjével $a \leq b$ adódik, tehát $a = b$.

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

$$m(x, y, z) = \big(x \wedge (y \vee z)\big) \vee (y \wedge z) =$$
$$= \big(x \vee (y \wedge z)\big) \wedge \big((y \vee z) \vee (y \wedge z)\big) = \big(x \vee (y \wedge z)\big) \wedge (y \vee z) = M(x, y, z)$$

(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.

♫ A 8.6. szakaszban vizsgált moduláris azonosság M_3-ban teljesül, de N_5-ben nem. Olyan konkrét azonosságot viszont nem könnyű találni, amely N_5-ben teljesül, de M_3-ban nem.

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

$$(x \wedge y) \wedge (x' \vee y') = (x \wedge y \wedge x') \vee (x \wedge y \wedge y') = 0 \vee 0 = 0\,.$$

A most bizonyított állítás 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 ekvivalenciareláció az X halmazon.

♫ 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).

A C egységeleme az egész X halmaz, hiszen az egységelem Boole-algebrákban művelettel van kijelölve, és így részalgebra egységeleme ugyanaz, mint az eredeti algebráé. Hasonlóképpen $\emptyset \in C$. Speciálisan a C-beli komplementumképzés a részhalmazok szokásos, X-re vett komplementuma.

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 (2^n darab) $\varphi : \{y_1, \ldots, y_n\} \to \{0, 1\} = L$ 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.

Könnyű 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 szerint az $X_1, \ldots, X_n$ halmazok szabad generátorrendszert alkotnak az általuk generált részalgebrában.

8.5.28. A 8.5.27. Feladat Útmutatójában szereplő 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, de ez nagyon hasonlít a 8.5.8. Feladat megoldásához, amit az előző mondatban fölhasználtunk. Ezt a feladatot a (4) bizonyításához is használhatnánk, 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 fölcserélhetők, 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 hasonló számolás, de abból is adódik, hogy ha $HK = KH$, akkor HK részcsoport (4.6.14. Gyakorlat), és mind $\theta \circ \rho$, mint $\rho \circ \theta$ könnyen láthatóan a HK bal oldali 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.

Tegyük föl, hogy az L hálóban igaz a (2)-beli egyenlőtlenség minden x, y, z esetén. 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).

Megfordítva, ha a háló disztributív, akkor a (2)-beli egyenlőtlenség minden x, y, z esetén fennáll. Valóban, $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) \leq x \vee (y \wedge z)$, mert $x \wedge z \leq x$.

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. Így

$$[x \wedge (y \vee z)] \vee [z \wedge (x \vee y)] = \\ = \big([x \wedge (y \vee z)] \vee z\big) \wedge (x \vee y) = \big((x \vee z) \wedge (y \vee z)\big) \wedge (x \vee y)\,.$$

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, azt kell meggondolni, hogy amikor a bizonyításban az intervallumizomorfizmus-tételt alkalmazzuk, akkor csoportelméleti izomorfiát is kapunk az első izomorfizmustétel miatt.

8.6.27. Az Útmutatóban bevezetett jelöléseket használjuk. Az összes $c \wedge q_j$ elem metszete b, és ezért az intervallumizomorfizmusnál nekik megfelelő $p_i \vee (c \wedge q_j)$ elemek metszete a b-nek megfelelő p_i. De p_i metszetirreducibilis, így 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 a most leírt 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 $b \leq c$ is komplementuma, akkor a modularitás miatt

$$c = 1 \wedge c = (b \vee a) \wedge c = b \vee (a \wedge c) = b \vee 0 = b\,.$$

♫ Ha $b \neq c$, akkor $\{0, a, b, c, 1\}$ az N_5-tel izomorf részháló lesz, ennek bizonyítása azonban eléggé vacakolós: nemcsak az összes egyesítést és metszetet kell ellenőrizni, hanem azt is, hogy a felsorolt öt elem különböző. Ezt

az utolsó lépést megkönnyíti annak felhasználása, hogy N_5 szubdirekt irreducibilis, ugyanúgy, mint a 8.6.10. Tétel bizonyításában.

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 segítségével hasonló módon kifejtve ugyanez az eredmény 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 $d(x) \le d(x \vee a) \le d(x) + 1$ a dimenzió-egyenlőség miatt, hiszen az atomok magassága 1, és ha a nincs x alatt, akkor $d(x \wedge a) = 0$ miatt $d(x \vee a) = d(x) + 1$. Ebből látszik az is, hogy atomok tetszőleges egyesítésének magassága legfeljebb a tagok száma lehet.

Ha tehát az a_i atomokat az Útmutatóban leírt módon választjuk ki, akkor $d(c \vee a_1 \vee \ldots \vee a_i) = d(c) + i$ mindegyik i-re. Mivel az L háló 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, 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 $a_1, \dots, a_n$ atomok, és az a egyesítésük rövidíthetetlen. A függetlenség igazolásához elég belátni, hogy ha $b = a_1 \vee \dots \vee a_{n-1}$, 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 $a_n \leq b$. De akkor $a = b \vee a_n = b$, ami ellentmond a rövidíthetetlenségnek. Ezzel (1)-et beláttuk.

A (2) bizonyításához elég belátni, hogy $a_1 \wedge (a_2 \vee \dots \vee a_n \vee a) = 0$ (hiszen az a_i elemeket ismét permutálhatjuk). Legyen $b = a_2 \vee \dots \vee a_n$. Tudjuk, hogy $a_1 \wedge b = 0$ és $(a_1 \vee b) \wedge a = 0$. Így az Útmutatóban szereplő azonosság miatt

$$a_1 \wedge (b \vee a) \leq (a_1 \vee b) \wedge (b \vee a) = b \vee \big((a_1 \vee b) \wedge a\big) = b \vee 0 = b\,.$$

De akkor $a_1 \wedge (b \vee a) \leq a_1 \wedge b = 0$.

A (3) igazolásához legyen $I \subseteq \{1, 2, \dots, n\}$ 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 $a_I \wedge a_J = a_{I \cap J}$ (mert akkor az $I \mapsto a_I$ megfeleltetés izomorfizmus az $\{1, 2, \dots, n\}$ összes részhalmazainak Boole-hálójával). 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 $U, V \subseteq \{1, 2, \dots, n\}$ 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 $a_1, \dots, a_n$ 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 beláttuk.

A 8.6.33. Feladat állításának igazolásához tegyük föl, hogy $c \in L$. Az 1 előáll véges sok a_i atom egyesítéseként, válasszuk ki ezek közül az $a_1, \dots, a_n$-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 $d = c \vee a_1 \vee \dots \vee a_n$ 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 $c, a_1, \dots, a_n$ 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 a d-hez tartozó kifejezésfüggvényre. Így B 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).

Így φ kölcsönösen egyértelmű megfeleltetés a θ-osztályok és a ρ-osztályok között, és 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 a 8.6.34. Feladat (és a 8.2.32. Állítás) fölhasználásával.

Speciálisan tekintsük a Boole-algebrák varietását, amely a 8.6.5. Állítás miatt kongruencia-fölcserélhető. 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 fogalomanalízis

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 [2], 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.

Az nyilvánvaló, hogy minden zárt halmaz altér, hiszen a skaláris szorzat tulajdonságai miatt egy adott vektorra merőleges összes vektor alteret alkot, és így $X^\sharp$ és $U^\flat$ is mindig altér (hiszen alterek metszete).

8.7.10. Az nyilvánvaló, hogy minden zárt halmaz altér, illetve balideál. 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 E.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 $t^{F_n}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$. 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 bizonyítást el lehet mondani a formális kifejezések használata nélkül is. Az F_n algebrát úgy kapjuk meg az $x_1, \ldots, x_n$ generátorokból, hogy K elemeit komponensenként hatva alkalmazzuk ezekre. Így van olyan $g \in K$, hogy a g-t komponensenként alkalmazva éppen $f(x_1, \ldots, x_n)$ adódik. Ekkor $f = g$, vagyis $f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n)$ tetszőleges $c_1, \ldots, c_n \in C$ 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, ahhoz hasonlóan, ahogy azt láttuk be, hogy a teljes mátrixgyűrű egyszerű (5.3.3. Feladat). 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 $M_1, \ldots, M_n \in L$ 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 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. Valóban, legyenek $\alpha, \beta : \mathbb{Q} \to R$ gyűrűhomomorfizmusok, melyekre $\alpha \circ \varphi = \beta \circ \varphi$. Ekkor $\alpha(1) = (\alpha \circ \varphi)(1) = (\beta \circ \varphi)(1) = \beta(1)$. Ezért $2\alpha(1/2)\beta(1/2) = \alpha(1)\beta(1/2) = \beta(1)\beta(1/2) = \beta(1/2)$. Ugyanígy $2\alpha(1/2)\beta(1/2) = \alpha(1/2)\beta(1) = \alpha(1/2)\alpha(1) = \alpha(1/2)$. Tehát $\alpha(1/2) = \beta(1/2)$. Az $1/2$ helyett a többi törttel is hasonlóan bánhatunk.

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 halmaz-leképezés, 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 $\mathrm{Hom}\big(F(M), K\big)$ minden eleme megkapható ily módon).

9. fejezet

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.

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 $u_1 \ldots u_9$ 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 $u_1 \ldots u_{10}$ sorozat egyetlen helyen megváltozik, és az eredményt $v_1 \ldots v_{10}$ 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 föl, hogy a küldés során u_i és u_{i+1} megcserélődött, 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.

9.2.9. 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" ekvivalenciarelációt (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 bal oldalon q^m áll, tehát az állítás következik a 9.2.9. Gyakorlatból.

9.2.11. Most $Q = \mathbb{F}_3$, tehát $q = 3$, legyen $m = 3$. Ekkor a 9.2.9. 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 $u(x) = u_1x^{k-1} + \dots + u_k$ 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 $u_1, \dots, u_k$. Ugyanígy válasszuk az $x^{n-1}, x^{n-2}, \dots, x, 1$ bázist a legfeljebb n-edfokú polinomok között.

A kódolás az $A\big(u(x)\big) = g(x)u(x)$ leképezéssel történik. Így a 9.2.2. Definíció előtti megjegyzések szerint a generátormátrixot úgy kaphatjuk meg, hogy vesszük ennek az A lineáris leképezésnek a mátrixát a fenti bázispárban (hiszen 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. Így a G generátormátrix a következő lesz:

$$\begin{bmatrix} a_{n-k} & 0 & 0 & \dots & 0 \\ a_{n-k-1} & a_{n-k} & 0 & \dots & 0 \\ a_{n-k-2} & a_{n-k-1} & a_{n-k} & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & \dots & a_k \\ a_0 & a_1 & a_2 & \dots & a_{k-1} \\ 0 & a_0 & a_1 & \dots & a_{k-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_0 \end{bmatrix}$$

(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 az $\mathbb{F}_{2^r}$ testnek az eleme (6.7.5. Tétel), a rendje miatt pedig generálja e test multiplikatív csoportját. Jelölje m_i az α^i minimálpolinomját $Q = \mathbb{F}_2$ fölött. Ennek foka a $Q(\alpha_i)$ dimenziója Q fölött (6.1.20. 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 $m_1, m_3, \dots, m_{2t-1}$ 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 az $\mathbb{F}_{2^r}$ test elemeivel. A kételemű test fölött két nem nulla vektor pontosan akkor párhuzamos, ha egyenlő. Ezért az $m = r$-hez tartozó Hamming-kód ellenőrző mátrixának oszlopait tekinthetjük az $\mathbb{F}_{2^r}$ nem nulla elemeinek is. Ezek pontosan az α elem hatványai, írjuk az oszlopokat az $\alpha^{n-1}, \alpha^{n-2}, \dots, \alpha^2, \alpha, 1 = \alpha^n$ sorrendben. Ekkor a $v_1 \dots v_n$ szó pontosan akkor van benne ebben a Hamming-kódban, ha $v_1\alpha^{n-1} + \dots + v_n = 0$, 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 $v_1 \dots v_n$ kódszavához tartozó polinom, akkor

$$\begin{aligned} xv(x) &= x(v_1x^{n-1} + v_2x^{n-2} + \dots + v_n) = \\ &= (v_2x^{n-1} + v_3x^{n-2} + \dots + v_nx + v_1) + v_1(x^n - 1)\,. \end{aligned}$$

A C kód ciklikussága miatt $w(x) = v_2x^{n-1} + v_3x^{n-2} + \dots + v_nx + v_1$ 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.

Irodalom

Kiegészítő tankönyvek

[1] Freud Róbert, Gyarmati Edit: *Számelmélet.* Nemzeti Tankönyvkiadó, 2006.
[2] Freud Róbert: *Lineáris Algebra.* ELTE Eötvös Kiadó, 2006.
[3] Laczkovich Miklós, T. Sós Vera: *Analízis I.* Nemzeti Tankönyvkiadó, 2005.
[4] Hajós György: *Bevezetés a geometriába.* Tankönyvkiadó, 1966.
[5] Elekes György, Brunczel András: *Véges matematika.* ELTE Eötvös Kiadó, 2006.
[6] Lovász László, Pelikán József, Vesztergombi Katalin: *Diszkrét matematika.* TypoTEX, 2006.

Kiegészítő algebra feladatgyűjtemények

[7] D. K. Fagyejev, I. Sz. Szominszkij: *Felsőfokú algebrai feladatok.* TypoTEX, 2000.
[8] B. Szendrei Mária, Czédli Gábor, Szendrei Ágnes: *Absztrakt algebrai feladatok.* Polygon Kiadó, Szeged, 2005.

Ajánlott ismeretterjesztő művek

[9] Fried Ervin: *Absztrakt algebra elemi úton.* Műszaki Könyvkiadó, 1972.
[10] I. Grossman, W. Magnus: *Csoportok és gráfjaik.* Műszaki Könyvkiadó, 1972.
[11] Péter Rózsa: *Játék a végtelennel.* TypoTEX, 2004.
[12] Rényi Alfréd: *Ars Mathematica.* TypoTEX, 2005.
[13] I. Stuart: *A matematika problémái.* Akadémiai Kiadó, 1991.
[14] Varga Tamás: *Matematikai logika kezdőknek I–II.* Tankönyvkiadó, 1960, 1966.

További bevezetők az algebrába

[15] Bódi Béla: *Algebra I–II.* Kossuth Egyetemi Kiadó, 1999-2000.
[16] P. M. Cohn: *Algebra I–III.* Wiley 1982, 1989, 1991.
[17] Czédli Gábor, Szendrei Ágnes: *Geometriai szerkeszthetőség.* Polygon Kiadó, Szeged, 1997.
[18] Fried Ervin: *Algebra (középiskolai tankönyv).* Tankönyvkiadó, 1988.
[19] Fried Ervin: *Algebra I.* Nemzeti Tankönyvkiadó, 2000.
[20] Fried Ervin: *Algebra II.* Nemzeti Tankönyvkiadó, 2002.
[21] Fuchs László: *Algebra.* ELTE egyetemi jegyzet.
[22] N. Jacobson: *Basic algebra I–II.* Freeman, 1985, 1989.
[23] N. Jacobson: *Lectures in abstract algebra I–III.* Springer, 1975.
[24] I. Herstein: *Abstract algebra.* Wiley, 2001.
[25] T. W. Hungerford: *Algebra.* Springer, 2003.
[26] I. M. Isaacs: *Algebra: a graduate course.* Brooks/Cole, 1993.
[27] Klukovits Lajos: *Klasszikus és lineáris algebra.* Polygon Kiadó, 2000.
[28] A. G. Kuros: *Felsőbb algebra.* Tankönyvkiadó, 1967.

[29] S. Lang: *Algebra.* Springer, 2005.
[30] Pelikán József, Gröller Ákos: *Algebra jegyzet.* Szabadon letölthető: `http://www.cs.elte.hu/~pelikan/algebra.html`
[31] V. V. Praszolov: *Lineáris algebra.* TypoTEX, 2005.
[32] Rédei László: *Algebra.* Akadémiai Kiadó, 1954.
[33] I. R. Safarevics: *Algebra.* TypoTEX, 2000.
[34] Sárközy András: *Komplex számok.* Műszaki Könyvkiadó, 1973.
[35] Surányi László: *Algebra — testek, gyűrűk, polinomok.* TypoTEX, 1998.
[36] Szele Tibor: *Bevezetés az algebrába.* Tankönyvkiadó, 1975.
[37] B. L. van der Waerden: *Algebra I–II.* Springer, 1993, 2006.

Csoportok

[38] P. J. Cameron: *Permutation groups.* Cambridge University Press, 2005.
[39] R. W. Carter, I. G. MacDonald, G. Segal: *Lectures on Lie Groups and Lie Algebras.* Cambridge University Press, 1995.
[40] 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.
[41] C. Curtis, I. Reiner: *Representation theory of finite groups and associative algebras.* Interscience Publishers, 1966.
[42] J. D. Dixon, B. Mortimer: *Permutation groups.* Springer, 1996.
[43] W. Feit, J. G. Thompson: Solvability of groups of odd order. *Pacific J. Math.*, **13** (1963), 775-1029.
[44] W. Fulton, J. Harris: *Representation theory, an introduction.* Springer, 1991.
[45] Fuchs László: *Infinite Abelian groups I–II.* Academic Press, 1970, 1973.
[46] D. Gorenstein, R. Lyons, R. Solomon: *Classification of the finite simple groups.* American Mathematical Society, 1998.
[47] B. Huppert: *Endliche Gruppen I.* Springer, 1967.
[48] I. M. Isaacs: *Character theory of finite groups.* Dover Publications, 1994.
[49] D. J. S. Robinson: *A course in the theory of groups.* Springer, 1982.
[50] J. J. Rotman: *An introduction to the theory of groups.* Springer, 1994.
[51] W. R. Scott: *Group theory.* Dover Publications, 1987.
[52] Seress Ákos: *Permutation group algorithms.* Cambridge University Press, 2003.
[53] S. Sternberg: *Group Theory and Physics.* Cambridge University Press, 1995.

Gyűrűk, homologikus algebra, algebrai geometria

[54] F. Anderson, K. Fuller: *Rings and categories of modules.* Springer, 1995.
[55] M. F. Atiyah, I. G. MacDonald: *Introduction to commutative algebra.* HarperCollins Canada, 1998.
[56] Yu. A. Drozd, V. V. Kirichenko: *Finite dimensional algebras.* Springer, 1993.
[57] D. Eisenbud: *Commutative algebra with a view toward algebraic geometry.* Springer, 1999.
[58] R. Hartshorne: *Algebraic geometry.* Springer, 1997.
[59] I. Herstein: *Noncommutative rings.* The Mathematical Association of America, 1968.
[60] J. E. Humphreys: *Introduction to Lie algebras and representation theory.* Springer, 1980.
[61] N. Jacobson: *Structure of rings.* American Mathematical Society, 1984.
[62] I. Kaplansky: *Fields and rings.* University of Chicago Press, 1972.
[63] Kertész Andor: *Lectures on Artinian rings.* Akadémiai Kiadó, 1987.
[64] T. Y. Lam: *A first course in non-commutative rings.* Springer, 1991.
[65] T. Y. Lam: *Lectures on modules and rings.* Springer, 1999.
[66] S. Mac Lane: *Homology.* Springer, 1995.

[67] R. Pierce: *Associative algebras.* Springer, 1982.
[68] J. J. Rotman: *An Introduction to homological algebra.* Springer, 2006.
[69] L. Rowen: *Ring theory I–II.* Academic Press, 1989, 1990.
[70] C. Weibel: *An introduction to homological algebra.* Cambridge University Press, 1996.
[71] O. Zariski, P. Samuel: *Commutative algebra.* Springer, 1997.

Testek, Galois-elmélet

[72] H. M. Edwards: *Galois theory.* Springer, 2004.
[73] K. Ireland, M. Rosen: *A classical introduction to modern number theory.* Springer, 2006.
[74] J. J. Rotman: *Galois theory.* Springer, 2004.
[75] I. Stewart: *Galois theory.* Chapman & Hall, 2003.

Általános algebrák, hálók

[76] K. A. Baker, R. Wille (szerkesztők): *Lattice theory and its applications.* Konferenciakötet. Heldermann, 1995.
[77] G. Birkhoff: *Lattice theory.* American Mathematical Society, 1984.
[78] S. N. Burris, H. P. Sankappanavar: *Bevezetés az univerzális algebrába.* Tankönyvkiadó, 1988.
[79] S. N. Burris, H. P. Sankappanavar: *A course in universal algebra.* Springer, 1981. Szabadon letölthető a következő internet címről:
`http://www.thoralf.uwaterloo.ca/htdocs/ualg.html`
[80] Czédli Gábor: *Hálóelmélet.* JATEpress, 1999.
[81] R. S. Freese, J. Ježek, J. B. Nation: *Free lattices.* American Mathematical Society, 1995.
[82] R. S. Freese, R. N. McKenzie: *Commutator theory for congruence modular varieties.* Cambridge University Press, 1987.
[83] Grätzer György: *General lattice theory.* Akademie-Verlag, 1978.
[84] D. Hobby, R. McKenzie: *The structure of finite algebras* (Tame congruence theory). American Mathematical Society *Contemporary Mathematics* Series 76, 1988. Szabadon letölthető a következő internet címről: `http://www.ams.org/online_bks/conm76/`
[85] S. Mac Lane: *Categories for the working mathematician.* Springer, 1971.
[86] R. N. McKenzie, G. F. McNulty, W. F. Taylor: *Algebras, lattices, varieties I.* Wadsworth Pub. Co., 1987.

Kódelmélet

[87] E. Berlekamp: *Algebraic coding theory.* Aegean Park Press, 1984.
[88] G. Birkhoff, T. C. Bartee: *A modern algebra a számítógéptudományban.* Műszaki Könyvkiadó, 1974.
[89] Györfi László, Győri Sándor, Vajda István: *Információ- és kódelmélet.* TypoTEX, 2002.
[90] Lakatos Piroska: *Kódelmélet.* Kossuth Lajos Tudományegyetem, egyetemi jegyzet, 1999.

Számelmélet

[91] Erdős Pál, Surányi János: *Válogatott fejezetek a számelméletből.* Polygon Kiadó, 2004.
[92] Sárközy András, Surányi János: *Számelmélet feladatgyűjtemény.* ELTE egyetemi jegyzet.
[93] W. Sierpiński: *200 feladat az elemi számelméletből.* Tankönyvkiadó, 1972.
[94] Szalay Mihály: *Számelmélet (középiskolai tankönyv).* TypoTEX, 1998.
[95] I. M. Vinogradov: *A számelmélet alapjai.* Tankönyvkiadó, 1968.
[96] Yong-Gao Chen, Kun Gábor, Pete Gábor, Ruzsa Z. Imre, Timár Ádám: Prime values of reducible polynomials, II. *Acta Arithmetica*, **104** (2002), 117-127.

További témák

[97] Mayer Gyula, Sudár Csaba, Wettl Ferenc: *LaTeX kezdőknek és haladóknak.* Panem Kiadó, 2004.
[98] K. C. Pohlmann: *Principles of digital audio.* McGraw-Hill, 2000.
[99] Hao Wang: *A logical journey.* From Gödel to Philosophy. MIT Press, 1997.