U. függelék

Útmutatások, ötletek a feladatokhoz

[Ez] az ismeretlen jelenségek vizsgálatának klasszikus dilemmája. Ahhoz, hogy szabatosan elhatároljuk őket, ismerni kellene az oksági mechanizmust, ahhoz pedig, hogy megismerjük az oksági mechanizmust, jól körül kell határolni a jelenségeket.

Stanisław Lem: *Szénanátha*
(Murányi Beatrix fordítása)

U.1. Komplex számok

1.1.7. Használjuk föl, hogy ha x és y egész számok, akkor $x = mp + \overline{x}$ és $y = mq + \overline{y}$ alkalmas p, q egészekre, és helyettesítsük ezt be a bizonyítani kívánt képletekbe.

1.1.16. Teljes négyzetté alakítással vezessük vissza a feladatot négyzetgyökvonásra modulo 101. A 20 helyett a 121-ből vonjunk négyzetgyököt.

1.1.18. Színezzünk a modulo m maradékokkal. Vagdossunk le a sakktábláról olyan darabokat, ahol mindegyik maradékból ugyanannyi van. Ha r a k szám m-mel való osztási maradéka, akkor a bal felső $r \times r$-es négyzetben hány $r-1$ és hány 0 van?

1.1.19. Vizsgáljuk meg, hogy ezek a számok milyen maradékot adhatnak 3-mal osztva.

1.2.12. Mutassuk meg, hogy ha az x elegendően nagy abszolút értékű szám, akkor $ax^3 + bx^2 + cx + d$ előjele ugyanaz, mint ax^3 előjele, mert az $|ax^3|$-höz képest a többi tag abszolút értékben még együttvéve is eltörpül.

1.3.13. Végezzük el a négyzetre emelést, és írjuk föl az eredmény valós, illetve képzetes részét. Így két egyenletet kapunk c-re és d-re.

1.4.12. A négyszöget a komplex számsíkra rajzolva képzeljük el, tehát a csúcsok komplex számok lesznek. Fejezzük ki a megfelelő négyzetek középpontjait a csúcsok segítségével. Használjuk föl, hogy két vektor akkor és csak akkor egyenlő hosszú és merőleges, ha az egyik a másiknak i-szerese.

1.4.13. A háromszög csúcsai segítségével fejezzük ki a szabályos háromszögek középpontjait. Használjuk föl, hogy egy háromszög akkor és csak akkor szabályos, ha az egyik oldalvektorát 60°-kal elforgatva egy másik oldalvektorát kapjuk. A $\cos 60^\circ + i \sin 60^\circ$ és a $\cos 120^\circ + i \sin 120^\circ$ számok közötti összefüggéseket ne az algebrai alakjukból, hanem a szabályos hatszög geometriai tulajdonságaiból vezessük le.

1.4.14. Mutassuk meg, hogy a $(z_3 - z_1)/(z_3 - z_2)$ szöge a $z_1 z_2 z_3$ háromszögnek a z_3-nál levő szöge. Használjuk a látókörről szóló geometriai tételt.

1.4.15. Használjuk föl az $(A-B)(C-D)+(A-D)(B-C) = (A-C)(B-D)$ azonosságot.

1.4.16. Legyen $\eta = \cos x + i \sin x$. Ekkor a keresett kifejezés az $\eta+\eta^2+\ldots+\eta^n$ képzetes része. Ezt az összeadást könnyű elvégezni, hiszen ez egy mértani sor. A végeredmény képzetes részét azonban nehézkes leolvasni, mert az összegképlet nevezőjében is komplex szám keletkezik (próbálja ki az Olvasó). Ezért hasznos ötlet, hogy a fenti η helyett az $\varepsilon = \cos(x/2) + i \sin(x/2)$ páros hatványait adjuk össze, majd az eredményt leosztjuk ε egy olyan hatványával, hogy felhasználhassuk az $\varepsilon - (1/\varepsilon) = 2i \sin(x/2)$ és $\varepsilon^n - (1/\varepsilon)^n = 2i \sin(nx/2)$ összefüggéseket.

1.5.9. Számozzuk be az n-szög csúcsait a $0, 1, \ldots, n-1$ számokkal, és képzeljük azt, hogy a bolha a 0 csúcsról indul. Melyik pontban lesz a bolha m lépés után? Hogyan írhatjuk föl oszthatóság segítségével, hogy ez a kiindulópont?

1.5.19. Keressük meg $-\varepsilon$ jó kitevőit.

1.5.23. Használjuk föl a binomiális tételt az $(1+1)^n$, $(1-1)^n$, $(1+i)^n$ összegekre.

1.5.24. Hatványozzuk a $\cos x + i \sin x$ számot a Moivre-képlet alapján is, és a binomiális tétel segítségével is.

U.2. Polinomok

2.1.12. Mivel ε^{k^2} abszolút értéke 1, ezért konjugáltja ε^{-k^2}. Az $S\overline{S}$ összegben végezzük el a beszorzást a 2.1.4. Gyakorlat alapján. Ekkor az $\varepsilon^{j^2-k^2}$ számok n^2 tagú összegét kapjuk, ahol j és k egymástól függetlenül 0-tól $n-1$-ig fut. Használjuk föl a $j^2 - k^2 = (j-k)(j+k)$ azonosságot, és csoportosítsuk az összeg tagjait $\ell = j - k$ szerint. Ha p páratlan prímszám, akkor az S kiszámításához használjuk föl az E.4.8. Tétel állításait.

2.2.2. Először az $\big((a*b)*(c*d)\big)*e = a*\Big(b*\big(c*(d*e)\big)\Big)$ speciális esetet mutassuk meg. Az általános esetben is arra törekedjünk, hogy minden szorzatot olyan alakra hozzunk, mint a fenti azonosság jobb oldala, ahol az összes

csukózárójel „annyira jobbra van, amennyire csak lehet”. Alkalmazzunk teljes indukciót a szorzat hosszára nézve.

2.2.5. Mutassuk meg, hogy ha egy könyvespolcra a könyvek összevissza vannak feltéve, akkor rendet tudunk csinálni úgy, hogy mindig csak két szomszédos könyvet cserélünk ki.

2.2.8. Ha volna kettő, akkor számítsuk ki kétféleképpen a szorzatukat.

2.2.10. Tegyük föl, hogy v balinverze, és w jobbinverze u-nak. Számítsuk ki kétféleképpen a $v * u * w$ szorzatot.

2.2.16. Legyen a H részcsoport neutrális eleme f, és jelölje f^{-1} az f elemnek a G csoportbeli inverzét. Számítsuk ki kétféleképpen az $f * f * f^{-1}$ szorzatot.

2.2.18. Álljon S az egész számok halmazának összes részhalmazaiból, és legyen a művelet a metszetképzés.

2.2.22. A disztributivitást alkalmazzuk a $(0+0)r$ és az $r\big(s+(-s)\big)$ kifejezésekre.

2.2.26. Alkalmazzuk a 2.2.16. Feladat állítását.

2.2.32. Legyenek $u_1, \ldots, u_k$ a $\mathbb{Z}_m$-nek az m-hez relatív prím elemei, és u ezek egyike. Mutassuk meg, hogy $u *_m u_1, \ldots, u *_m u_k$ páronként különbözők.

2.2.39. Az (1)-hez mutassuk meg, hogy S minden b eleme $b = de$ alakban írható alkalmas $d \in S$ segítségével (d választható b balinverze balinverzének). A (2)-t az (1)-re vezessük vissza.

2.2.40. Tudjuk, hogy $(\sqrt{2}-1)(\sqrt{2}+1) = 1$, tehát ezek invertálhatók. Hogyan lehetne ebből az összefüggésből további invertálható elemeket gyártani?

2.2.41. Egy nem nulla elem „abszolút értéke” lehet-e nulla?

2.2.44. Egy csoportban mely g elemekre igaz, hogy $g^2 = g$?

2.2.45. Tegyük föl, hogy van ilyen leképezés. Mutassuk meg, hogy az 1 képe szükségképpen 1 lesz, majd vizsgáljuk meg, hogy milyen tulajdonságú elem lehet az i képe.

2.4.18. Legyen $f \in R[x]$. A 2.4.4. Gyakorlat miatt $f(x) = (x-b)q_0(x) + b_0$ alkalmas $q_0 \in R[x]$ polinomra és $b_0 \in R$ elemre. Alkalmazzuk ugyanezt a q_0 polinomra, majd a kapott q_1 polinomra, és így tovább. (Ez az eljárás hasonlít ahhoz, ahogy egy számot egy másik számrendszerbe alakítunk.)

Az egyértelműség bizonyításához tegyük föl, hogy

$$f(x) = b_0 + b_1(x-b) + \ldots + b_n(x-b)^n = c_0 + c_1(x-b) + \ldots + c_n(x-b)^n$$

alkalmas $b_i, c_i \in R$ elemekre. A két polinomot kivonva

$$0 = (c_0 - b_0) + (c_1 - b_1)(x-b) + \ldots + (c_n - b_n)(x-b)^n .$$

Ezért azt kell megmutatni, hogy ha

$$d_0 + d_1(x-b) + \ldots + d_n(x-b)^n$$

a nullapolinom, akkor mindegyik $d_i = 0$. Helyettesítsünk x helyére b-t, és alkalmazzunk n szerinti indukciót.

2.4.19. Ha a nullosztó, akkor hány gyöke van legalább az ax polinomnak?

2.4.20. Mivel $f(14) = 440$, az f-et kereshetjük $(x-14)g(x) + 440$ alakban, ahol g is egész együtthatós polinom.

2.4.21. Nem lehetséges. Ehhez az interpoláció egyértelműsége miatt elég megmutatni, hogy van olyan egész együtthatós, n-nél kisebb fokú polinom, ami elvégzi az interpolációt. Legyenek az alappontok $a_1, \ldots, a_n$, és f a legalacsonyabb fokú olyan egész együtthatós polinom, amely ezeken a helyeken a kívánt értékeket veszi föl. Tegyük föl indirekt, hogy $\mathrm{gr}(f) \geq n$, és tekintsük az $f(x) - cx^k(x-a_1)\ldots(x-a_n)$ polinomot, ahol $k = \mathrm{gr}(f) - n$, a c pedig az f főegyütthatója.

2.4.22. A „racionális” esetben használjuk föl az interpolációról tanultakat. Az „egész” esetben képzeljük az $\binom{x}{k}$ binomiális együtthatót x polinomjának, miközben k rögzített.

2.4.23. Az előző 2.4.22. Feladat szerint f racionális együtthatós, azaz felírható $f(x) = g(x)/m$ alakban alkalmas m egészre. Mutassuk meg, hogy $f(x) - f(x+km)$ egész szám minden x és k egészre.

2.4.24. Mutassuk meg a Lagrange-alappolinomok képletének felhasználásával, hogy $n!f(x)$ már egész együtthatós. Alkalmazzunk f foka szerinti indukciót.

2.4.25. Keressük meg g-nek az előző 2.4.24. Feladatban szereplő felbontását. Először a 10 helyett kisebb számokkal kísérletezzünk.

2.4.26. Írjuk föl $f(x)$-et $(x-a)(x-b)(x-c)(x-d)q(x) + 5$ alakban.

2.4.27. Legyen $r \neq 0$ eleme R-nek. Mivel az interpoláció korlátlanul elvégezhető, van olyan $f \in R[x]$ polinom, melyre $f(0) = 0$ és $f(r) = 1$.

2.4.29. Álljon S azokból a függvényekből, melyeknek a 2 gyöke. A másik kérdésre a válasz nemleges. Ennek igazolásához használjuk föl, hogy nullosztómentes gyűrűben nem nulla elemmel szabad egyszerűsíteni (2.2.28. Gyakorlat).

2.5.2. Vizsgáljuk az elsőfokú polinomokat.

2.5.13. Emeljük négyzetre az $(x_1 + \ldots + x_n)$ összeget a 2.1.4. Gyakorlat felhasználásával.

2.5.15. A (4)-hez: helyezzük el a sokszöget úgy, hogy a csúcsai az n-edik egységgyökök legyenek, az 1 csúcsból induló oldalak és átlók hosszainak szorzatát írjuk föl abszolút érték segítségével, majd használjuk föl a feladat (2) állítását.

2.5.16. Legyen $f(x) = (x-a)(x-b)(x-c)$. Alkalmazzuk a gyökök és együtthatók összefüggéseit. A konstans tag meghatározásához helyettesítsük be x helyére az a, b, c számokat, és adjuk össze a kapott egyenleteket. Tegyük meg ezt úgy is, hogy a megfelelő egyenletet az összeadás előtt rendre a^{j-3}-mal, b^{j-3}-mal, c^{j-3}-mal megszorozzuk.

2.5.18. Először olyan polinomot próbáljunk készíteni, amelynek gyöke az illető test mindegyik eleme. Ezt módosítsuk olyan (nem konstans) polinommá, amelynek nincs gyöke az adott testben.

2.6.10. Igaz, alkalmazzunk indukciót a határozatlanok száma szerint.

2.6.11. Használjuk a 2.6.9. Gyakorlatban bevezetett jelöléseket. Legyen T test, $\mathbf{a}^1, \dots, \mathbf{a}^k \in T^n$ páronként különböző „pontok” és $b_1, \dots, b_k \in T$. Olyan $f \in T[x_1, \dots, x_n]$ polinomot keresünk, amelyre $f(\mathbf{a}^j) = b_j$, ha $1 \le j \le k$. Próbáljuk a Newton-interpolációt modellezni. Meg kell adnunk egy olyan n-határozatlanú polinomot, amelybe az $\mathbf{a}^1, \dots, \mathbf{a}^{k-1}$-et helyettesítve nullát kapunk, de $\mathbf{a}^k$-t helyettesítve nem. Minden $j < k$-ra keressünk egy olyan koordinátát, amelyben $\mathbf{a}^k$ különbözik $\mathbf{a}^j$-től, és csak erre a koordinátára koncentráljunk.

2.7.17. Igazoljuk, hogy $\sigma_1^{k_1} \dots \sigma_n^{k_n}$ homogén polinom, amely szükségképpen k-adfokú.

2.7.18. Legyen f gyöktényezős alakja $(x-b_1)(x-b_2)\dots(x-b_n)$. Tekintsük az $f_N(x) = (x-b_1^N)(x-b_2^N)\dots(x-b_n^N)$ polinomot minden $N > 0$ egészre. A szimmetrikus polinomok alaptételének felhasználásával igazoljuk, hogy ez egész együtthatós. Becsüljük meg az együtthatóit, és ebből vezessük le, hogy mindegyik b_j-nek csak véges sok hatványa van.

2.7.19. Használjuk föl, hogy ha $m_1 \ge m_2 \ge m_3 \ge \dots$ nemnegatív egész számok, akkor van olyan $k \ge 1$, hogy onnantól kezdve ez a sorozat már állandó, azaz $m_j = m_k$ minden $j \ge k$-ra. Alkalmazzuk ezt arra a sorozatra, ahol m_i a P_i polinomban az x_1 kitevője.

U.3. A polinomok számelmélete

3.1.28. Tegyük föl, hogy $p_1 \dots p_k = q_1 \dots q_\ell$ egy elem két felbontása irreducibilisek szorzatára. A p_1 prímtulajdonságát kihasználva keressük meg egy asszociáltját a q_j-k között, majd egyszerűsítsünk p_1-gyel.

3.1.33. Tudjuk, hogy $2 \mid 2 \cdot 2$. Osztója-e a 2 valamelyik tényezőnek a páros számok gyűrűjében is? Mutassuk meg, hogy $2 \cdot 18 = 6 \cdot 6$ a 36-nak két lényegesen különböző felbontása felbonthatatlanok szorzatára a páros számok gyűrűjében.

3.1.34. Használjuk föl, hogy $3 \cdot 3 = 9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$.

3.1.35. Az x^3y^2 és az x^2y^3 polinomoknak mik az osztói R-ben?

3.2.5. Ha $g = 0$, akkor nem oszthatunk vele maradékosan, hogyan végezzük ilyenkor az eljárást? Az is előfordulhat, hogy egyáltalán nincs nem nulla maradék az algoritmusban, mi ilyenkor a kitüntetett közös osztó?

3.2.8. Van I-ben legalacsonyabb fokú polinom?

3.2.9. Mutassuk meg, hogy minden ilyen I halmaz a legkisebb pozitív elemének a többszöröseiből áll. A 3.2.7. Tétel bizonyítását kövessük.

3.2.13. Alkalmazzuk a 3.2.3, 3.1.27, 3.1.28. Gyakorlatokat, illetve Feladatot.

3.2.14. Tegyük föl, hogy van olyan nem konstans polinom, amely nem bontható föl irreducibilisek szorzatára. Legyen f a(z egyik) lehető legkisebb fokú ilyen polinom. Irreducibilis-e f?

3.3.18. Használjuk a racionális gyöktesztet (3.3.10. Tétel). Keressünk olyan m egészet, hogy az 1 szám gyöke legyen $f(x) + mx^j$-nek.

3.3.22. Használjuk föl a binomiális tételt. Illusztrációként érdemes elolvasni a 3.3.21. Gyakorlat megoldásának a középrészét is. A kis Fermat-tétel bizonyításához emeljük (tagonként) p-edik hatványra azt a b tagból álló $\mathbb{Z}_p$-beli összeget, amelynek mindegyik tagja 1.

3.3.24. Mutassuk meg a gyöktényezős alak beszorzásával, hogy $x^4 - 10x^2 + 1$ összes gyökei $\pm\sqrt{2}\pm\sqrt{3}$. A beszorzást végezzük el háromféleképpen is, mindig máshogy összepárosítva két-két gyöktényezőt. A $\mathbb{Q}$ fölötti irreducibilitás bizonyításához a 3.3.12. Példában leírt módszert használjuk. Vizsgáljuk meg, hogy a $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ gyökvonások melyike végezhető el $\mathbb{Z}_5$, $\mathbb{Z}_7$, illetve $\mathbb{Z}_{11}$ fölött.

♫ Az $x^4-10x^2+1=0$ egyenletet $y=x^2$ helyettesítéssel másodfokúra vezethetjük vissza. Innen $y = 5\pm\sqrt{6}$, de nem könnyű rájönni, hogy ez $\pm\sqrt{2}\pm\sqrt{3}$ négyzete.

3.4.14. Legyen $f^n + g^n = h^n$ olyan nemtriviális megoldás, ahol g és h fokának maximuma a lehető legkisebb. Feltehető, hogy f, g és h páronként relatív prímek. Bontsuk föl az $f^n = h^n - g^n$ polinomot a $h - \varepsilon^j g$ polinomok szorzatára, ahol $1 = \varepsilon^0, \dots, \varepsilon^{n-1}$ az n-edik egységgyökök, és mutassuk meg, hogy e tényezők páronként relatív prímek. Mivel $\mathbb{C}[x_1, \dots, x_n]$ alaptételes, és minden egység teljes n-edik hatvány, ezért mindegyik $h - \varepsilon^j g$ polinom maga is teljes n-edik hatvány. Legyen

$$u^n = h - g\,, \quad v^n = h - \varepsilon g\,, \quad w^n = h - \varepsilon^2 g\,.$$

Mutassuk meg, hogy $\varepsilon u^n + w^n = (\varepsilon + 1)v^n$. Készítsünk ebből az eredetinél kisebb fokú, nemtriviális megoldást.

3.4.20. Mutassuk meg, hogy ha $f = gh$ nemtriviális felbontás, akkor g és h egyike több, mint fokszámnyi helyen 1 vagy -1. Használjuk föl a polinomok azonossági tételét.

3.4.21. Ha az $f \in \mathbb{Z}[x]$ egy k-adfokú g osztóját keressük, akkor használjuk föl, hogy minden m egészre $g(m) \mid f(m)$, és alkalmazzunk interpolációt.

3.5.8. Mutassuk meg, hogy $g(x) = x^n f(1/x)$.

3.5.15. Használjuk föl a következő összefüggést:

$$1 + x + \ldots + x^{p-1} = \frac{x^p - 1}{x - 1},$$

valamint hogy $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (3.3.22. Feladat).

3.5.16. Fogalmazzuk meg a Schönemann–Eisenstein-kritériumot abban az esetben, amikor $\mathbb{Z}$ helyett a $\mathbb{C}[y]$ gyűrű fölötti polinomokat vizsgáljuk. Megy-e a 3.5.3. Gyakorlatban leírt bizonyítás ebben az esetben is?

3.5.17. Mutassuk meg, hogy $f\big(x + f(x)\big)$ osztható $f(x)$-szel.

3.5.18. Tegyük föl, hogy $\sqrt[3]{4} = a + b\sqrt[3]{2}$. Mi lehet az $x^3 - 2$ és az $x^2 - ax - b$ polinomok kitüntetett közös osztója? Van-e közös gyökük?

3.5.20. Legyen $z = x + (1/x)$. Az $x + 1$ gyöktényező kiemelése után kapott polinomot osszuk le x^3-nel, és ezt írjuk föl z (harmadfokú) polinomjaként.

3.6.11. Legyen $b \in \mathbb{C}$ gyöke f'-nek. Használjuk föl a 3.6.10. Gyakorlatot.

3.6.13. Az $f/(f, f')$ polinomnak mik a gyökei, és hányszorosak?

3.6.15. Mutassuk meg, hogy ha f irreducibilis, akkor (f, f') csak akkor lehet nem konstans, ha $f' = 0$. Milyen f polinomokra teljesül ez $\mathbb{Z}_2$ fölött? Használjuk föl, hogy $\mathbb{Z}_2$ fölött tagonként lehet négyzetre emelni (3.3.22. Feladat).

A megfordítás igazolásához tekintsük (f, f')-nek egy irreducibilis g osztóját. Ha $\mathbb{Q}$ fölött vagyunk, akkor ennek van egy b gyöke $T = \mathbb{C}$-ben, ha meg $\mathbb{Z}_2$ fölött, akkor b választható egy $\mathbb{Z}_2$-t tartalmazó algebrailag zárt T test egy alkalmas elemének (6.4.6. Tétel). Annak felhasználásával, hogy g-nek nincs többszörös gyöke T-ben, mutassuk meg, hogy $g^2 \mid f$.

3.6.17. Ha $f'(b) = 0$, tudjuk-e módosítani f-et úgy, hogy b gyöke legyen?

3.6.18. Mutassuk meg, hogy ha c kivételes érték, akkor f'-nek és $f(x) - c$-nek van közös gyöke.

3.8.8. Az összes állítás közvetlen (de hosszadalmas) számolással igazolható a gyökök és együtthatók összefüggését fölhasználva. Ehelyett az α_1, α_2, α_3, α_4 gyököket a 3.7.2. Állítás bizonyításához hasonlóan képzeljük határozatlanoknak. (Ezt megtehetjük, hiszen (6) kivételével csupa azonosságot kell bizonyítani.) Ekkor az u_1, u_2, u_3 kifejezések páronként különbözők, és így (1)-hez elég azt belátni, hogy mindegyik u_i gyöke a harmadfokú rezolvensnek (hiszen a főegyüttható biztosan 8). Keressünk olyan $K_1(x)$ és $L_1(x)$ polinomokat, hogy

$K_1(x) + L_1(x) = (x - \alpha_1)(x - \alpha_2)$ és $K_1(x) - L_1(x) = (x - \alpha_3)(x - \alpha_4)$ teljesüljön.

3.8.9. Használjuk föl a 3.8.8. Feladatot.

3.8.10. Használjuk föl a 3.8.8. Feladatot és a 3.8.4. Gyakorlatot.

3.8.13. Teljes négyzet-e $\mathbb{C}$ fölött a $-(2x^2 + 4x + 2)$ polinom?

3.9.12. Használjuk föl az 1.5.19. Feladat eredményét.

3.9.14. Legyen η primitív m-edik egységgyök, ahol $m \mid n$. Számítsuk ki, hogy a feladatbeli szorzatban az $x - \eta$ hányadik hatványon szerepel, majd alkalmazzuk az E.4.6. Állítást.

3.9.15. Használjuk föl az előző feladatot.

3.9.18. Alkalmazzuk a gyökök és együtthatók közötti összefüggéseket az n-edik körosztási polinomra. Mutassuk meg, hogy az n-edik primitív egységgyökök összege $\mu(n)$ (ahol μ a Möbius-függvény), szorzatuk pedig 1, kivéve $n = 2$-re, amikor -1.

3.9.19. Osszuk le a $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggést $x - 1$-gyel, és azután helyettesítsünk $x = 1$-et.

3.9.20. Attól függően, hogy n osztható-e néggyel, számítsuk ki a $\Phi_n(-x)$ polinomot a 3.9.15. Feladat, illetve a 3.9.12. Gyakorlat segítségével, majd használjuk föl az előző feladat eredményét.

3.9.21. Az előző gyakorlat szerint Φ_{nm}-et fölírhatjuk az $x - \eta\varepsilon$ gyöktényezők szorzataként, ahol $o(\eta) = m$ és $o(\varepsilon) = n$. Csoportosítsuk ezeket a gyöktényezőket η szerint.

3.9.23. A $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggésből kiindulva, n szerinti indukcióval bizonyítsunk. Számoljunk eleve $\mathbb{Z}_p$ fölött. Használjuk föl a 3.9.6. Gyakorlatot és a 3.3.22. Feladatot (azaz a tagonkénti p-edik hatványozás lehetőségét).

3.9.25. Térjünk át $\mathbb{Z}_p[x]$-re, alkalmazzuk a 3.9.23. Feladatot, majd ezután a 3.6.14. Gyakorlat megoldásának azt az állítását, hogy $p \nmid m$ esetén $x^m - 1$-nek nincs többszörös tényezője $\mathbb{Z}_p[x]$-ben.

3.9.26. Legyen ε primitív n-edik egységgyök. Mutassuk meg, hogy a kívánt sokszög akkor létezik, ha az $1, 2, \ldots, n$ számoknak van olyan $a_0, a_1, \ldots, a_{n-1}$ sorrendje, melyre $a_0 + a_1\varepsilon + a_2\varepsilon^2 + \ldots + a_{n-1}\varepsilon^{n-1} = 0$. A körosztási polinomok felhasználásával igazoljuk, hogy ha n prímhatvány, akkor ez nem lehetséges. Ha n nem prímhatvány, akkor bontsuk föl mk alakban, ahol m és k egymáshoz relatív prím, 1-nél nagyobb számok. A 3.9.17. Gyakorlat segítségével állítsuk elő ε hatványait egy m-edik és egy k-edik egységgyök szorzataként, az $1, 2, \ldots, n$ számokat pedig írjuk $ik + j$ alakban, ahol $1 \le j \le k$ és $0 \le i < m$.

U.4. Csoportok

4.1.29. Igazoljuk, hogy a transzformációnak van valós sajátértéke, és minden valós sajátérték 1, vagy -1. Használjuk föl, hogy a determináns a karakterisztikus polinom gyökeinek a szorzata. Elemi geometriai megoldás is adható.

4.1.39. Ha $f(P) \neq P$ akkor tekintsük P és $f(P)$ felező merőleges síkját.

4.2.30. Igazoljuk, hogy két transzpozíció szorzata mindig fölírható hármasciklusok szorzataként.

4.2.31. Bizonyítsuk be j szerinti indukcióval, hogy ha $f(1)$ értékét i jelöli, akkor $f(j) = j +_n (i-1)$ (mod n összeadás).

4.2.32. Mutassuk meg a „bolhás feladat” (vagyis az 1.5.9. Feladat) felhasználásával, hogy az $(1, 2, \ldots, n)$ ciklus k-adik hatványa (n, k) darab $n/(n, k)$ hosszú diszjunkt ciklus szorzata.

4.2.33. Használjuk a 4.2.27. Gyakorlatban szereplő könyvespolc-modellt.

4.2.34. Vegyük az $(1, 2, \ldots, n)$ ciklus egy előállítását transzpozíciók szorzataként, és készítsük el ezekből az előző feladatban vizsgált gráfot. Mutassuk meg, hogy ez összefüggő lesz, majd alkalmazzuk az E.2.5. Tételt.

4.2.35. Készítsük el a megadott transzpozíciók halmazából a 4.2.33. Feladatban szereplő gráfot. Ha $k+t-1 > n$, akkor ennek $(n-k)+(n-t)$, azaz $n-1$-nél kevesebb éle van, és így nem lehet összefüggő. Ha $k+t-1 \leq n$, akkor alkalmazunk n szerinti indukciót az összefüggőség bizonyítására. Az indukció során a k, t, n hármasról a $k, t-k, n-k$ hármasra lépjünk (a $k < t$ esetben).

4.3.40. Induljunk ki az $(ab)^2 = 1$ összefüggésből. Negyedik hatványokra az állítás nem igaz, a D_4 diédercsoport például ellenpélda lesz (lásd 4.1.23. Állítás).

4.3.41. Igazoljuk, hogy ha $d = (a^n-1, a^m-1)$, akkor a $\mathbb{Z}_d^\times$ csoportban $o(a) \mid n$.

4.4.18. Feleltessük meg mindegyik bal oldali mellékosztálynak a komplexusinverzét.

4.4.27. A második kérdéshez vizsgáljuk a $\mathbb{Z}_8^\times$ csoportot.

4.4.31. Igazoljuk, hogy az AB szorzat minden eleme $|A \cap B|$-féleképpen írható föl ab alakban, ahol $a \in A$ és $b \in B$. Használjuk föl, hogy $c \in A \cap B$ esetén $ab = (ac)(c^{-1}b)$, és itt $ac \in A$, $bc \in B$.

4.4.32. Párosítsunk minden elemet az inverzével. Mely elemek egyenlők a párjukkal?

4.4.33. A 2.4.7. Tétel miatt egy T test multiplikatív csoportjában az $x^d - 1$ polinomnak legfeljebb d gyöke lehet. Igazoljuk, hogy legfeljebb $\varphi(d)$ darab d rendű elem van. Alkalmazzuk a 3.9.6. Gyakorlat állítását.

4.4.34. Készítsünk egy páros gráfot, melynek az A csúcshalmazát a H részcsoport szerinti összes bal mellékosztályok alkotják, a B csúcshalmazt pedig az összes jobb mellékosztályok. (Az egyszerre bal és jobb mellékosztályokat két példányban vesszük föl.) Kössünk össze két mellékosztályt, ha van közös elemük. Alkalmazzuk az E.2.7. König–Hall–Ore-tételt.

4.5.22. Számoljuk meg mindkét csoportban a másodrendű elemeket.

4.5.29. Tekintsük a kocka szimmetriacsoportjának a hatását a szemköztes lappárok alkotta háromelemű halmazon.

4.5.30. Számoljuk meg egyszer rögzített g, egyszer pedig rögzített x mellett azokat a (g, x) párokat, melyekre $g * x = x$.

4.5.31. Legyen X az összes színezések halmaza, ahol a szimmetriával egymásba átvihetőket is különbözőnek tekintjük. Hasson a D_4 csoport az X halmazon a természetes módon, és alkalmazzuk a Burnside-lemmát (vagyis a 4.5.30. Feladat állítását).

4.5.32. Alkalmazzuk a 4.5.30. Feladatot. A tranzitivitás szükséges, keressünk a Klein-csoporttal izomorf ellenpéldát S_6-ban.

4.5.34. A G csoport alaphalmazán berajzolunk minden $g \in G$ elemhez $|G|$ darab g „színű” nyilat: tetszőleges x-ből g színű nyíl megy xg-be. Ennek a gráfnak a szimmetriái épp a G elemeivel való balszorzások (a Cayley-tételbeli G-vel izomorf csoport). Hogyan szüntethetjük meg a színeket és az irányítást?

4.6.14. Számoljunk komplexusokkal, használjuk föl a 4.4.3. és a 4.4.4. Gyakorlatokat.

4.6.15. Igazoljuk, hogy $\langle a/c, b/d\rangle = \langle (a, c)/[b, d]\rangle$.

4.6.16. Mutassuk meg, hogy a racionális számok egy X részhalmaza akkor és csak akkor generátorrendszer, ha minden q prímhatványhoz van olyan (már egyszerűsített alakban fölírt) tört X-ben, melynek nevezője osztható q-val.

4.6.17. Tegyük föl, hogy X egy k elemű generátorrendszer a G csoportban, feltehető, hogy X-be belevettük minden elemének az inverzét is. Legyen továbbá $|G : H| = n$, és válasszunk minden H szerinti bal mellékosztályból egy reprezentánselemet úgy, hogy H-ból az egységelemet választjuk. Jelölje R ezeknek a reprezentánselemeknek a halmazát. Ha $x \in X$ és $r \in R$, akkor xr is benne van valamelyik mellékosztályban, és így $r'h$ alakban írható alkalmas $r' \in R$ és $h \in H$ elemekre. Legyen Y az így kapott kn darab $h \in H$ elem halmaza. Mutassuk meg, hogy Y generálja H-t.

4.6.18. Legyen $f = ts$. Igazoljuk, hogy $tf^i t = f^{-i}$. Járjunk el hasonlóan, mint a 4.1.23. Állítás bizonyításában.

4.6.19. Alkalmazzuk a 4.1.18. Gyakorlatot annak igazolására, hogy ha G véges részcsoport, akkor az elemeinek van egy közös P fixpontja. A 4.4.33. Feladat miatt a P körüli forgatások csoportjának minden véges részcsoportja ciklikus.

4.8.43. Használjuk föl, hogy SO(3) minden eleme forgatás (4.1.29. Feladat), és hogy e csoportban bármely két, egyforma szögű forgatás konjugált (4.1.30. Gyakorlat). Mutassuk meg, hogy ha f egy $90^\circ \leq \alpha < 180^\circ$ szögű forgatás az (origón átmenő) e_1 egyenes körül, akkor van olyan (origón átmenő) e_2 egyenes, mely merőleges az f-nél vett képére. Legyen g az e_2 körüli 180 fokos forgatás. Igazoljuk, hogy $g^{-1}f^{-1}gf$ szintén 180 fokos forgatás. Alkalmazzuk a 4.1.38. Gyakorlat állítását.

4.8.44. Használjuk föl, hogy egy homomorfizmust egy generátorrendszeren felvett értékei egyértelműen meghatároznak (4.6.9. Gyakorlat).

4.8.45. Mutassuk meg, hogy ha α fixpontmentes automorfizmus, akkor G minden eleme egyértelműen fölírható $g^{-1}\alpha(g)$ alakban.

4.8.48. Igazoljuk az $[x, y]^{-1} = [y, x]$ és $[x, yz] = [x, y]y[x, z]y^{-1}$ azonosságokat.

4.9.31. Ha a részcsoport nem tartalmazza $\{id\} \times \mathbb{Z}_2^+$-t, akkor a 4.9.27. Gyakorlatot alkalmazzuk, ha igen, akkor a moduláris szabályt (4.7.30. Gyakorlat).

4.9.32. A kocka egyik rögzített csúcsából kiinduló három lapátló végpontjai egy szabályos tetraédert alkotnak (melynek mindegyik éle lapátlója a kockának). A kocka 8 csúcsa és 12 lapátlója összesen két ilyen tetraédert ad. Mutassuk meg, hogy azok az egybevágóságok, amelyek egy ilyen tetraédert önmagába visznek, S_4-gyel izomorf normálosztót alkotnak. Tekintsük továbbá a kocka mozgásait, azaz irányítástartó egybevágóságait (ezek a kockának pontosan azok a szimmetriái, melyek determinánsa 1).

4.9.33. Használjuk föl azt a geometriából ismert tényt, hogy ha A egy origót fixáló egybevágósági transzformáció a térben, akkor ha mozgás, akkor tartja a vektoriális szorzatot, azaz $A(u \times v) = A(u) \times A(v)$, ha viszont nem mozgás (más szóval irányításváltó), akkor a vektoriális szorzat az ellentettjére változik, azaz $A(u \times v) = -A(u) \times A(v)$.

4.9.34. A $\mathbb{Z}_4^+$ csoportban értelmezzük a $\mathbb{Z}_2$ test elemeivel való szorzást úgy, hogy $0 * a = 0$ és $1 * a = a$ legyen minden $a \in \mathbb{Z}_4^+$ elemre. Teljesülnek-e a vektortér-axiómák?

4.9.36. Használjuk föl, hogy véges sok szám legkisebb közös többszöröse pontosan akkor egyezik meg a szorzatukkal, ha a számok páronként relatív prímek. Legyen G véges részcsoportja a T test multiplikatív csoportjának, és e a G exponense. Mutassuk meg, hogy G minden eleme gyöke az $x^e - 1$ polinomnak.

4.9.39. Legyen M maximális az A csoport azon részcsoportjai között, melyekre $M \cap \langle a \rangle = \{0\}$ teljesül. Mutassuk meg, hogy $\langle a \rangle + M = A$. Ehhez válasszunk egy olyan minimális rendű c elemet, amely még nincs benne $\langle a \rangle + M$-ben, és vizsgáljuk pc-t. Az A helyett az A/M faktorcsoportban dolgozzunk.

4.10.7. Legyen N az F szabad csoportnak az a normálosztója amelyet az összes w^2 és $[u, v]$ szavak generálnak, ahol $u, v, w \in F$. Mutassuk meg, hogy az F/N csoport kommutatív, és minden elemének a négyzete az egységelem, így vektortérnek tekinthető a $\mathbb{Z}_2$ test fölött a 4.9.34. Feladat értelmében. Igazoljuk, alkalmas $F \to \mathbb{Z}_2^+$ homomorfizmusokat választva, hogy mind az X, mind az Y szabad generátorrendszerek képe bázis ebben a vektortérben.

4.10.8. Mutassuk meg, hogy ha u és v szabadon generálják az $F(u, v)$ csoportot, akkor az $u^i v u^{-i}$ $(i > 0)$ elemek szabad generátorrendszert alkotnak az általuk generált részcsoportban.

4.10.18. Használjuk föl a 4.3.40. Feladatot.

4.10.19. Mutassuk meg, hogy $B(k, 3)$-ban a konjugált elemek egymással fölcserélhetők, és ezért minden elem benne van egy kommutatív normálosztóban. Bizonyítsunk k szerinti indukcióval.

4.10.21. Csak néhány esetben adunk ötletet:

(7) Mutassuk meg, hogy $b = 1$.
(8) Ez a 4.9.38. Gyakorlat (2) pontjában szereplő csoport.
(9) Ez a 4.9.38. Gyakorlat (6) pontjában szereplő csoport.
(10) Mutassuk meg, hogy $f = ab$ és $t = a$ kielégíti D_3 definiáló relációit.
(12) Mutassuk meg, hogy $\{1, b, aba^{-1}, a^{-1}ba\}$ normálosztó.
(13) Mutassuk meg, hogy $u = a^2$ és $v = (ab)^2$ kielégítik az előző pontban szereplő definiáló relációkat, és az általuk generált részcsoport normálosztó.
(14) Mutassuk meg, hogy az a, b, cbc^{-1} elemek által generált részcsoport legfeljebb nyolcelemű, kommutatív normálosztó.

4.10.22. Használjuk föl D_4 definiáló relációit annak megmutatására, hogy f tetszőleges 90 fokos forgatásba, t pedig tetszőleges tengelyes tükrözésbe, egymástól függetlenül elvihető automorfizmussal. Minden α automorfizmushoz rendeljük hozzá azt a permutációt, amelyet α a tengelyes tükrözések négyelemű halmazán hoz létre.

4.10.23. Legyen X az F szabad generátorrendszere, és válasszuk ki minden $x \in X$ esetén a $\varphi(x)$ elem egy tetszőleges ősképét α-nál. Legyen $\psi(x)$ ez az ősképe. Mivel F szabad, ψ-t kiterjeszthetjük homomorfizmussá.

4.10.24. A szó hossza szerinti indukcióval igazoljuk, hogy minden nullösszegű szó benne van F kommutátor-részcsoportjában.

4.11.10. Mutassuk meg, hogy van negyedrendű elem. Ha az általa generált részcsoporton kívül van másodrendű elem, akkor D_4-et kapjuk, egyébként pedig a kvaterniócsoportot. Ennek megmutatásához használjuk föl a 4.10.15. Példában szereplő definiáló relációkat.

4.11.13. Mutassuk meg, hogy az $\alpha(x) = (p+1)x$ leképezés p rendű automorfizmusa a $N = \mathbb{Z}_{p^2}^+$ csoportnak. Készítsünk ennek alapján az N normálosztóból és a $H = \mathbb{Z}_p^+$ részcsoportból nemkommutatív szemidirekt szorzatot.

4.11.26. Vegyünk egy olyan elemet, amely nincsen benne az egyetlen maximális részcsoportban. Mi lesz az általa generált részcsoport?

4.11.30. A 4.4.31. Feladatban belátott $|AB| = |A||B|/|A \cap B|$ összefüggést ismételten felhasználva igazoljuk, hogy páronként relatív prím rendű normálosztók szorzatának a rendje a tényezők rendjeinek a szorzata.

4.11.31. Elsőként az alábbi állításokat érdemes belátni. Az S_4 csoportban a 2-Sylow részcsoport nem lehet normálosztó, mert 8-nál több 2-hatvány rendű elem van. Az A_5 esetében minden pont stabilizátora tartalmaz egy 2-Sylow részcsoportot. A D_n-ben a forgatásokból álló normálosztó minden részcsoportja is normálosztó, és tartalmazza a páratlan prímekhez tartozó Sylowokat. Legyen $n = 2^k m$, ahol m páratlan. Ekkor minden 2-Sylow 2^k tükrözésből, és az összes 2-hatvány rendű forgatásból áll.

4.11.33. Tegyük föl, hogy $p < q < r$. Mutassuk meg, hogy az r-Sylowok száma pq. Számoljuk össze a p, q, r rendű elemeket.

4.11.34. Ha bármely két p-Sylow metszete csak az egységelemből áll, akkor számoljuk meg a p-hatvány rendű elemeket. Ha nem így van, akkor mi lesz két p-Sylow p elemű metszetének a normalizátora?

4.11.35. Legyenek P_1 és P_2 olyan p-Sylowok, melyek D metszete a lehető legnagyobb elemszámú. Igazoljuk, hogy D normálosztó G-ben. Ha $|D| = 1$, akkor számoljuk meg a p-hatvány rendű elemeket.

4.11.36. Legyen $g \in G$. Ekkor gPg^{-1} is p-Sylowja N-nek, ezért N-ben is konjugáltak. A második állítás bizonyításához mutassuk meg, hogy P normálosztó G mindegyik P-t tartalmazó p-Sylowjában.

4.11.37. A P részcsoport p-Sylow K-ban, ami normálosztó $N_G(K)$-ban. Alkalmazzuk a Frattini-elvet. A második állítás bizonyításához használjuk föl, hogy a p-Sylow részcsoportok száma K-ban is kongruens 1-gyel mod p.

4.11.38. Tegyük föl, hogy $q < p$, tehát $q \mid p-1$. A 4.11.20. Következmény miatt minden nemkommutatív pq rendű G csoport egy $P \rtimes Q$ szemidirekt szorzat, ahol P-t egy p rendű a elem, Q-t egy q rendű b elem generálja. Legyen $bab^{-1} = a^t$. Ekkor a b-vel való konjugálás a $P \cong \mathbb{Z}_p^+$ normálosztónak

az $\alpha_t : x \mapsto x^t$ automorfizmusa. Mivel b rendje q, ezért α_t rendje ennek osztója, vagyis 1 vagy q. De 1 nem lehet, mert akkor G kommutatív lenne, ezért α_t rendje q. Az $\mathrm{Aut}(\mathbb{Z}_p^+) \cong \mathbb{Z}_p^\times$ izomorfizmus miatt tehát t egy q rendű eleme $\mathbb{Z}_p^\times$-nek. A G csoportot izomorfia erejéig meghatározza a t szám.

Tegyük föl, hogy s egy másik q rendű eleme $\mathbb{Z}_p^\times$-nek. Mutassuk meg, hogy a b elem helyettesíthető egy alkalmas c hatványával úgy, hogy c az a elemet az s-edik hatványába konjugálja.

4.12.8. Legyen $\alpha(aH) = a * x$. Jóldefiniált ez a leképezés?

4.12.42. Tekintsük G hatását a H szerinti bal mellékosztályokon, és mutassuk meg, hogy ennek magja H.

4.12.43. Mutassuk meg, hogy ha $\mathrm{Aut}(G)$ tranzitív a $G - \{1\}$ halmazon, akkor a csoport minden elemének rendje ugyanaz a p prím, a centruma pedig az egész csoport. Alkalmazzuk a véges Abel-csoportok alaptételét, majd a 4.9.35. Gyakorlatot.

4.12.45. Tegyük föl, hogy $\sim$ kongruencia X-en. Legyen $x \in X$, és K azon N-beli n elemek halmaza, melyekre $n(x) \sim x$. Mutassuk meg, hogy $K \triangleleft G$.

4.12.46. Kössük össze a b és c pontokat, ha $(bc) \in G$. Mutassuk meg, hogy a kapott gráf komponensei kongruenciát alkotnak.

4.12.47. Használjuk föl, hogy a -1 hatványa Q minden elemének, és ezért minden nem egyelemű stabilizátorban benne van.

4.12.48. Alkalmazzuk az 4.12.7. Gyakorlat (5) pontját.

4.12.49. Használjuk föl, hogy az A_n részcsoport az S_n mindegyik részcsoportját legfeljebb 2 indexű normálosztóban metszi az első izomorfizmustétel miatt.

4.12.50. A szokásos, Sylow-tételeket használó érvelés mellett használjuk föl a 4.12.48. Feladat állítását is. Amikor G rendje 180, akkor a 4.11.34. Feladat megoldásának ötletét is föl kell használni.

4.12.51. Használjuk föl, hogy a 4.12.49. Feladat szerint $4k+2$ rendű csoportban van kettő indexű normálosztó.

4.12.52. Alkalmazzuk a 4.12.7. Gyakorlatot és a 4.12.8. Feladatot.

4.13.16. Igazoljuk, hogy a kommutátorlánc minden eleme karakterisztikus részcsoport, és a faktorai mindig kommutatívak.

4.13.17. Azt kell belátni, hogy ha G feloldható csoport, H részcsoport, N pedig normálosztó G-ben, akkor H és G/N is feloldható. Használjuk a feloldhatóság kommutátorlánccal való jellemzését (4.13.16. Feladat) és a 4.8.48. Feladatot.

4.13.18. Használjuk az izomorfizmustételeket.

4.13.25. Jelölje U_k azoknak a T fölötti $n \times n$-es felső háromszög-mátrixoknak a halmazát, amelyekben a főátlótól számított, azzal párhuzamos ferde sorok közül k darab azonosan nulla (a főátlót is beleszámítva). Képletben: az $M = ((m_{i,j}))$ akkor eleme U_k-nak, ha $i > j - k$ esetén $m_{i,j} = 0$. Igazoljuk a következő állításokat (E az $n \times n$-es egységmátrix).

(1) Ha $M \in U_m$ és $K \in U_k$, akkor $MK \in U_{m+k}$.
(2) $(E+M)^{-1} = E - M + M^2 - M^3 + \ldots + (-1)^{n-1} M^{n-1}$ minden $M \in U_1$ esetén.
(3) Ha $M \in U_m$ és $K \in U_k$, akkor $[E + M, E + K] - E \in U_{m+k}$.

A fentieken kívül használjuk föl a 4.11.25. Gyakorlat állítását is.

4.13.28. Az SO(3) nemkommutatív egyszerű csoport (4.8.43. Feladat).

4.13.29. Tekintsük G hatását egy p-Sylow részcsoport bal mellékosztályain. Mutassuk meg, hogy a hatás magja és képe is feloldható.

4.13.30. Használjuk föl, hogy (a 4.8.18. Gyakorlat szerint) normálosztó karakterisztikus részcsoportja normálosztó.

4.13.31. Legyen M maximális részcsoport a G feloldható csoportban. Tekintsük G egy minimális N normálosztóját, és válasszunk szét két esetet aszerint, hogy N része-e M-nek.

4.14.7. Számoljuk meg az invertálható lineáris transzformációkat a következőképpen. Rögzítsünk egy bázist, és vizsgáljuk meg, hányféleképpen választhatók ki a bázisvektorok képei úgy, hogy függetlenek legyenek. A $\mathrm{PSL}(n, T)$ rendjének kiszámításához használjuk föl, hogy T multiplikatív csoportja ciklikus (4.3.22. Tétel).

4.14.13. Mutassuk meg, hogy két alkalmas 2-Sylow részcsoport metszetének normalizátora 5 indexű részcsoport lesz, és így létezik beágyazás A_5-be.

U.5. Gyűrűk

5.1.7. Tekintsük a valós elemű 2×2-es mátrixok gyűrűjét.

5.1.28. Fejtsük ki az $(1 + 1)(r + s)$ szorzatot kétféleképpen.

5.1.29. Ha e bal oldali egységelem, akkor $e + r - re$ is az.

5.1.30. Ha s balinverze r-nek, akkor $s + 1 - rs$ is az.

5.1.31. Ha $K \lhd (R \times S)$ és $(r, s) \in K$, akkor $(r, s)(1, 0) = (r, 0) \in K$.

5.1.32. Ha r inverze $1 - ab$-nek, akkor $1 + bra$ inverze lesz $1 - ba$-nak.

5.2.17. Jelölje u az $x + (x^2, xy, y^2)$ és v az $y + (x^2, xy, y^2)$ elemet a faktorgyűrűben. Ha $r \in \mathbb{R}$ esetén az r elemet azonosítjuk $r + (x^2 + xy + y^2)$-tel, akkor az

$R = \mathbb{R}[x, y]/(x^2, xy, y^2)$ gyűrű elemei az $a + bu + cv$ alakú kifejezések, ahol $a, b, c \in \mathbb{R}$, és tudjuk, hogy $u^2 = uv = v^2 = 0$.

5.2.18. Az alább megadott homomorfizmusokra a homomorfizmustételt kell alkalmazni.

(1) $\varphi(f) = f(\sqrt{2}i)$.
(2) Nullosztómentes-e a bal oldalon álló gyűrű?
(3) $\varphi(f) = \big(f(1), f(-1)\big) \in \mathbb{R} \times \mathbb{R}$.
(4) $\varphi(a + bi) = (\overline{a + 2b}, \overline{a - 2b})$, ahol a fölülvonás mod 5 maradékot jelent.
(5) $\varphi(a + bi) = (\overline{a} + \overline{b}x) + I$, ahol $I = (x^2 + 1) \lhd \mathbb{Z}_3[x]$, és a fölülvonás mod 3 maradékot jelent.
(6) $\varphi\big(f(x, y)\big) = f(0, y)$.

5.2.19. Az első kérdés megválaszolásához legyen $R = 3\,\mathbb{Z}$ a hárommal osztható egészek gyűrűje, és $I = 6\,\mathbb{Z}$ a hattal osztható egészekből álló ideál R-ben.

5.3.3. Legyen $E^{i,j}$ az a mátrix, amelyben az i-edik sor j-edik eleme 1, a többi elem nulla. Vizsgáljuk meg, mi történik, ha ezzel balról, illetve jobbról megszorzunk egy tetszőleges mátrixot. Ha az I ideálnak eleme egy nem nulla mátrix, akkor a fenti szorzásokkal készítsünk belőle egy olyan mátrixot, amelyben egy előre megadott helyen nem nulla elem van, a többi elem pedig nulla.

5.3.18. Legyen I ideál az $R^{n\times n}$ teljes mátrixgyűrűben, és $J \subseteq R$ az összes I-beli mátrixok összes elemeinek halmaza. Az 5.3.3. Feladat megoldásában bemutatott számolás alapján igazoljuk, hogy $I = J^{n\times n}$.

5.4.9. Ha L balideál R-ben és $a \in L$, akkor tekintsük az Ra^k balideálok láncát. Mutassuk meg, hogy R balideálmentes (5.3.8. Tétel).

5.4.10. Alkalmazzuk a Zorn-lemmát a valódi részcsoportok halmazára. Ha a $\mathbb{Q}^+$ csoportnak lenne egy M maximális részcsoportja, akkor $\mathbb{Q}^+/M$ prímrendű lenne a 4.4.23. Tétel miatt. Legyen ez a prím a p, és tekintsük a q/p elemet, ahol $q \notin M$.

5.4.11. Igazoljuk, hogy a J által R-ben generált ideál $J + RJ + JR + RJR$ (komplexusműveletekről van szó az 5.1.12. Definíció értelmében). Az analóg csoportelméleti állítás nem igaz: tekintsük egy véges egyszerű csoport direkt négyzetének a $\mathbb{Z}_2$-vel vett nemtriviális szemidirekt szorzatát.

5.5.15. Tekintsük a $\mathbb{Q}[x_1, x_2, \ldots]$ végtelen sok határozatlanú polinomgyűrűt.

5.5.16. Legyen $I_n = (2^n, 2^{n-1}x, 2^{n-2}x^2, \ldots, x^n) \lhd \mathbb{Z}[x]$. Igazoljuk, hogy a $\mathbb{Z}[x]/I_{n+1}$ faktorgyűrű I_n/I_{n+1} ideálját az $x + I_{n+1}$ és a $2 + I_{n+1}$ elemek bármelyikével szorozva nullát kapunk, és ezért egyrészt I_n/I_{n+1} egy $\mathbb{Z}_2$ fölötti vektortérnek tekinthető, másrészt ha $g_1, \ldots, g_k \in I_n/I_{n+1}$, akkor a $g_1, \ldots, g_k$ elemek által $\mathbb{Z}[x]/I_{n+1}$-ben generált ideál a $\lambda_1 g_1 + \ldots + \lambda_k g_k$ alakú elemek halmaza,

ahol mindegyik λ_i értéke 0 vagy 1. Használjuk föl, hogy egy vektortérben minden generátorrendszer elemszáma legalább akkora, mint a dimenzió.

5.6.8. Használjuk föl, hogy a radikál végesen generált, továbbá az 5.6.4. Gyakorlat megoldásában található számolás ötletét.

5.6.15. Használjuk föl az 5.5.13. Gyakorlatnak azt az állítását, hogy főideálgyűrűben $(r) \cap (s)$ az r és s legkisebb közös többszöröse által generált ideál.

5.6.23. Tekintsük $\mathbb{Z}[x]$-ben a $(4, 2x)$ ideált.

5.6.24. A (2) állításra ellenpélda $\mathbb{Z}[x]$-ben a $(4, 2x)$ ideál. A (3) bizonyításához legyen $M = \sqrt{I}$. Tegyük föl, hogy $bc \in I$, de $c \notin M$, be kell látni, hogy $b \in I$. Ehhez igazoljuk, hogy $1 = m + rc$ alkalmas $m \in M$-re és $r \in R$-re, és innen a binomiális tételt felhasználva, hogy $1 + sc \in I$ alkalmas $s \in R$-re.

5.6.29. A (2) bizonyításához legyen $P_i = \sqrt{Q_i}$. Mivel a P_i ideálok nem mind egyenlők, feltehető, hogy például $P_1 \not\subseteq P_2$. Készítsünk ebből egy olyan c elemet, amely Q_1-ben benne van, de P_2-ben nincs. A metszet rövidíthetetlenségének felhasználásával keressünk olyan b elemet, amelyre $b \notin Q_1$, de $b \in Q_2 \cap \ldots \cap Q_n$.

5.6.38. Legyen $I = (xy, z)$. Mutassuk meg, hogy ha $I_1 I_2 = I$, de I_1 és I_2 is valódi módon tartalmazza I-t, akkor I_1 és I_2 egyik polinomjában sem szerepelhet nem nulla konstans tag.

5.6.40. Alkalmazzuk az 5.6.39. Gyakorlatot, majd osszunk $g_1, \ldots, g_m$-mel maradékosan (5.6.31. Definíció).

5.6.41. Használjuk föl, hogy az I-beli polinomok főtagjai által generált ideál végesen generált, továbbá az előző 5.6.40. Feladatot.

5.6.42. Tegyük föl indirekt, hogy van olyan $f \in I$ polinom, melynek főtagja egyik g_i főtagjával sem osztható. Minden ilyen f fölírható $p_1 g_1 + \ldots + p_m g_m$ alakban, tekintsük az összes ilyen előállítást. Legyen G_i a g_i-nek, P_i a p_i-nek a főtagja. Átszámozással feltehető, hogy a $P_1 G_1 \succeq P_2 G_2 \succeq \ldots \succeq P_m G_m$ (e jelölésben az „egyenlőség” konstansszorost jelent). Válasszuk f-nek ezt az előállítását (azaz a $p_1, \ldots, p_m$ polinomokat) úgy, hogy $P_1 G_1$ lexikografikusan a lehető legkisebb legyen, és ezen belül úgy, hogy a $P_i G_i$ között a lehető legkevesebb olyan legyen, ami $P_1 G_1$-nek konstansszorosa.

A $P_1 G_1$ nem lehet az f főtagja, mert $P_1 G_1$ osztható g_1 főtagjával. Ugyanakkor lexikografikusan nagyobb vagy egyenlő mindegyik $p_i g_i$ mindegyik tagjánál. Ezért az f-et előállító összegből ki kell esnie. Így $P_2 G_2$ biztosan konstansszorosa $P_1 G_1$-nek (és esetleg még néhány további $P_i G_i$ is). Használjuk az $S(g_1, g_2)$ polinomot arra, hogy a $p_1, \ldots, p_m$ helyett olyan f-et előállító rendszert kapjunk amelyben már kevesebb olyan főtag szerepel, amely $P_1 G_1$-nek konstansszorosa.

5.6.43. Tekintsük minden egyes lépésnél az összes f_i polinomok főtagjai által generált ideált. Mutassuk meg, hogy ha valamelyik r_{ij} nem a nullapolinom, akkor a főtagja nincs benne ebben az ideálban.

5.7.10. Igazoljuk, hogy ha $r/s \in S$, ahol r és s relatív prímek, akkor $1/s \in S$. Mutassuk meg, hogy ha $I \lhd S$, akkor az $I \cap R \lhd R$ ideál tetszőleges R-beli generátora S-ben I-t generálja.

5.7.11. Ha a és b relatív prím nem nulla elemek R-ben, akkor tekintsük az $r + (sa/b^k)$ elemekből álló S részgyűrűt, ahol $r, s \in R$ és $k \geq 1$ egész. Alkalmazzuk ebben az (a/b^k) főideálokra az 5.5.8. Tétel (1) feltételét.

5.8.14. Használjuk föl, hogy $p \nmid n$ miatt az $x^n - 1$ polinomnak nincs többszörös gyöke T-ben (5.8.13. Gyakorlat).

5.8.15. Mutassuk meg, hogy $\Phi_n(nN)$ minden prímosztója $nk + 1$ alakú.

5.8.16. Legyen $n = pm$. A $\Phi_{pm}(x) \mid (x^{pm} - 1)/(x^m - 1)$ összefüggést mod p vizsgálva mutassuk meg, hogy $c^m = ap + 1$ alkalmas $a \in \mathbb{Z}$-re. Ezt helyettesítsük be az előbbi oszthatóságba, és alkalmazzuk a binomiális tételt. A $c = \pm 1$ eset vizsgálatához használjuk föl a 3.9.19. és a 3.9.20. Feladatokat.

5.8.17. A 3.9.23., az 5.8.14. és az 5.8.16. Feladatok segítségével vizsgáljuk meg $\Phi_n(c)$ és $\Phi_m(c)$ közös prímosztóit.

5.9.9. Próbálkozzunk a $P = \{a/b \in T : a, b > 0\}$ pozitivitástartománnyal.

5.9.10. Mutassuk meg, hogy két rendezés van: az egyik a szokásos, a másik pedig az, amelynek a pozitivitástartománya az $a - b\sqrt{2}$ alakú számokból áll, ahol $a + b\sqrt{2}$ a hagyományos értelemben pozitív. Használjuk föl az $(a + b\sqrt{2})(-a + b\sqrt{2}) = -a^2 + 2b^2$ azonosságot $a + b\sqrt{2}$ előjelének meghatározásához.

5.9.12. Nevezzünk egy nem nulla polinomot pozitívnak, ha a legkisebb fokú nem nulla tagjának pozitív az együtthatója. Módosítsuk az így kapott elrendezést úgy, hogy a polinomokat $x - b$ polinomjaként írjuk, ahol $b \in \mathbb{R}$ rögzített (2.4.18. Feladat).

5.9.13. Az R helyett az R gyűrű T hányadostestével foglalkozzunk. Legyen P_0 a nem nulla elemek négyzetösszegeinek halmaza. Igazoljuk, hogy ez pozitivitástartomány egy részben rendezésre. Mutassuk meg, hogy ha $P \supseteq P_0$ pozitivitástartomány egy részben rendezésre, $0 \neq r \in T$, és $-r$ nem írható föl p/q alakban, ahol $p, q \in P$, akkor a $pr + q$ alakú elemek halmaza, ahol $p, q \in P$, szintén pozitivitástartomány. Alkalmazzuk a Zorn-lemmát.

5.10.15. A feladat megoldása előtt feltétlenül ismételjük át az irreducibilitás ellenőrzésére a 3. fejezetben tanult módszereket. Az (1) – (3) esetekben alkalmazzuk az 5.10.2. Gyakorlat előtt a $\sqrt{2} + \sqrt{3}$ esetében bemutatott technikát: a számot z-vel egyenlővé tesszük, majd átrendezéssel és hatványozással

eltüntetjük a gyökvonásokat, és a kapott polinomról belátjuk, hogy irreducibilis. A (2) pontban az irreducibilitás ellenőrzéséhez olvassuk el a 3.3.12. Példa megoldását. A (4) és (5) esetben használjuk föl, hogy a körosztási polinom irreducibilis $\mathbb{Q}$ fölött (3.9.9. Tétel), a (6) esetben pedig a $\cos 3\alpha$ fölírását $\cos\alpha$ segítségével (vö. 1.5.24. Feladat).

5.11.14. Alkalmazzuk az 5.11.8. Állítást.

5.11.15. Alkalmazzuk az 5.11.7. Állítás utáni megjegyzést.

U.6. Galois-elmélet

6.1.25. Mutassuk meg, hogy $c = \sqrt{2} + \sqrt{3}$ megfelelő. Ehhez számítsuk ki c^2 és c^3 értékét.

6.1.26. Kövessük a 6.1.24. Gyakorlat megoldását, ahol $K = \mathbb{Q}$, $c = 2$, $b = 3$.

6.1.27. Használjuk a 6.1.26. Feladatot, és alkalmazzunk indukciót n szerint.

6.2.9. Legyen ε primitív harmadik egységgyök. Tekintsük az $\alpha = \varepsilon\sqrt[3]{2}$ fokát $K = \mathbb{Q}$ és $L = \mathbb{Q}(\sqrt[3]{2})$ fölött.

6.2.16. Alkalmazzuk a 6.1.27. Feladat (2) pontját.

6.2.22. A 6.2.13. Tétel bizonyításához hasonlóan járjunk el.

6.3.7. Mivel a $K \leq L$ bővítés véges, léteznek olyan $\alpha_1, \ldots, \alpha_m \in L$ elemek, hogy $L = K(\alpha_1, \ldots, \alpha_m)$ (például a bővítés egy bázisa). Véges bővítés minden eleme algebrai (6.2.4. Állítás), legyen α_i minimálpolinomja K fölött s_i, és $f \in K[x]$ az s_i polinomok szorzata. Mutassuk meg, hogy f felbontási teste K fölött L.

6.3.15. Használjuk föl a 3.7.9. és az 5.8.12. Gyakorlatokat.

6.4.18. Használjuk föl a 6.4.15. Gyakorlatot és a 6.2.22. Feladatot. (Valójában a 6.2.13. Tétel bizonyítását kell általánosítani.)

6.4.20. Vegyük észre, hogy ha $f \in K[x]$ normált, n-edfokú, irreducibilis polinom, akkor $f(x) - (x - x_1^f) \ldots (x - x_n^f)$ mindegyik együtthatója az I ideálnak generátoreleme a gyökök és együtthatók összefüggése miatt. Ezért ha egy I-t tartalmazó ideállal faktorizálunk majd, akkor f (képe a faktorban) gyöktényezőkre fog bomlani.

Tegyük föl, hogy a megadott elemek által generált I ideál az egész R, vagyis tartalmazza az 1-et. A generált ideál képlete (5.1.15. Gyakorlat) szerint ez azt jelenti, hogy az 1 fölírható $r_1g_1 + \ldots + r_kg_k$ alakban, ahol $r_i \in R$, a g_i pedig az I ideálnak generátoreleme. Ebben a képletben összesen csak véges sok határozatlan szerepel, mindegyik valamelyik f irreducibilis polinomhoz tartozik. Legyen S az e határozatlanok és K által generált részgyűrűje R-nek, h pedig az

összes olyan f polinom szorzata, amely e határozatlanok valamelyikéhez tartozik. A 6.4.5. Következmény miatt a h polinomnak létezik egy N felbontási teste K fölött. Mutassuk meg, hogy van olyan $\varphi : S \to N$ gyűrűhomomorfizmus, amely a g_i elemeket nullába, az 1-et pedig az N egységelemébe viszi. Ez az ellentmondás fogja mutatni, hogy az I ideál valódi.

6.4.21. Használjuk föl, hogy egy végtelen sok elemmel generált bővítés minden eleme véges sok generátor hozzávételével megkapható (6.1.10. Gyakorlat).

6.4.22. A 3.6.15. Feladat megoldásának első bekezdését általánosítsuk.

6.4.23. Alkalmazzuk a Schönemann–Eisenstein-kritériumnak az 5.7.9. Gyakorlat megoldásában megfogalmazott általánosítását.

6.4.24. Használjuk föl, hogy ha a $p \neq 0$ karakterisztikájú K testnek α eleme, akkor $x^p - \alpha$ minden nem elsőfokú irreducibilis tényezője inszeparábilis.

6.4.25. Legyen K tökéletes test, $K \leq L$ algebrai bővítés, és $f \in L[x]$ irreducibilis polinom. Bővítsük L-et f egy α gyökével, és használjuk föl, hogy a 6.2.22. Feladat miatt $K \leq L(\alpha)$ is algebrai bővítés.

6.4.26. Alkalmazzuk a 6.4.24. Feladatban adott jellemzést.

6.4.27. Alkalmazzuk a 6.4.24. Feladatban adott jellemzést.

6.5.14. A Galois-elmélet főtételének (6.6.7. Tétel) és a 6.5.13. Gyakorlatnak a felhasználásával igazoljuk, hogy $\sqrt{2}$ nincs benne az $x^4 - 5$ polinom $\mathbb{Q}$ fölötti felbontási testében.

6.6.12. Legyen ε egy n-edik komplex primitív egységgyök. A 6.3.13. Gyakorlatban már láttuk, hogy $\mathbb{Q} \leq \mathbb{Q}(\varepsilon)$ egy $\varphi(n)$ fokú normális bővítés, amely az $x^n - 1$, illetve a $\Phi_n(x)$ polinomok közös felbontási teste. Mutassuk meg, hogy e bővítés relatív automorfizmusai azok a ψ_j leképezések, amelyekre $\psi_j(\varepsilon) = \varepsilon^j$, ahol $0 \leq j < n$ tetszőleges, az n-hez relatív prím szám.

6.6.14. Igazoljuk, hogy $x^4 - 5$ felbontási testében nincs benne egyik primitív nyolcadik egységgyök sem, ha viszont egy ilyennel bővítünk, akkor már $x^4 + 5$ gyökei is bekerülnek.

6.6.15. Mutassuk meg, hogy a polinom öt komplex gyöke közül pontosan három valós, és ezért a komplex konjugálás a gyökök halmazán transzpozícióként hat. Használjuk föl a 4.12.46. Feladatot.

6.6.17. Bővítsük L-et úgy, hogy K-nak normális bővítését kapjuk (6.4.16. Gyakorlat), majd alkalmazzuk a Galois-elmélet főtételét.

6.6.18. Alkalmazzuk az előző feladat ötletét.

6.6.20. Legyen α minimálpolinomja s, konjugáltjai $\alpha_1, \alpha_2, \ldots, \alpha_n$, továbbá β minimálpolinomja t, konjugáltjai pedig $\beta_1, \ldots, \beta_m$ (a K fölött). Jelölje L

az st felbontási testét K fölött, G pedig a $K \leq L$ bővítés Galois-csoportját. Mutassuk meg, hogy a G csoport tranzitívan hat az (α_i, β_j) párok halmazán.

Tekintsük az $f(x) = \prod(x-\alpha_i-\beta_j)$ polinomot, ahol $1 \leq i \leq n$ és $1 \leq j \leq m$ egymástól függetlenül. Elég belátni, hogy ez az nm fokú polinom irreducibilis K fölött, mert akkor ez $\alpha+\beta$ minimálpolinomja lesz, és így $\alpha+\beta$ foka tényleg nm. Ehhez a 6.6.19. Gyakorlat (2) pontját használjuk.

Annak igazolására, hogy az $\alpha_i+\beta_j$ számok páronként különbözők, tekintsük az α_i-k között azokat, amelyeknek a lehető legkisebb a valós része, és ha több ilyen van, akkor ezek között azt, amelynek a lehető legkisebb a képzetes része, legyen ez α_1. Válasszuk β_1-et ugyanígy. Ekkor $\alpha_1+\beta_1$ nyilván az összes többi $\alpha_i+\beta_j$-től különbözik.

6.7.18. Vegyük észre, hogy $x^2+x+1 = \Phi_3(x)$, és alkalmazzuk az 5.8.14. Feladatot. Használjuk föl, hogy egy másodfokú polinom irreducibilis, ha nincs az adott testben gyöke.

6.7.19. Mutassuk meg, hogy a polinom mindegyik 1-től különböző gyökének a rendje 11 lesz a $\mathbb{Z}_2$ fölötti felbontási test multiplikatív csoportjában, majd alkalmazzuk Lagrange tételét.

6.7.20. Alkalmazzuk Lagrange tételét, azt, hogy véges test multiplikatív csoportja ciklikus, továbbá az 5.8.14. Feladatot.

6.7.21. Használjuk föl a 6.7.20. Feladat állításait, a megoldásban szereplő ellenpéldát, valamint azt a tényt, hogy egy elem akkor generál egy testet, ha egyetlen valódi résztestben sincs benne.

6.7.23. Osztályozzuk $\mathbb{F}_{2^8}$ és $\mathbb{F}_{2^{12}}$ elemeit a prímtestük fölötti konjugáltság szerint. Minden ilyen osztály egy $\mathbb{Z}_2$ fölött irreducibilis polinomnak felel meg.

6.7.24. A gráf csúcsai legyenek az $\mathbb{F}_{16}$ test elemei, a három szín pedig az egyetlen négyelemű résztest három nem nulla eleme. Az α és β közötti élet színezzük $(\alpha+\beta)^5$ színűre.

6.8.21. Jelölje (a szokásos módon) az oldalakat a, b, c, a hozzájuk tartozó szögfelezők hosszát f_a, f_b, f_c, a szemköztes szögeket pedig α, β, γ. Vizsgáljuk azt az esetet, amikor $a = 1$, $b = 1$, $f_a = 1$. Ebben a speciális esetben számoljuk ki a háromszög szögeit.

6.8.22. Írjuk föl a háromszög területét kétféleképpen. Legyen a beírt kör sugara $\rho = 1$, a szár b hosszát pedig olyan számnak válasszuk, hogy a $2x$ alapot harmadfokú és irreducibilis polinom gyöke szolgáltassa.

6.8.23. Szerkeszthető-e 3°-os szög? És 2°-os?

6.8.24. Igazoljuk, hogy $i\sin(2\pi/n)$ másodfokú $\mathbb{Q}\big(\cos(2\pi/n)\big)$ fölött $(n > 2)$.

6.9.13. Tekintsük az n elemű $\mathbb{Z}_n$ halmaz $ax+b$ alakú permutációinak A csoportját a kompozícióra, ahol $a \in \mathbb{Z}_n^\times$ és $b \in \mathbb{Z}_n$ (ez hasonlít az $\mathrm{AGL}(1, T)$

csoporthoz, lásd 4.1.25. Definíció). Mutassuk meg, hogy ez (két lépésben) feloldható, és hogy a keresett Galois-csoport ennek részcsoportja.

6.9.14. Emeljük ki a minimálpolinomból a megfelelő gyöktényezőt, és helyettesítsük be a transzformációt.

6.9.15. Számítsuk ki az (ε_j, γ) elemek összegét $1 \le j \le p$-re.

6.10.7. Használjuk föl, hogy f irreducibilitása miatt G tranzitív részcsoportja S_4-nek (6.5.12. Állítás), továbbá, hogy S_4 minden tranzitív részcsoportjának rendje néggyel osztható (a 4.5.8. Tétel miatt). Keressük meg az összes ilyen tranzitív részcsoportot. Használjuk a diszkriminánst annak eldöntésére, hogy G részcsoportja-e A_4-nek (6.10.4. Lemma). Végül gondoljuk meg, hogy a 3.8.8. Feladat megoldása minden nulla karakterisztikájú test fölött működik, és így f harmadfokú rezolvensének gyökei benne vannak f felbontási testében.

6.10.8. Használjuk föl, hogy a harmadfokú rezolvens gyökei $b/2$ és $\pm\sqrt{d}$. Legyenek f gyökei $\alpha_1, \alpha_2 = -\alpha_1, \alpha_3, \alpha_4 = -\alpha_3$. Fejezzük ki $d(b^2 - 4d)$-t az α_i gyökökkel.

6.10.9. Mutassuk meg, hogy ha f gyökei $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ és $u = (\alpha_1\alpha_2 + \alpha_3\alpha_4)/2$ (3.8.8. Feladat), akkor

$$(2u - b)(2u + b)^2 - 4c^2 = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2(\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_4)^2 .$$

U.7. Modulusok

7.2.20. Kövessük a lineáris algebrában tanult elemi bizonyításokat.

7.2.21. Legyen $v \neq 0$ az $y = x$ egyenessel párhuzamos, $w \neq 0$ pedig egy rá merőleges vektor. Mutassuk meg, hogy v és w az $M = M(A, V)$ modulusnak gyenge bázisát alkotják. A második kérdés megválaszolásához vizsgáljuk a tükrözés helyett az origó körüli $+90$ fokos forgatást.

7.3.9. A (4) belátásához legyen $N \le \langle m \rangle$, és tekintsük az $\{r \in R : rm \in N\}$ ideált (a 4.3.26. Lemma analógiájára). Mutassuk meg, hogy ha ezt az ideált az r elem generálja, akkor $N = \langle rm \rangle$.

7.3.23. Álljon $M_i \le T^{n\times n}$ azokból a mátrixokból, amelyeknek az i-edik oszlopban lévő elemek kivételével mindegyik eleme nulla. Keressünk egy olyan invertálható B_{ij} mátrixot, amelyre $M_i B_{ij} = M_j$, és igazoljuk, hogy a $B \mapsto BA_{ij}$ modulus-izomorfizmus.

7.4.13. Használjuk föl, hogy

$$\det(v_1 + ru, v_2, \ldots, v_i) = \det(v_1, v_2, \ldots, v_i) + r \det(u, v_2, \ldots, v_i)$$

(itt a v_j és az u oszlopvektorok), továbbá a kitüntetett közös osztóra vonatkozó $(a + rb, b) = (a, b)$ azonosságot.

7.4.14. Használjunk lineáris algebrát R hányadosteste fölött, pontosabban a determinánsok szorzástételét, illetve az inverz mátrixnak a determináns ferde kifejtéséből származó képletét.

7.4.15. Az előző feladat miatt $L^{-1} \in R^{k\times k}$. E mátrix elemeivel fejezzük ki a b_i vektorokat a c_i vektorok segítségével. A második állítás igazolásához használjuk föl, hogy L determinánsa nem nulla.

7.6.7. Használjuk föl a determinánsosztókról szóló állításokat (7.4.13. Feladat).

7.6.12. Ha csak véges sok invariáns altér van, hány dimenziós lehet egy sajátaltér? Mutassuk meg, hogy ha p prím $T[x]$-ben, és az $M(A, V)$ felbontásában két p-hatvány rendű direkt összeadandó is szerepel, akkor végtelen sok invariáns altér van. Használjuk föl a 7.4.10. Gyakorlatot.

7.7.11. Azt igazoljuk, hogy

$$\mathrm{Hom}_R\left(\bigoplus_i M_i, K\right) \cong \prod_i \mathrm{Hom}_R(M_i, K) \quad \text{és}$$

$$\mathrm{Hom}_R\left(M, \prod_i K_i\right) \cong \prod_i \mathrm{Hom}_R(M, K_i)\,.$$

7.7.19. Osszunk el egy maximális rendű elemet a rendjével.

7.7.21. Tegyük föl, hogy $b_1, \ldots, b_n$ bázis a T test fölötti V vektortérben, és tekintsük a $V^* = \mathrm{Hom}(V, T)$ duális tér *duális bázisát.* Ez azokból a b_i^* leképezésekből áll, melyekre $b_i^*(b_j) = 0$ ha $i \neq j$, és 1 ha $i = j$.

7.7.29. A (2) esetében legyen $\varphi : \mathbb{Z}^+ \to \mathbb{Z}_n^+$ a mod n vett maradék képzése és $K = \mathbb{Z}_n^+$. A (4) esetében legyen φ a $\mathbb{Z}^+ \to \mathbb{Q}^+$ beágyazás és $K = \mathbb{Z}^+$.

7.8.22. A (3) pontban azt igazoljuk, hogy $\left(\bigoplus_i M_i\right) \otimes K \cong \bigoplus_i (M_i \otimes K)$.

7.8.25. A (2) esetében legyen φ a $\mathbb{Z}^+ \to \mathbb{Q}^+$ beágyazás és $K = \mathbb{Z}_n^+$ $(n > 1)$.

7.8.27. Ha $t, s \in T$, akkor a $t \otimes m$ elemet megszorozhatjuk s-sel úgy, hogy az eredmény $(st) \otimes m$ legyen. Így ezeknek a tenzoroknak a véges lineáris kombinációit is meg tudjuk szorozni s-sel. Mutassuk meg, hogy ez a szorzás jóldefiniált. A többi állítást először az $R = \mathbb{Z}$ és $T = \mathbb{Q}$ esetben érdemes meggondolni.

7.9.17. Igazoljuk, hogy a radikál azokból a mátrixokból áll, amelyek főátlója végig nulla.

7.9.18. Mutassuk meg, hogy R Jacobson-radikálja nulla, és az $R \cong R/\{0\}$ felbontásában csakis 1×1-es mátrixgyűrűk szerepelhetnek. Végül alkalmazzuk a 6.7.13. Wedderburn-tételt, miszerint minden véges ferdetest kommutatív.

7.9.19. A függetlenség 7.2.3. Gyakorlatban megadott jellemzése miatt részmodulusok egy rendszere akkor és csak akkor független, ha minden véges részrendszere az. Ezért ha tekintjük az I halmaz azon I' részhalmazait, amelyekre

az M_j ($j \in I'$) modulus-rendszer független, akkor ezekre teljesül a Zorn-lemma (E.1.2. Tétel) feltétele.

7.9.22. Mutassuk meg, hogy a Jr balideálok összege, ahol r befutja R-et, kétoldali ideál.

7.9.23. A keresett k-féle egyszerű modulus a k darab teljes mátrixgyűrű egy-egy minimális balideálja lesz, mint R-modulus.

7.9.24. Igazoljuk a Zorn-lemma felhasználásával, hogy R minden valódi balideálja része egy maximális balideálnak.

7.9.28. Legyen e idempotens elem. Mennyi $(er - ere)^2$?

U.8. Általános algebrák, hálók

8.1.17. Az $x \wedge \big(x \vee (x \wedge x)\big)$ kifejezést számítsuk ki a (4) segítségével kétféleképpen.

8.1.25. Legyen $x \equiv y$ akkor és csak akkor, ha x és y között van a feladatban leírt sorozat. Igazoljuk, hogy $\equiv$ ekvivalenciareláció.

8.2.20. Három új jelölést is be kell vezetnünk. Csoportok esetében, ha H részcsoport és N normálosztó, akkor az első izomorfizmustételben HN-ről beszélünk. Ennek általános algebrák esetében a következő a megfelelője. Legyen B részalgebrája és θ kongruenciája az A algebrának. Ekkor $B[\theta]$-val jelöljük a θ azon osztályainak unióját, amelyeknek van B-vel közös eleme. Mutassuk meg, hogy $B[\theta]$ részalgebrája A-nak.

A $H \cap N$ csoportok esetében normálosztója lesz a H részcsoportnak. Az általános esetben jelölje $\theta|_B$ azt a partíciót a B halmazon, amelynek osztályai a θ osztályainak a B-vel való metszetei (az esetleges üres metszeteket elhagyva). Másképp fogalmazva B két eleme akkor és csak akkor kongruens $\theta|_B$-nél, ha θ-nál kongruensek. Mutassuk meg, hogy B egy kongruenciáját kaptuk. Ennek neve a θ-nak a B-re vett *megszorítása*.

Végül legyen $\rho \geq \theta$ is egy kongruencia az A algebrán. Ekkor mindegyik ρ-osztály θ-osztályok uniója. Foglaljuk ezeket a θ-osztályokat ρ-osztályonként egy-egy halmazba. A kapott halmazok az A/θ algebra egy partícióját adják, amit ρ/θ-val jelölünk. Másképp fogalmazva, az x/θ és y/θ akkor kongruens ρ/θ-nál, ha x és y kongruensek ρ-nál. Igazoljuk, hogy ez a definíció nem függ az x és y reprezentánsok választásától, és A/ρ egy kongruenciáját kapjuk.

8.2.39. Tekintsük a $\{0, 1, 2, 3\}$ halmazon az $x * y = \min(x, y) +_4 1$ műveletet.

8.2.40. Egy elég sok tényezős szorzatnak tekintsük az első elemmel induló részletszorzatait. A kapott sorozatban a félcsoport végessége miatt van ismétlődés. Másrészt ha $se = s$, akkor e egy alkalmas hatványa nulla, és így s is nulla.

8.2.41. Haladjunk úgy, mint M_3 egyszerűségének bizonyításában (8.2.37. Gyakorlat). Igazoljuk, hogy ha egy nemtriviális kongruenciát veszünk, akkor van olyan atom (vagyis a nullának egy fedője), amely nullával kongruens. Tekintsük ennek az atomnak a komplementumait, ezek mind 1-gyel kongruensek.

8.3.15. Először olyan függvényt gyártsunk az e (ÉS) és a $\neg$ (NEM) segítségével, amelynek értéke egy előre adott $(a_1, \dots, a_n) \in A^n$ helyen 1, a többi helyen 0. Ezután a többi függvényt ezekből a v (VAGY) segítségével állítsuk össze.

8.3.16. A 8.3.15. Feladat megoldásához hasonlóan járjunk el.

8.3.30. Az első esetben a konstans tag nélküli egész együtthatós polinomokat, a másodikban az összes egész együtthatós polinomot tekintsük.

8.3.31. Tekintsük a $\{0, 1, 2, \dots, k-1\}$ halmazon az $x * y = \min(x, y) +_k 1$ műveletet (vö. 8.2.39. Gyakorlat). Fejezzük ki ezzel az $x \mapsto x +_k 1$ függvényt, a $\min(x, y)$ függvényt, majd a konstans függvényeket. Haladjunk tovább a 8.3.15. Feladat megoldásának módszerével, ahol az ÉS műveletet a min, a VAGY műveletet a $v(x, y) = \min(x -_k 1, y -_k 1) +_k 1$ helyettesíti.

8.4.11. Konstruáljuk meg a végesen generált szabad algebrákat Birkhoff módszerével $\mathcal{K}$ fölött. Ezek végesek, és szabadok $\mathsf{V}(\mathcal{K})$ fölött is.

8.4.20. Mutassuk meg, hogy egy szubdirekt irreducibilis Abel-csoport minden nemtriviális részcsoportja szubdirekt irreducibilis, és ha véges, akkor a véges Abel-csoportok alaptétele miatt prímhatványrendű ciklikus.

8.4.21. Tekintsük a szabad Abel-csoportokat, illetve a szabad kommutatív gyűrűket (lásd 8.3.30. Feladat).

8.4.22. Igazoljuk, hogy $D_4 \in \mathsf{HS}(Q \times Q)$ és $Q \in \mathsf{HS}(D_4 \times D_4)$. Használjuk föl a két csoport definiáló relációit (4.10.15. Példa).

8.4.23. Használjuk az $x^6 = 1$ és $x^2y^2 = y^2x^2$ azonosságokat. Mutassuk meg, hogy minden ezeknek eleget tevő csoportban van egy olyan normálosztó, amely elemi Abel-féle 3-csoport, és a szerinte vett faktor elemi Abel-féle 2-csoport. Használjuk föl, hogy minden másodrendű lineáris transzformáció diagonalizálható, továbbá hogy ha A és B fölcserélhető lineáris transzformációk, akkor A minden sajátaltere B-invariáns. Végül igazoljuk, hogy ha s és t másodrendű elemek egy G csoportban, $(st)^6 = 1$, és t fölcserélhető $(st)^4$-nel, akkor s-sel is.

8.4.24. Legyenek A_i $(i \in I)$ az A algebra összes végesen generált részalgebrái, és B az A_i algebrák direkt szorzata. Ennek definiáljuk egy C részalgebráját a következőképpen. A $\mathbf{c} = (\dots, c_i, \dots)$ akkor van C-ben, ha van olyan i, hogy $c_j = c_i$ teljesül bármely olyan j-re, amelyre $A_j \supseteq A_i$ (ezek a „majdnem konstans" sorozatok). Legyen $\varphi(\mathbf{c}) = c_i$. Mutassuk meg, hogy a φ leképezés jóldefiniált, és szürjektív homomorfizmusa C-nek A-ra.

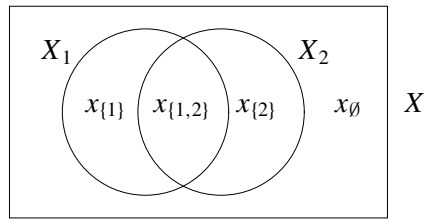
8.4.25. Tegyük föl, hogy az A algebrában teljesülnek a felsorolt azonosságok. Igazoljuk, hogy A minden végesen generált részalgebrája homomorf képe egy végesen generált $\mathcal{K}$-beli szabad algebrának. Alkalmazzuk a 8.4.24. Feladatot.

8.5.8. A (2) bizonyításához tegyük föl, hogy $a \vee c = b \vee c$ és $a \wedge f = b \wedge f$, ahol a feltétel miatt $c \leq f$ (itt $c \in I$ és $f \in F$). Számítsuk ki a disztributív azonosság segítségével az $(a \vee c) \wedge b$ kifejezést, és vezessük le, hogy $b \leq a$. A (3) esetében vegyünk egy $c \in L$ elemet, és legyen $I = (c]$ a c alatti, $F = [c)$ a c fölötti elemek halmaza.

8.5.23. Ha az R gyűrűben teljesül az $x^2 \approx x$ azonosság, akkor fejtsük ki a disztributivitás segítségével az $(x + y)^2$ kifejezést.

8.5.26. Tegyük föl, hogy C részalgebrája a $\mathcal{P}(X)$ Boole-algebrának, ahol X tetszőleges véges halmaz. Legyen az $x, y \in X$ elemekre $x \sim y$, ha C bármely Y elemére teljesül, hogy $x \in Y \iff y \in Y$. Igazoljuk, hogy $\sim$ ekvivalenciareláció, és mutassuk meg, hogy $\sim$ osztályainak tetszőleges uniója eleme C-nek.

8.5.27. A 8.5.26. Feladat megoldásának mintájára $x, y \in X$ esetén legyen $x \sim y$, ha minden i-re $x \in X_i \iff y \in X_i$. Ez ekvivalenciareláció, és ha X-et helyettesítjük a $\sim$ osztályaiból álló halmazzal (ahogy a 8.5.26. Feladat megoldásában), akkor az $X_1, \ldots, X_n$ halmazok továbbra is általános helyzetűek lesznek, de most már tetszőleges $I \subseteq \{1, 2, \ldots, n\}$ részhalmazhoz egyértelműen létezik olyan $x_I \in X$, amely pontosan akkor van benne az X_i halmazban, ha $i \in I$ (hiszen a $\sim$ relációval összevontuk az ilyen tulajdonságú elemeket). Így X elemszáma 2^n. Az U.1. ábra mutatja ezt a helyzetet $n = 2$ esetén (ez a szokásos Venn-diagram, amit logikai feladatok megoldására is használunk).



U.1. ábra. A két elemmel generált szabad Boole-algebra.

Megmutatjuk, hogy az X_i halmazok a teljes $\mathcal{P}(X)$ Boole-algebrát generálják. Az $\{x_I\}$ egyelemű halmaz megkapható úgy, hogy elmetsszük azokat az X_i halmazokat, ahol $i \in I$, és ehhez még hozzámetsszük azoknak az X_j halmazoknak a komplementumait, ahol $j \notin I$. Innen unióval az X minden részhalmaza megkapható, tehát $|F| = 2^{2^n}$.

Legyen B tetszőleges Boole-algebra és $b_1, \ldots, b_n \in B$. Rendeljük hozzá az x_I elemhez a

$$\varphi(x_I) = b_I = \Big(\bigwedge\nolimits_{i \in I} b_i\Big) \wedge \Big(\bigwedge\nolimits_{j \notin I} b'_j\Big)$$

elemet, és ha $Y \subseteq X$, akkor legyen

$$\varphi(Y) = \bigvee_{y \in Y} \varphi(y)\,.$$

Ekkor $\varphi : F \to B$ homomorfizmus lesz, amelyre $\varphi(X_i) = b_i$ minden i-re. Mivel ennek igazolása eléggé számolós, egy másik utat is mutatunk (aminek a lényege az, hogy tetszőleges B helyett elég a kételemű Boole-algebrát venni).

Legyen $\mathcal{K} = \{K\}$, ahol K a kételemű Boole-algebra. Készítsük el Birkhoff módszerével $\mathcal{K}$ fölött az n elemmel generált szabad algebrát. Ez a 8.4.10. Gyakorlat és a Stone-tétel miatt a Boole-algebrák varietása fölött is szabad lesz. Igazoljuk, hogy az előzőekben leírt algebrával izomorf Boole-algebrát kapunk.

8.5.28. Mutassuk meg, hogy az n elemmel generált szabad disztributív háló $f(n)$ elemszámára tetszőleges $0 \leq k \leq n$ esetén

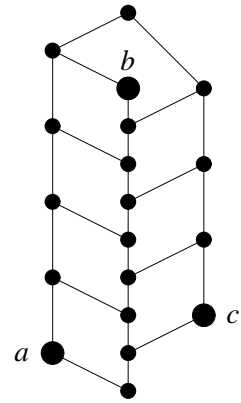
$$2^{\binom{n}{k}} \leq f(n) \leq 2^{2^n}$$

teljesül. A legjobb alsó becslést ebből akkor kapjuk, ha $k = \lfloor n/2 \rfloor$, vagyis páros n esetén n fele, páratlan n esetén az ennél $1/2$-del kisebb (egész) szám.

8.5.29. Tekintsük egy végtelen X halmaz összes részhalmazaiból álló $\mathcal{P}(X)$ Boole-algebrát. Legyen I az X véges részhalmazaiból álló ideál. Mutassuk meg, hogy a θ_I kongruencia (8.5.8. Feladat) szerinti faktor atommentes.

8.5.30. Az (5) bizonyításához tegyük föl, hogy I valódi ideál L-ben. Legyen $d \in L - I$, és $F = [d)$ a d-nél nagyobb vagy egyenlő elemekből álló filter. Tekintsük az L azon ideáljait, amelyek I-t tartalmazzák, de a d elemet nem. Mutassuk meg, hogy a Zorn-lemma miatt ezek között van maximális, és ez prímideál is, hiszen maximális az F filtertől diszjunkt ideálok között.

8.6.12. Igazoljuk, hogy az U.2. ábrán látható hálót generálják az a, b, c elemei.



U.2. ábra. A „halgerinc”-háló.

8.6.27. Tegyük föl, hogy $b = p_1 \wedge \ldots \wedge p_n = q_1 \wedge \ldots \wedge q_m$ két előállítás metszetirreducibilisek metszeteként. Igazoljuk a „kicserélési" tételt: mindegyik $1 \leq i \leq n$-hez van olyan $1 \leq j \leq m$, hogy az első felbontásban p_i-t q_j-re cserélve szintén a b egy felbontását kapjuk (vagyis ha

$$c = p_1 \wedge \ldots \wedge p_{i-1} \wedge p_{i+1} \wedge \ldots \wedge p_n\,,$$

akkor $c \wedge q_j = b$). Használjuk föl, hogy a $[b, c]$ és a $[p_i, p_i \vee c]$ intervallumok $c \wedge p_i = b$ miatt izomorfak.

8.6.33. Legyen $c \in L$. Vegyünk sorban a_i atomokat (addig, amíg lehet) úgy, hogy a_{i+1} ne legyen $c \vee a_1 \vee \ldots a_i$ alatt. Használjuk a dimenzió-egyenlőséget annak igazolására, hogy ez az eljárás véges sok lépésben véget ér, és a kapott atomok egyesítése c-nek komplementuma lesz.

8.6.34. Használjuk föl az $(x \vee y) \wedge (x \vee z) = x \vee \big((x \vee y) \wedge z\big)$ azonosságot (amely a modularitásból következik).

8.6.35. A 8.3.10. Gyakorlat miatt elég belátni, hogy a B szimmetrikus és tranzitív. Használjuk föl, hogy az A algebrának van Malcev-kifejezése (8.6.4. Tétel).

8.6.36. Definiáljuk a θ kétváltozós relációt a B algebrán a következőképpen: $(b_1, b_2) \in \theta$ pontosan akkor, ha van olyan $c \in C$, hogy $(b_1, c), (b_2, c) \in A$. Ez reflexív (mert A szubdirekt részalgebra) és nyilván kompatibilis, tehát a 8.6.35. Feladat miatt kongruencia. Ugyanígy legyen $(c_1, c_2) \in \rho$ akkor és csak akkor, ha van olyan $b \in B$, hogy $(b, c_1), (b, c_2) \in A$, ez kongruencia a C algebrán. Végül értelmezzük a φ leképezést így: $\varphi(b/\theta) = c/\rho$ akkor és csak akkor, ha $(b, c) \in A$. Mutassuk meg, hogy φ jóldefiniált, izomorfizmus, és teljesül rá a feladat állítása.

8.6.37. Alkalmazzuk a 8.6.36. Feladatot, és indukciót a tényezők száma szerint.

8.6.38. Legyen H részcsoport G-ben, és N a H által generált normálosztó. Jelölje D a $G \times G$-ben a (g, g) alakú elemek részcsoportját, ahol g befutja G-t, B pedig a (g, h) alakú párokból álló részcsoportot, ahol $g^{-1}h \in N$ (tehát B az N-hez tartozó kongruencia). Alkalmazzuk a modularitást a $H \times \{1\} \leq N \times \{1\}$ és a D részcsoportokra. A D és a $H \times \{1\}$ egyesítésének kiszámításához használjuk föl a 8.6.35. Feladatot.

8.7.10. Mátrixok helyett dolgozzunk lineáris transzformációkkal. Ha L balideál, akkor jelölje $W = L^\sharp \leq T^n$ a hozzá tartozó alteret. Nyilván $W^\flat \supseteq L$, tehát csak a fordított tartalmazást kell igazolni. Ha C tetszőleges lineáris transzformáció, akkor a lineáris algebrában bizonyított előírhatósági tétel segítségével könnyű konstruálni olyan D lineáris transzformációt, hogy DC magtere ugyanaz, mint C magtere, de DC már identikusan hat a saját képterén, más szóval DC négyzete önmaga (vagyis DC idempotens). Készítsünk ennek felhasználásával olyan L-beli transzformációt, amelynek magtere W.

8.7.11. Tekintsük a C fölötti szabad algebrák alaphalmazát, mint kompatibilis relációt.

8.7.12. Használjuk föl a 8.7.9. Gyakorlat állítását arra, hogy az állítást visszavezessük a 8.7.10. Feladatra.

8.8.3. Az injektivitás jellemzése minden varietásban igaz: használjuk az egy elemmel generált szabad algebrát. A szürjektivitásé nem: tekintsük a $\mathbb{Z} \to \mathbb{Q}$ identikus beágyazást a gyűrűk varietásában.

8.8.7. A (2) esetében legyen M az M_i modulusok direkt összege, és $m \in M_i$ esetén $\pi_i(m)$ az az elem, amelynek az i-edik koordinátája m, a többi nulla. A (3) esetében π_i úgy adódik, hogy az $X_i \to \bigcup X_i$ beágyazást kiterjesztjük egy $F(X_i) \to F(X)$ homomorfizmussá.

U.9. Hibajavító kódok

9.4.3. Legyen I a $v(x) + f(x)(x^n - 1) \in Q[x]$ alakú polinomok halmaza, ahol $v(x)$ befutja a C kódszavaihoz tartozó polinomokat, $f \in Q[x]$ pedig tetszőleges. Mutassuk meg, hogy I ideál, és használjuk föl, hogy test fölötti polinomgyűrű főideálgyűrű.