

MAGASABB FOKÚ EGYENLETEK
ÉS
GEOMETRIAI SZERKESZTHETŐSÉG

(Feladatok)

Dormán Miklós
2010/2011. őszi félév

JELÖLÉSEK

Halmazok, számhalmazok

- $P(X)$ \rightsquigarrow az X halmaz részhalmazainak halmaza,
azaz az X halmaz **hatványhalmaza**
- \mathbb{N} \rightsquigarrow a természetes számok halmaza, $\mathbb{N} = \{1, 2, \dots\}$
- \mathbb{Z} \rightsquigarrow az egész számok halmaza, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- \mathbb{Q} \rightsquigarrow a racionális számok halmaza
- \mathbb{R} \rightsquigarrow a valós számok halmaza
- \mathbb{C} \rightsquigarrow a komplex számok halmaza
- \mathbb{A} \rightsquigarrow a racionális számtest felett algebrai komplex számok halmaza

Relációk

- 0_A \rightsquigarrow $\{(a, a) \mid a \in A\}$ — az egyenlőségreláció az A halmazon
- 1_A \rightsquigarrow $A \times A$ — a teljesreláció az A halmazon

Mátrixok

- $K^{n \times n}$ \rightsquigarrow a K test feletti $n \times n$ -es **mátrixok** halmaza
- $\det(A)$ \rightsquigarrow az A négyzetes mátrix **determinánsa**
- A^T \rightsquigarrow az A mátrix **transzponáltja**
- $\mathfrak{V}(\alpha_1, \dots, \alpha_n)$ \rightsquigarrow az $\alpha_1, \dots, \alpha_n$ elemekhez tartozó **Vandermonde-mátrix**
- $V(\alpha_1, \dots, \alpha_n)$ \rightsquigarrow az $\alpha_1, \dots, \alpha_n$ elemekhez tartozó **Vandermonde-determináns**

Csoportok, permutációcsoportok

- $\langle X \rangle$ \rightsquigarrow a G csoport $X \subseteq G$ részhalmaz által generált részcsoportja
- S_H \rightsquigarrow a **szimmetrikus csoport** a H halmazon¹
- A_H \rightsquigarrow az **alternáló csoport** a H halmazon²
- D_n \rightsquigarrow az n -edfokú **diédercsoport**
- Q_8 \rightsquigarrow a **kvaterniócsoport**
- $[G, G]$ \rightsquigarrow a G csoport **kommutátor részcsoportja**
- $\mathbb{A} \hookrightarrow \mathbb{B}$ \rightsquigarrow injektív homomorfizmus \mathbb{A} -ból \mathbb{B} -be.

Polinomok

- $K[x]$ \rightsquigarrow a K test feletti x -határozatlanú **polinomgyűrű**
- f^* \rightsquigarrow az $f \in K[x]$ **polinom fokszáma**
- $K(x)$ \rightsquigarrow az x határozatlan **racionális kifejezéseinek** halmaza
a K test felett, azaz $Q_{K[x]}$
- $D_x(f)$ \rightsquigarrow az f polinom x határozatlan szerinti **formális deriváltja**

Gyűrűk, testek és vektorterek

- $a \sim b$ \rightsquigarrow az a és b elemek **asszociáltak**, azaz $a \mid b$ és $b \mid a$

¹ $S_H = \{\pi: H \rightarrow H \mid \pi \text{ permutáció}\}$, ha H véges ($|H| = n \in \mathbb{N}$), akkor $|S_H| = n!$. Amennyiben $H = \{1, 2, \dots, n\}$, akkor S_H helyett szokás az S_n jelölést használni.

² $A_H = \{\pi: H \rightarrow H \mid \pi \text{ páros permutáció}\}$, ha H véges ($|H| = n \in \mathbb{N}$), akkor $|A_H| = \frac{n!}{2}$. Amennyiben $H = \{1, 2, \dots, n\}$, akkor A_H helyett szokás az A_n jelölést használni.

Q_D \rightsquigarrow a D integritástartomány **hányadosteste**
 $\text{char}(K)$ \rightsquigarrow a K test **karakterisztikája**³
 $\dim_K V$ \rightsquigarrow a K test feletti V vektortér **dimenziója**

Testbővítések

$L : K$ \rightsquigarrow az L test a K test **testbővítése**
 $[L : K]$ \rightsquigarrow az $L : K$ **testbővítés foka**
 $m_{\alpha, K}$ \rightsquigarrow az α elem **minimálpolinomja** a K test felett
 $\text{gr}_K(\alpha)$ \rightsquigarrow az α **elem foka** a K test felett
 $\text{Aut}(K)$ \rightsquigarrow a K test **automorfizmusainak** halmaza
 $\text{Aut}_K(L)$ \rightsquigarrow a L test K fixen hagyó **automorfizmusainak** halmaza,
 azaz az $L : K$ testbővítés Galois-csoportja
 $\text{Gal}(L : K)$ \rightsquigarrow az $L : K$ **testbővítés Galois-csoportja**
 $\text{Gal}_K(f)$ \rightsquigarrow az $f \in K[x]$ **polinom Galois-csoportja**
 \mathfrak{F} \rightsquigarrow a **Frobenius-endomorfizmus**
 L^\times \rightsquigarrow az L **test multiplikatív csoportja**, azaz $L^\times = (L \setminus \{0\}; \cdot)$.

³a K test karakterisztikája 0 vagy prímszám.

12.1 Hálók

1. Legyen $(P; \leq)$ részbenrendezett halmaz. Definiáljuk a $< \subset P \times P$ relációt a következőképpen:

$$x < y \iff x \leq y, x \neq y \quad (x, y \in P).$$

Mutassuk meg, hogy

- (a) nincs olyan $x \in P$, amelyre $x < x$ teljesül;
- (b) ha $x < y$ és $y < z$, akkor $x < z$ ($x, y, z \in P$).

2. A P halmazon legyen $< \subseteq P \times P$ olyan reláció, amelyre teljesül, hogy

- nincs olyan $x \in P$, amelyre $x < x$ teljesül;
- ha $x < y$ és $y < z$, akkor $x < z$ ($x, y, z \in P$).

Definiáljuk a $\leq \subseteq P \times P$ relációt a következőképpen:

$$x \leq y \iff x < y \text{ vagy } x = y \quad (x, y \in P).$$

Mutassuk meg, hogy \leq részbenrendezés a P halmazon.

3. Tetszőleges A halmazra legyen

$$P = \{\alpha \subseteq A \times A \mid \alpha \text{ részbenrendezés } A\text{-n}\}.$$

A P halmazon definiáljuk a \leq relációt a következőképpen:

$$\alpha \leq \beta \iff (\forall a, b \in A)(a \alpha b \implies a \beta b).$$

Igazoljuk, hogy $(P; \leq)$ részbenrendezett halmaz.

4. Mutassuk meg, hogy a $\leq \subseteq A \times A$ reláció részbenrendezés A -n.

- (a) $A = P(X)$, az X halmaz összes részalmazainak halmaza, és $X_0 \leq X_1$ pontosan akkor teljesül, ha $X_0 \subseteq X_1$ ($X_0, X_1 \in P(X)$).
- (b) A az összes az X halmazból \mathbb{R} -be menő leképezések halmaza, és $f \leq g$ pontosan akkor teljesül, ha $f(x) \leq g(x)$ minden $x \in \mathbb{R}$ -re ($f, g \in A$).

- (c) A az emberek halmaza, és $a \leq b$ pontosan akkor teljesül, ha a őse b -nek vagy $a = b$ ($a, b \in A$).
- (d) $A = \mathbb{N}$ és $m \leq n$ pontosan akkor teljesül, ha $m \mid n$ ($m, n \in A$).

5. Legyen $A = \{1, 2, 3\}$. Rajzoljuk fel az összes $(A; \leq)$ részbenrendezett halmaz Hasse-diagramját.

6. Rajzoljuk fel az összes legfeljebb hatelemű hálószerűenrendezett halmaz Hasse-diagramját. Döntsük el, hogy mely \leq részbenrendezésekre lesz az $(A; \leq)$ hálószerűen rendezett halmaz moduláris háló, illetve disztributív háló.

7. Rajzoljuk fel a $(\text{Sub}(S_3); \subseteq)$ részbenrendezett halmaz Hasse-diagramját, ahol S_3 a harmadfokú szimmetrikus csoport.

8. Rajzoljuk fel a $(P(\{0, 1, 2, 3\}); \subseteq)$ részbenrendezett halmaz Hasse-diagramját.

9. Legyen L háló. Mutassuk meg, hogy az $a, b \in L$ elemekre pontosan akkor teljesül, hogy $a = a \wedge b$, ha $b = a \vee b$.

10. Legyen L háló és $a, b, c, d \in L$. Bizonyítsuk be, hogy ha $a \leq b$ és $c \leq d$, akkor $a \wedge c \leq b \wedge d$ és $a \vee c \leq b \vee d$.

11. Legyen L háló és $a, b, c \in L$. Bizonyítsuk be, hogy

- (a) $a \leq c$ és $b \leq c \iff a \vee b \leq c$;
 (b) $c \leq a$ és $c \leq b \iff c \leq a \wedge b \leq c$;
 (c) $a \wedge b \leq a \vee b$.

Vizsgáljuk meg, hogy a (c) esetben mikor van egyenlőség.

12. Mutassuk meg, hogy a hálóműveletek idempotenciája a többi tulajdonság (kommutativitás, asszociativitás és abszorptivitás) következménye.

13. Legyen L háló és $a, b, c, d \in L$. Bizonyítsuk be, hogy

- (a) $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$;
 (b) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$;
 (c) $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$;
 (d) $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee (a \wedge c))$.

14. Legyen $(L; \wedge, \vee)$ háló. Mutassuk meg, hogy ha $(L; \wedge, *)$ is háló, akkor $a * b = a \vee b$ teljesül minden $a, b \in L$ -re.

Legyen L háló. Azt mondjuk, hogy az L háló a és b elemei **összehasonlíthatatlanok**, ha $a \not\leq b$ és $b \not\leq a$ (jelölés: $a \parallel b$).

15. Legyenek \mathbb{L} és \mathbb{L}' hálók, valamint legyen $\varphi: L \rightarrow L'$ rendezéstartó bijektív leképezés. Bizonyítsuk be, hogy ha valahányszor $a \parallel b$ ($a, b \in L$), mindannyiszor $a\varphi \parallel b\varphi$, akkor a φ leképezés izomorfizmus.

16. Mutassuk meg, hogy tetszőleges \mathbb{L} háló esetén ekvivalensek a következők:

- (i) Az \mathbb{L} háló disztributív.
- (ii) Az $a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c)$ egyenlőtlenség teljesül minden $a, b, c \in L$ -re;
- (iii) Az $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ egyenlőség teljesül minden $a, b, c \in L$ -re;
- (iv) Az $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$ egyenlőség teljesül minden $a, b, c \in L$ -re;
- (v) Tetszőleges $a, b, c \in L$ -re, ha $a \wedge c = b \wedge c$ és $a \vee c = b \vee c$, akkor $a = b$.
- (vi) Az \mathbb{L} hálónak nincs az \mathbb{N}_5 vagy \mathbb{M}_3 hálókkal izomorf részhalója.

12.2 Testek és testbővítések

17. Legyen $\mathbb{Z}(\xi) = \{a + b\xi \mid a, b \in \mathbb{Z}\}$, ahol $\xi \in \mathbb{C} \setminus \mathbb{Q}$ egy másodfokú egész együttthatós polinom egyik gyöke (a másik gyököt jelölje ξ'). Mutassuk meg, hogy

- (a) $(\mathbb{Z}(\xi); +, \cdot)$ gyűrű;
- (b) $\mathbb{Z}(\xi)$ elemeinek $a + b\xi$ ($a, b \in \mathbb{Z}$) alakban való előállítása egyértelmű;
- (c) $\mathbb{Z}(\xi) = \mathbb{Z}(\xi')$.

Igazak maradnak-e a fenti állítások, ha $\xi \in \mathbb{C} \setminus \mathbb{Q}$ nem feltétlenül egy másodfokú polinom gyöke?

18. Legyen $\mathbb{Q}(\xi) = \{a + b\xi \mid a, b \in \mathbb{Q}\}$, ahol $\xi \in \mathbb{C} \setminus \mathbb{Q}$ egy másodfokú racionális együttthatós polinom egyik gyöke (a másik gyököt jelölje ξ'). Mutassuk meg, hogy

- (a) $\mathbb{Q}(\xi)$ számtest;
- (b) $\mathbb{Q}(\xi)$ elemeinek $a + b\xi$ ($a, b \in \mathbb{Q}$) alakban való előállítása egyértelmű;
- (c) $\mathbb{Q}(\xi) = \mathbb{Q}(\xi')$.

Igazak maradnak-e a fenti állítások, ha $\xi \in \mathbb{C} \setminus \mathbb{Q}$ nem feltétlenül egy másodfokú polinom gyöke?

19. Határozzuk meg az $L : K$ testbővítések fokát.

- (a) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{7})$;
- (b) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{7})$;
- (c) $K = \mathbb{Q}(\sqrt{19}), L = \mathbb{Q}(\sqrt{19} + \sqrt{73})$;
- (d) $K = \mathbb{Q}(\pi^2), L = \mathbb{Q}(\pi)$;
- (e) $K = \mathbb{Q}, L = \mathbb{R}$;
- (f) $K = \mathbb{R}, L = \mathbb{R}(\sqrt{31} + i\sqrt{41})$;

(d) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{7}, \sqrt{17})$.

Adjunk meg bázist L -ben mint K feletti vektortérben.

20. Legyenek p és q különböző prímszámok. Határozzuk meg a

- (a) $\mathbb{Q}(\sqrt{p}) : \mathbb{Q}$;
 (b) $\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})$;
 (c) $\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}$

testbővítések fokát.

21. Legyenek p_1, \dots, p_n páronként különböző prímszámok. Mutassuk meg, hogy $\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})$. Így

$$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})] = 2$$

és ennek következtében $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.

22. Legyenek K és L olyan számtestek, amelyekre $L : K$ teljesül. Legyenek u és v az L test olyan elemei, amelyekre u^2 és v^2 a K test különböző elemei. Mutassuk meg, hogy $K(u, v) = K(u + v)$.

23. Határozzuk meg az $L : K$ testbővítés közbülső testeit, ha tudjuk, hogy $[L : K]$ prímszám.

24. Tegyük fel, hogy K_1 és K_2 az $L : K$ testbővítés olyan közbülső testeit, amelyekre $L = K(K_1, K_2)$. Mutassuk meg, hogy $[L : K] \leq [K_1 : K] \cdot [K_2 : K]$.

25. Határozzuk meg az $1 + i$, $2 + \sqrt{3}$ és $1 + \sqrt[3]{2} + \sqrt[3]{4}$ komplex számok minimalpolinomját \mathbb{Q} felett.

26. Tegyük fel, hogy az $L : K$ testbővítés véges, és legyen f irreducibilis polinom K felett. Bizonyítsuk be, hogy ha $f^* \nmid [L : K]$, akkor f -nek nincs gyöke L -ben.

27. Mutassuk meg, hogy az $f = x^3 + 3x + 1$ polinom irreducibilis $\mathbb{Q}[x]$ -ben. Legyen $\alpha \in \mathbb{C}$ az f polinom egyik gyöke. Fejezzük ki az α^{-1} és $(1+\alpha)^{-1}$ elemeket az 1 , α és α^2 elemeknek racionális együtthatós lineáris kombinációjaként.

28. Tegyük fel, hogy $L(\alpha) : L$, $L : K$ teljesül és $[K(\alpha) : K]$, $[L : K]$ relatív prímek. Mutassuk meg, hogy $m_{\alpha, L} \in K[x]$.

29. Bizonyítsuk be, hogy ha $[L : K]$ prímszám, akkor az $L : K$ testbővítés egyszerű.

12.3 Algebrai elemek, algebrai bővítések

30. Legyen K megszámlálhatóan végtelen test és $L : K$ algebrai testbővítés. Mutassuk meg, hogy $|L|$ is megszámlálhatóan végtelen. Mutassuk meg, hogy vannak olyan valós számok, amelyek transzcendensek a racionális számok teste felett.

31. Legyen $L : K$ testbővítés, $\alpha \in L$ transzcendens elem K felett és $f \in K[x]$ nem konstans polinom. Mutassuk meg, hogy

- (a) $f(\alpha)$ transzcendens K felett;
- (b) ha $\beta \in L$ -re $f(\beta) = \alpha$ teljesül, akkor β is transzcendens K felett.

Igazak maradnak-e a fenti állítások, ha a „transzcendens” szót mindenütt az „algebrai” szóra cseréljük?

32. Legyenek a és b olyan komplex számok, amely transzcendensek \mathbb{Q} felett. Igaz-e, hogy a^b is transzcendens \mathbb{Q} felett?

33. Tegyük fel, hogy $K(\alpha, \beta) : K$ olyan testbővítést, ahol $\alpha \notin K$ algebrai elem K felett, míg β transzcendens. Mutassuk meg, hogy $K(\alpha, \beta) : K$ nem egyszerű.

34. Tegyük fel, hogy $L : K$ algebrai testbővítés, és legyen $\tau : L \rightarrow L$ olyan injektív homomorfizmus, amelyre $\tau(k) = k$ teljesül tetszőleges $k \in K$ esetén. Mutassuk meg, hogy τ izomorfizmus.

35. Adjunk példát olyan $L : K$ testbővítésre és olyan $\varphi : L \rightarrow L$ injektív testhomomorfizmusra, amely K elemeit fixen hagyja, mégsem szürjektív.

36. Tegyük fel, hogy α transzcendens elem K felett. Mutassuk meg, hogy ha $\beta \in K(\alpha) \setminus K$, akkor $K(\alpha) : K(\beta)$ testbővítés véges és β transzcendens K felett. Ha $\beta = f(\alpha)/g(\alpha)$ ($f, g \in K[x]$ főpolinomok, $g \neq 0$ és $\text{ln.k.o.}(f, g) \sim 1$), akkor $[K(\alpha) : K(\beta)] = \max(f^*, g^*)$.

37. Legyenek K és L olyan számtestek, amelyekre $[L : K] = 2$ teljesül, továbbá legyen

$$S(L) = \{a \in L^\times \mid a \text{ egy } L\text{-beli elem négyzete}\}.$$

Mutassuk meg, hogy $S(L)$ részcsoport L^\times -ban.

38. Legyenek L, L' és K olyan számtestek, amelyekre $[L : K] = [L' : K] = 2$ teljesül. Mutassuk meg, hogy pontosan akkor van olyan $\varphi : L \rightarrow L'$ izomorfizmus, amely fixen hagyja K elemeit, ha $S(L) = S(L')$.

39. Tegyük fel, hogy az $L : K$ testbővítés algebrai. Mutassuk meg, hogy ha az R gyűrűre $K \subseteq R \subseteq L$ teljesül, akkor R test.

40. Legyen D a komplex számtestet tartalmazó integritástartomány. Igazoljuk, hogy ha D véges dimenziós \mathbb{C} -vektortér, akkor $D = \mathbb{C}$.

41. Legyen K test, x határozatlan és $y = \frac{x^3}{x+1} \in K(x)$. Határozzuk meg x minimálpolinomját $K(y)$ felett.

42. Határozzuk meg a $\mathbb{Q}(x)$ test egy olyan K algebrai testbővítését, amelyben az $y^2 - \frac{x^3}{x^2+1} \in \mathbb{Q}(x)[y]$ polinomnak van gyöke.

43. A \mathbb{Q} számtest tetszőleges L véges testbővítésére legyen

$$w_L = |\{\varepsilon \in L \mid \text{van olyan } k \in \mathbb{N}, \text{ hogy } \varepsilon^k = 1\}|.$$

Határozzuk meg a $\max\{w_L \mid [L : \mathbb{Q}] = 4\}$ kifejezés értékét.

44. Legyen L n -edfokú egyszerű testbővítése a K testnek ($n \in \mathbb{N}$). Mutassuk meg, hogy az $L : K$ testbővítés közbülső testeinek száma legfeljebb $2^n - 1$.

45. Igazoljuk, hogy \mathbb{Q} minden egyszerű bővítése megszámlálhatóan végtelen sok elemet tartalmaz.

46. Legyen L a K test testbővítése. Tegyük fel, hogy az $\alpha \in L$ elemre a $K(\alpha) : K$ testbővítés véges. Legyen T_α az alábbi leképezés:

$$T_\alpha : K(\alpha) \rightarrow K(\alpha), \beta \mapsto \alpha\beta.$$

Mutassuk meg, hogy

- (a) T_α lineáris leképezése a $K(\alpha)$ (mint K feletti) vektortérnek;
- (b) $m_{\alpha, K} = \det(xE - T_\alpha)$, ahol E a $(\dim_K K(\alpha)) \times (\dim_K K(\alpha))$ méretű egységmátrix.

12.4 Polinomok irreducibilitása

47. Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ legalább elsőfokú, primitív polinom. Ha létezik olyan p prímszám, amelyre $p \mid a_1, \dots, a_n$, de $p \nmid a_0$ és $p^2 \nmid a_n$, akkor f irreducibilis \mathbb{Z} felett.

48. Mutassuk meg, hogy van olyan $f \in \mathbb{Z}[x]$ irreducibilis főpolinom, hogy az $f \rightarrow_s$ polinomok ($s \in \mathbb{Z}$) egyikére sem alkalmazható a Schönemann–Eisenstein-tétel.

49. Mutassuk meg, hogy tetszőleges p prímszámra az $x^n - p$ polinom irreducibilis $\mathbb{Q}[x]$ -ben.

50. Bizonyítsuk be, hogy $[\mathbb{A} \cap \mathbb{R} : \mathbb{Q}] = \infty$.

51. Legyen $H = \{\sqrt[p]{2} \mid p \text{ prímszám}\}$. Mutassuk meg, hogy ha H' véges részhalmaza H -nak, akkor a H' -beli elemek lineárisan függetlenek \mathbb{Q} felett.

52. Igazoljuk, hogy az

(a) $x^5 - 4x + 2$,

(b) $x^4 - 4x + 2$

polinomok irreducibilisek $\mathbb{Q}(i)$ felett.

53. Legyen p tetszőleges prímszám. Mutassuk meg, hogy az $x^p + x^{p-1} + \dots + x + 1$ polinom irreducibilis \mathbb{Q} felett.

54. Legyen $\vartheta = \frac{2\pi}{7}$. Határozzuk meg a $\cos \vartheta + i \sin \vartheta$ és a $2 \cos \vartheta$ komplex számok minimálpolinomját \mathbb{Q} felett.

55. Ha egy n -edfokú $f \in \mathbb{Z}[x]$ polinom ($n \geq 1$) legalább $2 \left\lfloor \frac{n}{2} \right\rfloor + 1$ egész helyen ± 1 értéket vesz fel, akkor f irreducibilis \mathbb{Z} (s így \mathbb{Q}) felett.

56. Igazoljuk, hogy az

(a) $x^5 + 9x^4 + 30x^3 + 2x + 3$,

(b) $x^n - px + p^2$ (p prímszám, $n > 3$)

polinomok irreducibilisek \mathbb{Q} felett.

57. Legyen n természetes szám. Mutassuk meg, hogy a $\sum_{k=0}^n \frac{x^k}{k!} \in \mathbb{Q}[x]$ polinom irreducibilis.

58. Legyen p prímszám és a olyan egész szám, amely nem osztható p -vel. Mutassuk meg, hogy az $x^p - x + a$ polinom irreducibilis \mathbb{Z} felett.

59. Legyenek a és b tetszőleges egész számok. Ekkor az $f = x^4 + \overline{a}x^2 + \overline{b}^2$ polinom nem irreducibilis \mathbb{Z}_p felett (p tetszőleges prímszám).

60. Legyen $g \in \mathbb{Z}[x]$ tetszőleges k -adfokú polinom ($k \in \mathbb{N}$), és legyenek $d_0 < d_1 < \dots < d_k$ egészek. Igazoljuk, hogy van olyan $i \in \{0, 1, \dots, k\}$, amelyre $|g(d_i)| \geq k!/2^k$.

61. Legyen $f \in \mathbb{Z}[x]$ tetszőleges n -edfokú polinom ($n \in \mathbb{N}$), és legyen $m = \lfloor (n+1)/2 \rfloor$. Tegyük fel, hogy vannak olyan különböző a_1, \dots, a_n egészek, amelyekre $0 < |f(a_i)| < m!/2^m$. Ekkor az f polinom irreducibilis.

62. Legyen $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + \varepsilon p \in \mathbb{Z}[x]$, ahol $\varepsilon \in \{-1, 1\}$ és p prímszám. Ha $p > 1 + |a_1| + \dots + |a_{n-1}|$, akkor f irreducibilis.

63. Az $i\sqrt{3}$ és $1 + i\sqrt{3}$ komplex számok gyökei az $f = x^4 - 2x^3 + 7x^2 - 6x + 12 \in \mathbb{Q}[x]$ polinomnak. Van-e olyan σ automorfizmusa az f polinom \mathbb{Q} feletti felbontási testének, amelyre $\sigma(i\sqrt{3}) = 1 + i\sqrt{3}$ teljesül?

64. Határozzuk meg az alábbi polinomok $L \leq \mathbb{C}$ felbontási testét \mathbb{Q} felett:

(a) $p_1 = x^4 - x^2 + 1$;

- (b) $p_2 = x^6 - 2$;
 (c) $p_3 = x^4 + 2$;
 (d) $p_4 = x^4 + 5x^3 + 10x^2 + 10x + 5$.

Határozzuk meg az $L : \mathbb{Q}$ testbővítés fokát is.

65. Mutassuk meg, hogy az alábbi testbővítések egyszerűek.

- (a) $\mathbb{Q}(\sqrt{5}, \sqrt{10}) : \mathbb{Q}$;
 (b) $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$;
 (c) $\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}$;
 (d) $\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}$;
 (e) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}$.

Határozzuk meg a generáló elem minimálpolinomját is \mathbb{Q} felett.

66. Legyen p tetszőleges prímszám, és legyen $f = x^p - 2 \in \mathbb{Q}[x]$. Bizonyítsuk be, hogy ha L az f polinom felbontási teste \mathbb{Q} felett, akkor $[L : \mathbb{Q}] = p(p-1)$.

67. Legyen $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Mutassuk meg, hogy $\mathbb{Q}(\varepsilon)$ felbontási teste az $x^6 - 1 \in \mathbb{Q}[x]$ polinomnak. Határozzuk meg a $\mathbb{Q}(\varepsilon) : \mathbb{Q}$ testbővítés fokát.

68. Legyenek $L : K$ és $M : L$ testbővítések. Tegyük fel, hogy $\alpha \in M$ algebrai elem K felett. Igaz-e, hogy $[L(\alpha) : L] \mid [K(\alpha) : K]$ mindig teljesül?

69. Határozzuk meg az $f \in \mathbb{Q}[x]$ polinom egy L felbontási testét \mathbb{Q} felett, valamint az $L : \mathbb{Q}$ testbővítés fokát.

- (a) $f = x^4 - 5x^2 + 6$;
 (b) $f = x^4 + 5x^2 + 6$;
 (c) $f = x^4 - 5$.

Van-e olyan $\alpha \in L$ elem, amelyre $L = \mathbb{Q}(\alpha)$ teljesül?

70. Legyen K számtest, és f tetszőleges $K[x]$ -beli n -edfokú polinom ($n \in \mathbb{N}$). Tegyük fel, hogy $\alpha \in K$. Mutassuk meg, hogy

$$f = f(\alpha) + \sum_{k=1}^n \frac{D_x^{(k)}(\alpha)}{k!} (x - \alpha)^k,$$

ahol $D_x^{(1)} = D_x$ és $D_x^{(k)} = D_x \circ D_x^{(k-1)}$ ($k \geq 2$).

71. Tegyük fel, hogy $L : K$ Galois-bővítés, melynek Galois-csoportja G , és legyen $\alpha \in L$. Igazoljuk, hogy $L = K(\alpha)$ pontosan akkor teljesül, ha bármely $\sigma, \sigma' \in G$ -re $\sigma \neq \sigma'$ esetén $\sigma(\alpha) \neq \sigma'(\alpha)$.

72. Határozzuk meg az S_n n -edfokú szimmetrikus csoport tranzitív részcsoportjait, ha $n \in \{3, 4, 5\}$.

73. Legyen K számtest, $f \in K[x]$. Az f polinom valamely L felbontási testében f gyökei legyenek $\alpha_1, \dots, \alpha_n$. Mutassuk meg, hogy

$$\Delta = \eta_n \prod_{j=1}^n D_x(f)(\alpha_j),$$

ahol $\eta_n = \begin{cases} 1, & \text{ha } 4 \mid n \text{ vagy } 4 \mid n-1, \\ -1, & \text{különben.} \end{cases}$

74. Legyen K számtest, $f = x^n + px + q \in K[x]$. Az f polinom valamely L felbontási testében f gyökei legyenek $\alpha_1, \dots, \alpha_n$. Legyen $\lambda_k = \alpha_1^k + \dots + \alpha_n^k$ ($k \in \mathbb{N}$). Mutassuk meg, hogy

$$\lambda_k = \begin{cases} 0, & \text{ha } 1 \leq k \leq n-2 \text{ vagy } n+1 \leq k \leq 2n-3, \\ -(n-1)p, & \text{ha } k = n-1, \\ -nq, & \text{ha } k = n, \\ (n-1)^p, & \text{ha } k = 2n-2, \end{cases}$$

és az f polinom Δ diszkriminánsa:

$$\Delta = \eta_{n+1} n^n q^{n-1} - \eta_n (n-1)^{n-1} p^n,$$

ahol $\eta_n = \begin{cases} 1, & \text{ha } 4 \mid n \text{ vagy } 4 \mid n-1, \\ -1, & \text{különben.} \end{cases}$

75. Legyen $f = x^3 + px + q \in \mathbb{Q}[x]$, α az f polinom gyöke valamely \mathbb{Q} feletti felbontási testében. Legyen $g = 3x^2 - 3\alpha x - p \in \mathbb{Q}(\alpha)[x]$, és legyen β a g polinom gyöke valamely $\mathbb{Q}(\alpha)$ feletti felbontási testében. Mutassuk meg, hogy β gyöke az $27x^6 + 27q^3 - p^3 \in \mathbb{Q}[x]$ polinomnak, valamint $\alpha = \beta - \frac{p}{3\beta}$, ahol

$$\beta = -\frac{q}{2} + \delta \text{ és } \delta^2 = \frac{q^2}{4} + \frac{p^3}{27}.$$

76. Mutassuk meg, hogy S_4 tranzitív részcsoportjai a következők: S_4 , A_4 , V (Viergruppe), D_4 és a 4-rendű ciklikus részcsoportok.

77. Legyen az $x^3 - 7 \in \mathbb{Q}[x]$ polinom felbontási teste \mathbb{Q} felett F . Mutassuk meg, hogy $\text{Gal}_{\mathbb{Q}}(x^3 - 7) \cong S_3$, és határozzuk meg az $F : \mathbb{Q}$ testbővítés közbülső testeit.

78. Határozzuk meg az $x^5 - 2 \in \mathbb{Q}[x]$ polinom G Galois-csoportját \mathbb{Q} felett. Döntsük el, hogy G Abel-csoport-e, illetve feloldható-e.

79. Határozzuk meg az alábbi $\mathbb{Q}[x]$ -beli polinomok Galois-csoportját \mathbb{Q} felett.

(a) $x^4 + 4x + 2$;

(b) $x^4 + 8x - 12$;

(c) $x^4 + 1$;

(d) $x^4 + x^3 + x^2 + x + 1$;

(e) $x^4 - 2$.

Mely polinomok esetén lesz a Galois-csoport Abel-csoport?

80. Ha az $f \in \mathbb{Q}[x]$ polinom Galois-csoportja páratlan rendű, akkor f minden gyöke valós szám.

81. Mutassuk meg, hogy a

$$\tau: \mathbb{R}(x) \rightarrow \mathbb{R}(x), \quad \frac{f(x)}{g(x)} \mapsto \frac{f(-x)}{g(-x)}$$

leképezés 2-rendű és eleme $\text{Aut}_{\mathbb{R}}(\mathbb{R}(x))$ -nek. Határozzuk meg a $\text{Aut}_{\mathbb{R}}(\mathbb{R}(x))$ csoport $\langle \tau \rangle$ részcsoportjának a fixtestét.

82. Legyen $L : K$ véges normális testbővítés. Mutassuk meg, hogy $\alpha \in L$ pontosan akkor primitív elem, ha bármely $\sigma \in \text{Gal}(L : K) \setminus \{\text{id}_L\}$ -re $\sigma(\alpha) \neq \alpha$ teljesül.

83. Legyen $f \in \mathbb{Q}[x]$ olyan n -edfokú irreducibilis polinom, amelynek van valós gyöke, de nem minden gyöke valós. Legyen $M \leq \mathbb{C}$ az f polinom felbontási teste. Mutassuk meg, hogy az $M \cap \mathbb{R} : \mathbb{Q}$ testbővítés legalább n -edfokú és nem normális, valamint $[M : \mathbb{Q}] \geq 2n$.

84. Mutassuk meg, hogy ha a K test véges testbővítése \mathbb{Q} -nak, akkor K csak véges sok egységgyököt tartalmaz.

12.5 Geometriai szerkeszthetőség

85. Tetszőleges n természetes számra legyen

$$P_n = \{ \varepsilon \in \mathbb{C} \mid \varepsilon^n = 1 \text{ és } \varepsilon^k \neq 1 \ (1 \leq k < n) \}.$$

Igazoljuk az alábbi állítások helyességét.

(a) Tetszőleges $\omega \in \mathbb{C}$ -re $\omega \in P_n$ pontosan akkor teljesül, ha $\omega = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$, ahol $\text{ln.k.o.}(k, n) = 1$.

(b) $|P_n| = \varphi(n)$, ahol φ az Euler-féle függvény.

(c) $\prod_{\varepsilon \in P_n} \varepsilon = 1$, ha $n \geq 3$.

(d) $\sum_{\varepsilon \in P_n} \varepsilon = \mu(n)$, ahol μ a Möbius-függvény.

Mely ismert csoporttal izomorf $(P_n; \cdot)$?

86. Tetszőleges n természetes számra legyen

$$\chi_n = \prod_{\varepsilon \in P_n} (x - \varepsilon).$$

A χ_n polinomot n -edik körosztási polinomnak nevezzük.

- (a) Mutassuk meg, hogy $\prod_{d|n} \chi_d = x^n - 1$.
- (b) Igazoljuk, hogy $\chi_n \in \mathbb{Z}[x]$.
- (c) Bizonyítsuk be, hogy tetszőleges $n > 1$ páratlan számra és tetszőleges z komplex számra $\chi_{2n}(z) = \chi_n(-z)$ teljesül.
- (d) Mutassuk meg, hogy tetszőleges p prímszámra a χ_p polinom irreducibilis \mathbb{Q} felett.
- (e) Mutassuk meg, hogy tetszőleges n természetes számra a χ_n polinom irreducibilis \mathbb{Q} felett.

Írjuk fel a χ_n polinomokat $n \in \{1, 2, 3, 4, 5, 6\}$ esetén.

87. Az alábbi szerkesztési feladatok mindegyikében határozzuk meg a szerkesztés K alaptestét, a szerkesztendő szám által generált testbővítés fokát K felett, és döntsük el, hogy a szerkesztés elvégezhető-e.

- (a) Adott az egységszakasz, szerkesztendő $\alpha = \sqrt[5]{2}$.
- (b) Adott az egységszakasz, szerkesztendő $\alpha = \sqrt[4]{2}$.
- (c) Adott az egységszakasz és egy $\sqrt[3]{2}$ hosszú szakasz, szerkesztendő $\alpha = \sqrt[6]{2}$.
- (d) Adott az egységszakasz és egy $\sqrt[3]{2}$ hosszú szakasz, szerkesztendő $\alpha = \sqrt[5]{2}$.
- (e) Adott $(0, 0)$, $(0, 1)$, $(0, \pi)$, az egység sugarú kört kell négyszögesíteni,
- (f) Adott egy szabályos 9-szög, szerkesztendő egy szabályos 18-szög

Amennyiben a szerkesztés elvégezhető végezzük is el.

88. Szerkeszthető-e a háromszög két oldalából, és az egyikhez tartozó szögfelezőből? (A szakaszok hossza adott.)

89. Mutassuk meg, hogy nem szerkeszthető egyenlő szárú háromszög a szárából és a beírt kör sugarából.

90. Mely n egészekre szerkeszthető n -fokos szög.

91. Határozzuk meg $\cos \frac{2\pi}{n}$ fokát \mathbb{Q} felett.

92. Legyen $L : K$ végesfokú normális testbővítés, ahol K tökéletes test. Mutassuk meg, hogy ha egy $f \in K[x]$ polinom irreducibilis K felett, akkor f az L test felett azonos fokszámú irreducibilis polinomok szorzata.

12.6 Automorfizmusok és fixtestek

93. Vannak-e olyan K , L_1 és L_2 testek, hogy L_1 és L_2 testbővítései K -nak, $L_1 \not\cong L_2$ és $\text{Gal}(L_1 : K) \cong \text{Gal}(L_2 : K)$.

94. Tegyük fel, hogy L olyan Galois-bővítése a K testnek, hogy $\text{Gal}(L : K) \cong \mathbb{Z}_2 \times \mathbb{Z}_{12}$. Hány olyan M közbülső teste van az $L : K$ testbővítésnek, amelyekre

- (a) $[L : M] = 4$,
 (b) $[L : M] = 9$,
 (c) $\text{Gal}(L : M) \cong \mathbb{Z}_4$

teljesül?

95. Mutassunk rá egy-egy példával, hogy ha az $L : K$ testbővítés végtelen, akkor $\text{Gal}(L : K)$ lehet véges és végtelen is.

96. Legyen K test, t határozatlan és $L = K(t)$. Tekintsük az $\text{Aut}_K(L)$ csoport alábbi elemeit:

$$\sigma: t \mapsto 1 - t \quad \text{és} \quad \tau: t \mapsto 1/t.$$

Mutassuk meg, hogy $G = \langle \sigma, \tau \rangle \cong S_3$. Határozzuk meg a $\langle \sigma \rangle$ és $\langle \tau \rangle$ részcsoporthat fixtestét. Bizonyítsuk be, hogy a $\langle \sigma\tau \rangle$ részcsoporthat fixteste $K(y)$, ahol $y = \frac{t^3 - 3t + 1}{t(t-1)}$. Igazoljuk, hogy G fixteste $K(z)$, ahol $z = y\sigma(y)$.

97. Legyen $f = x^{2n} - tx^n + 1 \in \mathbb{Q}(t)[x]$, és legyen L az f polinom egy felbontási teste. Határozzuk meg a $L : \mathbb{Q}(t)$ bővítés fokát és Galois-csoportját.

98. Legyen $\alpha = \sqrt[6]{(1 + \sqrt{2})(1 + \sqrt{3})}$. Mutassuk meg, hogy a $\mathbb{Q}(\alpha) : \mathbb{Q}$ bővítés Galois-féle testbővítés, melynek Galois-csoportja izomorf Q_8 -tal.⁴

99. Mutassuk meg, hogy $\mathbb{A} \sqrt{2}$ -t nem tartalmazó résztestei között van maximális, legyen egy ilyen résztest L . Igaz-e, hogy L minden véges testbővítése ciklikus?

100. Legyen $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, i\sqrt{3})$. Határozzuk meg az $L : \mathbb{Q}$ testbővítés G Galois-csoportjának kommutátor részcsoporthoz tartozó közbülső testét (azaz $[G, G]$ fixtestét).

101. Legyen ε primitív kilencedik egységgyök. Határozzuk meg a $\mathbb{Q}(\sqrt[3]{5}, \varepsilon) : \mathbb{Q}$ testbővítés közbülső testeit.

102. Legyen ε primitív n -edik egységgyök ($n \in \mathbb{N}$), $L = \mathbb{Q}(\varepsilon)$. Mutassuk meg, hogy $\{\sigma(\varepsilon) \mid \sigma \in \text{Gal}(L : \mathbb{Q})\}$ pontosan akkor (normális) bázisa $L : \mathbb{Q}$ -nak, ha n négyzetmentes.

103. Legyen $L : K$ Galois-bővítés, melynek Galois-csoportja G . Definiáljuk az $\text{Norm}_{L:K}$ („norma”) és $\text{Trace}_{L:K}$ („nyom”) leképezéseket az alábbi módon:

$$\text{Norm}_{L:K}: L \rightarrow L, \alpha \mapsto \prod_{\sigma \in G} \sigma(\alpha)$$

$$\text{Trace}_{L:K}: L \rightarrow L, \alpha \mapsto \sum_{\sigma \in G} \sigma(\alpha).$$

Bizonyítsuk be a következőket.

⁴ Q_8 a kvaterniócsoport, $Q_8 = (\{\pm 1, \pm i, \pm j, \pm k\}; \cdot)$, ahol a \cdot műveletet a következő összefüggések definiálják:

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j \quad \text{és} \quad ji = -k, \quad ik = -j, \quad kj = -i.$$

A kvaterniócsoport megadása definiáló relációkkal: $Q_8 \cong \langle x, y \mid x^4 = y^4 = xyxy^{-1} = 1 \rangle$.

- (a) Tetszőleges $\alpha \in L$ -re $\text{Norm}_{L:K}(\alpha) \in K$ és $\text{Trace}_{L:K}(\alpha) \in K$.
 (b) Tetszőleges $\alpha, \beta \in L$ -re teljesül, hogy

$$\begin{aligned}\text{Norm}_{L:K}(\alpha \cdot \beta) &= \text{Norm}_{L:K}(\alpha) \cdot \text{Norm}_{L:K}(\beta), \\ \text{Trace}_{L:K}(\alpha + \beta) &= \text{Trace}_{L:K}(\alpha) + \text{Trace}_{L:K}(\beta).\end{aligned}$$

- (c) Legyen $\xi \in L \setminus K$ olyan elem, amelyre $\xi^2 \in K$ teljesül, és legyen $L = K(\xi)$.
 Ekkor $\text{Norm}_{L:K}(a + b\xi) = a^2 - \xi^2 b^2$ és $\text{Trace}_{L:K}(a + b\xi) = 2a$.

Legyen $L \leq \mathbb{C}$ az $x^3 - 2 \in \mathbb{Q}[x]$ polinom felbontási teste. Határozzuk meg a $\text{Norm}_{L:\mathbb{Q}}$ és $\text{Trace}_{L:\mathbb{Q}}$ leképezéseket.

104. Legyen p prímszám, ε primitív p -edik egységgyök és $L = \mathbb{Q}(\varepsilon)$. Igaz-e, hogy bármely $(\mathbb{Q} \leq) M \leq L$ -re $M = \mathbb{Q}(\text{Trace}_{L:M}(\varepsilon))$?

105. Legyen K olyan test, amelynek karakterisztikája nem 2. Legyen $\alpha \in K$ olyan elem, amelyre $\sqrt{\alpha} \notin K$ és $L = K(\sqrt{\alpha})$. Legyenek továbbá b és c olyan K -beli elemek, amelyekre $\sqrt{b + c\sqrt{\alpha}} \notin L$, és legyen $N = L(\sqrt{b + c\sqrt{\alpha}})$. Ekkor

$$\begin{aligned}N : K \text{ Galois-bővítés} &\iff \sqrt{b + c\sqrt{\alpha}} \in L \\ &\iff \text{(a) } \sqrt{b + c\sqrt{\alpha}} \in K \text{ vagy (b) } \sqrt{b + c\sqrt{\alpha}}/\sqrt{\alpha} \in K\end{aligned}$$

Az (a) esetben $\text{Gal}(N : K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, míg a (b) esetben $\text{Gal}(N : K) \cong \mathbb{Z}_4$.

106. Legyen $L = \mathbb{C}(x, y)$ és $K = \mathbb{C}(x^n + y^n, xy)$. Mutassuk meg, hogy az $L : K$ testbővítés Galois-csoportja izomorf D_n -nel.⁵

107. Legyen n tetszőleges természetes szám. Határozzuk meg a

$$\mathbb{C}(\cos x) : \mathbb{C}(\cos nx)$$

testbővítés közbülső testeit.

108. Tegyük fel, hogy a K test karakterisztikája 0. Legyen f egy n -edfokú irreducibilis polinom K felett, melynek valamely L felbontási testében a gyökei: a_1, \dots, a_n . Tetszőleges $J \subseteq \{1, 2, \dots, n\}$ -re legyen $s_J = \sum_{j \in J} a_j$, és tetszőleges $r \in \{1, 2, \dots, n-1\}$ -re legyen $K_r = \mathbb{Q}(\{s_J \mid J \subseteq \{1, 2, \dots, n\} \text{ és } |J| = r\})$, $\tilde{f}_r = \prod_{J \subseteq \{1, 2, \dots, n\}, |J|=r} (x - s_J)$.

- (a) Mutassuk meg, hogy $K_1 = \dots = K_{n-1}$.
 (b) Igazoljuk, hogy $\tilde{f} \in K[x]$.
 (c) Bizonyítsuk be, hogy ha $\text{Gal}_K(f)$ -nak van A_n -nel izomorf részcsoportja, akkor \tilde{f}_r irreducibilis K felett minden r -re ($1 \leq r \leq n-1$).

⁵ A D_n diédercsoport a szabályos n -szög szimmetriacsoportja, $D_n = \langle t, \varphi \rangle$, ahol t egy tetszőleges tükrözése és φ egy $2\pi/n$ -szögű forgatása a szabályos n -szögnek; D_n definiáló relációkkal is megadható: $D_n \cong \langle x, y \mid x^2 = 1, y^n = 1, xy = y^{-1}x \rangle$.

Milyen fokú lesz az \tilde{f}_r polinom?

109. Legyen G az A_n alternáló csoport olyan valódi részcsoportja, amely tartalmaz hetedrendű elemet és $(st)(uv)$ típusú permutációt is. Bizonyítsuk be, hogy $G \cong \text{PSL}(2, 7)$.

110. Legyen $f = x^7 + ax + b \in \mathbb{Q}[x]$ olyan polinom, amely eleget tesz az alábbi feltételeknek:

- f irreducibilis \mathbb{Q} felett,
- $\sqrt{\Delta(f)} \in \mathbb{Q}$,
- f -nek pontosan három darab valós gyöke van,
- \tilde{f}_3 irreducibilis K felett.

Mutassuk meg, hogy $\text{Gal}_{\mathbb{Q}}(f) \cong \text{PSL}(2, 7)$.

111. Mutassuk meg, hogy az $x^7 - 154x + 99$ és $x^7 - 7x + 3$ racionális együtthatós polinomok \mathbb{Q} feletti Galois-csoportja izomorf $\text{PSL}(2, 7)$ -tel.

112. Legyen K olyan test, melynek karakterisztikája nem 2. Tegyük fel, hogy L másodfokú bővítése K -nak, és az $L : K$ testbővítés Galois-csoportja legyen $\{\text{id}_L, \sigma\}$. Legyen α tetszőleges eleme L -nek. Mutassuk meg, hogy az alábbi állítások ekvivalensek.

- (i) Az $L(\sqrt{\alpha}) : K$ testbővítés ciklikus és $\sqrt{\alpha} \notin L$.
- (ii) Van olyan $\beta \in L$ elem, amelyre $\frac{\sigma(\alpha)}{\alpha} = \beta^2$ és $\text{Norm}_{L:K}(\beta) = -1$.

113. Legyen K olyan test, melynek karakterisztikája nem 2. Tegyük fel, hogy L másodfokú bővítése K -nak. Mutassuk meg, hogy az alábbi állítások ekvivalensek.

- (i) Az L test a K test egy negyedfokú ciklikus bővítésének részteste.
- (ii) Van olyan $\alpha \in L$ elem, hogy $\text{Norm}_{L:K}(\alpha) = -1$.

12.7 Véges testek

114. Bizonyítsuk be, hogy ha $f \in \mathbb{Z}_p[x]$ irreducibilis (p prímszám), akkor az f polinom tetszőleges α gyökére $\mathbb{Z}_p(\alpha)$ felbontási teste f -nek.

115. Bizonyítsuk be, hogy ha $f \in \mathbb{Z}_{p^m}[x]$ irreducibilis (p prímszám, $m, n \in \mathbb{N}$), akkor f pontosan akkor osztója az $x^{p^{mn}} - x$ polinomnak, ha $f^* \mid n$.

116. Legyenek p és q prímszámok, $m \in \mathbb{N}$. Bizonyítsuk be, hogy $\frac{p^{mq} - p^m}{q}$ darab q -adfokú \mathbb{Z}_{p^m} feletti irreducibilis polinom van.

117. Legyen q tetszőleges prímszám és n tetszőleges természetes szám. Jelölje $N_{q,n}$ az n -edfokú irreducibilis polinomok számát $\text{GF}(q)[x]$ -ben. Mutassuk meg, hogy

$$N_{q,n} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d,$$

ahol μ a Möbius-féle függvény.

118. Legyen q tetszőleges prímszám és n tetszőleges természetes szám. Mutassuk meg, hogy

$$|\{\vartheta \in \text{GF}(q^n) \mid \text{GF}(q)(\vartheta) = \text{GF}(q^n)\}| = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d,$$

ahol μ a Möbius-féle függvény.

119. Legyen q prímszám, $n \in \mathbb{N}$, $K = \text{GF}(q)$ és $L = \text{GF}(q^n)$. Mutassuk meg, hogy tetszőleges $\alpha \in L$ -re

(a) $\text{Norm}_{L:K}(\alpha) = \alpha^{(q^n-1)/(q-1)}$,

(b) $\text{Trace}_{L:K}(\alpha) = \alpha + \alpha^q + \dots + \alpha^{q^{n-1}}$

teljesül. Bizonyítsuk be, hogy a $\text{Norm}_{L:K}$ és a $\text{Trace}_{L:K}$ leképezések értékkészlete is K .

120. Legyen q prímszám és $\alpha \in \text{GF}(q)^\times$. Igazoljuk, hogy

$$|\{(x, y) \in \text{GF}(q)^2 \mid x^2 - \alpha y^2 = 1\}| = \begin{cases} q-1, & \text{ha } \sqrt{\alpha} \in \text{GF}(q), \\ q+1, & \text{ha } \sqrt{\alpha} \notin \text{GF}(q). \end{cases}$$

121. Bizonyítsuk be a $\left(\frac{2}{p}\right)$ (p páratlan prímszám) Legendre-szimbólum kiszámítására vonatkozó formulát véges testek felhasználásával az alábbi lépéseket követve. Legyen L az $x^8 - 1$ polinom felbontási teste \mathbb{Z}_p felett.

(a) L tartalmaz primitív nyolcadik egységgyököt, azaz olyan $\varepsilon \in L$ elemet, amelyre $\varepsilon^8 = 1$, de $\varepsilon^4 \neq 1$.

(b) $\varepsilon + \varepsilon^{-1}$ négyzetgyöke 2-nek.

(c) 2 akkor és csak akkor áll elő egy \mathbb{Z}_p -beli elem négyzeteként, ha a K test Frobenus-automorfizmusa fixen hagyja az $\varepsilon + \varepsilon^{-1}$ elemet.

(d) $(\varepsilon + \varepsilon^{-1})^p = \varepsilon + \varepsilon^{-1}$ pontosan akkor áll fenn, ha $p \equiv \pm 1 \pmod{8}$.

(e) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

12.8 Régebbi írásbeli feladatok

- 1/1. Határozza meg a $\mathbb{Q}(\sqrt{5}) : \mathbb{Q}$ bővítés fokát.
- 1/2. Mutassa meg, hogy az $\alpha = \sqrt{2} + \sqrt[3]{2}$ valós szám algebrai szám. Határozza meg a minimálpolinomját és fokát \mathbb{Q} felett.
- 1/3. Legyen L az $f = x^4 - x \in \mathbb{Q}[x]$ polinom felbontási teste (\mathbb{Q} felett). Van-e olyan $\alpha \in L$ elem, amelyre $L = \mathbb{Q}(\alpha)$ teljesül?
- 1/4. Határozza meg az $f = x^3 - 6x + 6 \in \mathbb{Q}[x]$ polinom \mathbb{Q} feletti Galois-csoportját.
- 2/1. Határozza meg a $\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})$ bővítés fokát.
- 2/2. Mutassa meg, hogy az $\alpha = 1 - \sqrt[3]{4}$ valós szám algebrai szám. Határozza meg a minimálpolinomját és fokát \mathbb{Q} felett.
- 2/3. Legyen L az $f = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ polinom felbontási teste (\mathbb{Q} felett). Van-e olyan $\alpha \in L$ elem, amelyre $L = \mathbb{Q}(\alpha)$ teljesül?
- 2/4. Határozza meg az $f = x^3 - 3x^2 + 6x + 3 \in \mathbb{Q}[x]$ polinom \mathbb{Q} feletti Galois-csoportját.
- 3/1. Határozza meg a $\mathbb{Q}(\sqrt{5} + \sqrt{2}) : \mathbb{Q}(\sqrt{5} - \sqrt{2})$ bővítés fokát.
- 3/2. Mutassa meg, hogy az $\alpha = 3 - \sqrt[4]{3}$ valós szám algebrai szám. Határozza meg α fokát \mathbb{Q} felett.
- 3/3. Legyen L az $f = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ polinom felbontási teste (\mathbb{Q} felett). Van-e olyan $\alpha \in L$ elem, amelyre $L = \mathbb{Q}(\alpha)$ teljesül?
- 3/4. Határozza meg az $f = x^3 - 3x^2 + 1 \in \mathbb{Q}[x]$ polinom \mathbb{Q} feletti Galois-csoportját.
- 4/1. Mutassa meg, hogy $\mathbb{Q}(\sqrt{21}) \subseteq \mathbb{Q}(\sqrt{3} + \sqrt{7})$ és határozza meg a $\mathbb{Q}(\sqrt{3} + \sqrt{7}) : \mathbb{Q}(\sqrt{21})$ bővítés fokát.
- 4/2. Mutassa meg, hogy az $\alpha = 1 - \sqrt[4]{7}$ valós szám algebrai szám. Határozza meg α fokát \mathbb{Q} felett.
- 4/3. Legyen L az $f = x^4 - 10x^2 + 21 \in \mathbb{Q}[x]$ polinom felbontási teste (\mathbb{Q} felett). Van-e olyan $\alpha \in L$ elem, amelyre $L = \mathbb{Q}(\alpha)$ teljesül?
- 4/4. Határozza meg az $f = 8x^3 - 12x^2 + 1 \in \mathbb{Q}[x]$ polinom \mathbb{Q} feletti Galois-csoportját.

Az $f = a_3x^3 + a_2x^2 + a_1x + a_0$ polinom diszkriminánsa:

$$-27a_0^2a_3^2 + 18a_0a_1a_2a_3 + a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3.$$

IRODALOMJEGYZÉK

- [1] **Bálintné Szendrei Mária, Czédli Gábor, Szendrei Ágnes**, *Absztrakt algebrai feladatok*, POLYGON (Szeged, 2005).
- [2] **Csákány Béla**, *Algebra*, Nemzeti Tankönyvkiadó (1995).
- [3] **Czédli Gábor, Szendrei Ágnes**, *Geometriai szerkeszthetőség*, POLYGON (Szeged, 1997).
- [4] **Kiss Emil**, *Bevezetés az algebra*, TYPOTEX (Budapest, 2007).