1. Polinomok felbontási teste

Tétel. Legyen K test, $f \in (K[t])[x]$. Ekkor f pontosan akkor irreducibilis $K[t]$ felett, ha irreducibilis $K(t)$ felett.

Tétel. Legyen K test, $f \in (K[t])[x]$ és $s \in K[t]$. Tegyük fel, hogy az $a_0, a_1, \ldots, a_d \in K[t]$ elemekre

$$f = a_d(x-s)^d + \cdots + a_1(x-s) + a_0$$

teljesül, ahol $d = f^*$. Ha van olyan $p \in K[t]$ irreducibilis elem, amelyre

(1) $p \mid a_0, \ldots, a_{d-1}$,
(2) $p \nmid a_d$,
(3) $p^2 \nmid a_0$,

akkor f irreducibilis $(K(t))[x]$-ben, így $(K[t])[x]$-ben is.

1.1. 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 $\sigma(i\sqrt{3}) = 1+i\sqrt{3}$ és $\sigma(a) = a$ $(a \in \mathbb{Q})$ teljesül?

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

1.3. Mutassa meg, hogy az $f = x^3 - x + 1 \in \mathbb{Z}_3[x]$ polinom irrducibilis. Határozza meg az f polinom egy felbontási testét és írja fel a szorzás műveletének művelettáblázatát.

1.4. Határozzuk meg az $f \in \mathbb{Q}[x]$ polinom $L \leqslant \mathbb{C}$ felbontási testét $\mathbb{Q}$ felett:

(a) $f = x^4 - x^2 + 1$;
(b) $f = x^6 - 2$;
(c) $f = x^4 + 2$;
(d) $f = x^4 + 5x^3 + 10x^2 + 10x + 5$;
(e) $f = x^4 - 5x^2 + 6$;
(f) $f = x^4 + 5x^2 + 6$.

Határozza meg az $[L : \mathbb{Q}]$ testbővítés fokát és adjon meg primitív elemet az $L : \mathbb{Q}$ testbővítésben.

1.5. Legyen $n \geqslant 1$ tetszőleges egész szám. Adjon meg olyan n-edfokú $f \in \mathbb{Q}[x]$ polinomot, amelyre $[F : \mathbb{Q}] = n!$ teljesül, ahol F az f polinom felbontási teste.

Baker 3.5

1.6. Mutassa 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) $\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}$.

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

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

1.8. Legyen p prímszám és a olyan racionális szám, amelyre $a = \xi^p$ teljesül valamely $\xi \in \mathbb{C} \setminus \mathbb{Q}$-ra. Bizonyítsa be a következőket.

(a) A $\Phi_p = x^{p-1} + \cdots + x + 1$ polinom irreducibilis $\mathbb{Q}(\xi)$ felett.
(b) Az $x^p - a \in \mathbb{Q}[x]$ polinom F felbontási testére $[F : \mathbb{Q}] = p(p-1)$ teljesül.

1.9. 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?

2. Algebrai lezárt

2.1. Legyen U nemüres halmaz, valamint $V \subseteq W \subseteq U$. Igazolja, hogy ha $f\colon V \to P(U)$ injektív leképezés, akkor van olyan $g\colon W \to P(U)$ leképezés, amelyre $g|_V = f$.

2.2. Legyen K test, $U = K[x] \times \mathbb{N}$, valamint legyenek (i, K, L) és (j, L, M) algebrai testbővítések. Bizonyítsa be a következőket.

(a) Létezik $L \to U$ injektív leképezés.
(b) Ha $f\colon L \to P(U)$ injektív leképezés, akkor van olyan injektív $g\colon M \to P(U)$ leképezés, amelyre $f = gj$.

2.3. Legyen K test és $U = K[x] \times \mathbb{N}$. Bizonyítsa be a következőket.

(a) A $j\colon K \to P(U)$, $\alpha \mapsto \{(x - \alpha, 1)\}$ injektív leképezés, és a $j(K)$ halmazon definiálhatunk úgy egy teststruktúrát, hogy a $j\colon K \to j(K)$ leképezés izomorfizmus legyen.
(b) Legyen $\mathcal{F}$ azon $(S; +, \cdot)$ testek halmaza, amelykre teljesül, hogy $j(K) \subseteq S \subseteq P(U)$ és a $(i_{j(K)}, j(K), S)$ testbővítés algebrai. Az $\mathcal{F}$ halmazon definiáljuk a $\leqslant$ részbenrendezést az alábbi módon:

$$(S_1; +_1, \cdot_1) \leqslant (S_2; +_2, \cdot_2) \iff S_1 \subseteq S_2 \text{ és } (i_{S_1}, S_1, S_2) \text{ testbővítés.}$$

Mutassa meg, hogy az $(\mathcal{F}; \leqslant)$ részbenrendezett halmazban van maximális elem.
(c) Ha $(S; +, \cdot)$ maximális elem $(\mathcal{F}; \leqslant)$-ban, akkor (j, K, S) algebrai lezártja K-nak.

2.4. Mi a $\mathbb{Q}$ test algebrai lezártja $\mathbb{C}$-ben?

2.5. Bizonyítsa be, hogy minden algebrailag zárt test végtelen.

2.6. Tegyük fel, hogy α transzcendens elem K felett. Mutassa meg, hogy $K(\alpha)$ nem algebrailag zárt.

3. Normális bővítések

Azt mondjuk, hogy az $N : L$ testbővítés *normális lezártja* $L : K$ algebrai testbővítésnek, ha $N : K$ normális testbővítés és valahányszor az $N : L$ testbővítés M közbülső testére $M : K$ normális, mindannyiszor $M = N$ teljesül.

3.1. Mutassa meg, hogy minden algebrai testbővítésnek van normális lezártja.

3.2. Ha $L : K$ algebrai testbővítés, akkor a testbővítés közbülső testei között van egy legnagyobb M test, amelyre $M : K$ normális.

3.3. Legyenek M_1 és M_2 az $L : K$ testbővítés közbülső testei. Igazolja, hogy ha $M_1 : K$ és $M_2 : K$ normális testbővítések, akkor a $K(M_1 \cup M_2) : K$ és $(M_1 \cap M_2) : K$ testbővítések is normálisak.

3.4. Tegyük fel, hogy $N : L$ és $N' : L$ is normális lezártja az $L : K$ testbővítésnek. Mutassa meg, hogy van olyan $\nu\colon N \to N'$ izomorfizmus, amely L elemeit fixen hagyja.

3.5. Legyen $L : K$ véges normális testbővítés, $f \in K[x]$ irreducibilis polinom. Bizonyítsa be, hogy ha a $g, h \in L[x]$ irreducibilis főpolinomok osztói f-nel $L[x]$-ben, akkor van olyan $\sigma \in \mathrm{Aut}_K(L)$, hogy $\sigma_g = h$.

3.6. Mutassa meg, hogy tetszőleges $L : K$ algebrai testbővítésre ekvivalensek az alábbiak.

(1) Az $L : K$ testbővítés normális.
(2) Ha $j\colon L \to \overline{L}$ injektív homomorfizmus, amely fixen hagyja K elemeit, akkor $j(L) \subseteq L$.
(3) Ha $j\colon L \to \overline{L}$ injektív homomorfizmus, amely fixen hagyja K elemeit, akkor $j(L) = L$.

3.7. Tegyük fel, hogy az $L : K$ testbővítés véges és normális, és legyen $K \leqslant M \leqslant L$. Ekkor a következők ekvivalensek:

(1) az $M : K$ bővítés normális;
(2) ha $\sigma \in \mathrm{Aut}_K(L)$, akkor $\sigma(M) \subseteq M$;
(3) ha $\sigma \in \mathrm{Aut}_K(L)$, akkor $\sigma(M) = M$.

4. Szeparábilitás

4.1. Legyen $L : K$ véges testbővítés, melynek normális lezártja $L' : L$. Mutassa meg, hogy $L : K$ pontosan akkor szeparábilis, ha pontosan $[L : K]$ darab K elemeit fixen hagyó $L \to L'$ injektív homomorfizmus van.

4.2. Legyen p prímszám. Az $x^{p-1} - \overline{1} \in \mathbb{Z}_p[x]$ polinom szorzattá bontásával igazoljuk a Wilson-tételt.

4.3. Legyen p prímszám. Igazolja a következőket.

(a) Ha $p \equiv 1 \pmod 4$, akkor van olyan $k \in \mathbb{Z}$, amelyre $p \mid k^2 + 1$, p nem prímelem $\mathbb{Z}[i]$-ben és vannak olyan u, v egészek, hogy $u^2 + v^2 = p$.

(b) Ha $p \equiv 3 \pmod 4$, akkor p prímelem $\mathbb{Z}[i]$-ben.

4.4. Legyen K test, melynek karakterisztikája nem 0. Mutassa meg, hogy K pontosan akkor tökéletes, ha a Frobenius-leképezés automorfizmusa K-nak.

4.5. Mutassa meg, hogy a K test pontosan akkor tökéletes, ha minden véges testbővítése szeprábilis.

4.6. Legyen K test, melynek karakterisztikája $p > 0$ és $f \in K[x]$ irreducibilis polinom. Bizonyítsa be, hogy $f = g(x^{p^n})$ teljesül valamely $n \in \mathbb{N}_0$-ra és valamely $g \in K[x]$ irreducibilis és szeparábilis polinomra.

Azt mondjuk, hogy az $L : K$ testbővítés *teljesen inszeparábilis* algebrai testbővítés, ha $L \setminus K$ minden eleme inszeparábilis.

4.7. Legyen K test, melynek karakterisztikája $p > 0$, és legyen $L : K$ teljesen inszeparábilis algebrai testbővítés. Mutassa meg, hogy tetszőleges $\beta \in L$ elemre $m_{\beta,K} = x^{p^n} - \alpha$ ($n \in \mathbb{N}_0$, $\alpha \in K$).

4.8. Legyen K test, melynek karakterisztikája $p > 0$, f irreducibilis polinom, melynek felbontási teste K felett L. Ekkor van olyan $n \in \mathbb{N}_0$, hogy f valamennyi gyökének multiplicitása p^n.

5. Automorfizmusok és fixtestek

5.1. Legyen K test. Igazolja, hogy

$$\mathrm{Aut}_K(K[x]) \cong \mathrm{Aff}_1(K),$$

ahol $\mathrm{Aff}_1(K) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in K,\ a \neq 0 \right\}$.

5.2. Legyen K test. Igazolja, hogy

$$\mathrm{Aut}_K(K(x)) \cong \mathrm{PGL}_2(K),$$

ahol $\mathrm{PGL}_2(K)$ a $\mathrm{GL}_2(K)$ csoport (azaz a K *feletti általános lineáris csoport*) $\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in K,\ a \neq 0 \right\}$ normális részcsoportja szerint vett faktorcsoportja.

5.3. Igazolja, hogy $\mathrm{Aut}(\mathbb{R}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \mathrm{id}_{\mathbb{R}}$.

5.4. Igazolja, hogy $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \mathfrak{K}\}$, ahol $\mathfrak{K}\colon \mathbb{C} \to \mathbb{C},\ z \mapsto \overline{z}$. Igaz-e, hogy $\mathrm{Aut}(\mathbb{C}) = \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$?

5.5. Tetszőleges n természetes számra legyen $E_n = \mathbb{Q}(\sqrt[n]{2})$. Igazolja, hogy

(a) $|\mathrm{Aut}_{\mathbb{Q}}(E_n)| = ((-1)^n + 3)/2$;

(b) ha $E = \bigcup_{n \in \mathbb{N}} E_n$, akkor $\mathrm{Aut}_{\mathbb{Q}}(E) = \{\mathrm{id}_E\}$.

5.6. Legyen $L : K$ Galois-bővítés, $\alpha \in L$. Igazolja, hogy $L = K(\alpha)$ pontosan akkor teljesül, ha valahányszor $\sigma, \sigma' \in \mathrm{Gal}(L : K)$ és $\sigma \neq \sigma'$, mindannyiszor $\sigma(\alpha) \neq \sigma'(\alpha)$.

5.7. Tetszőleges $L : K$ testbővítésre $\mathrm{Gal}(L : K)$ lineárisan független részhalmaza a K feletti $\mathrm{End}_K(L)$ vektortérnek.

5.8. Legyen $L : K$ Galois-bővítés, melynek Galois-csoportja $G = \{\sigma_1, \ldots, \sigma_n\}$. Bizonyítsa be, hogy $\beta_1, \ldots, \beta_n$ pontosan akkor bázis L-ben (K felett), ha $\det(\sigma_i(\beta_j))_{n\times n} \neq 0$.

5.9. Legyen L véges testbővítése a 0 karakterisztikájú K testnek, és tegyük fel, hogy $\alpha_1, \ldots, \alpha_n$ bázisa L-nek K felett. Legyen $H \leqslant \mathrm{Gal}(L : K)$, $\beta_j = \sum_{\sigma\in H} \sigma(\alpha_j)$ $(1 \leqslant j \leqslant n)$. Igazolja, hogy $\varphi(H) = K(\beta_1, \ldots, \beta_n)$.

5.10. Legyen r teszőleges természetes szám és

$$f_r = (x^2 + 4)x \prod_{j=1}^{r} (x^2 - 4j^2).$$

Mutassa meg, hogy tetszőleges k egész számra teljesül, hogy $|f_r(2k+1)| \geqslant 5$. Igazolja, hogy a $g_r = f_r - 2 \in \mathbb{Q}[x]$ polinom irreducibilis. Határozza meg a g polinom Galois-csoportját $\mathbb{Q}$ felett, ha tudjuk, hogy $2r + 3$ prímszám.

5.11. Legyen G véges csoport. Mutassa meg, hogy van olyan $L : K$ testbővítés, melynek Galois-csoportja izomorf G-vel.

5.12. Legyenek K_1 és K_2 az L test olyan résztestei, amelyre $L : K_1$ és $L : K_2$ is Galois-bővítések. Bizonyítsa be, hogy $L : (K_1 \cap K_2)$ pontosan akkor Galois-bővítés, ha $\langle \mathrm{Gal}(L : K_1) \cup \mathrm{Gal}(L : K_2)\rangle$ véges; amennyiben ez utóbbi teljesül, akkor

$$\mathrm{Gal}(L : (K_1 \cap K_2)) \cong \langle \mathrm{Gal}(L : K_1) \cup \mathrm{Gal}(L : K_2)\rangle .$$

5.13. Kaplansky-tétel. Legyen $f = x^4 + ax^2 + b \in \mathbb{Q}[x]$ irreducibilis polinom, valamint legyen $\mathcal{N}_\mathbb{Q} = \{r^2 \mid r \in \mathbb{Q}\}$.

(a) Ha $b \in \mathcal{N}_\mathbb{Q}$, akkor $\mathrm{Gal}_\mathbb{Q}(f) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
(b) Ha $b(a^2 - 4b) \in \mathcal{N}_\mathbb{Q}$, akkor $\mathrm{Gal}_\mathbb{Q}(f) \cong \mathbb{Z}_4$.
(c) Ha $b, b(a^2 - 4b) \notin \mathcal{N}_\mathbb{Q}$, akkor $\mathrm{Gal}_\mathbb{Q}(f) \cong D_8$.

5.14. Vannak-e olyan K, L_1 és L_2 testek, hogy L_1 és L_2 testbővítései K-nak, $L_1 \ncong L_2$ és $\mathrm{Gal}(L_1 : K) \cong \mathrm{Gal}(L_2 : K)$.

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

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

teljesül?

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

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

$$\sigma\colon t \mapsto 1 - t \qquad \text{és} \qquad \tau\colon t \mapsto 1/t.$$

Mutassa meg, hogy $G = \langle \sigma, \tau\rangle \cong S_3$. Határozza meg a $\langle\sigma\rangle$ és $\langle\tau\rangle$ részcsoportok fixtestét. Bizonyítsa be, hogy a $\langle\sigma\tau\rangle$ részcsoport fixteste $K(y)$, ahol $y = \dfrac{t^3 - 3t + 1}{t(t-1)}$. Igazolja, hogy G fixteste $K(z)$, ahol $z = y\sigma(y)$.

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

5.19. Legyen $\alpha = \sqrt[6]{(1 + \sqrt{2})(1 + \sqrt{3})}$. Mutassa meg, hogy a $\mathbb{Q}(\alpha) : \mathbb{Q}$ testbővítés Galois-bővítés.

5.20. Legyen $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ és $E = M(\alpha)$, ahol $\alpha = \sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}$. Mutassa meg, hogy

(a) $M : \mathbb{Q}$ Galois-bővítés és $\mathrm{Gal}(M : \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$;

(b) $E : \mathbb{Q}$ Galois-bővítés és $\mathrm{Gal}(E : \mathbb{Q}) \cong Q_8$.[1]

5.21. Mutassa 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?

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

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

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

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

$$\mathrm{Norm}_{L:K} \colon L \to L,\ \alpha \mapsto \prod_{\sigma \in G} \sigma(\alpha)$$
$$\mathrm{Trace}_{L:K} \colon L \to L,\ \alpha \mapsto \sum_{\sigma \in G} \sigma(\alpha).$$

Bizonyítsa be a következőket.

(a) Tetszőleges $\alpha \in L$-re $\mathrm{Norm}_{L:K}(\alpha) \in K$ és $\mathrm{Trace}_{L:K}(\alpha) \in K$.

(b) Tetszőleges $\alpha, \beta \in L$-re teljesül, hogy

$$\mathrm{Norm}_{L:K}(\alpha \cdot \beta) = \mathrm{Norm}_{L:K}(\alpha) \cdot \mathrm{Norm}_{L:K}(\beta),$$
$$\mathrm{Trace}_{L:K}(\alpha + \beta) = \mathrm{Trace}_{L:K}(\alpha) + \mathrm{Trace}_{L:K}(\beta).$$

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

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

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

5.27. 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 $\sqrt{b + c\sqrt{a}} \notin L$, és legyen $N = L(\sqrt{b + c\sqrt{a}})$. Ekkor

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

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

5.28. Legyen $L = \mathbb{C}(x, y)$ és $K = \mathbb{C}(x^n + y^n, xy)$. Mutassa meg, hogy az $L : K$ testbővítés Galois-csoportja izomorf D_n-nel.[2]

---

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

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

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

[2] 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: $D_n \cong \langle x, y \mid x^2 = 1,\ y^n = 1,\ xy = y^{-1}x \rangle$.

5.29. Legyen n tetszőleges természetes szám. Határozza meg a

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

testbővítés közbülső testeit.

5.30. Tegyük fel, hogy a K test karakterisztikája 0. Legyen f egy n-edfokú irreduciblis 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 $K_r = \mathbb{Q}(\{s_J \mid J \subseteq \{1, 2, \dots, n\} \text{ és } |J| = r\})$, $\widetilde{f_r} = \prod_{J \subseteq \{1,2,\dots,n\},\ |J|=r} (x - s_J)$.

(a) Mutassa meg, hogy $K_1 = \cdots = K_{n-1}$.

(b) Igazolja, hogy $\widetilde{f} \in K[x]$.

(c) Bizonyítsa be, hogy ha $\mathrm{Gal}_K(f)$-nak van A_n-nel izomorf részcsoportja, akkor $\widetilde{f_r}$ irreducibilis K felett minden r-re ($1 \leqslant r \leqslant n-1$).

Milyen fokú lesz az $\widetilde{f_r}$ polinom?

5.31. Legyen G az A_n alternáló csoport olyan valódi részcsoportja, amely tartalmaz hetedrendű elemet és $(s\,t)(u\,v)$ típusú permutációt is. Bizonyítsa be, hogy $G \cong \mathrm{PSL}(2, 7)$.

5.32. 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,
- $\widetilde{f_3}$ irreducibilis K felett.

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

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

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

(1) Az $L(\sqrt{a}) : K$ testbővítés ciklikus és $\sqrt{\alpha} \notin L$.

(2) Van olyan $\beta \in L$ elem, amelyre $\dfrac{\sigma(\alpha)}{\alpha} = \beta^2$ és $\mathrm{Norm}_{L:K}(\beta) = -1$.

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

(1) Az L test a K test egy negyedfokú ciklikus bővítésének részteste.

(2) Van olyan $\alpha \in L$ elem, hogy $\mathrm{Norm}_{L:K}(\alpha) = -1$.

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

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

5.38. 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.

5.39. 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?

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

5.41. Mutassuk meg, hogy a

$$\tau\colon \mathbb{R}(x) \to \mathbb{R}(x),\ \frac{f(x)}{g(x)} \mapsto \frac{f(-x)}{g(-x)}$$

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

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

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

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

6. Véges testek

6.1. Legyen K egy q-elemű test, p prímszám. Ekkor a p-edfokú irreducibilis főpolinomok száma $K[x]$-ben $(q^p - q)/p$.

6.2. Bontsa irreducibilis polinomok szorzatára az $x^{p^p} - x \in \mathbb{Z}_p[x]$ polinomot.

6.3. Igazolja, hogy tetszőleges $a, b \in \mathbb{N}$-re $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{\text{ln.k.o.}(a,b)} \times \mathbb{Z}_{\text{lk.k.t.}(a,b)}$.

6.4. Minden véges Abel-csoport izomorf prímhatványrendű ciklikus részcsoportjainak direkt szorzatával.

6.5. Legyen G Abel csoport, $T = \{g \in G \mid o_G(g) < \infty\}$. Mutassa meg, hogy $T \triangleleft G$ és a G/T csoport egységelemtől különböző elemeinek rendje végtelen.

6.6. Mutassa meg, hogy ha a G csoport végesen generált Abel-csoport egységelemtől különböző elemeinek rendje végtelen, akkor $G \cong \mathbb{Z}^s$ teljesül valamely $s \in \mathbb{N}$-re. Hogyan határozhatjuk meg az s egészet?

6.7. Mutassa meg, hogy ha a G csoport végesen generált Abel-csoport, akkor $G \cong \mathbb{Z}^s \times T$ valamely $s \in \mathbb{N}$-re és T véges csoportra.

6.8. Legyenek $p < q$ különböző prímszámok. Bizonyítsa be, hogy ha $p \nmid q-1$, akkor van olyan $L : \mathbb{Z}_q$ testbővítés, amely felbontási teste az $\{x^p - a \mid a \in \mathbb{Z}_q\}$ polinomhalmaznak.

6.9. Legyen p prímszám, $J = \mathbb{Z}_p(\alpha)$ és $K = J(\beta)$, ahol α transzcendens $\mathbb{Z}_p$ felett és β transzcendens J felett. Legyen L az $(x^p - \alpha)(x^p - \beta) \in K[x]$ polinom felbontási teste. Igazolja az alábbi állításokat.

(a) Az $L : K$ testbővítés foka p^2.
(b) Ha $\gamma \in L$, akkor $\gamma^p \in K$.
(c) Az $L : K$ testbővítés nem egyszerű.

Határozza meg az $L : K$ testbővítés közbülső testeit $p = 2$ esetén.

6.10. Ha $L : K$ véges, szeparábilis és $M : L$ egyszerű testbővítés, akkor az $M : K$ testbővítés egyszerű.

6.11. Bizonyítsa 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.

6.12. Legyenek p és q prímszámok, $m \in \mathbb{N}$. Bizonyítsa be, hogy $\dfrac{p^{mq} - p^m}{q}$ darab q-adfokú $\mathbb{F}_{p^m}$ feletti irreducibilis polinom van.

6.13. Legyen q tetszőleges prímhatvány és n tetszőleges természetes szám. Jelölje $N_{q,n}$ az n-edfokú irreducibilis polinomok számát $\mathbb{F}_q[x]$-ben. Mutassa 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.

6.14. Legyen q tetszőleges prímhatvány és n tetszőleges természetes szám. Mutassa meg, hogy

$$|\{\vartheta \in \mathbb{F}_{q^n} \mid \mathbb{F}_q(\vartheta) = \mathbb{F}_{q^n}\}| = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d,$$

ahol μ a Möbius-féle függvény.

6.15. Legyen q prímhatvány, $n \in \mathbb{N}$, $K = \mathbb{F}_q$ és $L = \mathbb{F}_{q^n}$. Mutassa meg, hogy tetszőleges $\alpha \in L$-re

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

(b) $\mathrm{Tarce}_{L:K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$

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

6.16. Legyen q prímhatvány és $\alpha \in \mathbb{F}_q^\times$. Igazolja, hogy

$$|\left\{(x,y) \in \mathbb{F}_q^2 \mid x^2 - \alpha y^2 = 1\right\}| = \begin{cases} q-1, & \text{ha } \alpha \text{ van gyöke } \mathbb{F}_q\text{-ban,} \\ q+1, & \text{ha } \alpha\text{-nak nincs gyöke } \mathbb{F}_q\text{-ban.} \end{cases}$$

6.17. Bizonyítsa be a $\left(\dfrac{2}{p}\right)$ (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) $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

6.18. Legyen $w \in \mathbb{F}_{p^d}^\times$ primitív egységgyök. Mutassa meg, hogy ha $\ell < d$, akkor $w \notin \mathbb{F}_{p^\ell}^\times$, valamint $\mathrm{gr}_{\mathbb{F}_p}(w) = d$. Igazolja, hogy $d \mid \varphi(p^d - 1)$.

6.19. Legyen q páratlan prímhatvány, $\mathcal{N}_q = \left\{u^2 \mid u \in \mathbb{F}_q\right\}$ és tetszőleges $t \in \mathbb{F}_q$-ra $t - \mathcal{N}_q = \left\{t - u^2 \mid u \in \mathbb{F}_q\right\}$. Mutassa meg, hogy $|\mathcal{N}_q| = |t - \mathcal{N}_q| = (q+1)/2$. Igazolja, hogy $\mathbb{F}_q \subseteq \mathcal{N}_q + \mathcal{N}_q$.

7. A diszkrimináns

7.1. Legyen K test, melynek karakterisztikája 0, és legyen f tetszőleges $K[x]$-beli n-edfokú polinom ($n \in \mathbb{N}$). Tegyük fel, hogy $\alpha \in K$. Mutassuk meg, hogy

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

7.2. Legyenek az $f \in K[x]$ polinom gyökei $\alpha_1, \ldots, \alpha_n$ az f polinom valamely felbontási testében. Mutassa meg, hogy

$$\Delta(f) = (-1)^{\binom{n}{2}} \prod_{k=1}^{n} f'(\alpha_k).$$

7.3. Legyenek az $f = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ polinom gyökei $\alpha_1, \ldots, \alpha_n$ az f polinom valamely L felbontási testében. Igazolja az alábbiakat.

(a) Tetszőleges $1 \leqslant i \leqslant n$-re $f = (x-\alpha_i)g_i$, ahol

$$g_i = \sum_{k=1}^{n} a_k \sum_{l=0}^{k} \alpha_i^l x^{k-l}.$$

(b) $f' = g_1 + \cdots + g_n$.

(c) Ha $\lambda_k = \alpha_1^k + \cdots + \alpha_n^k$ ($k \in \mathbb{N}$), akkor

$$(n-k)a_k + \sum_{j=1}^{n-k} a_{k+j}\lambda_j = 0 \qquad (0 \leqslant k \leqslant n-1),$$
$$\sum_{j=0}^{n} a_j \lambda_{k+j} = 0 \qquad (k \in \mathbb{N}).$$

Ezek az ún. *Newton-azonosságok*.

7.4. Tegyük fel, hogy $f = x^n + px + q \in K[x]$ (K test). Mutassuk meg, hogy

$$\lambda_j = \begin{cases} 0, & \text{ha } 1 \leqslant j \leqslant n-2 \text{ vagy } n+1 \leqslant j \leqslant 2n-3, \\ -(n-1)p, & \text{ha } j = n-1, \\ -nq, & \text{ha } j = n, \\ (n-1)p^2, & \text{ha } j = 2n-2. \end{cases}$$

Igazolja, hogy $\Delta(f) = (-1)^{\binom{n+1}{2}} n^n q^{n-1} - (-1)^{\binom{n}{2}} (n-1)^{n-1} p^n$.

8. Geometriai szerkeszthetőség

8.1. Tetszőleges n természetes számra legyen

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

Igazolja 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 k és n relatív prímek.

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

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

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

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

8.2. Tetszőleges n természetes számra legyen

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

A Φ_n polinomot n-*edik körosztási polinomnak* nevezzük.

(a) Mutassa meg, hogy $\prod_{d|n} \Phi_d = x^n - 1$.
(b) Igazolja, hogy $\Phi_n \in \mathbb{Z}[x]$.
(c) Bizonyítsa be, hogy tetszőleges $n > 1$ páratlan számra és tetszőleges z komplex számra

$$\Phi_{2n}(z) = \Phi_n(-z)$$

teljesül.
(d) Mutassa meg, hogy tetszőleges p prímszámra a Φ_p polinom irreducibilis $\mathbb{Q}$ felett.
(e) Mutassa meg, hogy tetszőleges n természetes számra a Φ_n polinom irreducibilis $\mathbb{Q}$ felett.

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

8.3. Az alábbi szerkesztési feladatok mindegyikében határozza meg a szerkesztés K alaptestét, a szerkesztendő szám által generált testbővítés fokát K felett, és döntse 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 egységsugarú kört kell négyszögesíteni,
(f) Adott egy szabályos 9-szög, szerkesztendő egy szabályos 18-szög

Amennyiben a szerkesztés elvégezhető végezzük is el.

8.4. Szerkeszthető-e a háromszög két oldalából, és az egyikhez tartozó szögfelezőből? (Az oldalak hossza adott.)

8.5. Mutassa meg, hogy nem szerkeszthető egyenlő szárú háromszög a szárából és a beírt kör sugarából.

8.6. Mely n egészekre szerkeszthető n-fokos szög ($n \in \mathbb{N}$).

8.7. Határozza meg a $\cos \dfrac{2\pi}{n}$ valós szám fokát $\mathbb{Q}$ felett ($n \in \mathbb{N}$).

8.8. Mutassa meg, hogy $\cos \dfrac{2\pi}{17}$ egyenlő a

$$-\frac{1}{16} + \frac{\sqrt{17}}{16} + \frac{\sqrt{34 - 2\sqrt{17}}}{16} + \frac{\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}}{8}$$

valós számmal.[3]

[3] Gauss 18 éves korában igazolta ezt az egyenlőséget.