4. Feladatsor

Véges testek

1. Legyen L algebrailag zárt test. Mutassa meg, hogy L végtelen.

2. Adjon meg a $\mathbb{Z}_3[x]/(x^3 - x + 1)$ és $\mathbb{Z}_3[x]/(x^3 - x - 1)$ testek között izomorfizmust.

3. Mutassa meg, hogy az $f = x^6 - 11x^4 + 36x^2 - 36$ polinomnak nincs egész gyöke, de tetszőleges p prímszámra van gyöke $\mathbb{Z}_p$-ben.

4. Legyen p prímszám és $a \in \mathbb{Z}_p \setminus \{0\}$. Bizonyítsa be, hogy az $x^p - x - a$ polinom $\mathrm{Gal}_{\mathbb{Z}_p}(x^p - x - a)$ Galois-csoportja ciklikus.

5. Legyen p prímszám és $n \in \mathbb{N}$. Bizonyítsa be, hogy az $x^{p^n} - x + 1$ polinom pontosan akkor irreducibilis $\mathbb{Z}_p$ felett, ha $n = 1$ vagy $n = p = 2$.

6. Legyen $K = \mathrm{GF}(q)$ és p prímszám. Mutassa meg, hogy $(q^p - q)/p$ darab p-edfokú irreducibilis főpolinom van $K[x]$-ben.

7. Mutassa meg, hogy az $x^p - x - 1$ polinom irreducibilis $\mathbb{Z}_p$ felett.

8. Határozza meg az $x^{p^p} - x$ polinom irreducibilis felbontását $\mathbb{Z}_p$ felett.

9. Bizonyítsa be, hogy tetszőleges a és b egészekre

$$\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{\text{ln.k.o.}(a,b)} \times \mathbb{Z}_{ab/\text{ln.k.o.}(a,b)}$$

teljesül.

10. Mutassa meg, hogy van olyan $\sigma \in \mathrm{Aut}_{\mathrm{GF}(2^{10})}(\mathrm{GF}(2^{11}))$, amelynek rendje 2. Határozza meg a $\{a \in \mathrm{GF}(2^{11}) \mid \sigma(x) = x^{-1}\}$ halmaz elemszámát.

11. Legyenek p és q prímszámok, amelyekre $p < q$ és $p \nmid q - 1$ teljesül. Adjon meg olyan $L : \mathbb{Z}_q$ testbővítés, hogy L az $\{x^p - a \mid a \in \mathbb{Z}_q\}$ polinomhalmaz felbontási teste legyen $\mathbb{Z}_q$ felett.

12. Legyen p prímszám, $m \in \mathbb{N}$ és $\mathfrak{F}\colon \mathrm{GF}(p^m) \to \mathrm{GF}(p^m)$, $x \mapsto x^p$ a Frobenius-automorfizmus. Legyen n tetszőleges természetes szám. Igazolja a következőket.

(a) Tetszőleges $a \in \mathrm{GF}(p^m)$-re $\mathfrak{F}^m(a) = a$ teljesül.

(b) Ha $[L : \mathrm{GF}(p^m)] = n$, akkor $L \cong \mathrm{GF}(p^{mn})$.

(c) Ha az $L : \mathrm{GF}(p^m)$ testbővítés véges, akkor $\mathrm{Gal}(L : \mathrm{GF}(p^m))$ ciklikus, melynek generátora $\mathfrak{F}^m$.

(d) A $\mathrm{GF}(p^{mn}) : \mathrm{GF}(p^m)$ testbővítés közbülső testei és a $\{d \in \mathbb{N} \mid d \mid n\}$ halmaz között megadható bijekció.

13. Legyen p páratlan prímszám, $m \in \mathbb{N}$ és $q = p^m$.

(a) Legyen $\lambda_q\colon \mathrm{GF}(q)^\times \to (\{-1, 1\}; \cdot\,)$ az a leképezés, amelyre $\lambda_q(u) = 1$ pontosan akkor teljesül, ha van olyan $v \in \mathrm{GF}(q)^\times$, amelyre $u = v^2$. Mutassa meg, hogy λ_q homomorfizmus. Igaz-e, hogy λ_q szürjektív?

(b) Legyen $\Sigma_p = \{u^2 \in \mathrm{GF}(q) \mid u \in \mathrm{GF}(q)\}$, és tetszőleges $t \in \mathrm{GF}(q)$-ra legyen $t - \Sigma_q = \{t - u^2 \in \mathrm{GF}(q) \mid u \in \mathrm{GF}(q)\}$. Ekkor Σ_q és $t - \Sigma_q$ elemszáma is $(q + 1)/2$.

(c) Bizonyítsa be, hogy tetszőleges $a \in \mathrm{GF}(q)$ felírható két $\mathrm{GF}(q)$-beli elem négyzetének összegeként.

(d) Az $x^2 + y^2 + z^2 = 0$ egyenletnek van nemtriviális megoldása $\mathrm{GF}(p^m)$-ben.

Primitív elemek

14. Ha az $L : K$ testbővítés Galois-bővítés, akkor L valamely K feletti irreducibilis polinomnak a felbontási teste.

15. Legyen $K(t) : K$ egyszerű transzcendens testbővítés. Mutassuk meg, hogy a testbővítésnek végtelen sok közbülső teste van.

16. Legyen p prímszám, $J = \mathbb{Z}_p(\alpha)$, $K = J(\beta)$, ahol α transzcendens $\mathbb{Z}_p$ felett és β transzcendens J felett. Legyen L az $f = (x^2 - \alpha)(x^2 - \beta)$ polinom felbontási teste K felett. Igazolja, hogy

(a) $[L : K] = p^2$,

(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.

17. Tegyük fel, hogy az $L : K$ testbővítés véges szeparábilis bővítés, az $M : L$ pedg véges egyszerű. Mutassa meg, hogy $M : K$ egyszerű bővítés.

Harmad- és negyedfokú polinomok

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

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

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

19. Legyen $f = a_0 + a_1 x + \cdots + a_n x^n$ n-edfokú polinom a K test felett, Az f polinom valamely L felbontási testében gyökei legyenek $\alpha_1, \ldots, \alpha_n$. Tetszőleges $i \in \{1, 2, \ldots, n\}$-re legyen

$$g_i = \sum_{j=0}^{n-1} a_{j+1} \sum_{k=0}^{j} \alpha_i^k x^{j-k}.$$

(a) Mutassuk meg, hogy $L[x]$-ben $f = (x - \alpha_i) g_i$ teljesül tetszőleges $i \in \{1, \ldots, n\}$-re. Továbbá, $D_x(f) = g_1 + \cdots + g_n$.

(b) Tetszőleges $j \in \mathbb{N}$-re legyen $\lambda_j = \alpha_1^j + \cdots + \alpha_n^j$. Bizonyítsuk be, hogy

$$j a_{n-j} + \sum_{k=1}^{j} a_{n-j+k} \lambda_k = 0 \quad (j = 1, \ldots, n),$$

$$\sum_{k=0}^{n} a_k \lambda_{j+k} = 0 \quad (j \in \mathbb{N}).$$

20. Legyen K test, $f = x^n + px + q \in K[x]$. Az f polinom valamely L felbontási testében f gyökei legyenek $\alpha_1, \ldots, \alpha_n$. Mutassuk meg, hogy

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

és az f polinom Δ diszkriminánsa:

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

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

21. 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 $\alpha = \beta - \dfrac{p}{3\beta}$, ahol $\beta^3 = -\dfrac{q}{2} + \delta$ és $\delta^2 = \dfrac{q^2}{4} + \dfrac{p^3}{27}$.

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

23. 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.

24. Határozzuk meg az alábbi $\mathbb{Q}[x]$-beli polinomok Galois-csoportját $\mathbb{Q}$ felett: $x^4 + 4x + 2$; $x^4 + 8x - 12$; $x^4 + 1$; $x^4 + x^3 + x^2 + x + 1$; $x^4 - 2$.

25. Legyen K olyan test, melynek karakterisztikája nem 2 és nem 3. Legyen f egy K feletti irreducibilis negyedfokú polinom, melynek köbös rezolvense g. Legyen L az f polinom felbontási teste K felett, valamint legyen $M \leqslant L$ a g polinom felbontási teste K felett. Mutassuk meg az alábbi táblázat

helyességét.

$\delta(f)$	g	f	$\mathrm{Gal}_K(f)$
$\notin K$	irreducibilis K felett		$\cong S_4$
$\in K$	irreducibilis K felett		$\cong A_4$
$\in K$	felbomlik $K[x]$-ben		$\cong V_4$ (Viergruppe)
$\notin K$	felbomlik $K[x]$-ben	felbomlik $M[x]$-ben	$\cong \mathbb{Z}_4$
$\notin K$	felbomlik $K[x]$-ben	irreducibilis M felett	$\cong D_4$.

26. Tetszőleges n természetes számra legyen

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

Mutassuk meg az alábbiakat.

(a) Tetszőleges $\omega \in \mathbb{C}$-re $\omega \in P_n$ pontosan akkor teljesül, ha $\omega = \cos\dfrac{2k\pi}{n} + i\sin\dfrac{2k\pi}{n}$, ahol 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 $n \geqslant 3$.

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

27. Tetszőleges n természetes számra legyen

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

A Φ_n polinomot az n-edik körosztási polinomnak nevezzük.

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

(b) Mutassuk meg, hogy $\prod_{d|n} \Phi_d = x^n - 1$.

(c) Igazoljuk, hogy $\Phi_n \in \mathbb{Z}[x]$.

(d) Bizonyítsuk be, hogy tetszőleges $n > 1$ páratlan számra és tetszőleges z komplex számra $\Phi_{2n}(z) = \Phi_n(-z)$ teljesül.

(e) Mutassuk meg, hogy ha p prímszám, akkor Φ_p irreducibilis $\mathbb{Q}$ felett.

(f) Mutassuk meg, hogy tetszőleges n természetes számra a Φ_n polinom irreducibilis $\mathbb{Q}$ felett.