Algebra4 matematikus szakirány

Zárthelyi Dolgozat – megoldások 2023. május 5.

1. Egyrészt $\sqrt[10]{3}$ minimálpolinomja $x^{10}-3$, hiszen ennek gyöke (1 pont) és ez a polinom irreducibilis $\mathbb{Q}$ fölött a Schönemann–Eisenstein kritérium miatt $p=3$ prímmel (2 pont). Tehát a kérdés az, hogy $x^{10}-3$-nak hány gyöke van $\mathbb{Q}(\sqrt[10]{27})$-ben (3 pont). Mivel $\mathbb{Q}(\sqrt[10]{27}) \leq \mathbb{R}$ és $x^{10}-3$-nak két valós gyöke van (mégpedig $\pm\sqrt[10]{3}$), ezért $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[10]{3}), \mathbb{Q}(\sqrt[10]{27}))$ legfeljebb 2 elemű (2 pont). Viszont $\pm\sqrt[10]{3} = \pm\frac{(\sqrt[10]{27})^7}{9} \in \mathbb{Q}(\sqrt[10]{27})$, ezért a kérdéses halmaz 2 elemű (2 pont).

2. Egyrészt $x^6+1 = (x^2+1)(x^4-x^2+1)$ (1 pont), ami $\mathbb{F}_5$ fölött tovább-bomlik $(x-2)(x+2)(x^2-2x-1)(x^2+2x-1)$ (3 pont) és ezek a tényezők már irreducibilisek $\mathbb{F}_5$ fölött, mert egyik másodfokúnak sincs gyöke (3 pont). A felbontási test tehát $\mathbb{F}_{25}$, mert ez az egyetlen másodfokú bővítése $\mathbb{F}_5$-nek (3 pont). Úgy is lehet érvelni, hogy egyrészt $\mathbb{F}_5$ fölött nyilván nem bomlik gyöktényezők szorzatára a polinom, hiszen nincs többszörös gyöke, viszont $\mathbb{F}_5$-nek csak 5 eleme van (holott a felbontási testben x^6+1-nek 6 gyöke van). Másrészt $\mathbb{F}_{25}$ multiplikatív csoportja 24-edrendű ciklikus, tehát van benne 12-rendű α elem, melyre $\alpha^6 \neq 1$, de $(\alpha^6)^2 = 1$ miatt $\alpha^6 = -1$, ezért α (összesen 6 darab) páratlan kitevős hatványai gyökei az x^6+1 polinomnak, tehát ez a polinom $\mathbb{F}_{25}$ fölött gyöktényezők szorzatára bomlik.

3. Egyik irány: ha $\alpha \in \overline{\mathbb{Z}}$ (algebrai egész), akkor gyöke egy $f(x) \in \mathbb{Z}[x]$ *normált* polinomnak. Viszont ennek a polinomnak $\overline{\alpha}$ is gyöke, ezért $\overline{\alpha} \in \overline{\mathbb{Z}}$ (1 pont), és mivel $\overline{\mathbb{Z}} \leq \mathbb{C}$ részgyűrű, ezért $2\mathrm{Re}(\alpha) = \alpha + \overline{\alpha} \in \overline{\mathbb{Z}}$ és $|\alpha|^2 = \alpha\overline{\alpha} \in \overline{\mathbb{Z}}$ (2 pont). A hetedik feladatsor házi feladat szerint így $|\alpha| \in \overline{\mathbb{Z}}$ (2 pont).

   Másik irány: Tegyük föl, hogy $2\mathrm{Re}(\alpha), |\alpha| \in \overline{\mathbb{Z}}$. Ekkor $x^2-(2\mathrm{Re}(\alpha))x+|\alpha|^2$ egy $\overline{\mathbb{Z}}$-együtthatós normált polinom, melynek α gyöke (1 pont), hiszen $\overline{\mathbb{Z}}$ egy gyűrű, tehát $|\alpha|^2 \in \overline{\mathbb{Z}}$ (1 pont). Ebből az is következik, hogy $\alpha \in \overline{\mathbb{Z}}$: valóban, $\mathbb{Z}[2\mathrm{Re}(\alpha), |\alpha|]$ végesen generált $\mathbb{Z}$-modulus, $\mathbb{Z}[2\mathrm{Re}(\alpha), |\alpha|, \alpha]$ pedig végesen generált $\mathbb{Z}[2\mathrm{Re}(\alpha), |\alpha|]$-modulus, ezért végesen generált $\mathbb{Z}$-modulus is mely tartalmazza α-t (3 pont).

4. Az $\sqrt{1+\sqrt{3}}$ nyilván gyöke az $(x^2-1)^2-3 = x^4-2x^2-2$ polinomnak (1 pont), ami irreducibilis a Schönemann–Eisenstein kritérium szerint $p=2$ választással (1 pont). Tehát a keresett minimálpolinom x^4-2x^2-2. A polinom gyökei $\pm\sqrt{1+\sqrt{3}}, \pm\sqrt{\sqrt{3}-1}i$ (1 pont), a felbontási test Galois-csoportja ezen gyököknek egy tranzitív permutációcsoportja, speciálisan S_4 részcsoportja (1 pont). Belátjuk, hogy $|\mathbb{Q}(\pm\sqrt{1+\sqrt{3}}, \pm\sqrt{\sqrt{3}-1}i) \colon \mathbb{Q}| = 8$, így a Galois-csoport csak D_4 lehet, hiszen az S_4-ben D_4 a 2-Sylow részcsoport (1 pont). Valóban, $|\mathbb{Q}(\sqrt{1+\sqrt{3}}) \colon \mathbb{Q}| = 4$, hiszen negyedfokú a minimálpolinom (1 pont) és $\sqrt{3} = (\sqrt{1+\sqrt{3}})^2 - 1 \in \mathbb{Q}(\sqrt{1+\sqrt{3}})$ miatt $\mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt{1+\sqrt{3}})$ (1 pont). Tehát $\pm\sqrt{\sqrt{3}-1}i$ gyöke az $x^2-1+\sqrt{3} \in \mathbb{Q}(\sqrt{1+\sqrt{3}})[x]$ polinomnak, ezért $|\mathbb{Q}(\pm\sqrt{1+\sqrt{3}}, \pm\sqrt{\sqrt{3}-1}i) \colon \mathbb{Q}(\sqrt{1+\sqrt{3}})| \leq 2$ (1 pont). Másrészt $\pm\sqrt{\sqrt{3}-1}i$ nem valós, azaz nincs benne $\mathbb{Q}(\sqrt{1+\sqrt{3}}) \leq \mathbb{R}$-ben (1 pont), így $|\mathbb{Q}(\pm\sqrt{1+\sqrt{3}}, \pm\sqrt{\sqrt{3}-1}i) \colon \mathbb{Q}(\sqrt{1+\sqrt{3}})| = 2$ és a fokszámtétel miatt $|\mathbb{Q}(\pm\sqrt{1+\sqrt{3}}, \pm\sqrt{\sqrt{3}-1}i) \colon \mathbb{Q}| = 8$ (1 pont).

5. Mivel $\Phi_n(x)$ (az n-edik körosztási polinom) irreducibilis $\mathbb{Q}$ fölött (1 pont), ezért ε Galois-konjugáltjai a primitív n-edik egységgyökök (1 pont), azaz az ε^k alakú számok, ahol $(k,n)=1$ (1 pont). Tehát tetszőleges $\tau \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon), K)$ esetén $\tau(\varepsilon) = \varepsilon^k$ valamely n-hez relatív prím k egészre (1 pont) és $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon), K)$ elemszáma éppen azon $1 \leq k \leq n$ egész számok száma, melyre $\varepsilon^k \in K$ (1 pont). Ha nincs ilyen k szám, akkor a halmaz nyilván az üreshalmaz (1 pont) (ez $n \geq 3$ esetén elő is fordul pl. $K = \mathbb{Q}$ választásnál, de persze $n = 1, 2$ esetén $\mathbb{Q}(\varepsilon) = \mathbb{Q}$). Viszont ha $\varepsilon^k \in K$ valamely $(k,n) = 1$ egészre, akkor a maradékos osztás miatt van olyan $c \in \mathbb{Z}$, hogy $kc \equiv 1 \pmod{n}$ (1

pont), azaz $\alpha = \alpha^{kc} = (\alpha^k)^c \in K$ (1 pont), azaz az összes primitív n-edik egységgyök benne van K-ban (1 pont). Ekkor viszont $|\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon), K)| = \varphi(n)$ az n-hez relatív prím maradékosztályok száma (1 pont).

6. Mivel $x^{p^n} - x$-nek nincs többszörös gyöke (a gyökei épp $\mathbb{F}_{p^n}$ elemei) (1 pont), ezért $f(x) \mid x^{p^n} - x$ esetén f-nek sincs többszörös gyöke (az $\mathbb{F}_p$ algebrai lezártjában) (1 pont). Megmutatjuk, hogy ez a feltétel elégséges is ilyen n létezésére (1 pont a azért a sejtésért, hogy ez a válasz). Tegyük fel ugyanis, hogy $f(x) \in \mathbb{F}_p[x]$ egy olyan polinom, aminek nincs többszörös gyöke és legyen K a felbontási teste. Mivel K egy p-karakterisztikájú véges test, ezért van olyan n, hogy $K = \mathbb{F}_{p^n}$ (3 pont). De ekkor f minden gyöke egyszeres és gyöke $x^{p^n} - x$-nek, hiszen utóbbi gyökei épp $\mathbb{F}_{p^n}$ elemei (2 pont), de ez azt jelenti, hogy $f(x) \mid x^{p^n} - x$ (2 pont).

7. Először belátjuk, hogy vannak olyan $d_1 \neq d_2 \in \mathbb{Z}$ négyzetmentes számok, hogy $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ (1 pont a sejtésért). Írjuk fel a Galois-csoportot $\mathrm{Gal}(K/\mathbb{Q}) = H_1 \times H_2$ alakban, ahol $H_1 \cong H_2 \cong C_2$ és legyen $K_1 := K^{H_1}$, $K_2 := K^{H_2}$ a két részcsoport fixteste. Ekkor $|K_j : \mathbb{Q}| = 2$ (1 pont) és a másodfokú egyenlet megoldóképletéből van olyan $d_1, d_2 \in \mathbb{Z}$ négyzetmentes, melyre $K_j = \mathbb{Q}(\sqrt{d_j})$ $(j = 1, 2)$ (1 pont). Sőt, mivel $K_1 \neq K_2$, ezért $d_1 \neq d_2$. Belátjuk, hogy $K \leq \mathbb{Q}(\varepsilon_{4[d_1,d_2]})$ (1 pont a sejtésért), ahol $[d_1, d_2]$ a legkisebb közös többszöröst jelöli. Egyrészt $K \leq \mathbb{Q}(i, \sqrt{p_1}, \ldots, \sqrt{p_r})$, ahol $p_1, p_2, \ldots, p_r$ a $[d_1, d_2]$ szám (különböző) prímosztói, hiszen $\sqrt{d_j}$ előáll a d_j-t osztó prímek négyzetgyökének és ha $d_j < 0$, akkor az i-nek a szorzataként $(j = 1, 2)$ (1 pont). Másrészt $i = \pm\varepsilon_{4[d_1,d_2]}^{[d_1,d_2]} \in \mathbb{Q}(\varepsilon_{4[d_1,d_2]})$ (1 pont) és a kvadratikus reciprocitási tétel bizonyításából következik, hogy $\sqrt{(-1)^{\frac{p-1}{2}} p} \in \mathbb{Q}(\varepsilon_p)$, ha p páratlan prím (2 pont) és $\sqrt{2} = \varepsilon_8 + \varepsilon_8^7 \in \mathbb{Q}(\varepsilon_8)$ (1 pont), azaz $\sqrt{p_k} \in \mathbb{Q}(\varepsilon_{4p_k}) \leq \mathbb{Q}(\varepsilon_{4[d_1,d_2]})$ $(k = 1, \ldots, r)$ (1 pont).