Algebra4 matematikus szakirány

1. ZH – megoldások

2013. április 3.

1. A fokszám nyilván legfeljebb 3, hiszen $\sqrt[3]{2}$ gyöke az $x^3 - 2$ harmadfokú polinomnak. Másrészt ez a polinom $\mathbb{Q}$ felett irreducibilis, speciálisan $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3. Tehát a fokszámtétel miatt $\mathbb{Q}(\sqrt{2}, i, \sqrt[3]{2})$ test $\mathbb{Q}$ feletti foka osztható 3-mal. Ugyanakkor $\sqrt{2}$ és i foka is 2 $\mathbb{Q}$ fölött és $i \notin \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, ezért $3 \nmid |\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = 4$. Tehát a keresett fokszám 3, hiszen osztható 3-mal és legfeljebb 3.

2. Jelöljük K_f-fel illetve L_f-fel f felbontási testét K ill. L fölött. Ekkor nyilván $K \leq K(\alpha) \leq K_f \leq L_f$, ahol α egy gyöke $f(x)$-nek. Mivel f irreducibilis, ezért $|K(\alpha) : K| = \deg(f) = p$, így a fokszámtétel miatt $p \mid |L_f : K| = |L_f : L| \cdot |L : K|$. Másrészt vegyük észre, hogy L fölött f két p-nél kisebb fokú polinom szorzatára bomlik, tehát felbontási teste p-nél kisebb fokú bővítések egymásutánja. Speciálisan $p \nmid |L_f : L|$, ezért $p \mid |L : K|$.

3. Mivel a $\Phi_n(x) \in \mathbb{Q}[x]$ körosztási polinom irreducibilis, ezért ez ε minimálpolinomja. Vegyük észre, hogy ha K-ban van primitív n-edik egységyök, akkor az összes primitív n-edik egységgyök benne van, hiszen ezek egymás pozitív egész kitevős hatványai. Tehát ekkor Φ_n gyöktényezők szorzatára bomlik K felett. Az órán tanult állítás szerint $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\varepsilon), K)$ elemszáma éppen Φ_n K-beli gyökeinek számával egyenlő, ami pedig 0 vagy $\varphi(n)$ aszerint, hogy ε benne van-e K-ban.

4. $\mathbb{F}_5$ felett: $x^3 - 2 = (x-3)(x^2 - 2x - 1)$ az irreducibilis felbontás ($x^2 - 2x - 1$ irreducibilis, hiszen nincs gyöke). Tehát a felbontási test $\mathbb{F}_{25}$, mivel másodfokú bővítés $\mathbb{F}_5$-nek. Ugyanakkor $\mathbb{F}_7$ felett $x^3 - 2$ irreducibilis, mivel nincs gyöke. Tehát $\mathbb{F}_{7^3}$-ben van köbgyöke 2-nek, de mivel $\mathbb{F}_{7^3}^\times$ rendje osztható 3-mal, ezért van $\mathbb{F}_{7^3}$-ben primitív harmadik egységgyök, tehát 2-nek három köbgyöke is van ebben a testben. Így a felbontási test $\mathbb{F}_{7^3}$.

5. Először is, ha a $\mathbb{F}_q$ véges test karakterisztikája 2, akkor $x^4 + 1 = (x+1)^4$. Tegyük fel tehát, hogy $\mathrm{char}(\mathbb{F}_q) \neq 2$. Ekkor $x^4 + 1$ $\overline{\mathbb{F}_q}$-beli gyökei épp a 8-adrendű elemek („nyolcadik egységgyökök”, ez egyébként tetszőleges $\mathrm{char}(K) \neq 2$ testben igaz). Node vegyük észre, hogy $|\mathbb{F}_{q^2}^\times| = q^2 - 1$ osztható 8-cal mivel q páratlan. Mivel $\mathbb{F}_{q^2}^\times$ ciklikus, ezért van is benne 8-adrendű elem, azaz $x^4 + 1$-nek gyöke. Speciálisan $x^4 + 1$ nem lehet irreducibilis, hiszen akkor csak minimum 4-edfokú bővítésben lenne gyöke.

   Második megoldás: Vegyük észre, hogy $x^4 + 1 = (x^2 + i)(x^2 - i) = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1) = (x^2 - \sqrt{2}ix - 1)(x^2 + \sqrt{2}ix - 1)$ három különböző felbontás ($\mathbb{C}$ felett). Minden p prímszámra működik valamelyik felbontás a három közül modulo p, hiszen -1, 2 és -2 nem lehet egyszerre kvadratikus nemmaradék modulo p, hiszen két kvadratikus nemmaradék szorzata mindig kvadratikus maradék.

6. Legyen $\alpha = \sqrt{2 + \sqrt{2}}$. Ekkor $(\alpha^2 - 2)^2 = 2$, azaz α gyöke az $x^4 - 4x^2 + 2$ polinomnak. Ez lesz a minimálpolinom is, mivel ez irreducibilis $\mathbb{Q}$ fölött a Schönemann-Eisenstein kritérium miatt ($p = 2$-re). Vegyük észre, hogy ennek a polinomnak 4 darab (egyszeres) gyöke van, jelesül: $\pm\sqrt{2 \pm \sqrt{2}}$ (ezek mind valós számok). Vegyük észre, hogy $\frac{1}{\sqrt{2+\sqrt{2}}} =$

$\frac{\sqrt{2-\sqrt{2}}}{\sqrt{2}}$, és mivel $\sqrt{2} = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$, ezért az $x^4 - 4x^2 + 2$ polinom gyöktényezők szorzatára bomlik $\mathbb{Q}(\alpha)$ felett, tehát $\mathbb{Q}(\alpha)$ a felbontási test. Mivel ez egy 4-edfokú bővítés, ezért a G Galois-csoport vagy Z_4-gyel vagy $Z_2 \times Z_2$-vel izomorf. Van pontosan egy olyan $\sigma \in G$, melyre $\sigma(\alpha) = \sqrt{2-\sqrt{2}}$. Ekkor $\sigma(\sqrt{2}) = \sigma(\alpha^2 - 2) = \sigma(\alpha)^2 - 2 = -\sqrt{2}$, és $\sigma^2(\alpha) = \sigma(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}) = \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = -\alpha$. Tehát σ nem másodrendű, azaz $G \not\cong Z_2 \times Z_2$, így $G \cong Z_4$.

7. Írjuk L-et $L = K(\alpha)$ alakban (megtehetjük, hiszen L/K Galois, speciálisan szeparábilis), ekkor $L(\varepsilon) = K(\alpha, \varepsilon)$. Minden $\tau\colon K(\alpha,\varepsilon) \to \overline{K}$ K-homomorfizmusra $\tau(\alpha) \in K(\alpha) \subseteq K(\alpha,\varepsilon)$ és $\tau(\varepsilon) \in K(\varepsilon) \subseteq K(\alpha,\varepsilon)$, hiszen $K(\alpha)/K$ és $K(\varepsilon)/K$ is Galois-bővítések. Tehát $\tau(K(\alpha,\varepsilon)) \subseteq K(\alpha,\varepsilon)$, azaz $K(\alpha,\varepsilon)/K$ is Galois (ez egyébként volt előadáson is). Legyen $G = \mathrm{Gal}(L(\varepsilon)/K)$, $H_1 = \mathrm{Gal}(L(\varepsilon)/L)$, ill. $H_2 = \mathrm{Gal}(L(\varepsilon)/K(\varepsilon))$. Ekkor $H_1, H_2 \lhd G$, hiszen mind L mind $K(\varepsilon)$ normális bővítései K-nak. Továbbá $G/H_1 \cong \mathrm{Gal}(L/K)$ és $G/H_2 \cong \mathrm{Gal}(K(\varepsilon)/K)$ is Abel. Speciálisan $[G,G] \leq H_1, H_2$, azaz $[G,G] \leq H_1 \cap H_2$. Másrészt H_1 elemei fixálják $\alpha \in L$-et, H_2 elemei pedig $\varepsilon \in K(\varepsilon)$-t, azaz $H_1 \cap H_2$ elemei fixálják mindkettőt, tehát az egész $L(\varepsilon) = K(\alpha,\varepsilon)$-t. A Galois-elmélet főtétele szerint $H_1 \cap H_2 = \{1\}$, ezért $[G,G] = 1$, tehát G Abel.