Algebra4 matematikus szakirány

Dolgozat 2021. április 15. – megoldások

1. Egyrészt $\sqrt[14]{64} = \sqrt[7]{8}$ és $\sqrt[7]{4}$ egyike sem racionális, de mindkettő benne van $\mathbb{Q}(\sqrt[7]{2})$-ben, ami egy (heted-, azaz) prímfokú bővítése $\mathbb{Q}$ (hiszen $x^7 - 2$ irreducibilis a Schönemann–Eisenstein kritérium szerint). A fokszámtétel miatt $\mathbb{Q}(\sqrt[14]{64}) = \mathbb{Q}(\sqrt[7]{4}) = \mathbb{Q}(\sqrt[7]{2})$. Az $x^7 - 8$, ill. $x^7 - 4$ polinomokról közvetlenül is meg lehet mutatni, hogy irreducibilisek a Newton-poligon segítségével. Viszont $\sqrt[7]{8}$ minimálpolinomjának csak egyetlen valós gyöke van, ezért $|\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[14]{64}), \mathbb{Q}(\sqrt[7]{4}))| = 1$.

2. $x^8 + 1 = \Phi_{16}(x)$, aminek pontosan akkor van gyöke $\mathbb{F}_{3^k}$-ban, ha $\mathbb{F}_{3^k}^\times$-ban van 16-odrendű elem. Mivel ez a csoport ciklikus, ezért ez pontosan akkor teljesül, ha $16 \mid 3^k - 1$. A legkisebb ilyen k a 4, ezért $\mathbb{F}_{3^4} = \mathbb{F}_{81}$ a felbontási test.

3. A keresett polinom $(x - \sqrt{3} - i)(x - \sqrt{3} + i)(x + \sqrt{3} - i)(x + \sqrt{3} + i) = x^4 - 4x^2 + 16$, hiszen a minimálpolinomnak az összes Galois-konjugált gyöke és $\mathbb{Q}(\sqrt{3}, i)$-nek van olyan automorfizmusa, ami a $\sqrt{3} + i$ elemet $\pm\sqrt{3} \pm i$ elembe viszi. Ez a polinom semmilyen p-re sem lesz irreducibilis modulo p: $p = 2, 3$ esetén ez világos, ha pedig $p > 3$, akkor a 3, -1, -3 számok közül legalább az egyik kvadratikus maradék lesz modulo p így a háromféle

$$\begin{aligned} x^4 - 4x^2 + 16 &= (x^2 - 2\sqrt{3}x + 4)(x^2 + 2\sqrt{3}x + 4) = \\ &= (x^2 - 2ix - 4)(x^2 + 2ix - 4) = \\ &= (x^2 - 2 - 2\sqrt{3}i)(x^2 - 2 + 2\sqrt{3}i) \end{aligned}$$

   felbontás közül legalább az egyik megad egy modulo p felbontást.

4. A legelemibb felírni a minimálpolinomot és ellenőrizni, hogy valóban egész együtthatós. Egy másik érvelés, hogy a négyzete $\frac{p+q+2\sqrt{pq}}{4} = \frac{p+q-2}{4} + \frac{1+\sqrt{pq}}{2}$ benne van $\mathbb{Q}(\sqrt{pq})$ algebrai egészeiben, hiszen $pq \equiv 1 \pmod 4$ és $\frac{p+q-2}{4} \in \mathbb{Z}$.

5. Az $x^3 - 2i$ polinom komplex gyökei: $-\sqrt[3]{2}i, -\sqrt[3]{2}i\varepsilon, -\sqrt[3]{2}i\varepsilon^2$, ahol ε egy primitív harmadik egységgyök. Tehát ha K a felbontási test, akkor $K = \mathbb{Q}(\sqrt[3]{2}, i, \varepsilon)$. Belátjuk, hogy $|K : \mathbb{Q}| = 12$ és így $|K : \mathbb{Q}(i)| = 6$, azaz a Galois-csoport $\mathrm{Gal}(K/\mathbb{Q}(i)) \cong S_3$ (hiszen S_3 hatelemű részcsoportja). Egyrészt $|K : \mathbb{Q}(i)| \leq 6$ miatt $|K : \mathbb{Q}| = |K : \mathbb{Q}(i)| \cdot |\mathbb{Q}(i) : \mathbb{Q}| \leq 12$. Tehát elég belátni, hogy $i \notin \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, hiszen $|\mathbb{Q}(\sqrt[3]{2}, \varepsilon) : \mathbb{Q}| = 6$ és a fokszámtétel ismételt alkalmazásával $|K : \mathbb{Q}|$ ennek többszöröse. Tegyük föl indirekten, hogy $\mathbb{Q}(i) \leq \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$. Node $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ másodfokú résztestei a Galois elmélet főtétele miatt megfelelnek S_3 kettő indexű részcsoportjainak, amiből A_3 az egyetlen. Tehát $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ egyetlen másodfokú részteste $\mathbb{Q}(\varepsilon)$ és ebben nincs benne i, hiszen $\mathbb{Q}(\varepsilon, i)$-ben benne van a εi primitív 12-edik egységgyök, ezért $\mathbb{Q}$ fölötti foka (legalább) $\varphi(12) = 4$.

   Másik bizonyítás a végére: $\mathbb{Q}(\varepsilon, i)$ a 12-edik körosztási test, azaz $\mathbb{Q}$ fölötti foka 4. Ebben tehát nincs gyöke az $x^3 - 2$ polinomnak, hiszen annak minden gyöke harmadfokú $\mathbb{Q}$ fölött és $3 \nmid 4$. Tehát az $x^3 - 2$ polinom irreducibilis $\mathbb{Q}(\varepsilon, i)$ fölött, hiszen harmadfokú és nincs gyöke. Így $|K : \mathbb{Q}(\varepsilon, i)| = 3$, azaz $|K : \mathbb{Q}| = 12$.

6. A kínai maradéktétel miatt és mivel modulo prím létezik primitív gyök:

$$\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}) \cong (\mathbb{Z}/(21))^\times \cong (\mathbb{Z}/(3))^\times \times (\mathbb{Z}/(7))^\times \cong C_2 \times C_6 \cong C_2 \times C_2 \times C_3 \ .$$

A másodfokú résztestek a Galois-csoport 2 indexű részcsoportjaival állnak bijekcióban, ezért ebből 3 darab van (ugye a $C_2 \times C_2$ csoportnak három másodrendű részcsoportja van: a harmadik az „átló"). Másrészt a kvadratikus reciprocitási tétel bizonyításából következik, hogy $\sqrt{-3} \in \mathbb{Q}(\varepsilon^7)$ és $\sqrt{-7} \in \mathbb{Q}(\varepsilon^3)$, hiszen ε^7 (ill. ε^3) egy primitív harmadik (ill. hetedik) egységgyök, ezért $\mathbb{Q}(\sqrt{-3})$ és $\mathbb{Q}(\sqrt{-7})$ másodfokú résztestek. Viszont $\sqrt{21} = \sqrt{-3} \cdot \sqrt{-7} \in \mathbb{Q}(\varepsilon)$, ezért $\mathbb{Q}(\sqrt{21})$ a harmadik másodfokú résztest.

7. Vegyük észre, hogy $K(\alpha^p) \leq K(\alpha)$ mindig teljesül. Tegyük föl először, hogy α *nem* szeparábilis K fölött és legyen $f(x) \in K[x]$ az α minimálpolinomja. Volt előadáson, hogy ekkor $f(x) = g(x^p)$ alakú, ahol $g(x) \in K[x]$ (irreducibilis) polinom. Tehát $g(\alpha^p) = f(\alpha) = 0$, azaz α^p foka K fölött (legfeljebb) $\deg g = \frac{\deg f}{p} < \deg f = |K(\alpha) : K|$, így $K(\alpha^p) < K(\alpha)$ egy valódi résztest. Megfordítva tegyük föl, hogy $K(\alpha^p) < K(\alpha)$. Ekkor α gyöke az $x^p - \alpha^p \in K(\alpha^p)[x]$ polinomnak, sőt, ez az egyetlen gyök. Tehát α $K(\alpha^p)$ fölötti $h(x)$ minimálpolinomja osztója $x^p - \alpha^p$-nek, ezért h-nak is egyetlen gyöke az α. Mivel h nem lehet elsőfokú (különben $K(\alpha) = K(\alpha^p)$ lenne), ezért h is x^p polinomja, azaz foka legalább p. Azt kaptuk, hogy $h(x) = x^p - \alpha^p$, azaz $|K(\alpha) : K(\alpha^p)| = \deg h = p$ és $|K(\alpha) : K)| = p|K(\alpha^p) : K|$. Legyen most $g(x) \in K[x]$ az α^p minimálpolinomja. Ekkor α gyöke a $g(x^p)$ polinomnak, de mivel ennek foka $\deg g(x^p) = p \deg g = |K(\alpha) : K|$, azért ez a minmálpolinom. Viszont ennek α többszörös gyöke, hiszen deriváltja azonosan 0. Mivel α minimálpolinomjának van többszörös gyöke, α nem szeparábilis.