Gyakorlati kérdések

1. *Mi az $x^4 + 2x^2 - 1$ polinom felbontási testének foka $\mathbb{Q}$ fölött?* *(10 pont)*

Megoldás: $f(x)$ gyökei $\pm\sqrt{-1 \pm \sqrt{2}}$. Ha $\alpha := \sqrt{-1+\sqrt{2}}$ és β a $\sqrt{-1-\sqrt{2}}$ egyik értéke, akkor $\sqrt{2} = 1 + \alpha^2 \in \mathbb{Q}(\alpha)$, és az F felbontási testet megkaphatjuk legföljebb másodfokú (négyzetgyökökkel való) bővítések sorozatával:

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(\alpha, \beta).$$

Az első bővítés nyilván nem triviális, és az utolsó sem, mert $\mathbb{Q}(\alpha) \leq \mathbb{R}$, míg $\beta \notin \mathbb{R}$. A középső bővítésről azt kell belátni, hogy $-1+\sqrt{2}$ nem áll elő négyzetszámként $\mathbb{Q}(\sqrt{2})$-ben. Valóban, ha $(a + b\sqrt{2})^2 = -1 + \sqrt{2}$ valamely $a, b \in \mathbb{Q}$-ra, akkor $a^2 + 2b^2 = -1$, ami nem lehetséges. Tehát $(F : \mathbb{Q}) = 2 \cdot 2 \cdot 2 = 8$.

2. *Legyen $K = \mathbb{F}_5(\alpha)$, ahol α az $x^2 - 2x - 1$ polinom gyöke. Határozzuk meg $\alpha - 2$ rendjét K multiplikatív csoportjában!* *(10 pont)*

Megoldás: $x^2 - 2x - 1$ irreducibilis $\mathbb{F}_5[x]$-ben, mert másodfokú, és $0, \pm 1, \pm 2$ közül egyik sem gyöke. Így $\mathbb{F}_5(\alpha)$ elemei egyértelműen írhatók fel α $\mathbb{F}_5$ fölötti lineáris polinomjaként.

$$\begin{aligned} \alpha^2 &= 2\alpha + 1 \\ \alpha^3 &= 2\alpha^2 + \alpha = 5\alpha + 2 = 2 \\ \alpha^{12} &= 2^4 = 1, \end{aligned}$$

tehát α rendje osztója 12-nek, másrészt

$$\begin{aligned} \alpha^4 &= 2\alpha \neq 1 \\ \alpha^6 &= 2^2 = -1 \neq 1, \end{aligned}$$

így α rendje nem lehet 12 semelyik valódi osztója. Tehát $o(\alpha) = 12$.

3. *Tudjuk, hogy $\alpha = \cos 20^\circ$ minimálpolinomja $\mathbb{Q}$ fölött $f(x) = 8x^3 - 6x - 1$, és $\mathbb{Q}(\alpha)|\mathbb{Q}$ normális bővítés. Határozzuk meg a $f(x)(x^2 - 2)$ Galois-csoportját izomorfia erejéig!* *(10 pont)*

Megoldás: Mivel $\mathbb{Q}(\alpha)$ tartalmazza az $f(x)$ többi gyökét is, az $f(x)(x^2 - 2)$ polinom felbontási teste $F = \mathbb{Q}(\alpha, \sqrt{2})$. A

$$\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(\alpha, \sqrt{2}) = F$$

bővítéssorozatból látható, hogy $(F : \mathbb{Q}) \leq 3 \cdot 2 = 6$, másrészt $(\mathbb{Q}(\alpha) : \mathbb{Q}) = 3$ és $(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = 2$ miatt $(F : \mathbb{Q})$ osztható 2-vel és 3-mal is, tehát 6-tal is. Így $(F : \mathbb{Q}) = 6 \Rightarrow G = \mathrm{Gal}(F|\mathbb{Q})$ is 6-elemű. A $\mathbb{Q}(\alpha)$ és $\mathbb{Q}(\sqrt{2})$ közbülső testek mindegyike normális $\mathbb{Q}$ fölött $\Rightarrow G$-nek van 3 és 2 indexű, azaz 2 és 3-elemű normálosztója is, amelyek szükségképpen diszjunktak és kigenerálják a 6-elemű G-t $\Rightarrow G \cong C_2 \times C_3 \cong C_6$.

Elméleti kérdések

4. *Mit mondhatunk egy $L|K$ Galois-bővítés relatív automorfizmusainak a számáról? Mutassunk példát olyan $L|K$ véges fokú, de nem Galois-bővítésre, amelyre nem igaz ez az állítás! (Indokoljuk is, hogy miért jó az ellenpélda!)* *(5 pont)*

Megoldás: Ha $L|K$ Galois-bővítés, akkor $\mathrm{Aut}(L|K) = \mathrm{Gal}(L|K)$ elemszáma $(L : K)$. De például a $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$ harmadfokú bővítés ($\sqrt[3]{2}$ minimálpolinomja $x^3 - 2$), és $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}) = 1$, ugyanis a testbővítés minden automorfizmusa helyben hagyja $\sqrt[3]{2}$-t, mert ez az egyetlen gyöke $x^3 - 2$-nek, amelyik $\mathbb{Q}(\sqrt[3]{2})$-ben benne van (a másik kettő nem valós), és $\mathbb{Q}$ elemeit is, tehát triviálisan hat a testbővítésen.

5. *Mondjuk ki a következő definíciókat és tételeket!* *(10 pont)*

a) definíció: normális bővítés
b) definíció: a $*$ Galois-megfeleltetés, részcsoportra és közbülső testre is;
c) tétel: egyszerű algebrai bővítés bázisa és foka
d) tétel: az euklideszi szerkeszthetőség feltétele

6. *Mondjuk ki és bizonyítsuk a következő két tétel közül az* **egyiket** *(15 pont):*

a) Egyszerű bővítés előállítása faktorgyűrűként
b) Véges szeparábilis bővítés egyszerűsége