Mat-tanári gyakorlat, második évfolyam, második félév
Kilencedik alkalom — megoldásvázlatok

1. A $\mathbb{Q} \le \mathbb{Q}(\sqrt[4]{2})$ bővítés nem normális, mert x^4-2 irreducibilis polinom $\mathbb{Q}$ felett, melynek van gyöke $\mathbb{Q}(\sqrt[4]{2})$-ben, de nincs itt minden gyöke (hiszen $\pm i\sqrt[4]{2})$ nem valósak). Ha e polinom összes gyökével bővítünk, akkor az $L = \mathbb{Q}(i, \sqrt[4]{2})$ testet kapjuk, ami már normális bővítése $\mathbb{Q}$-nak, mert egy racionális együtthatós polinom felbontási teste. Könnyen láthatjuk, hogy ennek a testnek 8 a foka $\mathbb{Q}$ felett, sőt a szorzástétel bizonyításából kiindulva e bővítés egy bázisát is felírhatjuk. Ezek szerint L minden β eleme egyértelműen írható

$$\beta = a + b\sqrt[4]{2} + c(\sqrt[4]{2})^2 + d(\sqrt[4]{2})^3 + ei + fi\sqrt[4]{2} + gi(\sqrt[4]{2})^2 + hi(\sqrt[4]{2})^3$$

alakban, ahol $a, b, c, d, e, f, g, h \in \mathbb{Q}$.

Legyen G a $\mathbb{Q} \le L$ bővítés Galois-csoportja, és $\varphi \in G$. Mivel φ fixálja a racionális számokat, a fenti képletből látjuk, hogy $\varphi(\beta)$ kiszámításához elegendő a $\varphi(i)$ és a $\varphi(\sqrt[4]{2})$ ismerete (ez közvetlenül is látszik abból, hogy L-et ez a két elem generálja $\mathbb{Q}$ felett). Vegyük észre, hogy ha $p \in \mathbb{Q}[x]$ tetszőleges polinom, melynek egy $\alpha \in L$ szám gyöke, akkor $\varphi(\alpha)$ is gyöke p-nek. Valóban, ha $p(x) = a_0 + a_1x + \cdots + a_nx^n$, akkor, mivel φ fixálja a racionális számokat, $\varphi(a_i) = a_i$ minden i-re, és így

$$p(\varphi(\alpha)) = a_0 + a_1\varphi(\alpha) + \cdots + a_n\varphi(\alpha)^n = \varphi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = \varphi(0) = 0\,.$$

Ezt röviden úgy fogalmazhatjuk, hogy *a Galois-csoport elemei permutálják az alaptestbeli együtthatós polinomok gyökeit.* Speciálisan tehát az x^2+1 polinomot vizsgálva azt kapjuk, hogy $\varphi(i) = \pm i$, az x^4-2-ből pedig az adódik, hogy φ ennek az $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = i\sqrt[4]{2}$, $\alpha_3 = -\sqrt[4]{2}$, $\alpha_4 = -i\sqrt[4]{2}$ gyökeit is permutálja.

Próbáljuk meg áttekinteni G elemeit. Mivel φ két helyre viheti i-t, négy helyre viheti α_1-et, és ez a két érték, mint láttuk, már meghatározza φ-t, ezért G rendje legfeljebb 8 lehet. Mivel $\alpha_2/\alpha_1 = i$, ezért $\varphi(i) = \varphi(\alpha_2)/\varphi(\alpha_1)$. Ezért $\varphi(\alpha_1)$ és $\varphi(\alpha_2)$ is egyértelműen meghatározza φ-t. Az $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ számok egy négyzetet alkotnak a síkon. Belátjuk, hogy G elemei éppen e négyzet szimmetriáinak felelnek meg. Először is vegyük észre, hogy $\alpha_3 = -\alpha_1$, és ezért $\varphi(\alpha_3) = -\varphi(\alpha_1)$. Ez azt jelenti, hogy φ a négyzet átlóját átlóba kell, hogy vigye. Ez a csúcsok 24 lehetséges permutációjából könnyen láthatóan kizár 16-ot, és pont azt a nyolcat hagyja meg, amik a négyzet szimmetriáinak felelnek meg. Még azt kell belátni, hogy ez a nyolc permutáció tényleg a bővítés automorfizmusát adja.

Tekintsük például az (13) permutációt. Ehhez olyan φ kell, hogy tartozzon, amire $\varphi(\alpha_1) = \alpha_3 = -\sqrt[4]{2}$, $\varphi(\alpha_3) = \alpha_1$, az α_2 és α_4 pedig fixen marad. Innen $\varphi(i) = \alpha_2/\alpha_3 = -i$. Ezért a fenti képletből

$$\varphi(\beta) = a - b\sqrt[4]{2} + c(\sqrt[4]{2})^2 - d(\sqrt[4]{2})^3 - ei + fi\sqrt[4]{2} - gi(\sqrt[4]{2})^2 + hi(\sqrt[4]{2})^3\,.$$

Ez a képlet tehát egy φ függvényt definiál az L testen, és azt kellene belátni, hogy ez tényleg egy relatív automorfizmus. Ez elvégezhető lenne sok számolással. Gyorsabb azonban a következő út. Az alaptétel miatt tudjuk, hogy ennek a nyolcadfokú normális bővítésnek a Galois-csoportja nyolcelemű. De azt már beláttuk, hogy G-nek legfeljebb nyolc eleme lehet. Ezért ez a nyolc lehetőség meg is kell, hogy valósuljon, tehát a fenti négyzet minden szimmetriájához kell hogy tartozzon egy relatív automorfizmus. Tehát speciálisan a fenti φ függvény is automorfizmus kell, hogy legyen.

Így tehát azt kaptuk, hogy $G \cong D_4$. A közbülső testek meghatározásához az egyes automorfizmusok fixpontjait kell megkeresni. Például az előbbi φ-nek azok a β elemek a fixpontjai, melyekre $\varphi(\beta) = \beta$. Mivel β fenti felírása egyértelmű, azt kapjuk, hogy $b = -b$, $d = -d$, $e = -e$, $g = -g$, azaz φ fixpontjai az $a + c(\sqrt[4]{2})^2 + fi\sqrt[4]{2} + hi(\sqrt[4]{2})^3$ alakú számok. Könnyen láthatjuk, hogy ezek éppen a $\mathbb{Q}(i\sqrt[4]{2})$ test elemei. Ez a közbülső test tehát éppen az $\{id, (13)\}$ részcsoportnak felel meg.

Utólag, az eredmény birtokában látjuk, hogy gyorsabban is eljárhattunk volna. Tudjuk, hogy ennek a kételemű, azaz négy-indexű részcsoportnak az alaptétel szerint olyan közbülső test felel meg, mely negyedfokú $\mathbb{Q}$ felett. De mivel φ fixálja α_2-t, fixálja $\mathbb{Q}(\alpha_2)$-t is. Mivel ez már maga negyedfokú $\mathbb{Q}$ felett, ez kell, hogy legyen a fixpontok halmaza. Hasonló gondolatmenettel láthatjuk be, hogy az $\{id, (24)\}$ részcsoportnak a $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\sqrt[4]{2})$ test kell, hogy megfeleljen.

Ezek szerint a $\mathbb{Q}(\sqrt[4]{2})$ résztestei az $\{id, (24)\}$-et tartalmazó részcsoportoknak kell, hogy megfeleljenek. Egy ilyen valódi részcsoport elemszáma csak négy lehet, aminek az indexe kettő, és így normálosztó. A D_4

normálosztóit már kiszámoltuk, és innen láthatjuk, hogy csak a $\{id, (24), (13), (13)(24)\}$ jöhet szóba. Ehhez a részcsoporthoz csak a $\mathbb{Q}(\sqrt{2})$ közbülső test tartozhat (ellenőrizzük közvetlen számolással is, hogy $\mathbb{Q}(\sqrt{2})$ éppen az (13)-hoz és (24)-hez tartozó relatív automorfimusok közös fixpontjainak a halmaza).

Azt a meglepő eredményt kaptuk tehát, hogy a $\mathbb{Q} \leq \mathbb{Q}(\sqrt[4]{2})$ bővítésnek az egyetlen valódi közbülső teste a $\mathbb{Q}(\sqrt{2})$. Ebből következik, hogy minden olyan elemnek a foka négy kell, hogy legyen ($\mathbb{Q}$ felett), ami nincs benne $\mathbb{Q}(\sqrt{2})$-ben! Hiszen ha α ilyen elem, akkor a $\mathbb{Q}(\alpha)$ csakis $\mathbb{Q}(\sqrt[4]{2})$ lehet. Tehát számolás nélkül látjuk, hogy például $\sqrt{2} + \sqrt[4]{2}$ foka négy.

Hasonló számolással kapható az összes többi részcsoporthoz is a megfelelő közbülső test:

$$
\begin{array}{rlrl}
\{id\} \longleftrightarrow & \mathbb{Q}(i, \sqrt[4]{2}) & \{id, (13)\} \longleftrightarrow & \mathbb{Q}(i\sqrt[4]{2}) \\
\{id, (13), (24), (13)(24)\} \longleftrightarrow & \mathbb{Q}(\sqrt{2}) & \{id, (24)\} \longleftrightarrow & \mathbb{Q}(\sqrt[4]{2}) \\
\{id, (12)(34), (14)(23), (13)(24)\} \longleftrightarrow & \mathbb{Q}(i\sqrt{2}) & \{id, (13)(24)\} \longleftrightarrow & \mathbb{Q}(i, \sqrt{2}) \\
\{id, (1234), (13)(24), (1432)\} \longleftrightarrow & \mathbb{Q}(i) & \{id, (12)(34)\} \longleftrightarrow & \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) \\
D_4 \longleftrightarrow & \mathbb{Q} & \{id, (14)(23)\} \longleftrightarrow & \mathbb{Q}(\sqrt[4]{2} - i\sqrt[4]{2})
\end{array}
$$

2. Tegyük fel, hogy $K \leq L \leq C$ és $|L : K| = 2$. Legyen $\alpha \in L$, $\alpha \notin K$. Ekkor α másodfokú, az m minimálpolinomjának gyökei legyenek α és β. A gyökök és együtthatók összefüggése miatt $\alpha + \beta \in K$, és ezért $\beta \in L$. Tehát $K(\alpha, \beta) = L$. Így L az m felbontási teste K felett, és ezért normális bővítése K-nak. Ezzel a bizonyítás kész.

Gyakorlásul lássuk be közvetlenül is, hogy ha f egy K felett irreducibilis polinom, akkor vagy nincs gyöke L-ben, vagy minden gyöke L-ben van. Tegyük fel, hogy α egy L-beli gyök, és legyen m az α minimálpolinomja K felett. Ekkor $x - \alpha$ közös osztója f-nek és m-nek $L[x]$ felett. Ezért az (m, f) kitüntetett közös osztó nem konstans. De az euklideszi algoritmus végig $K[x]$-ben marad, és ezért (m, f) a K test felett számolva ugyanaz, mint L felett. Viszont K felett mindkét polinom irreducibilis, tehát asszociáltak, és így gyökeik egyenlők. A gyökök és együtthatók összefüggése miatt azonban m-nek mindkét gyöke L-ben van (hiszen m első, vagy másodfokú).

3. Legyen $K \leq L \leq N$, ahol $|L : K| = 4$, és N normális bővítése K-nak. Ha a $K \leq N$ Galois-csoportja G, és H az L testnek megfelelő részcsoport, akkor tehát $|G : H| = 4$, és keressük a H-t tartalmazó valódi részcsoportokat. Ha ilyen legfeljebb egy van, akkor készen vagyunk. Ha van két különböző, mondjuk H_1 és H_2, akkor mindkettő indexe G-ben kettő, és $H_1 \cap H_2$ csak H lehet. Ekkor $H \triangleleft G$ (mert két normálosztó metszete). Azaz a H-t tartalmazó részcsoportok a G/H összes részcsoportjainak felelnek meg. De G/H vagy ciklikus, vagy a Klein-csoporttal izomorf, és mindkét esetben ismerjük a részcsoportokat. Látjuk, hogy ha $K \leq L$ nem normális, akkor legfeljebb egy valódi közbülső test lehet.

4. Az $x^2 + 1$ felbontási teste $\mathbb{Q}(i)$, ennek foka 2 a $\mathbb{Q}$ felett, a Galois-csoport $\mathbb{Z}_2$, közbülső test csak a két triviális van. Mindez tetszőleges másodfokú irreducibilis polinomra is igaz. Az $x^4 - 1$ felbontási teste $\mathbb{Q}(i)$, a Galois-csoport tehát ugyanaz, mint az előbb. Az $x^4 + 1 = \Phi_8(x)$ gyökei a primitív nyolcadik egységgyökök, ha ε ilyen, akkor a többi ennek hatványa, vagyis a felbontási test $\mathbb{Q}(\varepsilon)$, melynek foka $\mathbb{Q}$ felett $\varphi(8) = 4$. A Galois-csoport $\mathbb{Z}_2^2$ lesz, a nemtriviális közbülső testek $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$. A relatív automorfizmusok hatványozzák ε-t. Az $x^6 - 1$ felbontási teste $\mathbb{Q}(\eta)$, ahol η hatodik primitív egységgyök, a Galois-csoport $\mathbb{Z}_2$. Az $x^6 - 2$ felbontási teste $\mathbb{Q}(\sqrt[6]{2}, \eta)$, ahol η hatodik primitív egységgyök. Ennek a bővítésnek a foka 12, hiszen η másodfokú $\mathbb{Q}$ felett, és mivel nem valós, másodfokú $\mathbb{Q}(\sqrt[6]{2})$ felett is. A Galois-csoport D_6, az egyes automorfizmusok az $x^6 - 2$ polinom gyökeiből álló szabályos hatszög egybevágóságainak felelnek meg. Az $(x^2 - 2)(x^3 - 2)$ felbontási teste $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \varepsilon)$, ahol ε primitív harmadik egységgyök. Könnyen láthatóan ez a test megegyezik az előző polinom esetében vizsgált $\mathbb{Q}(\sqrt[6]{2}, \eta)$ testtel, és így a Galois-csoport és a közbülső testek is ugyanazok. Az $(x^2 - 2)(x^2 - 3)$ felbontási teste a $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, ennek foka $\mathbb{Q}$ felett 4, a Galois-csoport a Klein-csoport, az összes résztest pedig $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. **Nagyon javaslom, hogy ezt a legutóbbi bővítést mindenki önállóan, részletesen számolja végig.**