**Matematikus gyakorlat, második évfolyam, első félév**

*Kilencedik alkalom — megoldásvázlatok*

**1.** Azt kell megmutatni, hogy $\sqrt{6}$ kifejezhető $\sqrt{3}$-ból, $\sqrt{2}+1$-ből és racionális számokból a négy alapművelet segítségével (ami nyilvánvaló, mert $\sqrt{6}=\sqrt{3}((\sqrt{2}+1)-1)$).

**2.** Nyilván $K(\sqrt{2},\sqrt[3]{2})\subseteq K(\sqrt[6]{2})$, hiszen $\sqrt{2}$ is és $\sqrt[3]{2}$ is hatványa $\sqrt[6]{2}$-nek. Megfordítva, $\sqrt[6]{2}=(\sqrt{2})/(\sqrt[3]{2})$.

**3.** $\alpha,\beta\in K(\alpha,\beta)$, és mivel ez test, tartalmazza $\alpha\beta$-t is. Ezért $K(\alpha,\alpha\beta)\subseteq K(\alpha,\beta)$. Megfordítva, $\alpha\neq 0$ miatt a $\beta$, ami $\alpha\beta$ és $\alpha$ hányadosa, benne van a $K(\alpha,\alpha\beta)$ testben. De $\alpha$ is benne van, így $K(\alpha,\alpha\beta)\supseteq K(\alpha,\beta)$.

**4.** Átszorozva, és a $\sqrt[3]{2}$ hatványai szerint rendezve $1=(1+\sqrt[3]{2}+\sqrt[3]{4})(a+b\sqrt[3]{2}+c\sqrt[3]{4})=(a+2b+2c)+(a+b+2c)\sqrt[3]{2}+(a+b+c)\sqrt[3]{4}$. Az 1 ilyen alakú felírása egyértelmű, és ezért $a+2b+2c=1$, $a+b+2c=0$, $a+b+c=0$. Az egyenletrendszert megoldva az eredmény $\sqrt[3]{2}-1$. (Ezt számolás nélkül is leolvashattuk volna az $a^3-b^3=(a-b)(a^2+ab+b^2)$ azonosságból. De a fenti módszer általános, minden esetben működik.)

**5.** Azt tudjuk, hogy $\theta^3+3\theta+1=0$. Innen $\theta^5+3\theta^3+\theta^2=0$. Ebből ki lehet fejezni $\theta^5$-t, és így $\theta^5+2\theta^3=-3\theta^3-\theta^2+2\theta^3=-\theta^3-\theta^2=-\theta^2+3\theta+1$. Látható, hogy $\theta$ valamennyi polinomja redukálható legfeljebb másodfokúvá úgy, hogy a legmagasabb fokú tagot mindig alacsonyabb fokúval helyettesítjük.

A $\theta/(\theta-3)$ kiszámításakor az eredményt $a+b\theta+c\theta^2$ alakban keressük, keresztbe szorzunk, nullára redukálunk, a $\theta$ kapott polinomját redukáljuk legfeljebb másodfokúvá, majd az együtthatókat nullává tesszük, és a kapott lineáris egyenletrendszert megoldjuk. Az eredmény: $\theta/(\theta-3)=(1/37)-(9/37)\theta-(3/37)\theta^2$. (Számítógéppel közelítőleg ellenőrizhető az eredmény, mert $\theta\approx-0,322185$.)

**6.** A $\pi$ transzcendens, minimálpolinomja a 0. Az $1+i$-hez olyan polinomot kell keresni, melynek ez gyöke. Ehhez legyen $1+i=x$, ekkor $i=x-1$, négyzetre emelve és rendezve $x^2-2x-2=0$. Ennek a polinomnak tehát gyöke az $1+i$, és ez akkor lesz a minimálpolinom, ha irreducibilis $\mathbb{Q}$ felett. Ez látszik abból, hogy másodfokú, és nincs gyöke $\mathbb{Q}$-ban. Ha $x=\sqrt{2}+i$, akkor $(x-i)^2=2$, azaz $x^2-3=2ix$, még egyszer négyzetre emelve és rendezve $x^4+2x^2+9$. E polinom irreducibilitása ugyanúgy látható be, mint az $x^4+9$ polinomé az első félévben: $\mathbb{C}$ felett kell először felbontani. (Láthatjuk, hogy ezzel a technikával az összetett gyökös kifejezésekhez néha tudunk olyan polinomot találni, aminek az gyöke, ha a megfelelő átrendezések után mindig hatványozunk.) Ennek alapján $\sqrt{2}+\sqrt{3}$ minimálpolinomja $x^4-10x^2+1$ (irreducibilitását az első félévben beláttuk), a $\sqrt[3]{2}$-é $x^3-2$, az $1+\sqrt[3]{2}$-é $(x-1)^3-2$ (ami $x^3-2$ eltoltja, ezért irreducibilis), $\sqrt[3]{2+\sqrt{2}}$-é pedig $x^6-4x^3+2$, ami a Schönemann-Eisenstein miatt irreducibilis.

Ha $u=\sqrt[3]{7+5\sqrt{2}}$, $v=\sqrt[3]{7-5\sqrt{2}}$, és $x=u+v$, akkor vaktában elindulva egy nagyon nagy fokú polinom keletkezne. Köbre emelve $x^3=14+3uv(u+v)$. De $uv=\sqrt[3]{49-50}=-1$ és $u+v=x$, ezért $x^3+3x-14=0$ is igaz. De ez még mindig nem a minimálpolinom, hiszen gyöke a kettő. Mivel ez az egyetlen valós gyök (ami például az $x-2$ kiemelésével adódik), és $u+v$ valós, ezért $u+v=2$, minimálpolinomja $x-2$.

A $\cos 3\alpha=4\cos^3\alpha-3\cos\alpha$ azonosságból kapjuk, hogy $\cos 20^\circ$ minimálpolinomja $x^3-(3/4)x-(1/8)$ (ez a racionális gyökteszt miatt irreducibilis $\mathbb{Q}$ felett). Végül az $n$-edik primitív egységgyökök közös minimálpolinomja az $n$-edik körosztási polinom, hiszen ez irreducibilis $\mathbb{Q}$ felett, és normált.

**7.** Ha a $\mathbb{Z}_2[x]/(x^2+x+1)$ faktorgyűrűben akarunk számolni, akkor minden osztályból egy „ügyes" reprezentánst kell kiválasztani. Nyilván $f$ és $g$ akkor és csak akkor van egy osztályban, ha $f-g\in(x^2+x+1)$, azaz ha $f$ és $g$ ugyanazt a maradékot adja $x^2+x+1$-gyel osztva. A lehetséges osztási maradékok éppen az $ax+b$ alakú polinomok, ahol $a,b\in\mathbb{Z}_2$, ezekkel kell számolni modulo $x^2+x+1$. Tehát négy polinomról van szó, legyen $N=0+(x^2+x+1)$, $E=1+(x^2+x+1)$, $A=x+(x^2+x+1)$ és $B=x+1+(x^2+x+1)$. Például $AB=E$ mert $x^2+x=x^2+x+1+1\equiv 1$ (hiszen minden elem kétszerese nulla). A táblák:

| $+$ | $N$ | $E$ | $A$ | $B$ |
|---|---|---|---|---|
| $N$ | $N$ | $E$ | $A$ | $B$ |
| $E$ | $E$ | $N$ | $B$ | $A$ |
| $A$ | $A$ | $B$ | $N$ | $E$ |
| $B$ | $B$ | $A$ | $E$ | $N$ |

| $*$ | $N$ | $E$ | $A$ | $B$ |
|---|---|---|---|---|
| $N$ | $N$ | $N$ | $N$ | $N$ |
| $E$ | $N$ | $E$ | $A$ | $B$ |
| $A$ | $N$ | $A$ | $B$ | $E$ |
| $B$ | $N$ | $B$ | $E$ | $A$ |

Testet kaptunk, mert az $E$ egységelem a szorzástábla minden sorában szerepel az elsőt kivéve. A prímtest nyilván $\{N,E\}$, ami a $\mathbb{Z}_2$-vel izomorf. Az $Ex^2+Ex+E$ polinom gyökei $A$ és $B$. Mivel ez irreducibilis $\{N,E\}$ felett (másodfokú, és nincs e testben gyöke), ezért ő az $A$ és $B$ közös minimálpolinomja. Az $E$ minimálpolinomja $Ex-E$, az $N$-é $Ex$.

**8.** Az ilyen alakú számok a $\mathbb{Q}(\sqrt[3]{2})$ testet alkotják. A $\sqrt[3]{2}$ foka $\mathbb{Q}$ felett három, mert $\mathbb{Q}$ feletti minimálpolinomja $x^3-2$. Így $|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}|=3$. Tehát e bővítés minden elemének foka osztója háromnak. De a $\sqrt[6]{2}$ foka $\mathbb{Q}$ felett 6, mert a Schönemann-Eisenstein kritérium miatt az $x^6-2$ polinom irreducibilis $\mathbb{Q}$ felett. Tehát sem ez a szám, sem a másodfokú $\sqrt{2}$ nem írható fel a kívánt alakban. Jegyezzük meg, hogy sok harmadfokú szám van, ami szintén nem írható fel ilyen alakban, ilyen például az $x^3-2$ polinom két nem valós gyöke.

**9.** Az eredmény 6, a 2. vagy a 10. feladat miatt.

**10.** Tekintsük a $K\le K(\alpha)\le K(\alpha)(\beta)=M$ testláncot. Az első bővítés foka $gr_K(\alpha)$. A második bővítés fokának meghatározásához meg kell vizsgálnunk a $\beta$ minimálpolinomját $K(\alpha)$ felett. Ha a $K$ feletti minimálpolinomot $m$ jelöli, akkor $m$ foka $gr_K(\beta)$. Az $m$ polinom $K[x]$-beli, és így minden együtthatója benne van a $K(\alpha)$ testben. A $K(\alpha)$ feletti minimálpolinom azonban osztója minden olyan $K(\alpha)[x]$-beli polinomnak, aminek $\beta$ gyöke, tehát speciálisan $m$-nek is. Ezért a foka, azaz $\beta$ foka $K(\alpha)$ felett legfeljebb annyi, mint $m$ foka, azaz $gr_K(\beta)$. Így a fenti testláncból azt kapjuk, hogy $|M:K|\le gr_K(\alpha)gr_K(\beta)$. Másrészt viszont $\alpha$ és $\beta$ $K$ feletti foka osztja $|M:K|$-t, és mivel e két szám relatív prím, a szorzatuk is osztja. Vagyis beláttuk, hogy $|M:K|=gr_K(\alpha)gr_K(\beta)$. (A fenti lánc alapján ebből azt is láthatjuk, hogy $\beta$ foka $K(\alpha)$ felett $gr_K(\beta)$, és ezért a fenti $m$ polinom a $K(\alpha)$ feletti minimálpolinom is egyben.)

**11.** Tekintsük a $\mathbb{Q}\le\mathbb{Q}(\sqrt{8})=\mathbb{Q}(\sqrt{2})\le\mathbb{Q}(\sqrt[4]{2})$ láncot. Tudjuk, hogy a nagy bővítés foka 4, a kicsié 2, ezért $|\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{8})|=2$. Így a keresett fokszám kettő. (Be lehet látni, hogy a $\sqrt[4]{2}$ minimálpolinomja $\mathbb{Q}(\sqrt{2})$ felett $x^2-\sqrt{2}$, de erre nincsen szükség.) A másik kérdéshez tekintsük a $\mathbb{Q}\le\mathbb{Q}(\sqrt[3]{7})\le\mathbb{Q}(\sqrt[3]{7},\sqrt[4]{2})$ láncot. A 10. feladat miatt itt a nagy bővítés foka 12, és a kicsié 3, ezért az eredmény 4.

**12.** Legyen $\varepsilon$ primitív harmadik egységyök, melyre $\theta=\varepsilon\sqrt[3]{2}$. Mivel $\theta$ minimálpolinomja is $x^3-2$, a $\theta$ foka $\mathbb{Q}$ felett 3. Továbbá $\varepsilon$ foka $\varphi(3)=2$ (a minimálpolinom a harmadik körosztási polinom, azaz $x^2+x+1$). Nyilván $\mathbb{Q}(\sqrt[3]{2},\varepsilon\sqrt[3]{2})=\mathbb{Q}(\sqrt[3]{2},\varepsilon)$, és így a 10. feladat miatt ez hatodfokú bővítése $\mathbb{Q}$-nak. Ezért $\theta$ másodfokú $\mathbb{Q}(\sqrt[3]{2})$ felett (és ez nem osztja a $\theta$ fokát $\mathbb{Q}$ felett). A $\mathbb{Q}(\theta)\cap\mathbb{R}$ test részteste $\mathbb{Q}(\theta)$-nak, és így $\mathbb{Q}$ feletti foka 1 vagy 3 lehet. Utóbbi lehetetlen, mert $\theta$ nem valós. Ezért a metszet $\mathbb{Q}$.

**13.** a): Ez a szám primitív 360-adik egységgyök, hiszen 23 és 360 relatív prímek. Ezért foka $\varphi(360)$. b): Legfeljebb hatodfokú, de négyzetre emeléssel kifejezhető a $\sqrt[3]{9}$, ezért az eredmény 6. c): Nyilván 2. d): Négyzetre emeléssel kifejezhető a $\sqrt{2}$, az eredmény 4.

**14.** Mivel $i$ algebrai, ha $a$ és $b$ algebrai, akkor $a+bi$ is az, hiszen az algebrai számok testet alkotnak. Megfordítva, ha $a+bi$ algebrai, akkor gyöke egy racionális együtthatós nem nulla polinomnak. Ennek $a-bi$ is gyöke (hiszen a polinom valós együtthatós), de $a$ és $b$ kifejezhető $a+bi$-vel, $a-bi$-vel és $i$-vel.

**15.** Ha $a=\pi+3$ algebrai lenne, akkor $a-3=\pi$ is az lenne, hiszen az algebrai számok testet alkotnak, ami ellentmondás. Hasonlóan látható, hogy $5\pi+6$ és $\pi+\sqrt{2}$ sem lehet algebrai. Ha $\sqrt{\pi}$ algebrai lenne, akkor négyzete is, ez sem lehet. Végül belátjuk, hogy $\pi$ semmilyen racionális együtthatós, nem nulla polinomja sem lehet algebrai. Ha ugyanis $g(\pi)$ algebrai lenne, azaz gyöke lenne egy racionális együtthatós $f\ne0$ polinomnak, akkor $f(g(\pi))=0$, azaz $\pi$ gyöke lenne a racionális együtthatós, nem nulla $f(g(x))$ polinomnak.

**16.** Algebrai plusz transzcendens mindig transzcendens. Nem nulla algebraiszor transzcendens is transzcendens. Algebrai szám $n$-edik hatványa és $n$-edik gyöke is algebrai, minden $n$ egészre.

**17.** A $\mathbb{Q}$ minden algebrailag zárt bővítése tartalmazza az $n$-edfokú $\sqrt[n]{2}$ számot minden $n$-re, és így foka végtelen. Ha $K$ véges test, és elemei $\{a_1,\dots,a_n\}$, akkor az $f(x)=(x-a_1)\dots(x-a_n)+1$ nem-konstans polinomnak nincs gyöke $K$-ban, ezért $K$ nem lehet algebrailag zárt. A $\mathbb{Z}_p$ test esetében vehetnénk ehelyett az $x^2-g$ polinomot, ahol $g$ kvadratikus nemmaradék.

**18.** Ha $K\le L$ és $L\le M$ algebrai, és $\alpha\in M$, akkor bővítsük $K$-t az $\alpha$ elem $L$ feletti minimálpolinomjának együtthatóival. A kapott $N$ test véges bővítése $K$-nak, mert véges sok algebrai elemmel bővítettünk. De $\alpha$ algebrai $N$ felett, ezért $K\le N(\alpha)$ véges, vagyis $\alpha$ algebrai $K$ felett.

**19.** A lineáris kombinációk felírásával, és $\pi$ transzcendens voltának kihasználásával kapjuk, hogy az első és a harmadik halmaz független. A második nem, mert $\mathbb{C}$ csak másodfokú $\mathbb{R}$ felett.

**20, 21, 22.** A $\sqrt{2}=a+b\sqrt{3}$-ból négyzetre emeléssel, és $\sqrt{3}$ irracionalitásának kihasználásával ellentmondást kapunk. A többi állítás bizonyítása ennek az észrevételnek a könnyű általánosítása.

**23.** Belátjuk, hogy $c = \sqrt{2} + \sqrt{3}$ jó. Nyilván ez eleme $\mathbb{Q}(\sqrt{2}, \sqrt{3})$-nak, kérdés, hogy $\sqrt{2}$ és $\sqrt{3}$ kifejezhető-e $c$-vel és racionális számokkal. Mivel $c^2 = 5 + 2\sqrt{6}$, ezért $\sqrt{6} \in \mathbb{Q}(c)$. Továbbá $c^3 = 2\sqrt{3} + 3\sqrt{3} + 3\sqrt{6}c$, ezért innen $2\sqrt{3} + 3\sqrt{3} \in \mathbb{Q}(c)$. De ezzel és $c = \sqrt{2} + \sqrt{3}$-mal nyilván kifejezhető a $\sqrt{2}$ és a $\sqrt{3}$. (Megjegyezzük, hogy ezzel másik bizonyítást kaptunk arra, hogy $x^4 - 10x^2 + 1$ irreducibilis $\mathbb{Q}$ felett.)

**24.** 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 $\beta$ 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 $\varphi$ 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). Tudjuk, 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 $\varphi$ 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 $\varphi$ két helyre viheti $i$-t, négy helyre viheti $\alpha_1$-et, és ez a két érték, mint láttuk, már meghatározza $\varphi$-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 $\varphi$-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 $\varphi$ 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 $\varphi$ kell, hogy tartozzon, amire $\varphi(\alpha_1) = \alpha_3 = -\sqrt[4]{2}$, $\varphi(\alpha_3) = \alpha_1$, az $\alpha_2$ és $\alpha_4$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$-nek azok a $\beta$ elemek a fixpontjai, melyekre $\varphi(\beta) = \beta$. Mivel $\beta$ fenti felírása egyértelmű, azt kapjuk, hogy $b = -b$, $d = -d$, $e = -e$, $g = -g$, azaz $\varphi$ 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 $\varphi$ fixálja $\alpha_2$-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 $\mathbb{Q} \le \mathbb{Q}(\sqrt[4]{2})$ 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 $\alpha$ 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:

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

**25.** 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 $\varepsilon$ 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 $\varepsilon$-t. Az $x^6-1$ felbontási teste $\mathbb{Q}(\eta)$, ahol $\eta$ hatodik primitív egységgyök, a Galois-csoport $\mathbb{Z}_2$. Az $x^6-2$ felbontási teste $\mathbb{Q}(\sqrt[6]{2},\eta)$, ahol $\eta$ hatodik primitív egységgyök. Ennek a bővítésnek a foka 12, hiszen $\eta$ 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 $\varepsilon$ 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 $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

**26.** Tegyük fel, hogy $K \le L$ és $|L:K|=2$. Legyen $\alpha \in L$, $\alpha \notin K$. Ekkor $\alpha$ másodfokú, minimálpolinomja legyen $m(x)=x^2+ux+v$. A gyökök és együtthatók összefüggése miatt $\beta=-u-\alpha$ az $m$ „másik” gyöke, és nyilván $\beta \in L$. Így $K(\alpha,\beta)=L$, azaz $L$ az $m$ felbontási teste $K$ felett, és ezért normális bővítése $K$-nak.

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 $\alpha$ egy $L$-beli gyök, és legyen $m$ az $\alpha$ 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 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 minden gyöke $L$-ben van (hiszen $m$ első, vagy másodfokú).

**27.** $M/K$ normális, így felbontási test. Ugyanannak a polinomhalmaznak az $M$ az $L$ felett is felbontási teste.

**28.** Nyilván $\mathbb{Z}_2^n$ (mindegyik $\sqrt{p_i}$ a többitől függetlenül vihető az ellentettjébe, vö. 22. feladat).

**29.** Legyen $K \le L \le N$, ahol $|L:K|=4$, és $N$ normális bővítése $K$-nak. Ha a $K \le N$ 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 $K \le L$ nem normális, akkor legfeljebb egy valódi közbülső test lehet.

**30.** Legyen $\varepsilon$ primitív kilencedik egységgyök, ekkor $\mathbb{Q}(\varepsilon+\overline{\varepsilon})$ jó lesz. Ugyanis $\mathbb{Q}(\varepsilon)$ Galois-csoportja $\mathbb{Z}_9^\times \cong \mathbb{Z}_6^+$, ez Abel, tehát minden részcsoportja normálosztó, azaz minden közbülső test normális. A $\mathbb{Q}(\varepsilon+\overline{\varepsilon})$ elemeit a másodrendű komplex konjugálás fixen hagyja, tehát ez legfeljebb harmadfokú. De nem elsőfokú, mert $\varepsilon+\overline{\varepsilon}$-nek konjugáltja a tőle különböző $\varepsilon^2+\overline{\varepsilon}^2$ (ezzel beláttuk azt is, hogy $\cos 40^\circ$ irracionális).