Algebra4 matematikus

1. ZH – megoldások

2019. április 4.

1. Mivel $x^{10}-125$ és $x^{20}-5$ is irreducibilis $\mathbb{Q}$ fölött (Newton-poligon $p=5$-re), ezért $\sqrt[10]{125}$ minimálpolinomja $x^{10}-125$. A kérdés tehát az, hány gyöke van $x^{10}-125$-nek $\mathbb{Q}(\sqrt[20]{5})$-ben. Mivel $\pm\sqrt[10]{125}=\pm(\sqrt[20]{5})^6\in\mathbb{Q}(\sqrt[20]{5})$, ezért 2 gyök van. Viszont a többi gyöke $x^{10}-125$-nek nem valós, ugyanakkor $\mathbb{Q}(\sqrt[20]{5})\subset\mathbb{R}$, ezért $|\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[10]{125}),\mathbb{Q}(\sqrt[20]{5}))|=2$.

2. A felbontási test $\mathbb{Q}(\sqrt[3]{5},\varepsilon)$, ahol ε primitív harmadik egységgyök, hiszen x^3-5 gyökei $\sqrt[3]{5}$, $\sqrt[3]{5}\varepsilon$, és $\sqrt[3]{5}\varepsilon^2$. A Galois-csoport ezen három gyököt permutálja, és 6 elemű, hiszen $|\mathbb{Q}(\sqrt[3]{5},\varepsilon):\mathbb{Q}|=6=|S_3|$. Így a Galois-csoport S_3.

3. $\Phi_6(x)=x^2-x+1$ másodfokú, ezért pontosan akkor irreducibilis, ha nincs gyöke $\mathbb{F}_p$-ben. Ha $p=2$, akkor irreducibilis, ha $p=3$, akkor ez $(x+1)^2$, azaz felbomlik, legyen tehát $p>3$ prím. Ekkor egy $\alpha\in\mathbb{F}_{p^2}$ elem pontosan akkor gyöke Φ_6-nak, ha α multiplikatív rendje 6, tehát az a kérdés, hogy mely $p>3$ prímekre van $\mathbb{F}_p^\times$-ben 6-odrendű elem. Mivel $\mathbb{F}_p^\times$ ciklikus, ez azzal ekvivalens, hogy $6\mid|\mathbb{F}_p^\times|=p-1$. Tehát a válasz: $p=2$ vagy $p\equiv 5\pmod 6$ esetén irreducibilis.

4. Ha $x^n-\alpha=f(x)g(x)$ felbomlik alacsonyabb fokúak szorzatára, akkor nyilván $x^{nm}-\alpha=f(x^m)g(x^m)$ is felbomlik. Hasonlóan ha $x^m-\alpha$ felbomlik, akkor $x^{nm}-\alpha$ is. Megfordítva tegyük fel, hogy $x^n-\alpha$ és $x^m-\alpha$ irreducibilis. Ekkor $|K(\sqrt[n]{\alpha}):K|=n$ és $|K(\sqrt[m]{\alpha}):K|=m$. Mivel mindkettő részteste $K(\sqrt[nm]{\alpha})$-nak, ezért utóbbi foka K fölött osztható n-nel és m-mel is. Ezért $|K(\sqrt[nm]{\alpha}):K|=nm$, azaz $x^{nm}-\alpha$ irreducibilis.

5. $x^{16}-x$ gyökei épp $\mathbb{F}_{16}$ elemei, ami $\mathbb{F}_2$-nek 4-edfokú, $\mathbb{F}_4$-nek pedig másodfokú bővítése. Tehát $\mathbb{F}_2$ fölött az összes, 1, 2, és 4-fokú irreducibilis polinom szorzata $x^{16}-x$, így

$$x^{16}-x=x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)\ .$$

A 4-edfokúakat úgy találhatjuk meg, hogy egy negyedfokú akkor irreducibilis, ha nincs gyöke, és nem áll elő két másodfokú irreducibilis szorzataként. $\mathbb{F}_2$ fölött pontosan akkor nincs gyöke egy polinomnak, ha se 0, se 1 nem gyök, azaz a konstans tag 1 és páratlan sok tag van. Végezetül másodfokú irreducibilis csak az x^2+x+1 van, ennek négyzete nem irreducibilis, így csak a fentiek maradnak. $\mathbb{F}_4$ fölött viszont $x^{16}-x$ az első- és másodfokú irreducibilisek szorzata, $x^2+x+1=(x+\alpha)(x+\alpha+1)$, és a fenti három negyedfokút kell két-két másodfokú szorzatára bontani. Végezetül egyszerű beszorzással adódik, hogy

$$\begin{aligned}(x^2+\alpha x+1)(x^2+(\alpha+1)x+1)&=x^4+x^3+x^2+x+1\\(x^2+\alpha x+\alpha)(x^2+(\alpha+1)x+\alpha+1)&=x^4+x^3+1\\(x^2+x+\alpha)(x^2+x+\alpha+1)&=x^4+x+1\ ,\end{aligned}$$

tehát az $\mathbb{F}_4$ fölötti felbontás

$$\begin{aligned}x^{16}-x=x(x+1)(x+\alpha)(x+\alpha+1)(x^2+\alpha x+1)(x^2+(\alpha+1)x+1)\cdot\\\cdot(x^2+\alpha x+\alpha)(x^2+(\alpha+1)x+\alpha+1)(x^2+x+\alpha)(x^2+x+\alpha+1)\ .\end{aligned}$$

6. Az egyik irány világos: ha $a=b^d$ valamely $d\mid n$-re, akkor $x^n-a=x^n-b^d=(x^{n/d}-b)(x^{n(d-1)/d}+\cdots+b^{d-1})$ felbomlik. A másik irányhoz tegyük fel, hogy $f(x)\mid x^n-a$ egy irreducibilis osztó, melyre $0<d:=\deg(f)<n$ és legyen $\zeta\in K$ egy primitív n-edik egységgyök. Jelöljük α-val az $f(x)$ polinom egyik gyökét a felbontási testben, ekkor nyilván $\alpha^n=a$ és f többi gyöke $\alpha\zeta^j$ alakú

alkalmas j egész számokkal. Speciálisan $K(\alpha)$ fölött f már $f(x)=\prod_{j\in J}(x-\alpha\zeta^j)$ gyöktényezős alakba írható alkalmas $J\subseteq\mathbb{Z}/n\mathbb{Z}$ halmazzal. Így $K(\alpha)/K$ egy Galois-bővítés, hiszen f egy szeparábilis polinom, melynek $K(\alpha)$ a felbontási teste. Mivel a Galois-csoport tranzitívan hat f gyökein, ezért minden $j\in J$-re van olyan $g_j\in\mathrm{Gal}(K(\alpha)/K)$, melyre $g_j(\alpha)=\alpha\zeta^j$. Viszont ha $k\in J$, akkor $g_j(\alpha\zeta^k)=g_j(\alpha)\zeta^k=\alpha\zeta^{j+k}$ (hiszen $\zeta\in K$ miatt $g_j(\zeta)=\zeta$) is gyöke f-nek. Speciálisan azt kaptuk, hogy ha $j,k\in J$, akkor $j+k\in J$, azaz J részcsoport $\mathbb{Z}/n\mathbb{Z}$-ben. Viszont ciklikus csoportnak egyetlen adott $|J|=d$-edrendű részcsoportja van (ha $d\mid n$, egyébként egy sincs), ezért $d\mid n$ és $J=\{0,n/d,\dots,n(d-1)/d\}$. Ekkor viszont a $\{\zeta^j\mid j\in J\}$ halmaz pontosan a d-edik egységgyökökből áll, és $f(x)=\prod_{j\in J}(x-\alpha\zeta^j)=x^d-\alpha^d\in K[x]$, azaz $a=(\alpha^d)^{\frac{n}{d}}$ egy n/d-edik hatvány K-ban az indirekt feltevéssel ellentétben. Ezzel a visszairányt is igazoltuk.

7. A $\mathbb{Q}(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\mathbb{Q}\}$ Galois-csoportja $\mathbb{Q}$ felett $Z_2\times Z_2$-vel izomorf, elemei $\mathrm{id},\sigma_1,\sigma_2,\sigma_3$ úgy, hogy σ_1 fixteste $\mathbb{Q}(\sqrt{2})$, σ_2 fixteste $\mathbb{Q}(\sqrt{3})$, $\sigma_3=\sigma_1\sigma_2$ fixteste pedig $\mathbb{Q}(\sqrt{6})$. Ha $\alpha=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ algebrai egész, akkor a Galois-konjugáltjai is azok. Továbbá az algebrai egészek gyűrűt alkotnak, ezért $\alpha+\sigma_1(\alpha)$, $\alpha+\sigma_2(\alpha)$, $\alpha+\sigma_3(\alpha)$, $\alpha\sigma_1(\alpha)$, $\alpha\sigma_2(\alpha)$, és $\alpha\sigma_3(\alpha)$ is algebrai egész – ezek vannak felsorolva a feladat szövegében: Pl. $\sigma_1(\alpha)=a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$, azaz $\alpha+\sigma_1(\alpha)=2a+2b\sqrt{2}$ és $\alpha\sigma_1(\alpha)=a^2+2b^2-3c^2-6d^2+(2ab-6cd)\sqrt{2}$. A feladat második részéhez azt kell észrevennünk, hogy $2,3$, és 6 négyzetmentes, és egyik sem ad 1-et maradékul 4-gyel osztva, ezért $\mathbb{Q}(\sqrt{d})$-ben az algebrai egészek halmaza $\mathbb{Z}+\mathbb{Z}\sqrt{d}$ $(d=2,3,6)$. Azt kaptuk, hogy az

$$a_1:=2a,\ b_1:=2b,\ c_1:=2c,\ d_1:=2d,$$
$$\frac{a_1^2+2b_1^2-3c_1^2-6d_1^2}{4}=a^2+2b^2-3c^2-6d^2,\quad \frac{2a_1b_1-6c_1d_1}{4}=2ab-6cd,$$
$$\frac{a_1^2-2b_1^2+3c_1^2-6d_1^2}{4}=a^2-2b^2+3c^2-6d^2,\quad \frac{2a_1c_1-4b_1d_1}{4}=2ac-4bd,$$
$$\frac{a_1^2-2b_1^2-3c_1^2+6d_1^2}{4}=a^2-2b^2-3c^2+6d^2,\quad \frac{2a_1d_1-2b_1c_1}{4}=2ad-2bc$$

számok mind egészek. Speciálisan $a_1+3c_1^2$ páros, azaz a_1 ás c_1 azonos paritásúak, viszont $4\mid 2a_1c_1-4b_1d_1$ miatt legalább az egyik páros, azaz mindkettő az. Tehát $a,c\in\mathbb{Z}$. Ugyanígy $b_1^2+3d_1^2$ páros, emiatt b_1 és d_1 azonos paritásúak. Ezzel (a)-t és a (c)-beli feltétel szükségességét megmutattuk. Másrészt $\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^2=\frac{8+4\sqrt{3}}{4}=2+\sqrt{3}$ algebrai egész, így $\frac{\sqrt{2}+\sqrt{6}}{2}$ is az. Speciálisan minden $a+b'\sqrt{2}+c\sqrt{3}+d'\frac{\sqrt{2}+\sqrt{6}}{2}$ alakú szám algebrai egész, ha $a,b',c,d'\in\mathbb{Z}$, ahol $b'=b-d$ és $d'=2d$ valóban egészek, ha b és d egész vagy mindkettő páratlan egész fele. Ezzel a megfordítást is igazoltuk.