Algebrai és transzcendens számok. Minimálpolinom. Testbővítés foka

1. *Írjuk fel* $\sqrt[26]{26}$ *minimálpolinomját. Mennyi a* $\sqrt[27]{27}$ *szám foka?*

Megoldás. $\sqrt[26]{26}$ kielégíti az $x^{26}-26$ polinomot, és mivel irreducibilis is (Schönemann–Eisenstein-kritérium $p=3$-mal vagy $p=13$-mal, ezért ez a minimálpolinom. Hasonlóan kaphatjuk az $x^{27}-27$ polinomot is, aminek meg $\sqrt[27]{27}$ lesz gyöke, de ez nem irreducibilis (nem is teljesül rá a SE-kritérium noha „nem ezért" nem irreducibilis): osztható (x^9-3)-mal. Ez utóbbi polinom viszont már irreducibilis (SE, $p=3$), és ennek is gyöke a $\sqrt[27]{27}$. Így ez lesz a minimálpolinom.

2. *Mennyi* $\sqrt[4]{2}$ *foka* $\mathbb{Q}$*, illetve* $\mathbb{Q}(\sqrt{8})$ *fölött?*

Megoldás. Legyen $\alpha=\sqrt{2}+\sqrt[4]{2}$. Ekkor $\alpha-\sqrt{2}=\sqrt[4]{2}$, és mindkét oldalt négyzetre emelve azt kapjuk, hogy $\alpha^2-2\alpha\sqrt{2}+2=\sqrt{2}$, vagyis $\sqrt{2}=\dfrac{\alpha^2+2}{1+2\alpha}$. Ez azt mutatja, hogy $\mathbb{Q}(\alpha)$-ban benne van $\sqrt{2}$ és így $\alpha-\sqrt{2}=\sqrt[4]{2}$ is. A bővítés foka tehát legalább 4, hiszen benne van a negyedfokú $\sqrt[4]{2}$ is. Ugyanakkor világos, hogy $\alpha\in\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})$, és ez utóbbi test két másodfokú bővítés egymásutánjaként negyedfokú bővítése $\mathbb{Q}$-nak. Az eddigiekből tehát: $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})$, és így α foka $\mathbb{Q}$ fölött 4, a $\mathbb{Q}(\sqrt{2})$ „köztes test" fölött viszont csak 2.

3. **a)** *Mutassuk meg, hogy* $\mathbb{Q}(\sqrt{6})\subseteq\mathbb{Q}(\sqrt{3},\sqrt{3}+\sqrt{2}+\sqrt{1})$.
b) *Igazoljuk, hogy* $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})=\mathbb{Q}(\sqrt[6]{2})$.

Megoldás. a) Elegendő azt megmutatnunk, hogy $\sqrt{6}\in\mathbb{Q}(\sqrt{3},\sqrt{3}+\sqrt{2}+\sqrt{1})$. De ez utóbbi testben nyilván benne van $\sqrt{3}$, majd $(\sqrt{3}+\sqrt{2}+\sqrt{1})-\sqrt{3}-1=\sqrt{2}$ is. Tehát ebben a testben benne van $\sqrt{2}\sqrt{3}=\sqrt{6}$ is.
b) Csak azt kell megmutatnunk, hogy mindkét test generátorelemei benne vannak a másik testben. De $\sqrt{2}=(\sqrt[6]{2})^3$ és $\sqrt[3]{2}=(\sqrt[6]{2})^2$, és így $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})\subseteq\mathbb{Q}(\sqrt[6]{2})$. Másrészt $\sqrt[6]{2}=\frac{2}{\sqrt[3]{2}\sqrt{2}}$, és így $\mathbb{Q}(\sqrt[6]{2})\subseteq\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$.

4. *Döntsük el, hogy* $\sqrt{3}$ *eleme-e a* $\mathbb{Q}(\sqrt{2})$ *testnek.*

Megoldás. Ha $\sqrt{3}$ eleme lenne a $\mathbb{Q}(\sqrt{2})=\left\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Q}\right\}$ testnek, akkor lenne olyan $a,b\in\mathbb{Q}$ szám, melyre $a+b\sqrt{2}=\sqrt{3}$. Nyilván $b\neq0$, hiszen ellenkező esetben $\sqrt{3}\in\mathbb{Q}$ teljesülne, ez viszont nem lehet igaz. Ha viszont $a=0$ lenne, akkor $b\sqrt{2}=\sqrt{3}$-ból $b=\frac{\sqrt{3}}{\sqrt{2}}$ teljesülne, ami a számelmélet alaptétele miatt ismét nem lehetséges: nincs olyan racionális szám, melynek egyszerűsített alakjából a négyzetre emelés után $\frac{3}{2}$-et kapnánk. Végezetül, ha $ab\neq0$, akkor az $a+b\sqrt{2}=\sqrt{3}$ egyenletet négyzetre emelve azt kapjuk, hogy $a^2+2ab\sqrt{2}+2b^2=3$, amiből azt kapnánk, hogy $\sqrt{2}=\frac{1}{2ab}\cdot(3-a^2-2)\in\mathbb{Q}$, tehát $\sqrt{2}$ racionális lenne. Ez nyilván ellentmondás.

5. *Igazoljuk, hogy* $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Megoldás. Mivel $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, ezért világos, hogy $\mathbb{Q}(\sqrt{2},\sqrt{3})\supseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Másrészt, ha használjuk az $\alpha=\sqrt{2}+\sqrt{3}$ jelölést, akkor $\alpha^2-2\alpha\sqrt{2}+2=3$, s ezért $\sqrt{2}\in\mathbb{Q}(\alpha)$. Ekkor azonban $\sqrt{3}$ is benne van a bővítésben. Ez azt jelenti, hogy $\mathbb{Q}(\sqrt{2}+\sqrt{3})\supseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$. Ez azt jelenti, hogy a két bővítés megegyezik.

6. *Mutassuk meg, hogy* $\sqrt[5]{5}$ *nem eleme a* $K=\mathbb{Q}(\sqrt[3]{3})$ *testnek. Mennyi a* $K(\sqrt[5]{5})$ *testbővítés foka* K*, illetve* $\mathbb{Q}$ *fölött?*

Megoldás. Tudjuk, hogy ha S és T testek, $S\leq T$, és $\alpha\in T$, akkor $\deg_S\alpha\,||T:S|$, hiszen a fokszámtétel alkalmazható az $S\leq S(\alpha)\leq T$ bővítésláncra: eszerint $\deg_S\alpha\cdot|T:S(\alpha)|=|T:S|$. Ez azt jelenti, hogy $K=\mathbb{Q}(\sqrt[3]{2})$, aminek a foka 3 a $\mathbb{Q}$ fölött, nem tartalmazhat $\mathbb{Q}$ fölött ötödfokú elemet, mint amilyen pl. $\sqrt[5]{5}$. (Hasonlóképpen igaz, hogy $\sqrt[3]{3}$ sem eleme a $\mathbb{Q}(\sqrt[5]{5})$ testnek.) Ebből az is következik, hogy a $K(\sqrt[5]{5})=\mathbb{Q}(\sqrt[3]{3})(\sqrt[5]{5})$ test, amely tartalmazza mind $\sqrt[3]{3}$-at, mind $\sqrt[5]{5}$-öt, azaz tartalmaz $\mathbb{Q}$ fölött 3-adfokú és 5-ödfokú elemet is, legalább 15-ödfokú $\mathbb{Q}$ fölött. Ugyanakkor, persze, $\left|K(\sqrt[5]{5}):K\right|\leq5$, így a szorzástételt alkalmazva a $\mathbb{Q}\leq K=\mathbb{Q}(\sqrt[3]{3})\leq K(\sqrt[5]{5})=\mathbb{Q}(\sqrt[3]{3})(\sqrt[5]{5})$ bővítésláncra azt kapjuk, hogy egyrészt $\left|\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}\right|\cdot\left|\mathbb{Q}(\sqrt[3]{5})(\sqrt[5]{5}):\mathbb{Q}(\sqrt[3]{3})\right|\leq3\cdot5=15$, másrészt ez a szorzat egyenlő a $\left|\mathbb{Q}(\sqrt[3]{3})(\sqrt[5]{5}):\mathbb{Q}\right|$ fokkal, ami legalább 15. Ez azt jelenti, hogy $\sqrt[5]{5}$ foka K fölött pontosan 5 (azaz nincs „új", alacsonyabb fokú polinom K fölött, aminek $\sqrt[5]{5}$ gyöke lenne, marad a $\mathbb{Q}$ fölötti minimálpolinom, azaz x^5-5).

7. **a)** *Mutassuk meg, hogy ha α n-edfokú algebrai szám, akkor $\sqrt[k]{\alpha}$ is algebrai szám, melynek foka legfeljebb nk.*

b) *Mutassunk példát $\alpha \notin \mathbb{Q}$ algebrai számra, amelyre* $\deg\sqrt{\alpha} = 2\deg\alpha$*, és olyanra is, amelyre* $\deg\sqrt{\alpha} = \deg\alpha$*.*

Megoldás. a) Ha α gyöke az $f(x) \in \mathbb{Q}[x]$ polinomnak, akkor $\sqrt[k]{n}$ gyöke a $g(x) = f(x^k) \in \mathbb{Q}[x]$ polinomnak, aminek a foka $\deg g = k \cdot \deg f$. Ez igazolja a kívánt összefüggést.
b) $\alpha = 2$ esetén $\deg\sqrt{2} = 2\sqrt{2}\deg 2$, ugyanakkor $\alpha = 4$-re $\deg\sqrt{4} = 1 = \deg 4$.

8. *Igazoljuk, hogy π^2, $\pi + 1$ és $\sqrt{\pi}$ is transzcendens szám.*

Megoldás. Ha π^2 algebrai lenne, akkor az előző feladat értelmében $\pi = \sqrt{\pi^2}$ is algebrai lenne, ami viszont nem igaz. Ugyanakkor, ha $\sqrt{\pi}$ algebrai lenne, akkor algebrai lenne a négyzete, azaz π is, ugyanis tudjuk, hogy az algebrai számok négyzete is algebrai (hiszen pl. az algebrai számok testet alkotnak). (*Megjegyzés:* Érdekesség, hogy az algebra számok halmazának a gyökvonásra való zártságát az előző feladat módszerével könnyebb igazolni, mint azt, hogy zárt az összeadásra és a szorzásra: ehhez kellett az egyszerű algebrai bővítések jellemzése a bővítés fokával.) Végezetül, ha $\pi + 1$ algebrai lenne, azaz gyöke egy $f(x) \in \mathbb{Q}[x]$ polinomnak, akkor π gyöke lenne a $g(x) = f(x+1)$ polinomnak, vagyis algebrai lenne. (Itt is hivatkozhatnánk arra, hogy az algebrai számok teste alkotnak, tehát ha $\pi + 1$ algebrai, akkor $(\pi + 1) - 1 = \pi$ is algebrai, hiszen 1 nyilvánvalóan algebrai.) – Lásd még a következő feladatot is!

9. **a)** *Igazoljuk, hogy egy algebrai és egy transzcendens szám összege mindig traszcendens szám.*

b) *Mikor lesz egy algebrai és egy transzcendens szám szorzata algebrai?*

Megoldás. a) Tudjuk, hogy az algebrai számok halmaza zárt az összeadásra, kivonásra, szorzásra és osztásra (sőt, még a gyökvonásra is). Ha α algebrai, τ pedig transzcendens, akkor $\alpha + \tau$ nem lehet algebrai, mert ellenkező esetben $(\alpha + \tau) - \alpha = \tau$ is algebrai lenne.
b) Az előző okoskodás majdnem elmondható egy algebrai és egy transzcendens szám szorzatára is: ha $\alpha\tau$ algebrai lenne, akkor $(\alpha\tau)/\alpha = \tau$ is algebrai lenne. A levezetéssel egyetlen esetben van gond: ha α-nak nincs reciproka, azaz $\alpha = 0$. Ilyenkor viszont valóban $\alpha\tau = 0\tau = 0$ algebrai.

10. *Legyen α az $x^3 + 3x + 1 = 0$ egyenlet egyik gyöke. Mi az α minimálpolinomja $\mathbb{Q}$ fölött? Írjuk fel $\alpha^2 + 1$ négyzetét és inverzét is $a\alpha^2 + b\alpha + c$ alakban alkalmas a, b, c racionális számokkal. Keressük meg $\alpha^2 + 1$ minimálpolinomját $\mathbb{Q}$ fölött.*

Megoldás. A megadott polinom irreducibilis $\mathbb{Q}$ fölött, mivel a racionális gyökteszt alapján nincs neki racionális gyöke, tehát nincs elsőfokú faktora. Ez azt jelenti, hogy α minimálpolinomja az x^3+3x+1. Vegyük észre, hogy most (más, korábbi feladatoktól eltérően, amikor pl. $\sqrt[5]{5}$ típusú számokkal kellett számolnunk) α-ról nincs más információnk, csak annyi, hogy gyöke a megadott polinomnak. A három gyök közül nem is tudjuk, melyikkel számolunk éppen („ugyanúgy kell számolni" mindhárommal!), de egy csomó mindent ki tudunk számolni (legalábbis α-val kifejezve). A legfontosabb eszköz a kezünkben az az összefüggés lesz, hogy $\alpha^3 + 3\alpha + 1 = 0$, azaz pl. $\alpha^3 = -3\alpha - 1$, továbbá $\alpha^4 = -3\alpha^2 - \alpha$. Így tehát

$$(\alpha^2 + 1)^2 = \alpha^4 + 2\alpha^2 + 1 = (-3\alpha^2 - \alpha) + 2\alpha^2 + 1 = -\alpha^2 - \alpha + 1.$$

A reciprokot a már jól ismert módszerrel számolhatjuk ki:

$$\begin{gathered}(\alpha^2 + 1)(a\alpha^2 + b\alpha + c) = 1\\ a\alpha^4 + b\alpha^3 + (a + c)\alpha^2 + b\alpha + c = 1\\ a(-3\alpha^2 - \alpha) + b(-3\alpha - 1) + (a + c)\alpha^2 + b\alpha + c = 1\\ (-2a + c)\alpha^2 + (-a - 2b)\alpha + (-b + c) = 1\end{gathered}$$

Az α-hatványok együtthatóit összehasonlítva azt kapjuk, hogy $-2a + c = 0$, $(-a - 2b) = 0$, és $-b + c = 1$. Ebből: $a = 2/5$, $b = -1/5$, $c = 4/5$, vagyis:

$$(\alpha^2 + 1)^{-1} = (2/5)\alpha^2 + (-1/5)\alpha + (4/5).$$

A $\beta = \alpha^2 + 1$ minimálpolinomjának a kiszámolásánál azt használjuk ki, hogy $1, \beta, \beta^2, \beta^3$ biztosan lineáriasan összefüggők, hiszen egy háromdimenziós vektortérnek az elemei. (Vagy, ha az eddig kiszámoltakat szeretnénk kihasználni, akkor a $\beta^2, \beta, 1, \beta^{-1}$ összefüggőségét is használhatnánk. De a tört együtthatók miatt mégis inkább β^3-bel jó számolni.) β^2-et már fölírtuk, maradt még, hogy kiszámoljuk β^3-öt α polinomjaként. Ehhez használjuk a β^2-re, illetve az α^3-re és az α^4-re korábban kapott kifejezéseket.

$$\begin{aligned}\beta^3 = (\alpha^2+1)^2(\alpha^2+1) = (-\alpha^2-\alpha+1)(\alpha^2+1) = -\alpha^4-\alpha^3+\alpha^2-\alpha^2-\alpha+1 = \\ = (3\alpha^2+\alpha)+(3\alpha+1)-\alpha+1 = 3\alpha^2+3\alpha+2\end{aligned}$$

Valójában azt is tudjuk, hogy β nem racionális (ellenkező esetben α legföljebb másodfokú lenne), továbbá hogy $\beta \in \mathbb{Q}(\alpha)$, tehát a foka osztja $|\mathbb{Q}(\alpha : \mathbb{Q}| = 3$-at, ezért azt kapjuk, hogy β harmadfokú, azaz gyöke lesz egy pontosan harmadfok polinomnak, aminek a főegyütthatója 1. Így tehát a következő lineáris egyenletet kell megoldanunk:

$$\begin{gathered}\beta^3 + x\beta^2 + y\beta + z = 0, \quad \text{azaz:} \\ (3\alpha^2+3\alpha+2) + x(-\alpha^2-\alpha+1) + y(\alpha^2+1) + z = 0, \quad \text{azaz:} \\ (3-x+y)\alpha^2 + (3-x)\alpha + (2+x+y+z) = 0\end{gathered}$$

Mivel az α^2, α és 1 lineárisan függetlenek, ezért ez utóbbi egyenlet csak úgy teljesülhet, ha minden együtthatója 0, vagyis az alábbi lineáris egyenletrendszert kapjuk:

$$\begin{array}{rcrcrcr} x & - & y & & & = & 3 \\ x & & & & & = & 3 \\ x & + & y & + & z & = & -2 \end{array}$$

Ebből: $x = 3$, $y = 0$ és $z = -5$ adódik. Mivel a megoldás egyértelmű, így azt kapjuk, hogy β egyetlen normált harmadfokú polinomnak gyöke: $m(x) = x^3 + 3x^2 - 5$, vagyis ez $\beta = \alpha^2 + 1$ minimálpolinomja.

11. **a)** *Legyen ε primitív 5-ödik egységgyök. Mivel egyenlő $|\mathbb{Q}(\varepsilon) : \mathbb{Q}|$?*
b) *Igazoljuk, hogy ha ε primitív 5-ödik egységgyök, akkor $-\varepsilon$ primitív 10-edik egységgyök.*
c) *Számítsuk ki ennek alapján a 10-edik körosztási polinomot.*

Megoldás. **a)** A bővítés foka megegyezik ε minimálpolinomjának a fokával, azaz $\deg \Phi_5$-tel, ami $\varphi(5)$-tel egyenlő (az ötödik körosztási polinom, mint tudjuk, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$).)
b) Ha ε ötödik egységgyök, akkor $\varepsilon^5 = 1$, és így $(-\varepsilon)^{10} = 1$. Ez viszont azt jelenti, hogy $-\varepsilon$ rendje 10-nek osztója. De 5 nem lehet, mert $(-\varepsilon)^5 = (-1)^5\varepsilon^5 = -1$. És nem lehet 2 sem a rend, mert ha $(-\varepsilon)^2 = 1$, akkor $\varepsilon^2 = 1$ is teljesülne, ami nem lehet. Ez tehát azt jelenti, hogy $-\varepsilon$ primitív 10-edik egységgyök. Mivel ezek száma $\varphi(10) = 4 = \varphi(5)$, ezért ily módon minden prmitív 10-edik egységgyököt megkapunk. (*Megjegyzés:* Az előbbi gondolatmenetet egy kicsit ügyesebben csinálva azt is megkaphatnánk, hogy ε és $-\varepsilon$ rendje legfeljebb egy 2-es faktorban térhet el; s ha ε rendje egy pártalan n szám, akkor pontosan a $-\varepsilon$ alakú számok lesznek a $2n$-edik primitív egységgyökök.)
c) Az előző két rész alapján $\Phi_{10}(x) = \Phi_5(-x) = x^4 - x^3 + x^2 - x + 1$. Ezt egyébként közvetlen számolással is ellenőrizhetjük. (*Megjegyzés:* Az előbbi általánosítás miatt az is igaz, hogy ha n páratlan, akkor $\Phi_{2n}(x) = \Phi_n(-x)$.)

12. *Legyen ε primitív 17-edik egységgyök és legyen $\lambda = 1-\varepsilon$. Igazoljuk, hogy az $1, \lambda, \lambda^2, \ldots, \lambda^{15}$ számok lineárisan függetlenek $\mathbb{Q}$ fölött, $1, \lambda, \lambda^2, \ldots, \lambda^{16}$ viszont összefüggők.*

Megoldás. Könnyű látni, hogy $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\lambda)$, és ezért $\deg_{\mathbb{Q}} \varepsilon = \deg_{\mathbb{Q}} \lambda = 16$, hiszen ε minimálpolinomja a 17-edik körosztási polinom, $\Phi_{17}(x)$, aminek a foka $\varphi(17) = 16$. Ez viszont azt jelenti, hogy λ-nak az első tizenhat hatványa lineárisan független (hiszen λ nem gyöke egyetlen legföljebb 15-ödfokú nem nulla polinomnak sem), ugyanakkor λ^{16} kifejezhető a kisebb (nemnegatív) kitevős hatványokkal, tehát $1, \lambda, \ldots, \lambda^{16}$ már lineárisan összefüggők.