**Irreducibilitás véges testek fölött. Algebrai és transzcendens elemek. Minimmálpolinom**

**1.** *Keressük meg $\mathbb{Z}_2[x]$-ben a negyedfokú irreducibilis polinomokat, a többit pedig bontsuk fel irreducibilisek szorzatára.*

**Megoldás.** Tudjuk, hogy tetszőleges test fölött a legföljebb harmadfokú polinomok között irreducibilisek az elsőfokúak, valamint azon másod- és harmadfokúak, melyeknek nincs gyöke az alaptestben. $\mathbb{Z}_2$ fölött pedig egyszerű ellenőrizni, hogy egy polinomnak van-e gyöke: a 0 pontosan akkor gyök, ha a konstans tagja a polinomnak 0, az 1 pedig pontosan akkor gyök, ha a polinomnak páros sok nem nulla együtthatója van. Ez azt jelenti, hogy a legföljebb harmadfokú irreducibiis polinomok az alábbiak: $x$, $x+1$, $x^2+x+1$, $x^3+x+1$, $x^3+x^2+1$. A negyedfokú irreducibilis polinomok esetén a gyök megléte továbbra is „tilos", de ez most már nem elegendő az irreducibilitáshoz: még azt is ki kell zárnunk, hogy a polinom két irreducibilis másodfokú polinom szorzatára bomoljon. Ez azt jelenti, hogy a gyöktelen negyedfokú polinomok közül ki kell még zárnunk az $(x^2+x+1)^2 = x^4+x^2+1$ polinomot is mint aminek létezik nem triviális faktorizációja. Az irreducibilisek tehát: $x^4+x+1$, $x^4+x^3+1$, $s^4+x^3+x^2+x+1$. Az alábbi táblázatban találhatjuk a 16 darab negyedfokú polinom faktorizációját:

| | | | |
|---|---|---|---|
| $x^4$ | $= x^4$ | $x^4+1$ | $= (x+1)^4$ |
| $x^4+x$ | $= x\cdot(x+1)\cdot(x^2+x+1)$ | $\boxed{x^4+x+1}$ | |
| $x^4+x^2$ | $= x^2\cdot(x+1)^2$ | $x^4+x^2+1$ | $= (x^2+x+1)^2$ |
| $x^4+x^2+x$ | $= x\cdot(x^3+x+1)$ | $x^4+x^2+x+1$ | $= (x+1)\cdot(x^3+x^2+1)$ |
| $x^4+x^3$ | $= x^3\cdot(x+1)$ | $\boxed{x^4+x^3+1}$ | |
| $x^4+x^3+x$ | $= x\cdot(x^3+x^2+1)$ | $x^4+x^3+x+1$ | $= (x+1)^2\cdot(x^2+x+1)$ |
| $x^4+x^3+x^2$ | $= x^2\cdot(x^2+x+1)$ | $x^4+x^3+x^2+1$ | $= (x+1)\cdot(x^3+x+1)$ |
| $x^4+x^3+x^2+x$ | $= x\cdot(x+1)^3$ | $\boxed{x^4+x^3+x^2+x+1}$ | |

**2.** *Hány ötödfokú polinom van $\mathbb{Z}_2[x]$ fölött, és ezek közül hány lesz irreducibilis?*

**Megoldás.** A $\mathbb{Z}_2[x]$-beli ötödfokú polinomok száma $2^5$ (hiszen a főegyüttható mindenképpen 1, a többi együtthatóra pedig 2 választásunk van). Ezek közül azok lesznek ireducibilisek (lásd még az előző feladat megoldását), amelyeknek: a) nincs gyökük, tehát a konstans tagjuk 1, továbbá a fügyütthatón és a konstans tagon kívül páratlan sok (1 vagy 3) együttható nem nulla – ilyenből van $\binom{4}{1}+\binom{4}{3}=8$; b) nem bomlanak egy másodfokú és egy harmadfokú irreducibilis polinom szorzatára – olyanból, ami fölbomlik, van összesen 2 darab, hiszen 1 másodfokú és 2 harmadfokú irreducibilis polinomunk van. Ez azt jelenti, hogy összesen van 6 darab ötödfokú irreducibilis polinomunk $\mathbb{Z}_2[x]$-ben. – Ezt a későbbiekben a testbővítések elméletét fölhasználva egyszerűbben is kiszámolhatjuk.

**3.** *Jelöljön $p$ egy prímszámot. Adott $f\in\mathbb{Z}[x]$ polinomhoz képezzük az $\overline{f}\in\mathbb{Z}_p[x]$ polinomot úgy, hogy $f$ minden együtthatóját helyettesítjük az általa reprezentált modulo $p$ maradékosztállyal. Ily módon egy $\mathbb{Z}[x]\to\mathbb{Z}_p[x]$ művelettartó leképezést kapunk.*

**a)** *Mutassuk meg, hogy ha $\deg\overline{f}=\deg f$ és $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött, akkor $f$ irreducibilis $\mathbb{Q}$ fölött. $\mathbb{Z}$ fölött is biztosan az lesz?*

**b)** *Mutassunk példát olyan $f\in\mathbb{Z}[x]$ polinomra, melyre $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött, de $f$ nem irreducibilis $\mathbb{Q}$ fölött.*

**Megoldás.** **a)** Ha $\overline{f}$ nem lenne irreducibilis $\mathbb{Q}[x]$-ben, akkor két alacsonyabb fokú polinom szorzatára bomlana, és a második Gauss-lemma alapján ezek választhatók egész együtthatósnak is: $f=g\cdot h$, és $g,h\in\mathbb{Z}[x]$, $\deg g,\deg h<\deg f$. Mivel $\deg\overline{p}\le\deg p$ általában teljesül minden polinomra, és most $\deg f=\deg\overline{f}$, ezért $\deg g=\deg\overline{g}$, és $\deg h=\deg\overline{h}$. Ez viszont azt jelentené, hogy $\deg\overline{f}$-nek van egy nem trviális

fölbontása, azaz deg $\overline{f}$ nem irredicibilis $\mathbb{Z}_p[x]$-ben. Ilyenkor tehát $\overline{f}(x)$ sem irreducibiis $\mathbb{Z}_p[x]$-ben, vagyis ha eredetileg irreducibilis $\mathbb{Z}_p[x]$-ben, akkor $\mathbb{Q}[x]$-ben is az. – A $\mathbb{Z}$ fölötti irreducibilitás nem következik, mert skalár konstans mindig kiemelhető lehet: pl. $2x+2$ irreducibilis $\mathbb{Z}_3[x]$-ben, de $\mathbb{Z}$ fölött kiemelhető belőle a 2.
**b)** Az előző rész alapján olyan példát kell megadnunk, amelynél a fokszámfeltétel nem teljesül, vagyis a $\mathbb{Z}[x]$-beli $f$ polinom főegyüttható oszthatóa $p$-vel, és így $\overline{f} \in \mathbb{Z}_p[x]$-ben a polinom alacsonyabb fokú lesz, és irreducibilissé válik, mert pl. elsőfokú. Így pl. $f(x) = 2x^2 + x \in \mathbb{Z}[x]$ nyilván nem irreducibilis $\mathbb{Q}[x]$-ben, mert a 0 gyöke neki, de $\overline{f} = x \in \mathbb{Z}_2[x]$, és mint elsőfokú polinom, irreducibilis.

**4.** *Mutassuk meg, hogy a $3x^4 + 4x^3 + 6x^2 + 7x + 9$ polinom irreducibilis $\mathbb{Q}$ és $\mathbb{Z}$ fölött.*

**Megoldás.** $\mathbb{Z}_2$ fölött nézve a polinom együtthatóit, az $x^4 + x + 1$ polinomot kapjuk. Ez viszont pl, az 1. feladat alapján irreducibilis $\mathbb{Z}[x]$-ben. Az előző feladat a) része értelmében tehát az eredeti polinomunk irreducibilis $\mathbb{Q}$ fölött, és mivel primitív is, ezért $\mathbb{Z}$ fölött is irreducibilis lesz.

**5.** *Legyen $f = \Phi_p$. Mely $p$ prímekre igaz, hogy $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött?*

**Megoldás.** $p = 2$-re $x + 1$ irreducibilis $\mathbb{Z}_2[x]$-ben. Ugyanakkor $\Phi_p(x) \,|\, (x^p - 1)$ teljesül $\mathbb{Z}[x]$-ben, és ekkor ez az oszthatóság modulo $p$ is fönnáll. De $\mathbb{Z}_p[x]$-ben $x^p - 1 = (x - 1)^p$, és ez azt jelenti, hogy $\Phi_p(x)$ is gyöktényezők szorzatára bomlik $\mathbb{Z}_p[x]$-ben. Mivel $p > 2$ esetén $\deg \Phi_p(x) = \varphi(p) = p - 1 > 1$, ezért $\Phi_p(x)$ soha nem lesz irreducibilis $p > 2$ esetén.

**6.** *Legyen $\alpha \in \mathbb{C}$, $f$ pedig olyan $\mathbb{Q}$ fölötti irreducibilis polinom, amelynek $\alpha$ gyöke. Mutassuk meg, hogy létezik $0 \neq c \in \mathbb{Q}$, amelyre $cf$ éppen az $\alpha$ minimálpolinomja.*

**Megoldás.** Ha $f(\alpha) = 0$, akkor $\alpha$ minimálpolinomja, $m_\alpha$ osztója $f$-nek. De $f$ irreducibilis, tehát csak a nem nulla konstansok és önmaga egységszeresei lesznek az osztói. Mivel a nem nulla konstansoknak nincs gyöke, ezért $m_\alpha = cf$ valamilyen $c \in \mathbb{C}$-re. (Nyilván $c = 1/a$, ahol $a$ az $f$ polinom főegyüttható.)

**7.** *Az alábbiak közül melyik polinom minimálpolinomja valamely algebrai számnak?*
**a)** $x^3 + 2x + 3$ **b)** $x^3 + 3x + 3$ **c)** $3x^3 + 3x + 1$

**Megoldás. a)** A polinomnak a $-1$ gyöke, ezért nem irreducibilis (hiszen osztható $(x + 1)$-gyel), tehát nem lehet minimálpolinomja egyetlen algebrai számnak sem.
**b)** A polinom irreducibilis (pl. a racionális gyökteszttel igazolhatjuk, hogy nincs neki elsőfokú faktora, de még természetesebb használni a Schönemann–Eisenstein-kritériumot $p = 3$-mal), így ha $\alpha \in \mathbb{C}$ az egyik komplex gyöke a polinomnak (ilyen van!), akkor ennek a számnak minimálpolinomja lesz.
**c)** Ez a polinom kielégíti a fordított Schönemann–Eisenstein-kritériumot, és ezért irreducibilis. Ugyanakkor nem 1 a főegyüttható, így az általunk használt definíció alapján nem lehet minimálpolinom. (A gyakorlaton szerepelt, hogy a normáltságot nem mindenhol követelik meg: ilyenkor a mininmálpolinom csak konstans szorzó erejéig egyértelmű. Ez utóbbi értelmezésben ez a polinom is minimálpolinomja a gyökeinek, hiszen irreducibilis.)

**8.** **a)** *Mutassuk meg, hogy ha $\alpha$ algebrai szám, akkor $-\alpha$ és $\sqrt{\alpha}$ is az.*
**b)** *Igazoljuk, hogy $\pi^2$ transzcendens szám.*
**c)** *Ha $\alpha$ minimálpolinomja $x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a + 0$, akkor mi a $-\alpha$ minimálpolinomja?*

**Megoldás. a)** Ha $\alpha$ gyöke egy $f(x)$ polinomnak, akkor $-\alpha$ gyöke a $g(x) = f(-x)$ polinomnak, $\sqrt{\alpha}$ pedig gyöke a $h(x) = f(x^2)$ polinomnak, tehát mindketten algebraiak.
**b)** Az előbbiek szerint, ha $\pi^2$ algebrai lenne, akkor $\sqrt{\pi^2} = \pi$ is algebrai lenne, ami viszont nem igaz.
**c** Az a) részben láttuk, hogy ha $\alpha$ gyöke az $f(x)$ polinomnak, akkor $-\alpha$ gyöke a $g(x) = f(-x)$ polinomnak. Sőt, a szimmetria miatt az összefüggés nyilván odavissza igaz. Ha tehát $\alpha$ minimálpolinomja $m_\alpha(x)$, akkor $-\alpha$ minimálpolinomja $m_{-\alpha}(x) = (-1)^n m_\alpha(-x)$. (A konstans szorzóra csak azért van szükség, hogy a főegyüttható 1 maradjon.)

**9.** *Írjuk fel $\sqrt[3]{3}$ minimálpolinomját.*

**Megoldás.** $m_{\sqrt[3]{3}}(x) = x^3 - 3$. Ennek a polinomnak nyilván gyöke a $\sqrt[3]{3}$, másrészt a polinom irreducibilis (pl. a Schönemann–Eisenstein-kritérium miatt), és így minimálpolinomja minden gyökének.

**10.** **a)** *Hozzuk egyszerűbb alakra az $(1 + 2\sqrt[3]{2} + 3\sqrt[3]{4})(3 + 2\sqrt[3]{2} + \sqrt[3]{4})$ kifejezést.*
**b)** *Keressük meg $1 + 2\sqrt[3]{2} + 3\sqrt[3]{4}$ inverzét $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ alakban, ahol $a, b, c$ racionális számok.*

**Megoldás. a)** Az „egyszerűbb alak" azt fogja jelenteni, hogy az eredményt $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ alakban írjuk föl. Ehhez kihasználjuk, hogy $\sqrt[3]{2}$ magasabb kitevős hatványaiban $\sqrt[3]{2^3} = 2$, azaz a magas kitevős hatányoknál „beváltjuk" $\sqrt[3]{8}$-at 2-re. Így tehát:

$$(1 + 2\sqrt[3]{2} + 3\sqrt[3]{4})(3 + 2\sqrt[3]{2} + \sqrt[3]{4}) = (3 + 2\sqrt[3]{2} + \sqrt[3]{4}) + (6\sqrt[3]{2} + 4\sqrt[3]{4} + 4) + (9\sqrt[3]{4} + 12 + 6\sqrt[3]{2}) = \\ = 19 + 14\sqrt[3]{2} + 14\sqrt[3]{4}$$

**b)** Itt azt használjuk ki, hogy tudjuk: $1 + 2\sqrt[3]{2} + 3\sqrt[3]{4} \neq 0$, tehát a reciproka létezik, és benne van a $\mathbb{Q}$-nak $\sqrt[3]{2}$-vel vett bővítésében, így – miként a bővítés tetszőleges eleme is – a reciprok is $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ alakban írható (méghozzá egyértelműen). Így, ha fölírjuk a reciprokot definiáló egyenletet, és megoldjuk a belőle fakadó egyenletrendszert, akkor megkapjuk a reciprok előállítását. Menetközben biztosak lehetünk abban, hogy az egyenletrendszernek van megodása. Az egyenletrendszer egyébként abból adódik, hogy az 1, $\sqrt[3]{2}$ és $\sqrt[3]{4}$ lineárisan függetlenek $\mathbb{Q}$ fölött, így minden előállítható elem egyértelműen áll elő:

$$(1 + 2\sqrt[3]{2} + 3\sqrt[3]{4}) \cdot (a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 1 \quad \Longleftrightarrow$$
$$(a + 6b + 4c) + (2a + b + 6c)\sqrt[3]{2} + (3a + 2b + c)\sqrt[3]{4} = 1 \quad \Longleftrightarrow$$
$$\begin{bmatrix} 1a & + & 6b & + & 4c & = & 1 \\ 2a & + & b & + & 6c & = & 0 \\ 3a & + & 2b & + & c & = & 0 \end{bmatrix}$$

Ez utóbbi lineáris egyenletrendszernek a (nem túl szép) megoldása: $a = -11/89$, $b = 16/89$, $c = 1/89$.

**11.** *Legyen $\varepsilon$ primitív 5-ödik egységgyök.*
**a)** *Írjunk fel olyan negyedfokú $\mathbb{Q}$ fölött irreducibilis polinomot, amelynek $\varepsilon$ gyöke.*
**b)** *Írjuk fel az $\varepsilon^4$ és az $(1 + \varepsilon)^{-1}$ számokat $a\varepsilon^3 + b\varepsilon^2 + c\varepsilon + d$ alakban, ahol $a, b, c, d \in \mathbb{Q}$.*

**Megoldás. a)** A primitív $n$-edik egységgyökök minimálpolinomja az $n$-edik körosztási polinom, így $\varepsilon$ minimálpolinomja $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$. Ez pont a keresett polinom, mivel negyedfokú és irreducibilis.
**b)** Használjuk $\varepsilon$ minimálpolinomját: $\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0$, ezért $\varepsilon^4 = -\varepsilon^3 - \varepsilon^2 - \varepsilon - 1$. Ami $1 + \varepsilon$ reciprokát illet, használhatjuk az előző feladatban alkalmazott módszert, és fölírhatjuk a megfelelő lineáris egyenletrendszert. Mi azonban most egy másik, gyorsabb eljárást alkalmazunk: a gyöktelenítést. Tudjuk ugyanis, hogy $(1 + \varepsilon^5) = (1 + \varepsilon)(1 - \varepsilon + \varepsilon^2 - \varepsilon^3 + \varepsilon^4)$. Ez azt jelenti, hogy:

$$\frac{1}{1+\varepsilon} = \frac{1}{1+\varepsilon} \cdot \frac{1 - \varepsilon + \varepsilon^2 - \varepsilon^3 + \varepsilon^4}{1 - \varepsilon + \varepsilon^2 - \varepsilon^3 + \varepsilon^4} = \frac{1 - \varepsilon + \varepsilon^2 - \varepsilon^3 + \varepsilon^4}{1 + \varepsilon^5} = \frac{1}{2}(1 - \varepsilon + \varepsilon^2 - \varepsilon^3 + \varepsilon^4).$$

Itt tehát azt használtuk ki a nevezőben, hogy $\varepsilon^5 = 1$. Ez még nem tökéletes alak, mert van egy meg nem engedett tagunk, az $\varepsilon^4$. De ezt helyettesíthetjük azzal a kifejezéssel, amit a rész elején kaptunk $\varepsilon^4$-re:

$$\frac{1}{1+\varepsilon} = \frac{1}{2}(1 - \varepsilon + \varepsilon^2 - \varepsilon^3 + \varepsilon^4) = -\varepsilon - \varepsilon^3.$$

A szokatlanul szép eredményt ellenőrizhetjük beszorzással: $(1 + \varepsilon)(-\varepsilon - \varepsilon^3) = -\varepsilon - \varepsilon^2 - \varepsilon^3 - \varepsilon^4 = 1$, amint azt az $\varepsilon$ minimálpolinomjából tudjuk.