Gyakorló feladatok

1. *Hány irreducibilis tényező szorzatára bomlik az $f(x) = -6x^3 + 6x^2 - 12$ polinom $\mathbb{Q}[x]$-ben, $\mathbb{Z}[x]$-ben, $\mathbb{R}[x]$-ben, illetve $\mathbb{C}[x]$-ben?*

Megoldás: A -6 kiemelése után racionális gyököket keresve megtaláljuk a -1-et, így az $f(x) = -6(x+1)(x^2-2x+2)$ felbontást kapjuk. Ez $\mathbb{Q}[x]$-ben és $\mathbb{R}[x]$-ben is irreducibilisekre bontás, mert az $x^2 - 2x + 2$ másodfokú polinomnak nincs valós gyöke. Itt a -6 egység, tehát bármelyik tényezőhöz hozzárakható, ezért $f(x)$ két irreducibilis tényező szorzatára bomlik $\mathbb{Q}[x]$-ben és $\mathbb{R}[x]$-ben is. $\mathbb{Z}[x]$-ben csak ± 1 az egységek, így a 6-ot is faktorizálni kell: $f(x) = -2 \cdot 3(x + 1)(x^2 - 2x + 2)$ négy irreducibilis tényező szorzata. Végül $\mathbb{C}$ fölött az összes gyököt kiszámolva az $f(x) = -6(x + 1)(x - 1 - i)(x - 1 + i)$ felbontást kapjuk $\mathbb{C}[x]$-ben, ahol három irreducibilis tényező szerepel.

2. *Határozzuk meg az $f(x) = -6x^3 + 6x^2 - 12$ és a $g(x) = 3x^2 - 3x - 6$ polinomok legnagyobb (azaz kitüntetett) közös osztóját $\mathbb{Q}[x]$-ben és $\mathbb{Z}[x]$-ben!*

Megoldás: Mivel $f(x)$-et már az előbb faktorizáltuk, és $g(x)$-et is könnyű irreducibilis tényezőkre bontani: $g(x) = 3(x - 2)(x + 1)$, a legnagyobb közös osztót itt érdemes a közös irreducibilis tényezők szorzataként meghatározni. Ez $\mathbb{Q}[x]$-ben $x + 1$, $\mathbb{Z}[x]$-ben $3(x + 1)$.

3. *Irreducibilis-e az $f(x) = x^4 - 6x^3 + 9x^2 + 3$ polinom $\mathbb{R}$ fölött, $\mathbb{Q}$ fölött és $\mathbb{Z}_2$ fölött?*

Megoldás: $\mathbb{R}$ fölött nyilván nem, mert $\mathbb{R}[x]$-ben minden irreducibilis polinom első vagy másodfokú. $\mathbb{Q}[x]$-ben irreducibilis a Schönemann–Eisenstein-kritérium alapján ($p = 3$-mal). $\mathbb{Z}_2[x]$-ben $f(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$ nem irreducibilis.

4. *Bontsuk fel a*

$$2x^6 - x^5 - 9x^4 + 4x^3 - 6x^2 + 5x + 5$$

polinomot irreducibilis polinomok szorzatára $\mathbb{Q}[x]$-ben és $\mathbb{Z}_5[x]$-ben!

Megoldás: A racionális gyökteszt alapján a polinom lehetséges racionális gyökei ± 1 ± 5, $\pm\frac{1}{2}$, $\pm\frac{5}{2}$. Ebből 1 és $-\frac{1}{2}$ (egyszeres) gyökök:

	2	-1	-9	4	-6	5	5
1	2	1	-8	-4	-10	-5	0
$-\frac{1}{2}$	2	0	-8	0	-10	0	

a hányadosként kapott negyedfokú polinomot pedig x^2 polinomjaként egyszerű tovább faktorizálni:

$$(x-1)(x+\frac{1}{2})(2x^4-8x^2-10) = (x-1)(2x+1)(x^4-4x^2-5) = (x-1)(2x+1)(x^2-5)(x^2+1).$$

Ezek a tényezők irreducibilisek $\mathbb{Q}[x]$-ben, mert a másodfokú tényezőknek nincs racionális gyöke. $\mathbb{Z}_5[x]$-ben viszont mindkettő tovább bontható:

$$f(x) = (x-1)(2x+1)x^2(x^2-4) = (x-1)(2x-4)x^2(x-2)(x+2) = 2(x-1)(x-2)^2x^2(x+2).$$

5. *Határozzuk meg az $x^3 + 3x^2 + 9x + 5$ polinom gyökeit a Cardano-képlet segítségével!*

Megoldás: A négyzetes tagot kiküszöbölhetjük az $y = x + 1$ behelyettesítéssel: $(x^3+3x^2)+9x+5 = (x+1)^3-3x-1+9x+5 = (x+1)^3+6(x+1)-2 = y^3+6y-2$. Az y megoldást $u+v$ alakban keresve az $(u^3+v^3-2)+(3uv+6)(u+v) = 0$ egyenletet kapjuk, és erre még akkor is találunk megoldást, ha feltesszük, hogy mindkét tag 0, pontosabban, hogy $u^3 + v^3 = 2$, és $3uv = -6$. A $v = -\frac{2}{u}$ behelyettesítéssel az $u^6 - 2u^3 - 8 = 0$ egyenlethez jutunk, amelynek megoldása $u^3 = 4$ vagy -2, amiből $u = \sqrt[3]{4}$ vagy $-\sqrt[3]{2}$ (komplex köbgyökök). Ebből elég egyet kiválasztani, mondjuk, az $u = \sqrt[3]{4}$ valós köbgyököt, és a hozzá tartozó $v = \frac{-2}{u} = -\sqrt[3]{2}$ értéket, és ezekből az $\varepsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ primitív harmadik egységgyökkel az

$$\begin{aligned} y_1 =& \sqrt[3]{4} - \sqrt[3]{2} \\ y_2 =& \varepsilon\sqrt[3]{4} - \varepsilon^2\sqrt[3]{2} \\ y_3 =& \varepsilon^2\sqrt[3]{4} - \varepsilon\sqrt[3]{2} \end{aligned}$$

megoldást kapjuk, azaz

$$\begin{aligned} x_1 =& \sqrt[3]{4} - \sqrt[3]{2} - 1 \\ x_2 =& \varepsilon\sqrt[3]{4} - \varepsilon^2\sqrt[3]{2} - 1\,, \\ x_3 =& \varepsilon^2\sqrt[3]{4} - \varepsilon\sqrt[3]{2} - 1 \end{aligned}$$

vagy algebrai alakban kiírva:

$$\begin{aligned} x_1 =& \sqrt[3]{4} - \sqrt[3]{2} - 1 \\ x_2 =& -\frac{1}{2}(\sqrt[3]{4} - \sqrt[3]{2}) - 1 + \frac{\sqrt{3}}{2}(\sqrt[3]{4} + \sqrt[3]{2})i\,. \\ x_2 =& -\frac{1}{2}(\sqrt[3]{4} - \sqrt[3]{2}) - 1 - \frac{\sqrt{3}}{2}(\sqrt[3]{4} + \sqrt[3]{2})i \end{aligned}$$

6. *Lássuk be, hogy ha p páratlan prím, akkor $\Phi_{2p}(x) = \Phi_p(-x)$, és bizonyítsuk be ennek a polinomnak az irreducibilitását!*

Megoldás: $\varphi(2p) = (2-1)(p-1) = p-1 = \varphi(p)$, ezért a két polinom foka megegyezik. $\Phi_p(-x)$ gyökei a p-edik primitív egységgyökök negatívjai, és ezeknek a rendje $2p$, ugyanis ha ε rendje p, akkor $(-\varepsilon)^{2p} = (-1)^{2p}\varepsilon^{2p} = 1$, de $(-\varepsilon)^2 = \varepsilon^2 \neq 1$ és $(-\varepsilon)^p = -\varepsilon^p = -1 \neq 1$. Tehát $\Phi_p(-x)$ gyökei $p-1$ darab különböző $2p$-edik primitív egységgyök, csakúgy mint Φ_{2p} gyökei. Végül mindkét polinom főegyütthatója 1, mert $(-1)^{p-1} = 1$, tehát $\Phi_{2p}(x) = \Phi_p(-x)$.

$\Phi_p(x)$-ről bizonyítottuk, hogy irreducibilis ($\Phi_p(x+1) = \frac{(x+1)^p-1}{(x+1)-1}$ kielégíti a Schönemann–Eisenstein-kritériumot a megadott p-vel), ezért $\Phi(-x)$ is az.

7. *Tekintsük a $\Phi_{12} = x^4 - x^2 + 1$ körosztási polinomot.*

a) Bizonyítsuk be, hogy $\Phi_{12}(ax+b)$ semelyik $a, b \in \mathbb{Z}$-vel ($a \neq 0$) nem teljesíti a Schönemann–Eisenstein-kritériumot!

b) Bizonyítsuk be, hogy $x^4 - x^2 + 1$ reducibilis minden $\mathbb{Z}_p$ fölött!

c) Lássuk be $\Phi_{12}(x)$ irreducibilitását más módszerrel!

Megoldás:

$$\Phi_{12}(x)=\frac{x^{12}-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)\Phi_4(x)}=\frac{x^{12}-1}{(x^6-1)(x^2+1)}=\frac{x^6+1}{x^2+1}=x^4-x^2+1.$$

a) $\Phi_{12}(ax+b)=a^4x^4+4a^3bx^3+a^2(6b^2-1)x^2+2ab(2b^2-1)x+(b^4-b^2+1)$ akkor teljesítheti a Sch.–E.-kritériumot, ha van olyan p prím, amely nem osztja a^4-t, de osztja az összes többi együtthatót. De ekkor p relatív prím a-hoz, és így az x^3 együtthatója miatt osztja 2-t vagy b-t, azaz $p \mid 2b$, és az x^2 együtthatója miatt és $p \mid (6b^2-1)$. Viszont $(2b, 6b^2-1)=(2b, 6b^2-1-3b\cdot 2b)=(2b,-1)=1$, tehát nem létezhet ilyen p. (Mellesleg fordított Sch.–E.-es sem lehet, mert akkor valamilyen prím csupán az első hatványon osztaná a^4-t.)

b) $x^4-x^2+1=\frac{1}{4}((2x^2-1)^2+3)=(x^2+1)^2-3x^2=(x^2-1)^2+x^2$. Tehát Φ_{12} reducibilis, ha -3, 3 vagy -1 négyzetszám modulo p, mert akkor a polinom $f(x)^2-g(x)^2=(f(x)-g(x))(f(x)+g(x))$ alakú. Belátjuk, hogy $3\cdot(-1)=-3$ miatt 3, -1 és -3 közül legalább az egyik négyzetszám.
Vegyük észre, hogy $\mathbb{Z}_p^*=\mathbb{Z}_p\setminus\{0\}$ elemeinek pontosan a fele négyzetszám, mert az $1^2, 2^2, \dots, (p-1)^2$ közül ketten-ketten ugyanazt az elemet adják ($a^2\equiv b^2 \pmod p$ $\Leftrightarrow p \mid a^2-b^2=(a-b)(a+b) \Leftrightarrow p \mid a-b$ vagy $p \mid a+b \Leftrightarrow b\equiv a \pmod p$ vagy $b\equiv -a \pmod p$). Egy $a\in\mathbb{Z}_p^*$-ra az $x\mapsto xa$ ($x\in\mathbb{Z}_p^*$) leképezés injektív, és ha a négyzetszám, akkor négyzetszámot négyzetszámba visz, így nem négyzetszámot nem négyzetszámba. Viszont ebből következik, hogy ha a nem négyzetszám, akkor ez a leképezés négyzetszámot nem négyzetszámba visz, tehát nem négyzetszámot négyzetszámba. Arra jutottunk, hogy $\mathbb{Z}_p^*$-ban ab négyzetszám $\Leftrightarrow$ a és b közül mindkettő négyzetszám vagy egyik sem, és ab nem négyzetszám $\Leftrightarrow$ a és b közül pontosan az egyik négyzetszám. Szóval ha -3 nem négyzetszám, akkor 3 és -1 közül valamelyiknek négyzetszámnak kell lennie.

c) Bontsuk fel $\Phi_{12}(x)$-et $\mathbb{R}$ fölött irreducibilisekre. $x^4-x^2+1=(x^2+1)^2-3x^2=(x^2+1)^2-(\sqrt{3}x)^2=(x^2+\sqrt{3}x+1)(x^2-\sqrt{3}x+1)$. (Másképp: a gyöktényezős felírásában párosíthatjuk a konjugált tényezőket.) Ennek a másodfokú komponensei irreducibilisek $\mathbb{R}$ fölött, mert nincs valós gyökük. Ha Φ_{12} felbontható lenne $\mathbb{Q}[x]$-ben, akkor (mivel racionális gyöke nincs) csak két másodfokúra bomolhatna, és azok már $\mathbb{R}$ fölött is irreducibilisek. De akkor az $\mathbb{R}[x]$-beli felbontás egyértelműsége miatt a $\mathbb{Q}[x]$-beli tényezők ennek a kettőnek skalárszorosai, ami nem lehet, mert itt két együttható hányadosa $\pm\sqrt{3}$, ami nem racionális. Ezzel beláttuk, hogy $\mathbb{Q}[x]$ fölött irreducibilis a $\Phi_{12}(x)$ körosztási polinom.

8. a) *Bizonyítsuk be, hogy ha $f(x)\in\mathbb{Z}[x]$, és $a,b\in\mathbb{Z}$, akkor $a-b \mid f(a)-f(b)$.*
b) *Keressünk olyan egész együtthatós polinomot, amelyre*
$\{f(-2), f(1), f(3)\}=\{2,6,11\}$ *(nem feltétlenül ebben a sorrendben)!*

Megoldás: a) Legyen $f(x)=c_nx^n+\ldots+c_1x+c_0$. Ekkor $f(a)-f(b)=c_n(a^n-b^n)+\ldots+c_k(a^k-b^k)+\ldots+c_1(a-b)$, és $a-b$ osztója (a^k-b^k)-nak minden $k\ge 1$-re, így $a-b$ osztója $(f(a)-f(b))$-nek.
Vagy másképp:
$a\equiv b \pmod{(a-b)} \Rightarrow a^k\equiv b^k \pmod{(a-b)}\ \forall k \Rightarrow f(a)\equiv f(b) \pmod{(a-b)}$ a kongruenciák műveleti tulajdonságai miatt.

b) Az a) rész miatt $5 \mid (f(3) - f(-2)$, így $\{ f(3), f(-2) \} = \{ 6, 11 \}$, és
$3 \mid (f(1) - f(-2)) \Rightarrow \{ f(1), f(-2) \} = \{ 2, 11 \}$,
ezért $f(-2)$ a két halmaz metszetében van, amiből $f(-2) = 11$, $f(1) = 2$, $f(3) = 6$, vagy táblázatosan:

x_k	-2	1	3
$f(x_k)$	11	2	6

Newton-interpolációval x_1-en:
$f_0(x) = 11$. Ezt módosítva $\{ x_1, x_2 \}$-höz:
$f_1(x) = f_0(x) + c_1(x+2)$, $x_2 = 1$-ben $2 = 11 + 3c_1 \Rightarrow c_1 = -3 \Rightarrow$
$f_1(x) = 11 - 3(x+2) = -3x + 5$. $\{ x_1, x_2, x_3 \}$-hoz:
$f_2(x) = f_1(x) + c_2(x+2)(x-1) = -3x+5+c_2(x+2)(x-1)$, $x_3 = 3$-ban: $6 = -4 + 10c_2$ $\Rightarrow c_2 = 1 \Rightarrow$
$f_2(x) = -3x + 5 + (x+2)(x-1) = x^2 - 2x + 3$.
Tehát a legkisebb fokú olyan $f(x)$ polinom, amely kielégíti a feltételt,
$f(x) = x^2 - 2x + 3$.
Természetesen bármely $x^2 - 2x + 3 + h(x)(x+2)(x-1)(x-3)$ megfelel, ahol $h(x) \in \mathbb{Z}[x]$.

9. *Legyenek a, b, c az $x^3 - 2x^2 + 4x + 6$ polinom gyökei $\mathbb{C}$-ben. Adjunk meg egy harmadfokú polinomot, amelynek gyökei $a + b$, $a + c$ és $b + c$. (Ne számítsuk ki a gyököket, használjuk a gyökök és együtthatók közti összefüggéseket!*

Megoldás: A Viète-formulákból tudjuk, hogy $a + b + c = 2$, $ab + ac + bc = 4$ és $abc = -6$.
Az új polinom $x^3 + px^2 + qx + r$, ahol
$-p = ((a + b) + (a + c) + (b + c)) = 2(a + b + c) = 4$,
$q = (a + b)(a + c) + (a + b)(b + c) + (a + c)(b + c)) = a^2 + b^2 + c^2 + 3(ab + ac + bc) = (a + b + c)^2 + (ab + ac + bc) = 8$, és
$-r = (a + b)(a + c)(b + c) = a^2b + a^2c + b^2a + b^2c + c^2a + c^2b + 2abc = (ab + ac + bc)(a + b + c) - abc = 8 + 6 = 14$.
Tehát a keresett polinom $x^3 - 4x^2 + 8x - 14$.