

5. Irreducibilis polinomok

Emlékeztető. A polinomokat egy tetszőleges T test felett tekintjük (pl. $T = \mathbb{C}$, $T = \mathbb{R}$, $T = \mathbb{Q}$, $T = \mathbb{Z}_p$).

5.1. Definíció. Az $f \in T[x]$ polinom **irreducibilis**, ha legalább elsőfokú, és csak úgy bontható két polinom szorzatára, hogy az egyik tényező asszociált f -hez. Ekkor a másik tényező szükségképpen asszociált 1-hez; ilyenkor **triviális faktORIZÁCIÓRÓL** beszélünk. Formálisan:

$$\forall g, h \in T[x]: f = gh \implies (g \sim f \text{ vagy } h \sim f).$$

$h \sim 1 \quad g \sim 1$

5.2. Definíció. Az $f \in T[x]$ polinom **prím**, ha legalább elsőfokú, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall g, h \in T[x]: f \mid gh \implies (f \mid g \text{ vagy } f \mid h).$$

5.3. Tétel. Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.

5.4. Tétel. Minden legalább elsőfokú T feletti polinom felbontható irreducibilis polinomok szorzatára. Ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelműen meghatározott, azaz ha $p_1 \dots p_n$ és $q_1 \dots q_m$ ugyanazon polinom két irreducibilis faktorizációja, akkor $n = m$, és létezik olyan $\pi \in S_n$ permutáció, hogy $p_i \sim q_{\pi(i)}$ minden $i = 1, \dots, n$ esetén.

5.5. Tétel. Egy legalább elsőfokú $f \in T[x]$ polinom akkor és csak akkor irreducibilis, ha f nem bontható $\deg f$ -nél kisebb fokszámú polinomok szorzatára.

Bizonyítás. Ha test feletti polinomokról van szó, akkor a felbontás (nem)triviális volta csak a fokszámoktól függ:

- $f = gh$ triviális felbontás, ha $\deg g = \deg f$ és $\deg h = 0$, vagy fordítva;
- $f = gh$ nemtriviális felbontás, ha $1 \leq \deg g, \deg h < \deg f$. □

$\mathbb{Z}[x]$ -ben $\underbrace{2x}_f = \underbrace{2}_g \cdot \underbrace{x}_h$ $2 \nmid 1$ $1 \nmid 2$ de $2 \nmid 1$
 $x \nmid f$ $x \nmid 2x$ de $2 \nmid 1x$

5.6. Tétel. Az elsőfokú polinomok bármely test felett irreducibilisek.

$f = \underset{\neq 0}{a}x + b = 0 \quad \alpha = -\frac{b}{a} \quad f(\alpha) = 0 \quad ax + b = a \cdot \left(x + \frac{b}{a}\right) \sim x - \left(-\frac{b}{a}\right) = x - \alpha$

5.7. Tétel. Ha $f \in T[x]$ irreducibilis és $\deg f \geq 2$, akkor f -nek nincs gyöke.

Bizonyítás. Tlh. f irr. $\exists \alpha \in T: f(\alpha) = 0$

Bérount: $f = \underbrace{(x - \alpha)}_{\substack{1 \\ \wedge \\ n}} \cdot \underbrace{(\dots)}_{\substack{n-1 \\ \wedge \\ n}}$ nemtriv. felb. $\nexists f$ irr.

□

5.8. Tétel. Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

Bizonyítás. irr. $\Rightarrow \nexists$ gyöke.

$\nexists$ gyöke $\stackrel{?}{\Rightarrow}$ irr.

$f = g \cdot h$ nemtriv. felb.

$$\left. \begin{array}{l} 2 = 1 + 1 \times \\ 3 = 1 + 2 \times \\ 3 = 2 + 1 \times \end{array} \right\} \Rightarrow f \text{ irr.}$$

pl. $T = \mathbb{R}, f = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$

$f = (x^2 + 1) \cdot (x^2 + 1)$ nem irr, pedig $\nexists$ gyöke $\mathbb{R}$ -ben

□

5.9. Feladat. Bontsuk irreducibilis tényezők szorzatára az alábbi polinomot.

$$f = x^6 + 3x^4 - x^3 + 2x^2 + x - 1 \in \mathbb{Z}_5[x]. \quad \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

$$f(0) = -1 = 4 \neq 0$$

	1	0	3	-1	2	1	-1
1	1	1	4	3	0	1	0 = f(1)
1	1	2	1	4	4	0	
1	1	3	4	3	2		
2	1	4	4	2	3		
3	1	0	1	2	0		
3	1	3	0	2			
4	1	4	2	0			
4	1	3	4				

$$f = (x-1) \cdot (x^5 + x^4 + 4x^3 + 3x^2 + 1)$$

$$= (x-1)^2 \cdot (x^4 + 2x^3 + x^2 + 4x + 4)$$

$$= (x-1)^2 \cdot (x-3) \cdot (x^2 + x + 2)$$

$$f = (x-1)^2 \cdot (x-3) \cdot (x-4) \cdot (x^2 + 4x + 2)$$

nincs több
és az utolsó
⇒ irr.

5.10. Feladat. Bontsuk irreducibilis tényezőkre az alábbi polinomot.

$$f = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]. \quad \mathbb{Z}_2 = \{0, 1\}$$

pp. $f(0) = 1, f(1) = 1 + 1 + 1 = 1$

f -re, min möre

$$f = g \cdot h$$

$$4 = 1 + 3$$

$$4 = 3 + 1$$

$$4 = \underset{\substack{\uparrow \\ \text{irr.}}}{2} + \underset{\substack{\uparrow \\ \text{irr.}}}{2}$$

$$\left[\begin{array}{l} g = x^2 + 1 \quad g(0) = 1 \quad g(1) = 1 + 1 = 2 = 0 \\ = (x+1)^2 = x^2 + 2x + 1 \end{array} \right]$$

$$g = x^2 + x + 1 \quad g(0) = 1, g(1) = 1 + 1 + 1 = 1$$

$$h = x^2 + x + 1$$

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

5.11. Feladat. Bontsuk irreducibilis tényezőkre az alábbi polinomot.

$$f = x^4 + x + 1 \in \mathbb{Z}_2[x].$$

$$f(0) = 1, f(1) = 1 \Rightarrow \text{ha nem irr., akkor}$$

$$f = (x^2 + x + 1)^2 \quad \nRightarrow f \text{ irr.}$$

6. Irreducibilis polinomok $\mathbb{C}$ felett, Viète-formulák

6.1. Tétel (az algebra alaptétele). Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

6.2. Következmény. A komplex számok teste felett pontosan az elsőfokú polinomok irreducibilisek.

6.3. Következmény.

(1) Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik.

(2) Ha $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$ ($n \geq 1, a_n \neq 0$), akkor f -nek multiplicitással számolva pontosan n gyöke van.

(3) Ha ezek a gyökök $\alpha_1, \dots, \alpha_n$ (mindegyiket annyszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n \cdot (x - \alpha_1) \cdot \dots \cdot (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontásának**.

6.4. Feladat. Határozzuk meg az alábbi polinom gyökeinek négyzetösszegét.

$$f = 3x^3 + 6x^2 + 24x + 18$$

Ha a gyökök $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$, akkor

$$\begin{aligned} f &= 3x^3 + 6x^2 + 24x + 18 = 3 \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot (x - \alpha_3) = \\ &= 3 \cdot (x^3 - \underbrace{(\alpha_1 + \alpha_2 + \alpha_3)}_{-2} x^2 + \underbrace{(\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3)}_8 x - \underbrace{\alpha_1 \alpha_2 \alpha_3}_{-6}). \end{aligned}$$

Ebből következik, hogy

$$\alpha_1 + \alpha_2 + \alpha_3 = -2 \quad \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 = 8 \quad \alpha_1 \alpha_2 \alpha_3 = -6$$

Ezekből ki tudjuk fejezni a gyökök négyzetösszegét:

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 \stackrel{pp.}{=} (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3) = (-2)^2 - 2 \cdot 8 = -12$$

$$(\alpha_1 + \alpha_2 + \alpha_3)^2 = \overbrace{\alpha_1^2 + \alpha_2^2 + \alpha_3^2} + 2(\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3)$$

6.5. Tétel (**Viète-formulák**). Legyenek az n -edfokú

$$f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{C}[x]$$

főpolinom komplex gyökei $\alpha_1, \dots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása). Ekkor fennállnak az alábbi összefüggések:

$$-a_{n-1} = \alpha_1 + \alpha_2 + \dots + \alpha_n;$$

$$a_{n-2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n;$$

$$-a_{n-3} = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \dots + \alpha_{n-2}\alpha_{n-1}\alpha_n;$$

$\vdots$

$$(-1)^{n-1}a_1 = \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_n + \dots + \alpha_2\alpha_3 \dots \alpha_{n-1}\alpha_n;$$

$$(-1)^n a_0 = \alpha_1\alpha_2\alpha_3 \dots \alpha_{n-1}\alpha_n.$$

6.6. Megjegyzés. A fenti képleteket **Viète-formuláknak** hívjuk. A k -adik sor bal oldalán $(-1)^k a_{n-k}$ áll, a jobb oldalon pedig az $\alpha_1, \dots, \alpha_n$ betűkből képezett összes k -tényezős szorzat összege, tehát egy $\binom{n}{k}$ -tagú összeg. Formálisan:

$$(-1)^k a_{n-k} = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \alpha_{i_1} \cdot \alpha_{i_2} \cdot \dots \cdot \alpha_{i_k}.$$

6.7. Feladat. Bontsuk $\mathbb{C}$ és $\mathbb{R}$ felett irreducibilis tényezők szorzatára az $f = x^3 - 1$ polinomot.

pp- $x^3 - 1 = 0$
 $x^3 = 1$

$$x = \sqrt[3]{1}$$

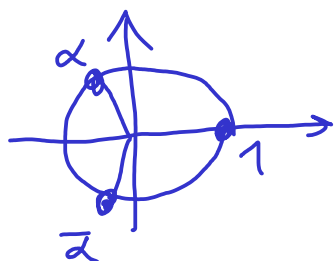
$$\alpha = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \quad \bar{\alpha} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

$$\mathbb{C} \text{ felett: } f = (x-1) \cdot (x-\alpha) \cdot (x-\bar{\alpha}) =$$

$$= (x-1) \cdot (x^2 - (\alpha + \bar{\alpha})x + \alpha \cdot \bar{\alpha}) =$$

$$= (x-1) \cdot (x^2 - 2\operatorname{Re}\alpha \cdot x + |\alpha|^2) =$$

$$\mathbb{R} \text{ felett: } f = (x-1) \cdot (x^2 + x + 1)$$



$\mathbb{R} \quad \mathbb{C}$

$$T_1 \subseteq T_2, f \in T_1[x] \subseteq T_2[x]$$

A: f irr. T_1 felett $\Rightarrow f$ irr. T_2 felett

B: f irr. T_2 felett $\Rightarrow f$ irr. T_1 felett ✓

C: "mindkettő" igaz -

D: "Egyik sem" igaz -

7. Irreducibilis polinomok $\mathbb{R}$ felett

7.1. Tétel. A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \quad \forall z \in \mathbb{C}: f(z) = 0 \implies f(\bar{z}) = 0.$$

Bizonyítás.

$$\begin{aligned} \overline{f(z)} &= \overline{a_n z^n + \dots + a_1 z + a_0} = \overline{(a_i \in \mathbb{R})} \\ &= \overline{a_n} \cdot \overline{z}^n + \dots + \overline{a_1} \cdot \overline{z} + \overline{a_0} = \\ &= a_n \cdot \overline{z}^n + \dots + a_1 \cdot \overline{z} + a_0 = f(\bar{z}) \end{aligned}$$

$$\text{Tehát } \underbrace{\overline{f(z)}}_0 = \underbrace{f(\bar{z})}_0.$$

□

7.2. Következmény. Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste felett, ha elsőfokú, vagy olyan másodfokú polinom, melynek nincs valós gyöke. Tehát az $\mathbb{R}$ feletti irreducibilis polinomok a következők:

- $ax + b$ ($a, b \in \mathbb{C}, a \neq 0$); ✓
- $ax^2 + bx + c$ ($a, b, c \in \mathbb{C}, a \neq 0, b^2 - 4ac < 0$). ✓

Bizonyítás.

$$\text{Tfl. } \deg f \geq 3.$$

$$1) \text{ van valós gyök. } \alpha \in \mathbb{R}, f(\alpha) = 0 \implies f = (x - \alpha) \cdot (\dots) \\ \implies f \text{ nem ir.}$$

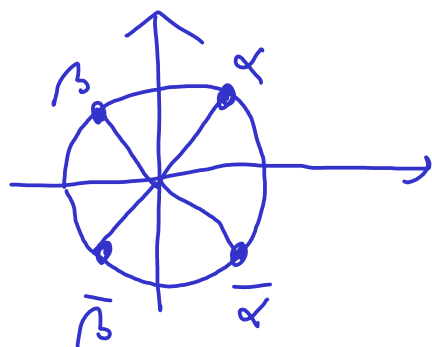
$$2) \text{ nincs valós gyök. } \alpha \in \mathbb{C} \setminus \mathbb{R}, f(\alpha) = 0 \implies f(\bar{\alpha}) = 0 \implies$$

$$\alpha \neq \bar{\alpha}$$

$$\begin{aligned} \implies f &= (x - \alpha) \cdot (x - \bar{\alpha}) \cdot (\dots) \\ &= (x^2 - 2\operatorname{Re}(\alpha) \cdot x + |\alpha|^2) \cdot (\dots) \\ &\in \mathbb{R}[x] \implies \in \mathbb{R}[x] \square \\ \implies f \text{ nem ir.} \end{aligned}$$

7.3. Feladat. Bontsuk $\mathbb{C}$ és $\mathbb{R}$ felett irreducibilis tényezők szorzatára az $f = x^4 + 1$ polinomot.

pp. $x^4 + 1 = 0 \quad x = \sqrt[4]{-1}$



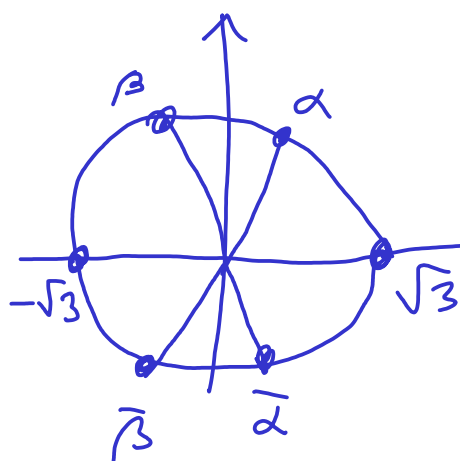
$$\alpha = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i, \quad \beta = -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$$

$\mathbb{C}$ felett: $f = (x - \alpha) \cdot (x - \bar{\alpha}) \cdot (x - \beta) \cdot (x - \bar{\beta})$

$\mathbb{R}$ felett: $f = (x^2 - \sqrt{2}x + 1) \cdot (x^2 + \sqrt{2}x + 1)$

7.4. Feladat. Bontsuk $\mathbb{C}$ és $\mathbb{R}$ felett irreducibilis tényezők szorzatára az $f = x^6 - 27$ polinomot.

pp. $\sqrt[6]{27} \quad \alpha = \sqrt{3} \cdot \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) \quad \beta = \sqrt{3} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$



$\mathbb{C}$ felett: $(x - \sqrt{3}) \cdot (x + \sqrt{3}) \cdot (x - \alpha) \cdot (x - \bar{\alpha}) \cdot (x - \beta) \cdot (x - \bar{\beta})$

$\mathbb{R}$ felett: $(x - \sqrt{3}) \cdot (x + \sqrt{3}) \cdot (x^2 - \sqrt{3}x + 3) \cdot (x^2 + \sqrt{3}x + 3)$

$\mathbb{Q}$ felett: $(x^2 - 3) \cdot (x^4 + 3x^2 + 9)$

ir. $\mathbb{Q}$ felett? $\checkmark$ $\text{ir. } \mathbb{Q}$ felett? $\checkmark$

$$\begin{aligned} a^3 - b^3 &= (a - b)(a^2 + ab + b^2) \\ x^6 - 27 &= (x^2)^3 - 3^3 = \\ &= (x^2 - 3) \cdot (x^4 + 3x^2 + 9) \end{aligned}$$

8. Irreducibilis polinomok $\mathbb{Q}$ felett

8.1. Példa ($\mathbb{Q}$ felett minden polinom asszociált egy $\mathbb{Z}$ felettihez).

$$\begin{aligned}\frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2} &= \frac{60}{28}x^2 + \frac{315}{28}x + \frac{70}{28} = \\ &= \frac{1}{28}(60x^2 + 315x + 70) \sim 60x^2 + 315x + 70 \\ &= 5(12x^2 + 63x + 14) \sim 12x^2 + 63x + 14\end{aligned}$$

8.2. Feladat. Keressük meg az $f = 2x^5 + 3x^4 - 7x^3 - 3x^2 + 8x - 12$ polinom racionális gyökeit. $\alpha = \frac{p}{q}$ $\gcd(p, q) = 1$

$$0 = f\left(\frac{p}{q}\right) = 2 \frac{p^5}{q^5} + 3 \frac{p^4}{q^4} - 7 \frac{p^3}{q^3} - 3 \frac{p^2}{q^2} + 8 \frac{p}{q} - 12 \quad | \cdot q^5$$

$$0 = 2p^5 + 3p^4q - 7p^3q^2 - 3p^2q^3 + 8pq^4 - 12q^5$$

$\underbrace{2p^5 + 3p^4q - 7p^3q^2 - 3p^2q^3 + 8pq^4}_{p \mid \dots} \quad \Rightarrow \quad p \mid 12q^5 \Rightarrow p \mid 12$
 $\gcd(p, q) = 1$

$$p = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12 \quad q = +1, +2$$

$$\frac{p}{q} = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm \frac{1}{2}, \pm \frac{3}{2}: \quad 16 \text{ lehetséges } \frac{p}{q} \text{-ra}$$

$$\text{rac. gyökök: } -2, -2, -\frac{3}{2}$$

Ho KANÉK: $f = (x - (-2))^2 \cdot (x - \frac{-3}{2}) \cdot (2x^2 - 2x + 2) = (x+2)^2 \cdot (2x+3) \cdot (x^2 + 1)$

nem rac. növe
 és 2-odh.
 $\Rightarrow$ irr $\mathbb{Q}$ felett

8.3. Tétel (Rolle(?) tétele). Legyen $f = a_n x^n + \dots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és $\text{Inko}(p, q) = 1$), akkor

$$f\left(\frac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

Bizonyítás. Tegyük fel, hogy $\frac{p}{q}$ gyöke f -nek ($\text{Inko}(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n -nel:

$$0 = \underbrace{a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1}}_{p \mid} + \underbrace{a_0 q^n}_{p \mid} \implies p \mid a_0$$

Hasonlóan:

$$q \mid a_n \iff \underbrace{a_n p^n}_{q \mid} + \underbrace{a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n}_{q \mid} = 0 \quad \square$$

8.4. Feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = 2x^7 + 5x^6 + 4x^5 + 13x^4 + 54x^3 + 84x^2 + 54x + 12$$

ROLLE: $q \mid 12$; $p \mid 12$

$$q = 1, 2 \quad ; \quad p = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$$

$$\frac{p}{q} : \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm \frac{1}{2}, \pm \frac{3}{2}$$

	2	5	4	13	54	84	54	12
-1	2	3	1	12	42	42	12	0
-1	2	1	0	12	30	12	0	
-1	2	-1	1	11	19	-7		
-1/2	2	0	0	12	24	0		
-1/2	2	-1	1/2	4 1/4	15 1/8			

$$f = (x - (-1))^2 \cdot \left(x - \frac{-1}{2}\right) \cdot (2x^4 + 12x + 24)$$

min ra. nide
im.?

$$f = (x+1)^2 \cdot (2x+1) \cdot (x^4 + 6x + 12)$$

im. ? $\checkmark$ $5-2$ 12
 $p=3$ 11
 $\dots + 6d$

$$x^4 + 6x + 12 = (x^2 + ax + b) \cdot (x^2 + cx + d) = x^4 + \dots$$

8.5. Tétel (Gauss-lemma). Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont.

Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

(1) $\exists g, h \in \mathbb{Z}[x] : f = gh$ és $0 < \deg g, \deg h < n$;

A: (1) $\Rightarrow$ (2) triviális ✓

B: (2) $\Rightarrow$ (1) triviális

(2) $\exists g, h \in \mathbb{Q}[x] : f = gh$ és $0 < \deg g, \deg h < n$.

C: Minkább triviális.

D: Egyszerűesen triviális.

8.6. Példa.

$$\begin{aligned}
 & 72x^5 - 102x^4 - 2244x^3 + 208x^2 - 1036x - 280 = \\
 & = \left(\frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2}\right) \cdot \left(\frac{168}{5}x^3 - 224x^2 + \frac{448}{5}x - 112\right) = \\
 & = \frac{5}{28}(12x^2 + 63x + 14) \cdot \frac{56}{5}(3x^3 - 20x^2 + 8x - 10) = \\
 & = \frac{5}{28} \frac{56}{5} \cdot (12x^2 + 63x + 14)(3x^3 - 20x^2 + 8x - 10) = \\
 & = 2 \cdot (12x^2 + 63x + 14)(3x^3 - 20x^2 + 8x - 10) = \\
 & = (24x^2 + 126x + 28) \cdot (3x^3 - 20x^2 + 8x - 10)
 \end{aligned}$$

8.7. Definíció. Azt mondjuk, hogy a p prímszám **pontos osztója** az a egész számnak, ha a osztható p -vel, de p^2 -tel már nem. Jelölés: $p \parallel a$.

8.8. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n, \quad p \mid a_{n-1}, \dots, p \mid a_1, \quad p \parallel a_0,$$

akkor f irreducibilis a racionális számok teste felett.

8.9. Következmény. Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n -edfokú polinom.

Bizonyítás. $p=2$ $x^n + 2$ $p=2$: $2 \nmid 1, 2 \mid 0, \dots, 2 \mid 0, 2 \parallel 2$

□

8.10. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám, amelyre

$$p \parallel a_n, \quad p \mid a_{n-1}, \dots, p \mid a_1, \quad p \nmid a_0,$$

akkor f irreducibilis a racionális számok teste felett.

8.11. Feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = 5x^8 - 5x^7 + 4x^2 - 2x - 2$$

ROLTE: $q|5, p|-2 \Rightarrow \frac{p}{q}: \pm 1, \pm 2, \pm \frac{1}{5}, \pm \frac{2}{5}$

rac. mól: 1

LEPKEP: $(x-1) \cdot (5x^7 + 4x + 2) = f$
 im. im. 5-E: $p=2$

8.12. Feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = 2x^{100} - 3x^{73} + 69x - 12$$

ROLTE: $q|2, p|-12 \quad \frac{p}{q}: \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm \frac{1}{2}, \pm \frac{3}{2}$

S-E $p=3 \Rightarrow f$ irred.

8.13. Feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = x^6 - 27$$

ROLTE: $q|1, p|27 \quad \frac{p}{q}: \pm 1, \pm 3, \pm 9, \pm 27$

rac. mól min

$\mathbb{C}: \dots$

$\mathbb{R}: (x-\sqrt{3}) \cdot (x+\sqrt{3}) \cdot (x^2 - \sqrt{3}x + 3) \cdot (x^2 + \sqrt{3}x + 3)$

$\mathbb{Q}: (x^2 - 3) \cdot (x^4 + 3x^2 + 9)$

8.14. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n, \quad p \mid a_{n-1}, \dots, p \mid a_2, \quad p \mid a_1, \quad p \nmid a_0,$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás. Tfh. van megfelelő p prímszám, de f mégsem irreducibilis $\mathbb{Q}$ felett. Ekkor, a Gauss-lemma szerint léteznek olyan **egész** együtthatós g, h polinomok, amelyekre $f = gh$ és $1 \leq \deg g, \deg h < n$. Legyen

$$g = b_k x^k + b_{k-1} x^{k-1} + \dots + b_2 x^2 + b_1 x + b_0 \in \mathbb{Z}[x] \quad \deg g = k < n$$

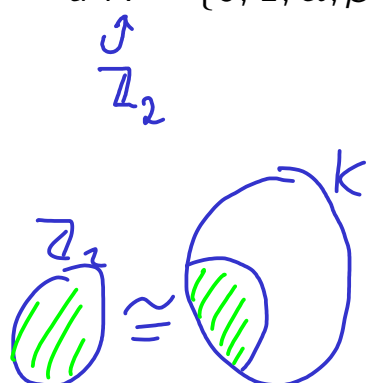
$$h = c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \dots + c_2 x^2 + c_1 x + c_0 \in \mathbb{Z}[x] \quad \deg h = \ell < n$$

Vizsgáljuk az $f = gh$ egyenlőséget együtthatónként: $(k + \ell = n)$

$$\begin{aligned} x^0 \text{ e.l.: } a_0 &= b_0 c_0 \xRightarrow{p \nmid a_0} p \nmid b_0 \vee p \nmid c_0 \\ x^1 \text{ e.l.: } a_1 &= b_1 c_0 + b_0 c_1 \xRightarrow{p \mid a_1} p \mid b_1 c_0 \xRightarrow{p \nmid b_1} p \mid c_0 \\ x^2 \text{ e.l.: } a_2 &= b_2 c_0 + b_1 c_1 + b_0 c_2 \xRightarrow{p \mid a_2} p \mid b_2 c_0 \xRightarrow{p \nmid b_2} p \mid c_0 \\ &\vdots \\ x^i \text{ e.l.: } a_i &= b_i c_0 + \dots \xRightarrow{p \mid a_i} p \mid b_i c_0 \xRightarrow{p \nmid b_i} p \mid c_0 \\ x^n \text{ e.l.: } a_n &= b_n c_\ell \xRightarrow{p \nmid a_n} p \nmid b_n \vee p \nmid c_\ell \end{aligned}$$

9. Egyszerű algebrai bővítés, véges testek

9.1. Példa. Az $m = x^2 + x + 1 \in \mathbb{Z}_2[x]$ polinomnak nincs gyöke $\mathbb{Z}_2$ -ben, ezért irreducibilis $\mathbb{Z}_2$ felett (hiszen csak másodfokú). Bővítsük ki a $\mathbb{Z}_2 = \{0, 1\}$ testet a $K = \{0, 1, \alpha, \beta\}$ testté:



+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$GF(4) = K = \mathbb{Z}_2(\alpha)$
 $\alpha^2 + \alpha + 1 = 0$

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$\beta + \alpha + 1 = 0$

Ebben a testben már van gyöke az m polinomnak: $m(\alpha) = \alpha^2 + \alpha + 1 = 0$.

A K test izomorf a $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ testtel; hogy ezt lássuk, csak be kell vezetni a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléseket:

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

$$m(\alpha) = m(\bar{x}) = \overline{x^2 + x + 1} = \overline{x^2 + x + 1} = \bar{0} = \bar{0}$$

9.2. Tétel. A $T[x]/\langle m \rangle$ maradékosztály-gyűrű akkor és csak akkor test, ha az $m \in T[x]$ polinom irreducibilis T felett. $\mathbb{Z}_m \text{ test} \Leftrightarrow m \text{ pr}$

9.3. Tétel. Legyen T test, $m \in T[x]$ irreducibilis polinom, $\deg f = n$. Ekkor a $K = T[x]/\langle m \rangle$ maradékosztály-gyűrű olyan test, amelyben az m polinomnak van gyöke. A K test minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} \quad (a_{n-1}, \dots, a_0 \in T)$$

alakban. Ha $T = \mathbb{Z}_p$, akkor $|K| = p^n$.

Bizonyítás. $\alpha = \bar{x}$

$$m(\alpha) = m(\bar{x}) = \overline{m(x)} = \bar{0} = \bar{0}, \text{ hiszen } m \equiv 0 \pmod{m}$$

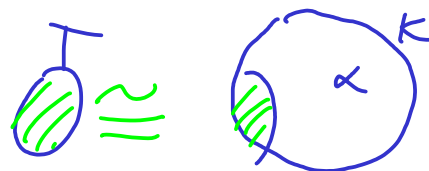
□

9.4. Következmény. Tetszőleges T test és $m \in T[x]$ irreducibilis polinom esetén létezik olyan K test, amelyre

- (1) K **bővítése** T -nek, azaz $K \supseteq T$;
- (2) létezik olyan $\alpha \in K$ elem, amely gyöke m -nek;
- (3) K elemei egyértelműen előállnak $a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0$ ($a_{n-1}, \dots, a_0 \in T$) alakban, ahol $n = \deg f$.

Bizonyítás. Legyen $K = T[x]/\langle m \rangle$.

$$\bar{a} = a$$



- (1) K -ban $\{ \bar{a} : a \in T \subseteq T[x] \}$ egy T -vel izomorf résztest.
- (2) Legyen $\alpha = \bar{x}$, ekkor $m(\alpha) = m(\bar{x}) = \overline{m(x)} = \bar{0}$, hiszen $m \equiv 0 \pmod{m}$.
- (3) K elemei egyértelműen előállnak így ($a_{n-1}, \dots, a_0 \in T$ együtthatókkal):

$$\begin{aligned} \overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} &= \overline{a_{n-1}}\bar{x}^{n-1} + \dots + \overline{a_1}\bar{x} + \overline{a_0} = \\ &= a_{n-1}\bar{x}^{n-1} + \dots + a_1\bar{x} + a_0 = \\ &= a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0. \end{aligned} \quad \square$$

9.5. Definíció. Azt mondjuk, hogy a K test T -ből az α elem **adjungálásával** keletkezik (jelölés: $K = T(\alpha)$), és az ilyen módon előálló testeket T **egyszerű algebrai bővítéseinek** nevezzük.

9.6. Példa. Mivel az $x^2 + 1$ polinom irreducibilis $\mathbb{R}$ felett, a $K := \mathbb{R}[x]/\langle x^2 + 1 \rangle$ maradékosztály-gyűrű test.

- elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$);
- számolási szabály: $\overline{x^2 + 1} = \bar{0}$.

$$\mathbb{C} = \mathbb{R}(i)$$

Menjünk le alfába...

- elemek: $a + b\alpha$ ($a, b \in \mathbb{R}$);
- számolási szabály: $\alpha^2 + 1 = 0$.

$$\alpha^2 = -1 \quad \alpha = i$$

9.7. Példa. Mivel $m := x^3 - 2$ irreducibilis $\mathbb{Q}$ felett, a $K := \mathbb{Q}[x]/\langle x^3 - 2 \rangle$ maradékosztály-gyűrű test.

- elemek: $\overline{a + bx + cx^2}$ ($a, b, c \in \mathbb{Q}$);
- számolási szabály: $\overline{x^3 - 2} = \overline{0}$.

Euklideszi algoritmussal kiszámítottuk, hogy $\overline{x^2 - 2x + 1}^{-1} = \overline{5 + 4x + 3x^2}$.

Menjünk le alfába...

$$= a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$$

- elemek: $a + b\alpha + c\alpha^2$ ($a, b, c \in \mathbb{Q}$);
- számolási szabály: $\alpha^3 - 2 = 0$. $\alpha^3 = 2$

A fenti inverz alfás felírása: $(\alpha^2 - 2\alpha + 1)^{-1} = 5 + 4\alpha + 3\alpha^2$.

$$\alpha = \sqrt[3]{2}$$

$$\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 1} = 5 + 4\sqrt[3]{2} + 3\sqrt[3]{4}$$

9.8. Tétel. Akkor és csak akkor létezik q -elemű test, ha q prímszám.

Bizonyítás.

- **akkor:** Ha $q = p^n$, akkor $K := \mathbb{Z}_p[x]/\langle m \rangle$ jó lesz tetszőleges $m \in \mathbb{Z}_p[x]$ irreducibilis n -edfokú polinom esetén. (Nem triviális, hogy van ilyen!)
- **csak akkor:** Ha K egy véges test, akkor a legkisebb részteste izomorf $\mathbb{Z}_p$ -vel valamilyen p prímszámra (nem triviális!), és K vektorteret alkot ezen test felett, így $|K| = p^n$, ahol $n = \dim K$. $\square$

9.9. Megjegyzés. Tetszőleges q prímszám esetén izomorfia erejéig egyetlen q -elemű test létezik. Jelölés: $\text{GF}(q)$. Galois field

9.10. Példa.

- $\text{GF}(2) \cong \mathbb{Z}_2$
- $\text{GF}(3) \cong \mathbb{Z}_3$
- $\text{GF}(4) \cong \mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$
- $\text{GF}(5) \cong \mathbb{Z}_5$
- $\text{GF}(6)$ nem létezik
- $\text{GF}(7) \cong \mathbb{Z}_7$
- $\text{GF}(8) \cong \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle \cong \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle$

pp.

$$x^3 + x^2 + x + 1$$

10. Lagrange-iterpoláció

10.1. Tétel. Egy test feletti nemnulla polinomnak nem lehet több gyöke, mint amennyi a fokszáma.

Bizonyítás. $\alpha_1, \dots, \alpha_r$ ^{kül.} ~~gyök~~ f -nek $\Rightarrow$

$$\Rightarrow (x - \alpha_1) \cdot \dots \cdot (x - \alpha_r) \mid f \Rightarrow r \leq \deg f \quad \square$$

10.2. Következmény. Ha az $f, g \in T[x]$ polinomok legfeljebb n -edfokúak, és $n + 1$ különböző helyen ugyanaz a helyettesítési értékük, akkor $f = g$.

Bizonyítás. A $h := f - g$ polinom legfeljebb n -edfokú és legalább $n + 1$ gyöke van, ezért a fenti tétel szerint $h = 0$. $\square$

10.3. Következmény. Ha a T test végtelen, akkor két T feletti polinom akkor és csak akkor egyenlő, ha a hozzájuk tartozó polinomfüggvények megegyeznek.

10.4. Megjegyzés. Ha a T test véges, akkor viszont mindig találhatók különböző T feletti polinomok, amelyekhez ugyanaz a polinomfüggvény tartozik, pl. ha $T = \{a_1, \dots, a_q\}$, akkor az $f = 0$ és $g = (x - a_1) \cdot \dots \cdot (x - a_q)$ polinomokhoz ugyanaz a polinomfüggvény tartozik (konstans nulla).

10.5. Tétel (Lagrange-iterpoláció). Tetszőleges $a_1, \dots, a_{n+1}$ páronként különböző és $b_1, \dots, b_{n+1}$ (nem feltétlenül különböző) T -beli elemekhez létezik pontosan egy $f \in T[x]$ legfeljebb n -edfokú polinom, amelyre $f(a_i) = b_i$ teljesül $i = 1, \dots, n + 1$ esetén.

Bizonyítás. Tekintsük az alábbi $f_i \in T[x]$ polinomokat ($i = 1, \dots, n + 1$):

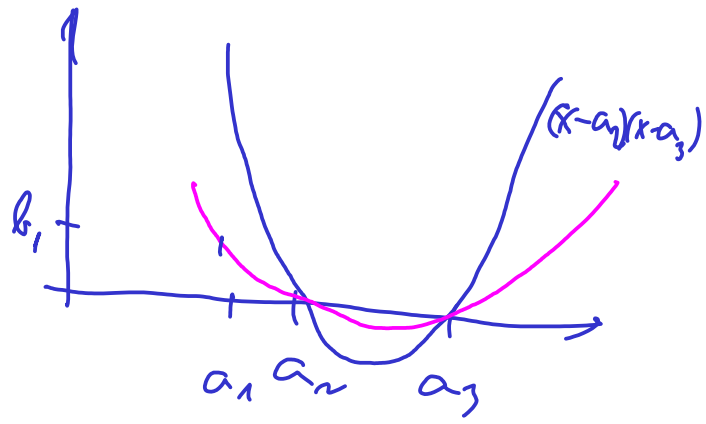
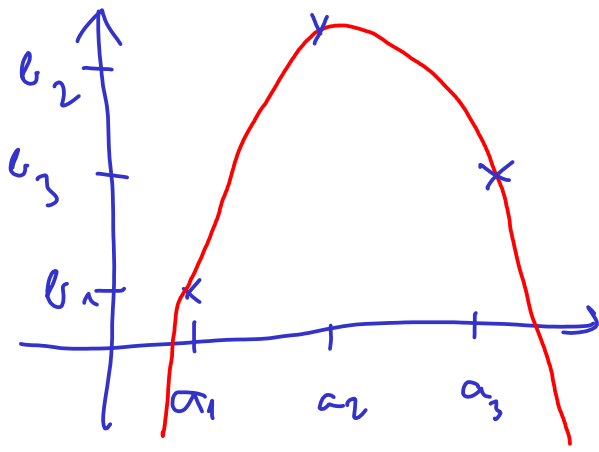
$$f_i := b_i \cdot \frac{(x - a_1) \cdot \dots \cdot (x - a_{i-1}) \cdot (x - a_{i+1}) \cdot \dots \cdot (x - a_{n+1})}{(a_i - a_1) \cdot \dots \cdot (a_i - a_{i-1}) \cdot (a_i - a_{i+1}) \cdot \dots \cdot (a_i - a_{n+1})}.$$

Ekkor f_i értéke az a_j helyen:

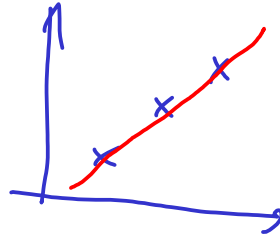
$$f_i(a_j) = \begin{cases} 0, & \text{ha } i \neq j; \\ b_i, & \text{ha } i = j. \end{cases}$$

Tehát az $f = f_1 + \dots + f_{n+1}$ polinom megfelelő lesz:

$$\begin{aligned} f(a_j) &= f_1(a_j) + \dots + f_{j-1}(a_j) + f_j(a_j) + f_{j+1}(a_j) + \dots + f_{n+1}(a_j) = \\ &= 0 + \dots + 0 + b_j + 0 + \dots + 0 = b_j. \end{aligned} \quad \square$$



$$f \in \mathbb{R}[x]$$



$$\begin{array}{c} a_1 \quad a_2 \quad a_3 \\ \hline \end{array}$$

$$f: \quad b_1 \quad b_2 \quad b_3$$

$$f_1: \quad b_1 \quad 0 \quad 0$$

$$f_2: \quad 0 \quad b_2 \quad 0$$

$$f_3: \quad 0 \quad 0 \quad b_3$$

$$f_1 = b_1 \cdot \frac{(x-a_2)(x-a_3)}{(a_1-a_2)(a_1-a_3)}$$

$$f_2 = b_2 \cdot \frac{(x-a_1)(x-a_3)}{(a_2-a_1)(a_2-a_3)}$$

$$f_3 = b_3 \cdot \frac{(x-a_1)(x-a_2)}{(a_3-a_1)(a_3-a_2)}$$

$$f = f_1 + f_2 + f_3$$

$$f(a_1) = f_1(a_1) + f_2(a_1) + f_3(a_1) = b_1 + 0 + 0 = b_1$$

$$\deg f \leq 2$$