

**3ME**



BUDAPESTI MŰSZAKI  
MATEMATIKA  
ÉS GAZDASÁGTUDOMÁNYI  
INTÉZET  
EGYETEM



# Bevezetés az algebra 1

BMETE92AX23



## Polinomok

H406 – 2016-10-03



## Wettl Ferenc

ALGEBRA TANSZÉK

# Alapfogalmak

---

# Alapfogalmak

---

Polinomok

D Legyen  $F$  test,  $a_0, a_1, \dots, a_n \in F$ ,  $x$  egy szimbólum (változó). A  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  formális kifejezést  **$F$ -beli együtthatós (vagy  $F$  feletti) egyváltozós polinomnak** nevezzük. Ha  $a_n \neq 0$ , akkor  $n$ -et a  $p$  **polinom fokának** hívjuk és  $\deg p$ -vel jelöljük.  $a_n$  a polinom **főegyütthatója**. A zéruspolinom foka  $-\infty$ . A  $p(x) = a_0$  polinomot konstans polinomnak nevezzük.

D Két polinom **azonos**, ha azonos fokúak, és megfelelő együtthatóik páronként azonosak.

J Az  $F$  fölötti polinomok halmaza  $F[x]$ : pl.  $\mathbb{Q}[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{C}[x]$ ,  $\mathbb{Z}_p[x]$ .

D Test helyett egységelemes kommutatív **gyűrű fölötti polinomok** halmaza is definiálható:  $\mathbb{Z}[x]$ ,  $\mathbb{Z}_n[x]$ .

D 
$$\sum_{k=0}^n a_k x^k + \sum_{k=0}^m b_k x^k := \sum_{k=0}^{\max(n,m)} (a_k + b_k) x^k.$$
 (A kisebb fokú polinomot kiegészítjük 0 együtthatókkal.)

D 
$$\sum_{i=0}^n a_i x^i \cdot \sum_{j=0}^m b_j x^j := \sum_{k=0}^{n+m} c_k x^k,$$
 ahol  $c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0$ .

Á Egy  $F$  testben  $ab = 0$  esetén  $a = 0$  vagy  $b = 0$  (testben nincs nullosztó).

B Ha  $ab = 0$  és  $a \neq 0$ , akkor  $b = 1b = a^{-1}ab = a^{-1}0 = 0$ .

Á Ha  $F$  test és  $p, q \in F[x]$ ,  $\deg p = m$ ,  $\deg q = n$ , akkor

a)  $\deg(p + q) \leq \max(m, n)$

b)  $\deg(pq) = m + n$ .

m Gyűrű felett b) nem igaz, pl.  $\mathbb{Z}_6[x]$ -ben  $(3x)(2x + 1) = 3x$ , mert  $\mathbb{Z}_6$ -ban  $3 \cdot 2 = 0$ .

B a) Ha  $m \neq n$ , akkor  $\deg(p + q) = \max(m, n)$ , de ha  $m = n$ , akkor a főegyütthatók összege lehet 0 is (pl.  $(x + 2) + (-x + 3) = 5$ ).

b)  $p(x) \cdot q(x) = (a_n x^n + \dots) \cdot (b_m x^m + \dots) = a_n b_m x^{n+m} + \dots$ , és  $a_n b_m \neq 0$ , mert testben nincs nullosztó.

# Alapfogalmak

---

Polinomgyűrű

T Ha  $R$  egységelemes kommutatív gyűrű (például test), akkor  $R[x]$  is az. Ha  $R$  nullosztómentes is, akkor  $R[x]$  is az.

- $R[x]$ -ben a '+' és a '.' kommutatív és asszociatív művelet.
- disztributivitás:  $\forall p, q, r \in R[x] : (p + q)r = pr + qr$
- az összeadás invertálható:  $\forall p, q \in R[x] \exists r \in R[x] : p + r = q$   
Ez azzal ekvivalens, hogy létezik egy 0-val jelölt zéruspolinom, melyre bármely  $p \in R[x]$  esetén  $p + 0 = p$ , és minden  $p$  polinomnak van  $-p$ -vel jelölt ellentettje (additív inverze), melyre  $p + (-p) = 0$ .
- $R[x]$ -nek létezik 1-gyel jelölt egységeleme, melyre bármely  $p \in R[x]$  esetén  $p \cdot 1 = p$ . (ez = az 1 konstanspolinommal)
- Ha  $p, q \in R[x]$  és  $pq = 0$ , akkor főegyütthatóik szorzata is 0, ami nem lehetséges nullosztómentes gyűrűben.

K  $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x], \mathbb{Z}_m[x]$  egységelemes kommutatív gyűrűk. Nullosztómentesek is, kivéve  $\mathbb{Z}_m$ -et összetett  $m$  esetén.

# Alapfogalmak

---

Polinomok oszthatósága



- D** **Oszthatóság egységelemes kommutatív gyűrűben:** Legyen  $R$  egységelemes kommutatív gyűrű,  $a, b \in R$ . AMH  **$b$  osztója  $a$ -nak** ( $a$  osztható  $b$ -vel), ha  $\exists q \in R$ , hogy  $a = bq$ . Jelölés:  $b \mid a$ .
- P**  $x - 1 \mid x^n - 1$  a  $\mathbb{Z}[x]$  gyűrűben ( $n \in \mathbb{N}^+$ ).
- P**  $3x \mid x^n$  a  $\mathbb{Q}[x]$  gyűrűben, mert  $x^n = (3x)(\frac{1}{3}x^{n-1})$ , de nem osztója  $\mathbb{Z}[x]$ -ben.
- P**  $x - i \mid x^2 + 1$  a  $\mathbb{C}[x]$  gyűrűben, mert  $x^2 + 1 = (x - i)(x + i)$ .
- P** Mik az egységek  $\mathbb{F}[x]$ -ben, ha  $\mathbb{F}$  test?
- M** Az  $1 \in \mathbb{F}[x]$  polinom osztói, azaz a nulladfokú polinomok ( $a_0 \in \mathbb{F} \setminus \{0\}$ ).
- P** Mik az egységek (a)  $\mathbb{Z}[x]$ -ben és (b)  $R[x]$ -ben, ha  $R$  egységelemes, kommutatív, nullosztómentes gyűrű?
- M** (a)  $1, -1 \in \mathbb{Z}[x]$ , (b)  $R$  egységei.
- P** Igazoljuk, hogy  $\mathbb{Z}_4[x]$ -ben  $2x + 1$  egység!
- M**  $(2x + 1)(2x + 1) = 1$ , tehát  $2x + 1$  minden polinomnak osztója.

**T** *Maradékos osztás polinomgyűrűben* Legyen  $F$  test, és  $a, b \in F[x]$  két polinom, ahol  $b \neq 0$ . Akkor egyértelműen léteznek olyan  $q, r \in F[x]$  polinomok, hogy

$$a = bq + r, \text{ és } \deg r < \deg b.$$

**B** *Létezés:* Ha  $a = 0$ , akkor  $q = r = 0$ .

Ha  $\deg a < \deg b$ , akkor  $q = 0$  és  $r = a$ , azaz  $a = b \cdot 0 + a$ .

A továbbiakban  $\deg a \geq \deg b$ .  $\deg a$ -ra vonatkozó teljes ind.:

**$\deg a = 0$ :**  $a = a_0$  ( $a_0 \in F$ )  $\rightsquigarrow b = b_0$ ,  $q = \frac{a_0}{b_0}$ ,  $r = 0$ ,  $\checkmark$

**$\deg a < n \rightarrow \deg a = n$ :**  $a(x) = a_n x^n + \dots$ ,  $b(x) = b_m x^m + \dots$

$\hat{a}(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x) \rightsquigarrow \deg \hat{a} < n$

ha  $\deg \hat{a} < \deg b$ , akkor  $r = \hat{a}$ ,  $a(x) = \frac{a_n}{b_m} x^{n-m} b(x) + r(x)$   $\checkmark$

ha  $\deg \hat{a} \geq \deg b$ , akkor az indukció miatt  $\hat{a} = bq + r \rightsquigarrow$

$a(x) = (q(x) + \frac{a_n}{b_m} x^{n-m})b(x) + r(x)$

**Egyértelműség:** Tfh  $a = qb + r = \hat{q}b + \hat{r} \rightsquigarrow (q - \hat{q})b = \hat{r} - r$ , de  $\deg(\hat{r} - r) < \deg b$ ,  $\deg((q - \hat{q})b) \geq \deg b$  vagy  $q = \hat{q} \rightsquigarrow r = \hat{r}$   $\checkmark$

**P** Legyen  $p(x) = x^4 - 4x^3 + 4x^2 + 2x - 1$ ,  $b(x) = x - 2$ . Osszuk el  $p$ -t maradékosan  $b$ -val.

**M**

$$\begin{array}{r} (x^4 - 4x^3 + 4x^2 + 2x - 1) : (x - 2) = x^3 - 2x^2 + 2 \\ \underline{-x^4 + 2x^3} \phantom{+ 4x^2 + 2x - 1} \\ -2x^3 + 4x^2 \phantom{+ 2x - 1} \\ \underline{2x^3 - 4x^2} \phantom{+ 2x - 1} \\ 2x - 1 \\ \underline{-2x + 4} \\ 3 \end{array}$$

**m**  $\mathbb{Z}[x]$ -ben a maradékos osztás nem végezhető el bármely két polinomra, például  $a(x) = x^3$  nem írható  $(3x^2)q(x) + r(x)$  alakba, ha  $q, r \in \mathbb{Z}[x]$  és  $\deg r(x) < \deg(3x^2) = 2$ .

**m** Az  $R$  egységelemes kommutatív gyűrűben lehet maradékosan osztani olyan  $R[x]$ -beli polinommal, melynek főegyütthatója  $R$ -ben egység (pl.  $\mathbb{Z}[x]$ -ben 1- vagy  $-1$ -főegyütthatóssal!).

P  $a(x) = x^3 + 4x - 2, b(x) = 2x - 1$

M  $(x^3 + 4x - 2) : (2x - 1) = \frac{1}{2}x^2 + \frac{1}{4}x + \frac{17}{8}$

$$\begin{array}{r} x^3 \phantom{+ 4x} - 2 \\ -x^3 + \frac{1}{2}x^2 \\ \hline \phantom{x^3} + \frac{1}{2}x^2 + 4x - 2 \\ -\frac{1}{2}x^2 + \frac{1}{4}x \\ \hline \phantom{x^3} \phantom{+ \frac{1}{2}x^2} + \frac{17}{4}x - 2 \\ -\frac{17}{4}x + \frac{17}{8} \\ \hline \phantom{x^3} \phantom{+ \frac{1}{2}x^2} \phantom{+ \frac{17}{4}x} - \frac{1}{8} \end{array}$$

F Osszuk el maradékosan az  $x^4 + x^3 + x + 2$  polinomot  $x^2 + 1$ -gyel  $\mathbb{Z}_3$ -ban!

**P**  $p(x) = x^4 - 4x^3 - x^2 + 16x - 12, q(x) = x^2 - 2x - 3$

**M**

$$(x^4 - 4x^3 - x^2 + 16x - 12) : (x^2 - 2x - 3) = x^2 - 2x - 2$$

$$\underline{-x^4 + 2x^3 + 3x^2}$$

$$-2x^3 + 2x^2 + 16x$$

$$\underline{2x^3 - 4x^2 - 6x}$$

$$-2x^2 + 10x - 12$$

$$\underline{2x^2 - 4x - 6}$$

$$6x - 18$$

# Alapfogalmak

---

Legnagyobb közös osztó

**D** *Polinomok legnagyobb közös osztója = kitüntetett közös osztó*  
Legyen  $F$  test,  $p, q \in F[x]$ . A  $d \in F[x]$  polinom a  $p$  és  $q$  polinomok *legnagyobb közös osztója*, ha

1. közös osztó, azaz  $d \mid p$ ,  $d \mid q$ ,
2. ha  $c \in F[x]$ ,  $c \mid p$  és  $c \mid q$ , akkor  $c \mid d$ .

Jelölés:  $(p(x), q(x))$ ,  $\text{lko}(p(x), q(x))$ ,  $\text{gcd}(p(x), q(x))$  vagy egyszerűen  $(p, q)$ ,  $\text{lko}(p, q)$ ,  $\text{gcd}(p, q)$ .

**T** *Test fölötti polinomok legnagyobb közös osztójának létezése:*  
Ha  $F$  test és  $a, b \in F[x]$ , akkor létezik a legnagyobb közös osztójuk, mely nemnulla konstans szorzótól eltekintve egyértelmű.

**B** Ha  $a(x) = 0$ , akkor  $(a, b) = b$ , ha  $b(x) = 0$ , akkor  $(a, b) = a$ .  
 Feltehető, hogy  $\deg a \geq \deg b$ . Ha  $b \mid a$ , akkor  $(a, b) = b$ .  
 Legyen  $r_0 = a, r_1 = b$ .

$$r_0 = r_1q_1 + r_2$$

$$r_n \mid r_0 = a$$

$$c \mid r_2 = r_0 - r_1q_1$$

$$r_1 = r_2q_2 + r_3$$

$$r_n \mid r_1 = b$$

$$c \mid r_3 = r_1 - r_2q_2$$

$$r_2 = r_3q_3 + r_4$$

$$r_n \mid r_2$$

$$c \mid r_4 = r_2 - r_3q_3$$

$\vdots$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n$$

$$r_n \mid r_{n-2}$$

$$c \mid r_n = r_{n-2} - r_{n-1}q_{n-1}$$

$$r_{n-1} = r_nq_n$$

$$r_n \mid r_{n-1}$$

Tehát  $d = r_n$  kitüntetett közös osztó. Az algoritmus véges lépésben véget ér, mivel  $\deg r_1 > \deg r_2 > \dots > \deg r_n$ , így elérjük, hogy  $\deg r_n \geq 0$ , de  $\deg r_{n+1} = -\infty$ , azaz  $r_{n+1}(x) = 0$ .  
 Ha  $d_1, d_2$  két lnko, akkor  $d_1 \mid d_2, d_2 \mid d_1 \rightsquigarrow \exists c_1, c_2 \in F[x] :$   
 $d_2(x) = d_1(x)c_1(x) = d_2(x)c_2(x)c_1(x) \rightsquigarrow c_1(x)c_2(x) = 1 \rightsquigarrow c_1(x)$  és  $c_2(x)$  egység  $F[x]$ -ben, azaz nemnulla konstans polinom. Tehát a lnko nemnulla skalárszorozótól eltekintve egyértelmű!



**P**  $a(x) = x^4 - 4x^3 - x^2 + 16x - 12$ ,  $b(x) = x^2 - 2x - 3$ ,  $(a(x), b(x)) = ?$

**M** Az euklideszi algoritmussal:

$$x^4 - 4x^3 - x^2 + 16x - 12 = (x^2 - 2x - 3) \cdot (x^2 - 2x - 2) + (6x - 18)$$

$$x^2 - 2x - 3 = (6x - 18) \cdot \left(\frac{1}{6}x + \frac{1}{6}\right) + 0$$

Tehát  $(a(x), b(x)) = 6x - 18$  vagy egyszerűbb alakban  $x - 3$ .

**P**  $a(x) = x^4 - 4x^3 - x^2 + 16x - 12$ ,  $b(x) = x^2 - 4x + 3$

**M**  $x^4 - 4x^3 - x^2 + 16x - 12 = (x^2 - 4x + 3) \cdot (x^2 - 4) + 0$

$$\rightsquigarrow (a(x), b(x)) = x^2 - 4x + 3.$$

**P**  $a(x) = x^3 - 2x^2 + x - 1$ ,  $b(x) = x^2 + 2$

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

$$x^2 + 2 = (-x + 3) \cdot (-x - 3) + 11$$

$$-x + 3 = 11 \cdot \left(-\frac{1}{11}x + \frac{3}{11}\right) + 0$$

$\rightsquigarrow (a(x), b(x)) = 1$ , azaz relatív prímek (a 11 konstansszorososa 1).

**T** Ha  $F$  test,  $a, b, d \in F[x]$  és  $d = (a, b)$ , akkor léteznek olyan  $u, v \in F[x]$  polinomok, hogy

$$d = ua + vb$$

**B** ugyanúgy, mint az egészekre, a kibővített euklideszi algoritlussal.

**P**  $a(x) = x^4 - 4x^3 - x^2 + 16x - 12$ ,  $b(x) = x^2 - 2x - 3$ ,  
 $u(x) = ?$ ,  $v(x) = ?$

**M**  $x^4 - 4x^3 - x^2 + 16x - 12 = (x^2 - 2x - 3)(x^2 - 2x - 2) + (6x - 18) \rightsquigarrow$   
 $x - 3 = \frac{1}{6}(x^4 - 4x^3 - x^2 + 16x - 12) + (-\frac{1}{6}x^2 + \frac{1}{3}x + \frac{1}{3})(x^2 - 2x - 3)$ .

**T** Legyen  $F$  test,  $a, b, h \in F[x]$ . Pontosán akkor léteznek olyan  $u, v \in F[x]$  polinomok, hogy

$$h = ua + vb,$$

ha  $(a, b) \mid h$ .

**P**  $a(x) = x^3 - 2x^2 + x - 1$ ,  $b(x) = x^2 + 2$ ,  $u(x) = ?$ ,  $v(x) = ?$

**M** A maradékos osztások eredményeit írjuk táblázatba:

$h(x)$	$r(x)$	$u(x)$	$v(x)$
	$x^3 - 2x^2 + x - 1$	1	0
$x - 2$	$x^2 + 2$	0	1
$-x - 3$	$-x + 3$	1	$-x + 2$
	11	$x + 3$	$-x^2 - x + 7$

Tehát  $11 = (x + 3)(x^3 - 2x^2 + x - 1) + (-x^2 - x + 7)(x^2 + 2)$  vagy

$$1 = \left(\frac{1}{11}x + \frac{3}{11}\right)(x^3 - 2x^2 + x - 1) + \left(-\frac{1}{11}x^2 - \frac{1}{11}x + \frac{7}{11}\right)(x^2 + 2)$$

**P** Állítsuk elő a  $h(x) = 22x - 11$  polinomot az előző feladatbeli  $a$  és  $b$  segítségével  $h = ua + vb$  alakba.

**M** Mivel  $22x - 11 = 11(2x - 1)$ , ezért az előző példa eredményét  $2x - 1$ -gyel szorozva:

$$22x - 11 = (2x^2 + 5x - 3)(x^3 - 2x^2 + x - 1) + (-2x^3 - x^2 + 15x - 7)(x^2 + 2)$$

# Irreducibilis polinomok

---

# Irreducibilis polinomok

---

Irreducibilitás

- D Legyen  $F$  test. A nem konstans (zérustól és egységtől különböző)  $p \in F[x]$  polinomot **irreducibilisnek** nevezzük, ha  $p = p_1 p_2$  és  $p_1, p_2 \in F[x]$  esetén  $p_1$  vagy  $p_2$  konstans polinom (egység  $F[x]$ -ben).
- D Általában, ha  $R$  **integritási tartomány (= egységelemes, kommutatív, nullosztómentes gyűrű)**, akkor egy zérustól és egységtől különböző  $p \in R$  elemet **irreducibilisnek** nevezünk, ha  $p = ab$  esetén az  $a, b \in R$  elemek valamelyike egység.
- D  $p$  **prím** tulajdonságú, ha  $p$  nem egység,  $p \mid fg \Rightarrow p \mid f$  vagy  $p \mid g$ .
- T  $L \neq F$  test,  $p \in F[x]$ .  $p$  irreducibilis  $\iff p$  prím tulajdonságú.
- B **(prím  $\Rightarrow$  irreducibilis)**  $p = fg \rightsquigarrow p \mid fg$ , de  $p$  prím tulajdonságú, így  $p \mid f$  vagy  $p \mid g$ , azaz  $fg \mid f$  vagy  $fg \mid g \rightsquigarrow g$  vagy  $f$  egység, tehát  $p$  irreducibilis.
- (irreducibilis  $\Rightarrow$  prím)** Tfh  $p$  irreducibilis,  $p \mid fg$ , de  $p \nmid f \rightsquigarrow (p, f) = 1 \rightsquigarrow \exists u, v \in F[x] : up + vf = 1$   
 $\rightsquigarrow upg + vfg = g \rightsquigarrow p \mid g$ .

# Irreducibilis polinomok

---

Egyértelmű felbonthatóság

**T** *(Számelmélet alaptétele test fölötti polinomokra)* Legyen  $F$  test, és  $p \in F[x]$  zérustól és egységtől különböző (nem konstans) polinom. Ekkor  $p$  egységszorzótól és sorrendtől eltekintve egyértelműen felbontható véges sok  $F[x]$ -beli irreducibilis polinom szorzatára.

**B** **Felbonthatóság:**  $\deg p$ -re vonatkozó teljes indukcióval.

$n = 1$ -re ✓

Ha  $p$  irreducibilis ✓

Ha  $p = p_1 p_2$  ( $p_1, p_2 \in F[x]$ ) és  $\deg p = n$ , akkor  $\deg p_1 < n$ ,  $\deg p_2 < n$ , az indukciós feltevés szerint  $p_1$  és  $p_2$  is felbomlik véges sok irred. pol. szorzatára  $\rightsquigarrow p$  is.

**Egyértelműség:** Indirekt. Legyen  $p_1 \dots p_r = q_1 \dots q_s$  a legkisebb fokú polinom, mely két különböző módon is felbomlik.

$p_1 \mid$  bal oldal  $\rightsquigarrow p_1 \mid$  jobb oldal.  $p_1$  irreducibilis  $\rightsquigarrow p_1$  prím

$\rightsquigarrow \exists j : p_1 \mid q_j \rightsquigarrow q_j = p_1 \cdot \text{egység}$

$\rightsquigarrow$  egyszerűsítünk  $p_1$ -gyel  $\rightsquigarrow$  kisebb fokú szorzatot kaptunk: ⚡



- K** A  $\mathbb{C}[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{Q}[x]$ ,  $\mathbb{Z}_p[x]$  polinomgyűrűkben minden polinom véges sok irreducibilis polinom szorzata (sorrendtől és nem nulla konstans szorzótól eltekintve egyértelműen).
- P**  $\mathbb{Q}[x]$ -ben:  $x^4 - 2x^2 - 3 = (x^2 + 1)(x^2 - 3) = (\frac{1}{3}x^2 - 1)(3x^2 + 3)$ ,  
 $\mathbb{R}[x]$ -ben:  $x^4 - 2x^2 - 3 = (x^2 + 1)(x + \sqrt{3})(x - \sqrt{3})$ ,  
 $\mathbb{C}[x]$ -ben:  $x^4 - 2x^2 - 3 = (x + i)(x - i)(x + \sqrt{3})(x - \sqrt{3})$ ,
- P**  $x^2 + 1$  felbontása  $\mathbb{Z}_5[x]$ -ben és  $\mathbb{Z}_7[x]$ -ben?
- M**  $\mathbb{Z}_5[x]$ -ben:  $(x + 2)(x + 3) = x^2 + 1$   
 $\mathbb{Z}_7[x]$ -ben irreducibilis.
- \* Ált.: ha  $p$  prím és  $p \equiv 3 \pmod{4}$ , akkor  $x^2 + 1$  irreducibilis  $\mathbb{Z}_p$ -ben (sőt, pontosan akkor).
- P**  $\mathbb{Z}_8$  nem test,  $\mathbb{Z}_8[x]$ -ben nem igaz a számelmélet alaptétele:  
 $x^2 - 1 = (x + 1)(x - 1) = (x + 3)(x - 3)$ .

# Polinomok gyökei

---

# Polinomok gyökei

---

Horner-elrendezés

D Legyen  $p(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x]$ , ahol  $R$  egységelemes kommutatív gyűrű. Azt mondjuk, hogy  $\alpha \in R$  a  $p$  polinom **gyöke**, ha  $p(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0 \in R$

T **Horner-elrendezés**  $L!$   $R$  egységelemes kommutatív gyűrű,  $p(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x]$ .  $L!$   $b_{n-1} = a_n$ ,  $b_{k-1} = b_k \alpha + a_k$  ( $k = 1, 2, \dots, n-1$ ) és  $r = b_0 \alpha + a_0$  elrendezve egy táblázatban:

$$\begin{array}{cccccc} & a_n & a_{n-1} & \dots & a_1 & a_0 \\ \hline \alpha & b_{n-1} & b_{n-2} & \dots & b_0 & r \end{array}$$

Ekkor

$$p(x) = (x - \alpha)(b_{n-1}x^{n-1} + \dots + b_1x + b_0) + r. \quad (1)$$

Innen leolvasható a  $p(x)$  polinom  $(x - \alpha)$ -val való maradékos osztásának hányadosa és maradéka. A maradék  $r = p(\alpha)$ .

B Az (1) egyenlőséget a zárójel felbontása igazolja. (1)-ben  $x$  helyébe  $\alpha$ -t helyettesítve kapjuk, hogy  $p(\alpha) = r$ .

T Legyen  $R$  egységelemes kommutatív gyűrű,  $p \in R[x]$ .

$$\alpha \in R \text{ gyöke } p\text{-nek} \iff (x - \alpha) \mid p(x).$$

B  $(\Rightarrow)$  Ha  $\alpha$  gyöke  $p$ -nek, akkor a Horner-elrendezés alsó sorából leolvasható  $p(x)$  hányadosa  $(x - \alpha)$ -val osztva.

$$(\Leftarrow) (x - \alpha) \mid p(x) \rightsquigarrow p(x) = (x - \alpha)h(x) \rightsquigarrow p(\alpha) = 0.$$

m Polinomok maradékos osztását test fölötti polinomgyűrűkben definiáltuk, de a Horner-elrendezés is mutatja, hogy ha  $R$  egységelemes kommutatív gyűrű és  $\alpha \in R$ , akkor az  $(x - \alpha)$ -val való maradékos osztás elvégezhető  $R[x]$ -ben (korábban is láttuk).

D Ha az  $R$  gyűrű fölötti  $p \in R[x]$  polinomnak  $\alpha \in R$  gyöke, akkor az  $x - \alpha$  polinomot a  $p(x)$  **gyöktényezőjének**, a  $p(x) = a_n(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$  alakú felírását a  $p$  **gyöktényező alakjának** nevezzük.

## Polinomok gyökei

---

Test fölötti polinomok gyökei

- T *Test fölötti elsőfokú polinomok irreducibilisek.*
- T *Algebrailag zárt testben (pl.  $\mathbb{C}$ -ben) az irreducibilis polinomok pontosan az elsőfokúak.*
- T *Egy  $F$  test fölötti másod- vagy harmadfokú  $p \in F[x]$  polinom pontosan akkor irreducibilis, ha nincs gyöke  $F$ -ben.*
- B  $(\Rightarrow)$  Ha van gyöke, akkor  $p$  a gyöktényezővel osztható, ami elsőfokú, tehát  $p$  nem irreducibilis.
- $(\Leftarrow)$  Ha nem irreducibilis, akkor felbomlik alacsonyabb fokú polinomok szorzatára, melyek egyike elsőfokú, mondjuk  $bx + c$ . Ekkor  $x = -c/b$  a  $p$  egy gyöke.
- P Az állítás magasabb fokú polinomokra már nem igaz: a  $p(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$  polinom nem irreducibilis, mert  $p(x) = (x^2 - 2)(x^2 - 3)$ , de nincs racionális gyöke (gyökei  $\mathbb{R}$ -ben  $\pm\sqrt{2}, \pm\sqrt{3}$ ).

D Legyen  $F$  test, és

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = \sum_{k=0}^n a_k x^k \in F[x]$ . A  $p$  **polinom deriváltján** a

$$p'(x) = \sum_{k=1}^n k \cdot a_k x^{k-1} \in F[x]$$

polinomot értjük.

Á  $' : F[x] \rightarrow F[x]$  tulajdonságai: bármely  $p, q \in F[x]$  polinom,  $c \in F[x]$  konstans polinom,  $\alpha \in F$  testelem és  $m \in \mathbb{N}^+$  esetén:

- $c' = 0 \in F[x]$
- $(p + q)' = p' + q'$
- $(\alpha p)' = \alpha p'$
- $(pq)' = p'q + pq'$
- $(p^m)' = mp^{m-1}p'$

P  $\mathbb{Z}_{11}$ -ben:  $(6x^8 + 5x^4 + 8x + 4)' = 4x^7 + 9x^3 + 8$ .

P Ha  $p, q, r \in F[x]$ , akkor  $(pqr)' = p'qr + pq'r + pqr'$ .

P  $F[x]$ -ben:  $((x - \alpha)^n)' = n(x - \alpha)^{n-1}$ .



D Amh  $\alpha \in F$  a  $p \in F[x]$  polinomnak pontosan  **$k$ -szoros gyöke**, ha  $p(x) = (x - \alpha)^k q(x)$  ( $q \in F[x]$ ), de  $q(\alpha) \neq 0$ .

m Ez azt jelenti, hogy  $(x - \alpha)^k \mid p(x)$ , de  $(x - \alpha)^{k+1} \nmid p(x)$ .

T  $\alpha \in F$  a  $p \in F[x]$  polinomnak pontosan akkor többszörös gyöke, ha  $p(\alpha) = p'(\alpha) = 0$ .

B  $(\Rightarrow)$   $p(x) = (x - \alpha)^k q(x)$ , ahol  $k > 1 \rightsquigarrow$

$$p'(x) = k(x - \alpha)^{k-1} q(x) + (x - \alpha)^k q'(x) \rightsquigarrow p'(\alpha) = 0$$

$(\Leftarrow)$  Legyen  $p(\alpha) = p'(\alpha) = 0$ . Indirekt tfh  $\alpha$  csak egyszeres gyök, azaz  $p(x) = (x - \alpha)q(x)$  és  $q(\alpha) \neq 0 \rightsquigarrow$

$$p'(x) = q(x) + (x - \alpha)q'(x) \rightsquigarrow p'(\alpha) = q(\alpha) + 0 \neq 0, \nexists$$

m A tétel bizonyításából látszik, hogy ha  $\alpha$  a  $p$  polinom  $k$ -szoros gyöke, akkor  $p'$ -nek **legalább  $k - 1$ -szeres gyöke**.

K Az  $F$  test fölötti  $p \in F[x]$  polinom többszörös gyökei megegyeznek  $(p, p')$  gyökeivel.

B  $(\Rightarrow)$   $p$ -nek  $\alpha$  többsz. gyöke  $\rightsquigarrow p'$ -nek gyöke  $\rightsquigarrow (p, p')$ -nek gyöke

$(\Leftarrow)$   $\alpha$  gyöke  $(p, p')$ -nek  $\rightsquigarrow \alpha$  nem lehet  $p$ -nek csak egysz. gyöke

P Igazoljuk, hogy  $\mathbb{Z}_{11}$  fölött a  $x^4 + 4x^3 + 9x^2 + 5x + 5$  polinomnak a  $2 \in \mathbb{Z}_{11}$  többszörös gyöke.

1M  $p(2)$  kiszámítása Horner-módszerrel:

$$\begin{array}{r} 1 \quad 4 \quad 9 \quad 5 \quad 5 \\ \hline \end{array}$$

$$2 \quad 1 \quad 6 \quad 10 \quad 3 \quad 0$$

$$p'(x) = 4x^3 + x^2 + 7x + 5, p'(2) = ?$$

$$\begin{array}{r} 4 \quad 1 \quad 7 \quad 5 \\ \hline \end{array}$$

$$2 \quad 4 \quad 9 \quad 3 \quad 0$$

$$p''(x) = x^2 + 2x + 7, p''(2) = ?$$

$$\begin{array}{r} 1 \quad 2 \quad 7 \\ \hline \end{array}$$

$$2 \quad 1 \quad 4 \quad 4$$

Tehát a 2 pontosan kétszeres gyöke  $p$ -nek, mivel többszörös gyök és ha legalább háromszoros gyök lenne, akkor  $p''(\alpha) = 0$  lenne.

**2M** Most csak a Horner-elrendezést alkalmazva:

$$\begin{array}{r} 1 \quad 4 \quad 9 \quad 5 \quad 5 \\ \hline 2 \quad 1 \quad 6 \quad 10 \quad 3 \quad 0 \end{array}$$

Eszerint  $x^4 + 4x^3 + 9x^2 + 5x + 5 = (x^3 + 6x^2 + 10x + 3)(x - 2)$ .

$$\begin{array}{r} 1 \quad 6 \quad 10 \quad 3 \\ \hline 2 \quad 1 \quad 8 \quad 4 \quad 0 \end{array}$$

Tehát  $p(x) = (x^2 + 8x + 4)(x - 2)^2$ .

$$\begin{array}{r} 1 \quad 8 \quad 4 \\ \hline 2 \quad 1 \quad 10 \quad 2 \end{array}$$

Tehát  $p(x)$  már nem osztható  $(x - 2)^3$ -nel.

# Polinomok gyökei

---

Gyökök és együtthatók

M  $ax^2 + bx + c = a(x - \alpha_1)(x - \alpha_2) = ax^2 - a(\alpha_1 + \alpha_2)x + a\alpha_1\alpha_2 \rightsquigarrow$   
 $\alpha_1 + \alpha_2 = -\frac{b}{a}, \alpha_1\alpha_2 = \frac{c}{a}$

T *Gyökök és együtthatók kapcsolata* L! F test, és tfh  $F[x]$ -ben

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = a_n (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

Ekkor

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

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

$\vdots$

$$(-1)^n \frac{a_0}{a_n} = \alpha_1\alpha_2 \dots \alpha_n$$

**F** Mi az  $2x^4 - x^3 + 3x^2 - 5$  polinom gyökeinek összege, szorzata?  
Bizonyítsuk be, hogy van nem valós gyöke! Hány valós gyöke van?

**M**  $e_1 = x_1 + x_2 + x_3 + x_4 = \frac{1}{2}$ ,  $e_4 = x_1x_2x_3x_4 = -\frac{5}{2}$   
 $e_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = \frac{3}{2} \rightsquigarrow$   
 $x_1^2 + x_2^2 + x_3^2 + x_4^2 = e_1^2 - 2e_2 = \frac{1}{4} - 2 \cdot \frac{3}{2} = -\frac{11}{4} \rightsquigarrow$  van komplex gyök  
ha csak komplex gyök van, akkor  $e_4 > 0 \rightsquigarrow$  2 valós gyök van

**P** Mennyi az  $n$ -edik egységgyökök összege?

**M**  $x^n - 1$  gyökeinek összege  $x^{n-1}$  egyh-ja: 0 ha  $n > 1$ , 1, ha  $n = 1$ .

**P** Mennyi a primitív 15-ödik egységgyökök összege?

**M**  $\varepsilon$  primitív 15-ödik egységgyök.

$$\text{Előző példából } 1 + \varepsilon^5 + \varepsilon^{10} = 0, 1 + \varepsilon^3 + \varepsilon^6 + \varepsilon^9 + \varepsilon^{12} = 0,$$

$$1 + \varepsilon + \varepsilon^2 + \dots + \varepsilon^{14} = 0 \rightsquigarrow$$

$$1 + \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^7 + \varepsilon^8 + \varepsilon^{11} + \varepsilon^{13} + \varepsilon^{14} = 1.$$

# Polinomok gyökei

---

Komplex és valós együtthatós polinomok

m Az Algebra alaptételének két alakja:

1.  $\mathbb{C}$  algebrailag zárt (azaz minden  $\mathbb{C}[z]$ -beli legalább elsőfokú polinomnak van gyöke).
2. Minden  $a_n z^n + \dots + a_1 z + a_0 \in \mathbb{C}[z]$  polinom, ahol  $n \in \mathbb{N}^+$ ,  $a_n \neq 0$ , a tényezők sorrendjétől eltekintve egyértelműen felírható

$$a_n(z - \alpha_1)(z - \alpha_2) \dots (z - \alpha_n) \quad (2)$$

alakban, ahol  $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$ .

B (1.  $\Rightarrow$  2.) Teljes indukció: ha  $\deg p = 1$ , azaz  $p(z) = a_1 z + a_0$ , akkor  $\alpha_1 = -a_0/a_1$  az egyetlen gyök ( $a_1 \neq 0$ ).

Legyen  $p \in \mathbb{C}[z]$   $n$ -edfokú, és legyen  $\alpha \in \mathbb{C}$  az 1. szerint létező gyök, azaz  $p(\alpha) = 0$ .

$\alpha$  gyök  $\rightsquigarrow z - \alpha \mid p(z)$ , azaz  $p(z) = (z - \alpha)h(z)$ , ahol  $\deg h = n - 1$ . Az indukciós feltevés szerint az  $n$ -nél kisebb fokúakra fennáll (2). Így  $p$  összesen  $n$  elsőfokú tényező szorzatának konstansszorosa.



T Ha a  $p \in \mathbb{R}[x]$  polinomnak  $\alpha \in \mathbb{C} \setminus \mathbb{R}$  gyöke, akkor  $\bar{\alpha}$  is gyöke, és e két gyök multiplicitása megegyezik.

B (A konjugált is gyök)  $p(\alpha) = a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0$   
( $a_0, a_1, \dots, a_n \in \mathbb{R}$ )  $\rightsquigarrow$

$$\begin{aligned} 0 &= \bar{0} = \bar{a}_n \bar{\alpha}^{\bar{n}} + \dots + \bar{a}_1 \bar{\alpha} + \bar{a}_0 & a_k \in \mathbb{R} \text{ így } \bar{a}_k &= a_k \\ &= a_n \bar{\alpha}^n + \dots + a_1 \bar{\alpha} + a_0 \\ &= p(\bar{\alpha}) \end{aligned}$$

(Azonos a multiplicitás)  $p$  fokára vonatkozó teljes indukcióval.

$\deg p = 1$  vagy  $2$  esetén  $\checkmark$

$p$ -nek  $\alpha$  és  $\bar{\alpha}$  gyöke, azaz  $p(z) = (z - \alpha)(z - \bar{\alpha})q(z)$ .

Mivel  $(z - \alpha)(z - \bar{\alpha}) = z^2 - (\alpha + \bar{\alpha})z + \alpha\bar{\alpha} = z^2 - (2 \operatorname{Re} \alpha)z + |\alpha|^2$  valós együtthatós, így  $q$  is valós együtthatós, melyben az indukciós feltevés szerint  $\alpha$  és  $\bar{\alpha}$  multiplicitása azonos.  $\checkmark$

- K**  $\mathbb{R}[x]$ -ben irreducibilisek az elsőfokú polinomok és azok a másodfokúak, amelyeknek nincs valós gyöke.
- B** Ha egy  $p \in \mathbb{R}[x]$  polinom irreducibilis, és  $\alpha \in \mathbb{C}$  egy gyöke, akkor  $\alpha \in \mathbb{R}$  esetén  $x - \alpha$  osztója,  $\alpha \in \mathbb{C} \setminus \mathbb{R}$  esetén  $(x - \alpha)(x - \bar{\alpha}) \in \mathbb{R}[x]$  osztója  $p(x)$ -nek.
- K** Minden  $n$ -edfokú  $p \in \mathbb{R}[x]$  polinom felírható

$$p(x) = a_n \prod_{j=1}^r (x - \alpha_j) \prod_{k=1}^s (x^2 + b_k x + c_k)$$

alakban, ahol  $n = r + 2s$ ,  $\alpha_j \in \mathbb{R}$  és  $x^2 + b_k x + c_k$  irreducibilis  $\mathbb{R}$  fölött (azaz negatív diszkriminánsú).

**P**  $x^5 - x^4 + 2x^3 - 2x^2 + x - 1 = (x - 1)(x^2 + 1)^2$

# Polinomok gyökei

---

Harmadfokú egyenlet megoldása

m Az  $x^3 + ax^2 + bx + c \in \mathbb{C}$  polinom

$$\left(x + \frac{a}{3}\right)^3 + \left(b - \frac{a^2}{3}\right)\left(x + \frac{a}{3}\right) + \left(c - \frac{ab}{3} + \frac{2a^3}{27}\right)$$

átalakra hozása azt mutatja, hogy harmadfokú egyenlet gyökeinek meghatározásához elég az  $x^3 + px + q$  alakúakat vizsgálni!

**P** Küszöböljük ki az  $x^2$ -es tagot a  $x^3 + 3x^2 - 4x - 12$  polinomból!

**1M** Az első két tag alapján  $x + 1$  polinomjaként kell felírunk a megadott polinomot!

$$\begin{aligned}x^3 + 3x^2 - 4x - 12 &= x^3 + 3x^2 + 3x + 1 - 7x - 13 \\ &= (x + 1)^3 - 7(x + 1) - 6 = y^3 - 7y - 6\end{aligned}$$

**2M**  $(x + 1)$ -gyel való ismételt maradékos osztással:

	1	3	-4	-12	
-1	1	2	-6	<b>-6</b>	$(x^2 + 2x - 6)(x + 1) - 6$
-1	1	1	<b>-7</b>		$(x + 1)(x + 1) - 7$
-1	1	<b>0</b>			$1(x + 1) + 0$
-1	<b>1</b>				$0(x + 1) + 1$

Tehát a polinom:  $(x + 1)^3 - 7(x + 1) - 6 = y^3 - 7y - 6$ , a helyettesítés  $x = y - 1$ .

- Keressük az  $x^3 + px + q$  gyökeit  $x = u + v$  alakban. Mivel  $(u + v)^3 = u^3 + v^3 + 3uv(u + v)$ , ezért

$$(u + v)^3 - 3uv(u + v) - u^3 - v^3 = 0.$$

- Ha találunk olyan  $u, v$  párt, melyre  $p = -3uv$ ,  $q = -u^3 - v^3$ , akkor találtunk egy gyököt! Ez  $u^3$ -re és  $v^3$ -re a következő egyenletrendszer megoldását kívánja:

$$u^3 v^3 = - \left( \frac{p}{3} \right)^3 \quad (3)$$

$$u^3 + v^3 = -q \quad (4)$$

- A gyökök és együtthatók összefüggése szerint  $u^3$  és  $v^3$  a  $z^2 + qz - \left(\frac{p}{3}\right)^3$  polinom gyökei, azaz  $u^3, v^3 = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$ .

- Már csak e két számból kell köbgyököt vonni:

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Kérdés, hogy a 3-3 gyök alkotta 9 párból melyek összege lesz valóban gyöke a polinomnak, és megkajuk-e így az összes gyököt?

- A (3) egyenlet helyett az eredeti  $uv = -\frac{p}{3}$  összepárosítja  $u$  és  $v$  lehetséges értékeit, azaz így valóban 3  $\{u, v\}$  párt kapunk.
- Behelyettesítés igazolja, hogy ha  $\varepsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$  a harmadik egységgyök,  $u + v$  gyök, akkor a három gyök:

$$x_1 = u + v$$

$$x_2 = u\varepsilon + v\varepsilon^2 = -\frac{1}{2}(u + v) + \frac{\sqrt{3}}{2}(u - v)i \quad (\text{ui. } u\varepsilon v\varepsilon^2 = uv = -\frac{p}{3})$$

$$x_3 = u\varepsilon^2 + v\varepsilon = -\frac{1}{2}(u + v) - \frac{\sqrt{3}}{2}(u - v)i \quad (\text{ui. } u\varepsilon^2 v\varepsilon = uv = -\frac{p}{3})$$

- Legyen  $D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$ ,  $u, v = \sqrt[3]{-\frac{q}{2} \pm \sqrt{D}}$
- **D>0:** A gyökvonások **valós** gyökvonásokként számolhatók,  $u, v \in \mathbb{R}$ , így  $x_1 \in \mathbb{R}$ . Mivel  $u \neq v$ , azaz  $u - v \neq 0$ , ezért  $x_{2,3} \in \mathbb{C} \setminus \mathbb{R}$ .
- **D=0:**  $x_1 = 2u = -\sqrt[3]{4q}$ ,  $u = v$ ,  $x_{2,3} = -\frac{1}{2}(u + v) = -u = \sqrt[3]{\frac{q}{2}}$
- **D<0:**  $|u^3| = \sqrt{u^3 \bar{u}^3} = \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}$ , azaz  $|u| = \sqrt{-\frac{p}{3}}$ .  
Másképp  $uv = -\frac{p}{3}$ , ezért  $v = \bar{u}$ .  
Ha  $u = a + bi$ , akkor  $x_1 = 2a$ ,  $x_{2,3} = -a \pm b\sqrt{3}$
- Bizonyítható, hogy  $a$  és  $b$  meghatározására sajnos nincs csak az alpműveleteket és **valós** gyökvonásokat tartalmazó általános képlet!
- Általában, az ötöd- vagy annál nagyobb fokú polinomok gyökeinek meghatározására még komplex gyökvonást tartalmazó képlet sincs! (Abel-tétel, Galois-elmélet)



$$P \quad x^3 + 6x^2 + 21x + 52$$

$$M \quad y = x + 2$$

$$\begin{array}{r} 1 \quad 6 \quad 21 \quad 52 \\ \hline -2 \quad 1 \quad 4 \quad 13 \quad 26 \\ \hline -2 \quad 1 \quad 2 \quad 9 \\ \hline -2 \quad 1 \quad 0 \end{array}$$

$$y^3 + 9y + 26$$

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} = \sqrt[3]{-13 + \sqrt{13^2 + 3^3}} = \sqrt[3]{-13 + 14} = 1$$

$$uv = -\frac{p}{3} = -3 \rightsquigarrow v = -3$$

$$y_1 = u + v = 1 - 3 = -2,$$

$$y_2 = u\varepsilon + v\varepsilon^2 = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) - 3\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = 1 + 2\sqrt{3}i$$

$$y_3 = 1 - 2\sqrt{3}i.$$

$$\text{Tehát } x_1 = -4, x_{2,3} = -1 \pm 2\sqrt{3}i,$$

$$x^3 + 6x^2 + 21x + 52 = (x + 4)(x + 1 + 2\sqrt{3}i)(x + 1 - 2\sqrt{3}i)$$

**P**  $x^3 - 3x + 2$

**M**  $u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} = \sqrt[3]{-1 + \sqrt{1^2 + (-1)^3}} = -1, v = u$

$x_1 = 2u = -2, x_{2,3} = -u = 1, \text{ tehát } x^3 - 3x + 2 = (x + 2)(x - 1)^2.$

**P**  $x^3 - 6x + 4$

**M**  $u, v = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} = \sqrt[3]{-2 \pm \sqrt{4 + (-2)^3}} = \sqrt[3]{-2 \pm 2i}$

$u = \sqrt[3]{-2 + 2i} = \{1 + i, (1 + i)\varepsilon, (1 + i)\varepsilon^2\}$

$v = \sqrt[3]{-2 - 2i} = \{1 - i, (1 - i)\varepsilon^2, (1 - i)\varepsilon\}$

$1 + i$  és  $1 - i$  összetartozó párok, mert  $(1 + i)(1 - i) = 2 = -\frac{p}{3}$

$x_1 = 2,$

$x_2 = (1 + i)\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) + (1 - i)\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = -1 - \sqrt{3},$

$x_3 = (1 + i)\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) + (1 - i)\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = -1 + \sqrt{3}.$

Tehát  $x^3 - 6x + 4 = (x - 2)(x + 1 - \sqrt{3})(x + 1 + \sqrt{3}).$

**P**  $x^3 + 3x^2 + 9x + 5$

**M**  $x^3 + 3x^2 + 9x + 5 = (x + 1)^3 + 6(x + 1) - 5 = y^3 + 6y - 2, p = 6,$   
 $q = -2$

$$u, v = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} = \sqrt[3]{1 \pm \sqrt{1 + 2^3}} = \sqrt[3]{1 \pm 3}$$

$$u = -\sqrt[3]{2} = -2^{1/3}, v = \sqrt[3]{4} = 2^{2/3}$$

$$y_1 = \sqrt[3]{4} - \sqrt[3]{2}$$

$$x_1 = -1 - \sqrt[3]{2} + \sqrt[3]{4},$$

$$y_2 = \frac{1 - i\sqrt{3}}{\sqrt[3]{4}} - \frac{1 + i\sqrt{3}}{\sqrt[3]{2}}$$

$$x_2 = -1 + \frac{1 - i\sqrt{3}}{\sqrt[3]{4}} - \frac{1 + i\sqrt{3}}{\sqrt[3]{2}}$$

$$y_3 = \frac{1 + i\sqrt{3}}{\sqrt[3]{4}} - \frac{1 - i\sqrt{3}}{\sqrt[3]{2}}$$

$$x_3 = -1 - \frac{1 - i\sqrt{3}}{\sqrt[3]{2}} + \frac{1 + i\sqrt{3}}{\sqrt[3]{4}}$$

# Polinomok gyökei

---

Egész együtthatós polinomok

**T** *Racionális gyökteszt (Rolle)* Ha egy  $p(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$  polinomnak egy  $\frac{a}{b} \in \mathbb{Q}$  szám gyöke, ahol  $(a, b) = 1$ , akkor

$$a \mid a_0, b \mid a_n,$$

azaz a számláló a konstans tagnak, a nevező a főegyütthatónak osztója.

**B**  $0 = p\left(\frac{a}{b}\right) = a_n \left(\frac{a}{b}\right)^n + \dots + a_1 \left(\frac{a}{b}\right) + a_0 \rightsquigarrow$   
 $0 = a_n a^n + a_{n-1} a^{n-1} b + \dots + a_1 a b^{n-1} + a_0 b^n \rightsquigarrow$   
 $b \mid a_n a^n \rightsquigarrow b \mid a_n$  (mivel  $(a, b) = 1$ )  
 $a \mid a_0 b^n \rightsquigarrow a \mid a_0$  (mivel  $(a, b) = 1$ )

**K** Ha  $p \in \mathbb{Z}[x]$  főegyütthatója 1, akkor  $p$  racionális gyökei egész számok, és osztói a konstans tagnak.

**m** E teszt nem garantálja, hogy  $p$ -nek van racionális gyöke!

**P** Keressük meg a  $2x^4 - 5x^3 - 8x^2 + 17x - 6$  polinom racionális gyökeit!

**M** A szóba jöhető gyökök:  $\pm 6, \pm 3, \pm 2, \pm 1, \pm \frac{3}{2}, \pm \frac{1}{2}$ .  
Horner-elrendezéssel próbálkozunk:

$$\begin{array}{r}
 2 \quad -5 \quad -8 \quad 17 \quad -6 \\
 \hline
 \frac{1}{2} \quad 2 \quad -4 \quad -10 \quad 12 \quad 0 \quad \checkmark \\
 \hline
 1 \quad 2 \quad -2 \quad -12 \quad 0 \quad \checkmark \\
 \hline
 \cancel{1} \quad \cancel{2} \quad \cancel{4} \quad \cancel{8} \quad !! \\
 \hline
 3 \quad 2 \quad 4 \quad 0 \quad \checkmark \\
 \hline
 -2 \quad 2 \quad 0 \quad \checkmark
 \end{array}$$

A !!-es sorban nem találtunk gyököt, a sort töröljük.

$$2x^4 - 5x^3 - 8x^2 + 17x - 6 = (2x - 1)(x - 1)(x - 3)(x + 2)$$

- M** A racionális együtthatós polinomokból kiemelhető az együtthatók közös nevezője és a számlálók legnagyobb közös osztója.
- D** Amh egy  $\mathbb{Z}$  fölötti polinom **primitív**, ha együtthatóinak legnagyobb közös osztója 1.
- T** Minden  $p \in \mathbb{Q}[x]$  polinom előjeltől eltekintve egyértelműen felírható  $p(x) = \frac{a}{b}q(x)$  alakban, ahol  $q \in \mathbb{Z}[x]$  primitív,  $a, b \in \mathbb{Z}$  és  $(a, b) = 1$ .
- B** Az együtthatókat közös nevezőre hozzuk, majd a közös nevezőt (jelölje  $d$ ) kiemeljük, így egy  $p(x) = \frac{1}{d}r(x)$  alakot kapunk, ahol  $r(x)$  egészegyütthatós. Ezután  $r$  együtthatóinak legnagyobb közös osztóját is kiemeljük:  $p(x) = \frac{c}{d}q(x)$ . Ha  $c$  és  $d$  nem lennének relatív prímek, egyszerűsítünk: így kapjuk, hogy  $p(x) = \frac{a}{b}q(x)$ .  $q$  primitív polinom, mivel együtthatói lnko-ja 1.
- P**  $\frac{6}{5}x^3 + \frac{14}{15}x - \frac{2}{3} = \frac{18}{15}x^3 + \frac{14}{15}x - \frac{10}{15} = \frac{2}{15}(9x^3 + 7x - 5)$

T **1. Gauss-lemma:** Primitív polinomok szorzata primitív.

B Legyen

$$a(x) = \sum_{i=0}^n a_i x^i, b(x) = \sum_{j=0}^m b_j x^j, \text{ és } c(x) = a(x)b(x) = \sum_{k=0}^{n+m} c_k x^k,$$

azaz  $c_0 = a_0 b_0$ ,  $c_1 = a_0 b_1 + a_1 b_0, \dots$

tfh  $\exists p$  prím, hogy  $p \mid c_k$  ( $k = 0, \dots, n + m$ )

**1B** ekkor  $\mathbb{Z}_p[x]$ -ben tekintve a polinomokat, a szorzat 0,  $a$  és  $b$  nem 0, de  $\mathbb{Z}_p[x]$  nullosztómentes,  $\nexists$

**2B** és tfh  $p \mid a_0, \dots, a_{i-1}$ , de  $p \nmid a_i$ , és  $p \mid b_0, \dots, b_{j-1}$ , de  $p \nmid b_j$ .

Ekkor

$$p \mid c_{i+j} = a_0 b_{i+j} + a_1 b_{i+j-1} + \dots + a_i b_j + \dots + a_{i+j-1} b_1 + a_{i+j} b_0$$

$$\rightsquigarrow p \mid a_i b_j \rightsquigarrow p \mid a_i \text{ vagy } p \mid b_j, \nexists$$



**K** Mik az egységek  $\mathbb{Z}[x]$ -ben?

Az 1 és  $-1$  konstans polinomok.

**T**  $\mathbb{Z}[x]$  irreducibilis polinomjai a prím és ellentettje konstans polinom, valamint az irreducibilis primitív polinomok.

**P** A  $2x + 2 \in \mathbb{Z}[x]$  irreducibilis-e?

**M**  $\mathbb{Z}[x]$ -ben nem irreducibilis, mert a  $2(x + 1)$  felbontásban egyik tényező sem egység!  $\mathbb{Q}[x]$ -ben irreducibilis!

- L** **2. Gauss-lemma:** Legyen  $p \in \mathbb{Z}[x]$  primitív nem konstans polinom.  $p$  pontosan akkor irreducibilis  $\mathbb{Z}[x]$ -ben, ha  $\mathbb{Q}[x]$ -ben.
- B** ( $\Leftarrow$ ) Ha  $p$  felbomlik alacsonyabb fokúak szorzatára  $\mathbb{Z}[x]$ -ben, akkor ez felbontás  $\mathbb{Q}[x]$ -ben is.

( $\Rightarrow$ )  $!$   $p = p_1 p_2$  a  $p$  felbontása alacsonyabb fokúak szorzatára  $\mathbb{Q}[x]$ -ben. Állítsuk elő  $p_1$ -et és  $p_2$ -t egy racionális szám és egy primitív polinom szorzataként:  $p = \frac{a_1}{b_1} \tilde{p}_1 \frac{a_2}{b_2} \tilde{p}_2$ , ahol  $\tilde{p}_1$  és  $\tilde{p}_2$  primitívek.

Tehát a  $p$  primitív polinom egy másik primitív polinom ( $\tilde{p}_1 \tilde{p}_2$ ) racionális számszorosa, azaz  $p = \frac{a}{b} \tilde{p}_1 \tilde{p}_2$ , ahol  $(a, b) = 1$ .  $b$  nem lehet  $\pm 1$ -től különböző, különben  $\tilde{p}_1 \tilde{p}_2$  nem lenne primitív (minden együtthatójának  $\frac{a}{b}$ -szerese egész, de  $(a, b) = 1$ , tehát  $b$  osztana minden együtthatót). Így  $a$  sem különbözhet  $\pm 1$ -től, különben  $p$  nem lenne primitív.

Tehát  $\frac{a}{b} = 1$  esetén  $p = \tilde{p}_1 \tilde{p}_2$ , vagy  $\frac{a}{b} = -1$  esetén  $p = (-\tilde{p}_1) \tilde{p}_2$   $\mathbb{Z}[x]$ -beli felbontás.

- L** *3. Gauss-lemma:* Ha  $p \in \mathbb{Z}[x]$  felbomlik két alacsonyabb fokú polinom szorzatára  $\mathbb{Q}[x]$ -ben, akkor felbomlik alacsonyabb fokúak szorzatára  $\mathbb{Z}[x]$ -ben is.
- B** Osszuk le  $p$ -t együtthatói legnagyobb közös osztójával! Ha  $p = p_1 p_2$ , akkor  $\frac{1}{d}p = (\frac{1}{d}p_1)p_2$ , azaz ez is felbomlik  $\mathbb{Q}[x]$ -ben. Másrészt  $\frac{1}{d}p$  primitív, így az előző lemma szerint felbomlik egészegyütthatós primitív polinomok szorzatára. Ezek egyikét megszorozva  $d$ -vel, a két polinom szorzata  $p$  lesz.
- K**  $\mathbb{Q}[x]$  irreducibilis polinomjai a nem konstans irreducibilis primitív polinomok nem nulla racionális számszorosai.
- P** Felbomlik-e a  $p(x) = 2x^3 - 9x^2 + 6x - 1$  polinom alacsonyabb fokúak szorzatára  $\mathbb{Q}[x]$ -ben? És  $\mathbb{Z}[x]$ -ben?
- M**  $p(x)$ -nek egyetlen racionális gyöke van:  $\frac{1}{2}$ . Osztva  $x - \frac{1}{2}$ -del:  
 $2x^3 - 9x^2 + 6x - 1 = (x - \frac{1}{2})(2x^2 - 8x + 2)$  ( $\mathbb{Q}$  fölött föl bomlik, így  $\mathbb{Z}$  fölött is):  $(2x - 1)(x^2 - 4x + 1)$ .

**T** *Schönemann–Eisenstein-kritérium:* Ha  $a(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$  nem konstans polinom, és van olyan  $p \in \mathbb{N}^+$  prímszám, hogy

1.  $p \nmid a_n$ ,
2.  $p \mid a_0, a_1, \dots, a_{n-1}$ ,
3.  $p^2 \nmid a_0$ ,

akkor  $a(x)$  irreducibilis  $\mathbb{Q}[x]$ -ben. (Ha  $a(x)$  primitív, akkor  $\mathbb{Z}$  fölött is irreducibilis.)

**P**  $x^n - p$  irreducibilis  $\mathbb{Q}[x]$ -ben, és mivel primitív,  $\mathbb{Z}[x]$ -ben is, ha  $p$  prímszám.  $\rightsquigarrow \mathbb{Q}[x]$ -ben van akármilyen nagyfokú irred. pol.

**m** A tétel csak **elégséges feltételt** ad az irreducibilitás eldöntésére, a tétel megfordítása nem igaz: pl.  $x + 1$  irreducibilis, de nincs megfelelő prím.

**m**  $\mathbb{Z}[x]$ -beli irreducibilitás eldöntésére nem alkalmas: a kritériumot  $p = 2$ -re alkalmazva  $3x + 6$  irreducibilis  $\mathbb{Q}[x]$ -ben, de  $\mathbb{Z}[x]$ -ben nem, mert  $3(x + 2)$  egy felbontása.

**B** Indirekt. Ha  $a(x)$  felbomlik  $\mathbb{Q}[x]$ -ben, akkor  $\mathbb{Z}[x]$ -ben is: tfh  $b(x) = \sum b_j x^j$ ,  $c(x) = \sum c_k x^k$  és  $a(x) = b(x)c(x)$ , azaz  $a_0 = b_0 c_0$ ,  $a_1 = b_0 c_1 + b_1 c_0, \dots$ , és  $\deg b = m < n$ ,  $\deg c = \ell < n$ .

**1B** modulo  $p$ , azaz  $\mathbb{Z}_p[x]$ -beli polinomként  $\hat{a}(x) = \hat{a}_n x^n$ . A számelmélet alaptétele  $\mathbb{Z}_p[x]$ -ben igaz, így  $\hat{a}(x) = \hat{a}_n x^m x^\ell$  egy felbontás, így  $\hat{b}$  és  $\hat{c}$  konstansszor  $x$ -hatvány alakú  $\mathbb{Z}_p$  fölött  $\rightsquigarrow p \mid b_0, p \mid c_0 \rightsquigarrow p^2 \mid a_0 \nmid$

**2B**  $p \mid a_0, p^2 \nmid a_0 \rightsquigarrow p \mid b_0 c_0, p^2 \nmid b_0 c_0 \rightsquigarrow$  pl.  $p \mid b_0$ , de  $p \nmid c_0$   
 $p \mid a_1 = b_0 c_1 + b_1 c_0 \rightsquigarrow p \mid b_1$

...

$$p \mid a_i = b_0 c_i + b_1 c_{i-1} + \dots + b_{i-1} c_1 + b_i c_0 \rightsquigarrow p \mid b_i$$

$$b_i = 0, \text{ ha } i > \deg b,$$

$$p \mid b_0 c_n + b_1 c_{n-1} + \dots + b_{n-1} c_1 + b_n c_0 = a_n, \text{ de } p \nmid a_n,$$

ellentmondás, tehát  $a(x)$  irreducibilis.

**P** Irreducibilis-e  $\mathbb{Z}$  fölött az  $a(x) = 2x^4 + 3x^3 - 9x + 6$  polinom?

**M** A  $p = 3$  prímmel a S-E-kritérium feltételei fennállnak  $\rightsquigarrow a(x)$  irreducibilis  $\mathbb{Q}$  fölött, de primitív, mert az együtthatók lnko-ja 1, így  $\mathbb{Z}$  fölött is irreducibilis.

**T** *Fordított Schönemann–Eisenstein-kritérium:* Ha

$a(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$  polinomhoz van olyan  $p \in \mathbb{N}^+$  prímszám, hogy

1.  $p \nmid a_0$ ,

2.  $p \mid a_1, \dots, a_n$ ,

3.  $p^2 \nmid a_n$ ,

akkor  $a(x)$  irreducibilis  $\mathbb{Q}[x]$ -ben.

**B** A S-E-hez hasonlóan.

**P** Irreducibilis-e az  $a(x) = 6x^4 - 12x^2 + 6x - 4$ ?

**M** A fordított S-E  $p = 3$ -mal igazolja, hogy  $\mathbb{Q}$  fölött irreducibilis.  $\mathbb{Z}$  fölött nem, mert  $a(x) = 2(3x^4 - 6x^2 + 3x - 2)$ .

**Á** Legyen  $p \in \mathbb{Q}[x]$ .  $p$  pontosan akkor irreducibilis  $\mathbb{Q}$  fölött, ha valamely  $c \in \mathbb{Q}$  számra  $q(x) = p(x + c)$  irreducibilis.

**B** Ha  $p(x) = a(x)b(x)$ , akkor  $q(x) = p(x + c) = a(x + c)b(x + c)$ , ha  $q(x) = a(x)b(x)$ , akkor  $p(x) = q(x - c) = a(x - c)b(x - c)$ .

**P** Igazoljuk, hogy  $x^4 - x^3 + x^2 - x + 1$  irreducibilis!

**M**  $x^4 - x^3 + x^2 - x + 1 = \frac{x^5 + 1}{x + 1}$ . Legyen  $y = x + 1$ , ekkor

$$\frac{x^5 + 1}{x + 1} = \frac{(y - 1)^5 + 1}{y} = y^4 - 5y^3 + 10y^2 - 10y + 5,$$

és erre már alkalmazható a S-E-kritérium.

**P** Irreducibilisek-e az  $x^4 + 4$  és az  $x^5 + 4$  polinomok?

**M** A S-E egyikre sem használható!

$$x^4 + 4 = x^4 + 4 + 4x^2 - 4x^2 = (x^2 + 2)^2 - (2x)^2 = (x^2 + 2 + 2x)(x^2 + 2 - 2x)$$

reducibilis.

$$x^5 + 4 = (y + 1)^5 + 4 = y^5 + 5y^4 + 10y^3 + 10y^2 + 5y + 5, \text{ S-E:}$$

irreducibilis.

**P**  $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$  irreducibilis, ha  $p$  prím!

**M**  $\frac{x^p - 1}{x - 1} = \frac{(y + 1)^p - 1}{y} = y^{p-1} + py^{p-2} + \dots + p$  a S-E miatt irred.

**m**  $x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1} = \prod_{k=1}^{p-1} (x - \varepsilon_p^k)$ , ahol  $\varepsilon_p$  egy primitív  $p$ -edik egységgyök, hisz a gyökök az 1-től különböző egységgyökök (amik egyúttal primitív egységgyökök is).

**D** Az  $n$ -edik **körosztási polinom (cyclotomic polynomial)**

$$\Phi_n(x) = \prod_{\varepsilon} (x - \varepsilon),$$

ahol  $\varepsilon$  végigfut a primitív  $n$ -edik egységgyökökön.

**Á** Ha  $p$  prím  $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ .

**Á**  $x^n - 1 = \prod_{d|n} \Phi_d(x)$

**B** hisz minden  $n$ -edik egységgyök  $d$ -edik primitív egységgyök valamely  $d | n$ -re és minden  $d$ -edik primitív egységgyök  $n$ -edik egységgyök.



Á  $\deg \Phi_n = \varphi(n)$  (Euler-függvény)

Á  $\Phi_n$  egészegyütthetős és irreducibilis  $\mathbb{Q}$  és  $\mathbb{Z}$  fölött.

Á\*  $\Phi_n$  az egyetlen olyan egészegyütthetős irreducibilis polinom, mely osztója  $x^n - 1$ -nek, de nem osztója egyetlen  $k < n$ -re sem  $x^k - 1$ -nek.

P Határozzuk meg a  $\Phi_8$  polinomot!

$$\text{M } \Phi_8(x) = \frac{x^8 - 1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)} = \frac{x^8 - 1}{(x-1)(x+1)(x^2+1)} = x^4 + 1$$

P Az első néhány (nem prím indexű)  $\Phi_1(x) = x - 1$ ,  $\Phi_2(x) = x + 1$ ,  
 $\Phi_3(x) = x^2 + x + 1$ ,  $\Phi_4(x) = x^2 + 1$ ,  $\Phi_6(x) = x^2 - x + 1$ ,  
 $\Phi_8(x) = x^4 + 1$ ,  $\Phi_9(x) = x^6 + x^3 + 1$ ,  $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$ ,  
 $\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ ,  
 $\Phi_{12}(x) = x^4 - x^2 + 1$ ,  $\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$ ,  
 $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ ,  $\Phi_{16}(x) = x^8 + 1$ ,  
 $\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36}$   
 $+ x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16}$   
 $+ x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1.$

**Á** Ha  $p \nmid a_n$  és  $a(x) \in \mathbb{Z}[x]$  irreducibilis  $\mathbb{Z}_p$  fölött, akkor  $\mathbb{Q}$  fölött is!

**B** Feltehető, hogy  $a(x)$  primitív. Ha  $\exists$  valódi felbontás  $\mathbb{Q}$  fölött, akkor  $\mathbb{Z}$  fölött is, ami az együtthatókat modulo  $p$  tekintve felbontás  $\mathbb{Z}_p$  fölött is. (A  $\mathbb{Z}$  fölötti tényezők főegyütthatóinak egyike sem osztható  $p$ -vel, mivel a szorzatuk  $a_n$  sem).

**P**  $x^4 - 3x^3 - 4x^2 + 2x + 1$  irreducibilis?

**M** nincs racionális gyöke, a S-E nem használható.

$\mathbb{Z}_2$  fölött  $x^4 + x^3 + 1$

$\mathbb{Z}_2$ -ben nincs gyöke, az egyetlen másodfokú irreducibilis polinommal nem osztható, mivel

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

$\rightsquigarrow \mathbb{Z}_2$  fölött irreducibilis  $\rightsquigarrow \mathbb{Q}$  fölött is  $\rightsquigarrow \mathbb{Z}$  fölött is, mivel primitív.

- T** *(Számelmélet alaptétele  $\mathbb{Z}[x]$ -ben)* Minden  $\mathbb{Z}$  fölötti legalább elsőfokú polinom felbomlik irreducibilis polinomok szorzatára, és ez a felbontás sorrendtől és egységsszorzóktól eltekintve egyértelmű.
- B**  $L! a(x) \in \mathbb{Z}[x] \rightsquigarrow a(x) = cg(x)$  alakba írható, ahol  $c > 0$  egész, és  $g$  primitív.  
 $c = p_1 p_2 \dots p_k$  a prímtényezős felbontás  $\mathbb{Z}$ -ben.  
 $g$  „egyértelműen” felbontható  $\mathbb{Q}[x]$ -ben (mert  $\mathbb{Q}$  test)  $\rightsquigarrow$  felbontható  $\mathbb{Z}[x]$ -ben is. Egyértelműen?  
 $g = g_1 g_2 \dots g_r = h_1 h_2 \dots h_r$  primitív irreducibilisek.  
 $g_i = ah_j$   $a \in \mathbb{Q} \rightsquigarrow a = \pm 1$ .
- K**  $\mathbb{Z}[x]$ -ben van lko, bár nincs maradékos osztás, és így euklideszi algoritmus sem.
- T** *(Lenstra-Lenstra-Lovász, 1982, LLL-algoritmus)* Van olyan polinom idejű (hatékony) algoritmus, mely  $\mathbb{Q}[x]$ -ben faktorizál.

**P** Bontsuk fel irreducibilisek szorzatára  $\mathbb{Q}$  és  $\mathbb{Z}$  fölött is a  $6x^5 - 3x^4 + 12x^2 + 6x - 6$  polinomot!

**M** Kiemelve az eh-k loko-ját:  $3(2x^5 - x^4 + 4x^2 + 2x - 2)$ .

A primitív polinom racionális gyökei Horner-módszerrel:  $\frac{1}{2}$

$(x - \frac{1}{2})(2x^4 + 4x + 4) = (2x - 1)(x^4 + 2x + 2)$ , a második tényező S-E miatt irreducibilis  $\mathbb{Q}$  fölött, tehát

$\mathbb{Q}[x]$ :  $(6x - 3)(x^4 + 2x + 2)$ ,  $\mathbb{Z}[x]$ :  $3(2x - 1)(x^4 + 2x + 2)$  a két felbontás.

Egyebek

---

# Egyebek

---

## Szimmetrikus polinomok

D Legyen  $R$  egy egységelemes, kommutatív gyűrű, és  $x_1, x_2, \dots, x_n$  egymástól különböző szimbólumok. A

$$p(x_1, x_2, \dots, x_n) = \sum a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \quad (a_{i_1 i_2 \dots i_n} \in R, i_1, \dots, i_n \in \mathbb{N}_0)$$

alakú kifejezéseket  **$R$  fölötti  $n$ -határozatlanú ( $n$ -változós) polinomnak** nevezzük. Halmazukat  $R[x_1, x_2, \dots, x_n]$  jelöli.

M I! összevonva, ami összevonható: pl.  $2x_1^3x_2^2 - 5x_1^3x_2^2 = -3x_1^3x_2^2$ .

P  $3x_1^3x_3 - x_2^2x_1^2 + 5x_2x_3 - 2x_3 \in \mathbb{Z}[x_1, x_2, x_3]$

M E fogalom rekurzív módon is definiálható.  $R[x_1, x_2]$  nem más, mint az  $R[x_1]$  gyűrű fölötti polinomgyűrű:  $R[x_1, x_2] = (R[x_1])[x_2]$ .

Általában  $R[x_1, x_2, \dots, x_n] = (R[x_1, x_2, \dots, x_{n-1}])[x_n]$ .

P  $x^3y^2 + 3x^2y^2 - xy^3 + xy^2 + 2xy - y^2 + 7 \in \mathbb{Z}[x, y]$ ,  
 $(-x)y^3 + (x^3 + 3x^2 + x - 1)y^2 + (2x)y + 7 \in (\mathbb{Z}[x])[y]$

T Az  $R[x_1, x_2, \dots, x_n]$  egységelemes, kommutatív gyűrű és egységei azok a konstans polinomok, ahol a konstans  $R$ -ben is egység. Ha  $R$  nullosztómentes, akkor  $R[x_1, x_2, \dots, x_n]$  is az.

D Az  $ax_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$  ( $a \in R \setminus \{0\}$ ) tag foka  $i_1 + i_2 + \dots + i_n$ . A  $p \in R[x_1, x_2, \dots, x_n]$  polinom foka a  $p$  tagjai fokának maximuma.

P  $\deg(x^3y^2 + 3x^2y^4 - xy + 1) = \max\{5, 6, 2, 0\} = 6$

m tagok sorrendje? szorzat alakban „lexikografikus”: xxxyy, xxyyyy, xy.

D A  $p$  polinom tagjainak **lexikografikus rendezésén** tagjainak olyan sorrendbe való írását értjük, melyben

- $x_1 \succ x_2 \succ \dots \succ x_n$
- $ax_1^{i_1}x_2^{i_2}\dots x_n^{i_n} \succ bx_1^{j_1}x_2^{j_2}\dots x_n^{j_n}$  ( $a \neq 0, b \neq 0$ ), ha valamilyen  $k = 1, 2, \dots, n$  indexre  $i_k > j_k$ , de minden  $m < k$  indexre  $i_m = j_m$ .

P  $x_1x_2^3x_3^2 \succ x_1x_2^2x_3, x_1^2x_2^5x_3 \succ x_2^5x_3, x_1x_2 \succ x_1x_3^3$

P Rendezzük lexikografikusan az

$x_2^8x_3 - 7x_1^2x_3^7 + 3x_1^2x_3 + x_1^3x_2^2x_3 + 2x_1^3x_2^2 - 5x_1$  polinom tagjait!

M  $x_1^3x_2^2x_3 + 2x_1^3x_2^2 - 7x_1^2x_3^7 + 3x_1^2x_3 - 5x_1 + x_2^8x_3$



- D** A  $p \in R[x_1, x_2, \dots, x_n]$  polinomot **szimmetrikus polinomnak** nevezzük, ha változóinak tetszőleges permutációja után  $p$ -vel egyenlő polinomot kapunk.
- m** elég kikötni, hogy nem változik  $p$ , ha bármely két változóját kicseréljük, mert minden permutáció megkapható elemek cseréjével.
- P** Az  $x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2 - 7x_1x_2x_3$  polinom szimmetrikus, de a  $x_1^2x_2 + x_2^2x_3 + x_1x_3^2 - 7x_1x_2x_3$  polinom nem!

D A változók összes  $k$ -tényezős szorzatának összegeként kapott  $e_k \in R[x_1, x_2, \dots, x_n]$  polinomot  **$k$ -adik elemi szimmetrikus polinomnak** nevezzük, azaz

$$e_k(x_1, x_2, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}, \quad \text{specilisan}$$

$$e_0(x_1, x_2, \dots, x_n) = 1,$$

$$e_1(x_1, x_2, \dots, x_n) = \sum_{1 \leq i \leq n} x_i,$$

$$e_2(x_1, x_2, \dots, x_n) = \sum_{1 \leq i < j \leq n} x_i x_j,$$

...

$$e_n(x_1, x_2, \dots, x_n) = x_1 x_2 \dots x_n$$

P  $e_0(x) = 1, e_1(x) = x, e_0(x, y) = 1, e_1(x, y) = x + y, e_2(x, y) = xy,$   
 $e_0(x, y, z) = 1, e_1(x, y, z) = x + y + z, e_2(x, y, z) = xy + xz + yz,$   
 $e_3(x, y, z) = xyz.$

**T** *Szimmetrikus polinomok alaptétele*: Tekintsük az  $F$  test fölötti  $F[x_1, x_2, \dots, x_n]$  polinomgyűrűt. Minden szimmetrikus  $p \in F[x_1, x_2, \dots, x_n]$  polinom felírható az elemi szimmetrikus polinomok  $F$  fölötti polinomjaként, azaz létezik olyan  $f \in F[y_1, y_2, \dots, y_n]$  polinom, hogy

$$p(x_1, x_2, \dots, x_n) = f(e_1(x_1, x_2, \dots, x_n), \dots, e_n(x_1, x_2, \dots, x_n)).$$

**B** A lexikografikus rendezés szerinti indukcióval bizonyítunk. Konstans polinomra az állítás igaz.

- Az

$$e_1^{k_1} \dots e_n^{k_n} = (x_1 + x_2 + \dots + x_n)^{k_1} (x_1 x_2 + \dots + x_{n-1} x_n)^{k_2} \dots (x_1 x_2 \dots x_n)^{k_n}$$

polinom főtagja  $x_1^{k_1 + k_2 + \dots + k_n} x_2^{k_2 + \dots + k_n} \dots x_n^{k_n}$ .

- Másrészt ha a szimmetrikus  $p$  polinom főtagja  $c x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ , akkor  $i_1 \geq i_2 \geq \dots \geq i_n$  (miért?).

- Mivel  $p$  főtagja és

$$c \cdot (x_1 + x_2 + \dots + x_n)^{i_1 - i_2} (x_1 x_2 + \dots + x_{n-1} x_n)^{i_2 - i_3} \dots (x_1 x_2 \dots x_n)^{i_n}$$

főtagja megegyezik, ezért  $p(x) - ce_1^{k_1} \dots e_n^{k_n}$  polinom főtagja a lexikografikus rendezés szerint kisebb, mint  $p$  főtagja, így az indukciós feltevés szerint e polinom már elemi szimmetrikus polinomok polinomja, s ezzel  $p$  is.

- A bizonyítás konstruktív, az alkalmazott „főtag kiküszöbölési eljárás” a gyakorlatban is használható.

**m** egy mankó arra, mi lesz a kivonandó elemi polinomok polinomja:

$$x_1^6 x_2^4 x_3^3 x_4 \quad (\text{és van még } x_5 \text{ is}) \rightsquigarrow \begin{array}{cccccc} x_1 & x_1 & x_1 & x_1 & x_1 & x_1 \\ x_2 & x_2 & x_2 & x_2 & & \\ x_3 & x_3 & x_3 & & & \\ x_4 & & & & & \end{array}$$

oszloponként megszámlálva a változókat:  $e_4 e_3^2 e_2 e_1^2$

**P** Legyen  $p(x, y, z) = x^2 + y^2 + z^2$ . Állítsuk elő elemi polinomok polinomjaként.

**M** A lexikografikus rendezésben legyen  $x \succ y \succ z$ . A főtag  $x^2y^0z^0$ , tehát  $i_1 = 2, i_2 = 0, i_3 = 0$ .

Innen  $k_1 = 2, k_2 = 0, k_3 = 0$ , azaz  $p_1(x, y, z) =$

$$p(x, y, z) - (x + y + z)^2 = -2xy - 2xz - 2yz = -2(xy + xz + yz)$$

$$p(x, y, z) = (x + y + z)^2 - 2(xy + xz + yz) = e_1(x, y, z)^2 - 2e_2(x, y, z).$$

P Legyen  $p(x, y) = x^5 + 2x^4y + 3x^3y^2 + 3x^2y^3 + 2xy^4 + y^5$ . Állítsuk elő elemi polinomok polinomjaként.

- A főtag  $x^5$ ,  $i_1 = 5, i_2 = 0 \rightsquigarrow k_1 = 5, k_2 = 0 \rightsquigarrow$

$$\begin{aligned} - p_1(x, y) &= p(x, y) - (x + y)^5 \\ &= x^5 + 2x^4y + 3x^3y^2 + 3x^2y^3 + 2xy^4 + y^5 \\ &\quad - (x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5) \\ &= -3x^4y - 7x^3y^2 - 7x^2y^3 - 3xy^4 \end{aligned}$$

- A főtag  $-3x^4y$ ,  $i_1 = 4, i_2 = 1 \rightsquigarrow k_1 = 3, k_2 = 1, \rightsquigarrow$

$$\begin{aligned} - p_2(x, y) &= p_1(x, y) + 3(x + y)^3(xy) \\ &= -3x^4y - 7x^3y^2 - 7x^2y^3 - 3xy^4 \\ &\quad + 3(x^4y + 3x^3y^2 + 3x^2y^3 + xy^4) \\ &= 2x^3y^2 + 2x^2y^3 = 2(x + y)(xy)^2 \end{aligned}$$

-  $p = e_1^5 + p_1 = e_1^5 - 3e_1^3e_2 + p_2 = e_1^5 - 3e_1^3e_2 + 2e_1e_2^2$ , tehát  
 $p = e_1^5 - 3e_1^3e_2 + 2e_1e_2^2$ .

- P** Legyen  $a, b, c$  az  $x^3 - 2x^2 + 4x + 3$  polinom három gyöke. Adjunk meg olyan 1-főegyütthetős polinomot, melynek gyökei  $ab, ac, bc$ .
- M** A gyökök és együtthetők összefüggései szerint

$$a + b + c = 2$$

$$ab + ac + bc = 4$$

$$abc = -3$$

A gyökök és együtthetők kapcsolata a keresett  $(x - ab)(x - ac)(x - bc)$  polinomra:

$$ab + ac + bc = 4$$

$$a^2bc + ab^2c + abc^2 = abc(a + b + c) = -6$$

$$(ab)(ac)(bc) = (abc)^2 = 9$$

innen a keresett polinom:  $x^3 - 4x^2 - 6x - 9$ .

# Egyebek

---

## Polinominterpoláció



**K** Adva vannak az  $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n \in F$  számok, ahol  $F$  test, és  $x_i \neq x_j$ , ha  $i \neq j$ . Keresünk olyan  $p \in F[x]$  polinomot, melyre  $p(x_i) = y_i$  ( $i = 1, 2, \dots, n$ ).

**M** Ha ilyen  $p$  van, akkor  $\infty$  sok van, mert  $p(x) + f(x) \prod_{i=1}^n (x - x_i)$  is jó, ahol  $f$  tetszőleges polinom.

T **Lagrange-interpoláció** Adva vannak az

$x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n \in F$  számok, ahol  $F$  test, és  $x_i \neq x_j$ , ha  $i \neq j$ . Ekkor **pontosan egy** olyan **legfeljebb  $n - 1$ -edfokú**  $p \in F[x]$  polinom létezik, melyre  $p(x_i) = y_i$  ( $i = 1, 2, \dots, n$ ).

B **(Létezés)** 
$$L_i(x) = \frac{(x - x_1) \dots (x - x_{i-1})(x - x_{i+1}) \dots (x - x_n)}{(x_i - x_1) \dots (x_i - x_{i-1})(x_i - x_{i+1}) \dots (x_i - x_n)}$$

$$L_i(x_j) = \begin{cases} 1, & \text{ha } i = j, \\ 0, & \text{ha } i \neq j. \end{cases}$$

$$p(x) = \sum_{i=1}^n y_i L_i(x)$$

**(Egyértelműség)** ha  $p, q \in F[x]$  két legfeljebb  $n - 1$ -edfokú polinom, melyre  $p(x_i) = q(x_i)$ , azaz  $(p - q)(x_i) = 0$  minden  $i = 1, 2, \dots, n$ -re.

$p - q$  foka legfeljebb  $n - 1$ , gyökeinek száma  $n$ , akkor  $p - q = 0$ , azaz  $p = q$ .

$$\mathbf{P} \begin{array}{c} x_k \quad -1 \quad 0 \quad 1 \quad 2 \\ \hline y_k \quad -5 \quad 5 \quad 5 \quad 7 \end{array}$$

$$\mathbf{M} \quad L_1(x) = \frac{(x)(x-1)(x-2)}{(-1)(-1-1)(-1-2)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 - \frac{1}{3}x$$

$$L_2(x) = \frac{(x+1)(x-1)(x-2)}{(0+1)(0-1)(0-2)} = \frac{1}{2}x^3 - x^2 - \frac{1}{2}x + 1$$

$$L_3(x) = \frac{(x+1)(x)(x-2)}{(1+1)(1)(1-2)} = -\frac{1}{2}x^3 + \frac{1}{2}x^2 + x$$

$$L_4(x) = \frac{(x+1)(x)(x-1)}{(2+1)(2)(2-1)} = \frac{1}{6}x^3 - \frac{1}{6}x$$

$$-5L_1 + 5L_2 + 5L_3 + 7L_4 = 2x^3 - 5x^2 + 3x + 5$$

## Egyebek

---

Polinominterpoláció véges testek fölött

- T** Véges testek fölött minden függvény egyenlő egy polinomfüggvénnyel. Ráadásul minden függvényhez végtelen sok ilyen polinom is létezik.
- m** Mi eddig csak a  $\mathbb{Z}_p$  testet tanultuk, vannak prímszámrendű véges testek is (jelölésük  $\mathbb{F}_q$  vagy  $\text{GF}(q)$ , ahol  $q = p^e$  valamilyen  $p$  prímszámra és  $e$  egészre), és az állítás ezekre is igaz.
- B** Ha  $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  tetszőleges függvény, akkor az  $f(i)$  ( $i \in \mathbb{Z}_p$ ) értékekből képezhetünk egy legfőbb  $p - 1$ -edfokú interpolációs polinomot, mely  $f$ -fel azonos értékeket vesz fel. A „kis” Fermat-tétel szerint  $x^p \equiv x \pmod{p}$  minden  $x \in \mathbb{Z}$ -re, így  $x^p - x = 0$  a  $\mathbb{Z}_p$ -ben. Ha  $g$  olyan polinom, hogy minden  $c \in \mathbb{Z}_p$  esetén  $f(c) = g(c)$ , akkor  $g(x)$ -et maradékosan osztva  $x^p - x$ -szel olyan egy legfőbb  $p - 1$ -edfokú polinomot kapunk, ami megegyezik a Lagrange-féle interpolációs polinommal, azaz a  $g(x) - a(x)(x^p - x)$  polinommal, ahol  $a(x) \in \mathbb{Z}_p[x]$  a maradékos osztás hányadosa.

- F Egy széf kódja egy  $[0, p - 1]$ -be eső egész, és  $p$  prím. Osszuk meg ezt  $n$  ember közt úgy, hogy közülük bármelyik 3 ki tudja nyitni a széfet, de semelyik 2 ne tudjon meg a kódról semmit.
- M Legyen  $f \in \mathbb{Z}_p[x]$  egy másodfokú polinom, a széf kódja legyen  $f(0)$ . A  $k$ -adik embernek adjuk oda  $f(k)$  értékét ( $k = 1, 2, \dots, n$ ). Bármely 3 ember a három  $(i, y_i), (j, y_j), (k, y_k)$  párból egyértelműen fel tudja írni  $f$ -et, amiből megkapja  $f(0)$ -t, de 2 ember nem tud még a kódról semmit, mert minden  $t \in \mathbb{Z}$  értékre pontosan egy legfőbb másodfokú polinom van, melynek grafikonja átmegy az  $(i, y_i), (j, y_j), (0, t)$  pontokon.
- K **(Titokmegosztás)** Egy széf kódja egy  $[0, p - 1]$ -be eső egész, ahol  $p$  prím.  $n$  résztvevő mindegyike megkapja egy legfőbb  $k - 1$ -fokú  $a(x) \in \mathbb{Z}_p[x]$  polinom  $(x_i, a(x_i))$  párját ( $i = 1, 2, \dots, k, k < p$ ). Bármely  $k$  résztvevő fel tudja tárni a titkot, de semelyik legfőbb  $k - 1$  résztvevő nem tud meg semmit a titokról.