

Diszkrét Matematika III

ALGEBRA

Polinomok

Gabor Farkas

farkasg@inf.elte.hu

gaborfarkasphd.wixsite.com/gaborfarkasphd

2017 Tavasz

ELTE

Legyen R gyűrű. R feletti egyváltozós (egy határozatlanú) **polinomoknak** nevezzük az

$$(a_0, a_1, \dots, a_n, \dots)$$

végtelen sorozatokat, amelyekben $a_i \in R$ ($i = 0, 1, \dots$), és csak véges sok a_i különbözik 0-tól. Az a_i elemek a polinom **együtthatói**.

Az R feletti egyváltozós polinomok halmazát $R[x]$ -szel jelöljük.

Ha n a legnagyobb olyan index, amire $a_n \neq 0$ de bármely $i > n$ -re $a_i = 0$: a_n **főegyüttható**.

A továbbiakban legyen:

$f = (a_0, a_1, \dots, a_n, \dots)$ és $g = (b_0, b_1, \dots, b_m, \dots)$ R feletti polinom.

$$f = g \iff \forall i : a_i = b_i$$

Def

Műveletek $R[x]$ -en:

1. $u = f + g = (c_0, \dots, c_q, \dots), \quad c_i = a_i + b_i \quad (i \in \mathbf{N}_0)$

2. $v = f \cdot g = (d_0, \dots, d_s, \dots),$ ahol

$$d_k = \sum_{i=0}^k a_i \cdot b_{k-i} = a_0 \cdot b_k + a_1 \cdot b_{k-1} + \dots + a_k \cdot b_0$$

3. $a \in R$ esetén $a \cdot f = (a \cdot a_0, \dots, a \cdot a_n, \dots).$

Tétel (polinomgyűrű)

Ha R (egységelemes/ kommutatív/ nullosztómentes) gyűrű, akkor $R[x]$ is (egységelemes/ kommutatív/ nullosztómentes) gyűrű.

1. Egységelem az $(e, 0, \dots, 0, \dots)$ polinom, ahol e az R egységeleme.
2. Az $a \rightarrow f_a = (a, 0, \dots, 0, \dots)$ megfeleltetés injektív és művelettartó.

Ekkor $\forall f$ R feletti polinomra

$$a \cdot f = f_a \cdot f$$

$\Rightarrow R$ elemei R feletti polinomoknak tekinthetők (**konstans polinomok**).

A változó fogalma

Legyen $x = (0, e, 0, \dots, 0, \dots)$

Lehet, hogy $e \notin R$!!!

2. művelet definíciója $\Rightarrow$

$$x^2 = x \cdot x = (0 \cdot 0 = 0, e \cdot 0 + 0 \cdot e = 0, 0 \cdot 0 + e \cdot e + 0 \cdot 0 = e, \\ 0 \cdot 0 + e \cdot 0 + 0 \cdot e + 0 \cdot 0 = 0, \dots).$$

$$\Rightarrow x^n = (0, \dots, e, 0, \dots), \quad n \in \mathbb{N}.$$

$n+1$ edik pozíció (n . index)

Legyen továbbá $x^0 = (e, 0, \dots, 0, \dots)$, ekkor

$$f = (a_0, a_1, \dots, a_n, \dots) =$$

$$= (a_0, 0, \dots, 0, \dots) + \dots + (0, 0, \dots, a_n, \dots) =$$

$$= a_0 + a_1 x + \dots + a_n x^n + \dots,$$



ahol az $a_i \in R$ az $(a_i, 0, \dots, 0, \dots)$ polinomnak felel meg.

Def

Legyen $f = a_0 + a_1x + \dots + a_nx^n \in R[x]$ és $1 \leq i \leq n$, ekkor

a_i az **i -edfokú tag együtthatója**.

A 0-adfokú tag együtthatója a polinom **konstanstagja**.

Ha $a_n \neq 0$, akkor a_n a polinom **főegyütthatója**, és n a polinom **foka** (jel: $\deg(f)$).

Nullpolinom : $(0, 0, \dots) \in R[x]$ (nincs főegyütthatója).

Nullpolinom foka -1 ($-\infty$).

Monom : $f(x) = a_ix^i$ alakú polinom.

Konstans polinom: $\deg(f) \leq 0$.

Lineáris polinom: $\deg(f) \leq 1$.

Főpolinom (normált polinom): a főegyütthatója R egységeleme

Ha R nullosztómentes és $f, g \in R[x]^* \Rightarrow$

$$\deg(f + g) \leq \max(\deg(f), \deg(g)).$$

Ha $h = fg$, akkor h főegyütthatója $h_k = a_n b_m$, ahol $k = n + m$

tehát $\deg(f \cdot g) = \deg(f) + \deg(g) \geq \max(\deg(f), \deg(g))$.

Tétel (polinomok maradékos osztása)

Legyen R egységelemes integritási tartomány, $f, g \in R[x]$ és g főegyütthatója b_k , legyen R -ben egység.

Ekkor **egyértelműen léteznek** olyan $q, r \in R[x]$ polinomok, melyekkel

$$f(x) = g(x) \cdot q(x) + r(x), \text{ ahol}$$

$$\deg(r) < \deg(g).$$

1. Egzisztencia.

1.1. Ha $f = 0$, vagy $n < k \Rightarrow$

$$q(x) \equiv 0, \quad r(x) = f(x) .$$

1.2. Legyen most $n \geq k$. n szerinti teljes indukció:

1.2.1. Ha $n = k = 0 \Rightarrow$ akkor

$$r = 0, \quad q = a_n \cdot b_k^{-1},$$

mivel b_k egység R -ben.

1.2.2. Legyen $n > 0$ és tfh az n -nél kisebb fokszámok esetén igaz az állítás.

$$f_1(x) = f(x) - g(x) \cdot a_n \cdot b_k^{-1} \cdot x^{n-k}. \quad (*)$$

1.2.2.1. Ha $f_1 = 0 \Rightarrow$

$$q(x) = a_n \cdot b_k^{-1} \cdot x^{n-k}, \quad r(x) = 0.$$

1.2.2.2. Ha $\deg(f_1) < \deg(g)$, ind. feltétel $\Rightarrow$

$$\exists q_1(x), r_1(x) \in R[x] :$$

$$f_1(x) = g(x) \cdot q_1(x) + r_1(x),$$

ahol

$$\deg(r_1) < \deg(g).$$

$$(*) \Rightarrow f(x) = g(x) \cdot a_n \cdot b_k^{-1} \cdot x^{n-k} + g(x) \cdot q_1(x) + r_1(x),$$

$$f(x) = g(x) \cdot (a_n \cdot b_k^{-1} \cdot x^{n-k} + q_1(x)) + r_1(x).$$

$q(x)$

$r(x)$

2. Unicitás.

$$\text{Tfh } f = g \cdot q_1 + r_1 = g \cdot q_2 + r_2 \Rightarrow$$

$$g \cdot (q_1 - q_2) = r_2 - r_1.$$

Tegyük fel indirekte, hogy $q_1 - q_2 \neq 0 \Rightarrow$

$$\deg(r_2 - r_1) = \deg(g \cdot (q_1 - q_2)) \geq \deg(g)$$



Kaptuk, hogy $q_1 - q_2 = 0 \Rightarrow$

$$r_2 - r_1 = 0.$$



Ész

Legyen R test, és $f \in R[x]^*$ esetén $\varphi : R[x]^* \rightarrow \mathbb{N}_0$, $\varphi(f) = \deg(f)$.

Ekkor $R[x]$ φ -vel euklidészi gyűrűt alkot.

Def

Legyen S egységelemes integritási tartomány, R részgyűrűje S -nek, és R tartalmazza S egységelemét (e). Egy $f \in R[x]$ polinom $c \in S$ -beli **helyettesítési értéke**

$$f(c) = a_0 + a_1c + \dots + a_nc^n.$$

c az f **gyöke**, ha a helyettesítési érték 0.

Polinomfüggvény :

$f: R \rightarrow R$, ahol $f(c) = a_0 + a_1 \cdot c + \dots + a_n \cdot c^n \in R$, és $c \in R$.

f és g polinomfüggvény egyenlő, ha minden $c \in R$ esetén $f(c) = g(c)$.

Ész

Két különböző polinom polinomfüggvénye megegyezhet! Legyen például $R = \mathbb{Z}_3$:

$$f = x^4 + x + 2 \neq g = x^3 + x^2 + 2 ,$$

$$f(0) = 2 = g(0) , \quad f(1) = 1 = g(1) , \quad f(2) = 2 = g(2) .$$

Tétel(gyöktényező leválasztása)

Legyen R egységelemes integritási tartomány, $f \in R[x]^*$, és $c \in R$ az f gyöke. Ekkor $\exists q \in R[x]^*$:

$$f(x) = (x - c) \cdot q(x).$$

Biz

$x - c$ polinom főegyütthatója egység $\Rightarrow$

maradékos osztás :

$$f(x) = (x - c) \cdot q(x) + r(x),$$

a. $r = 0 \Rightarrow$ kész.

b. $\deg(r) < \deg(x - c) = 1 \Rightarrow$

$$f(c) = (c - c) \cdot q(c) + r(c) = r(c) = 0.$$



Tétel(gyökök száma)

Legyen $f \in R[x]^*$, ahol R egységelemes integritási tartomány, és $\deg(f) = n \geq 0$. Ekkor f -nek legfeljebb n különböző gyöke van R -ben.

Biz

(n szerinti teljes indukció)

$n = 0$ esetén $f \in R$: kész

Tegyük fel, hogy $n > 1$, és az n -nél kisebb fokúakra igaz az állítás.

Legyen $c \in R$ gyöke f -nek :

$$f(x) = (x - c) \cdot g(x), \text{ ahol } \deg(g) = \deg(f) - 1 = n - 1$$

$$\text{Ha } d \text{ is gyöke } f\text{-nek, akkor } f(d) = 0 = (d - c) \cdot g(d) = 0,$$

$$R \text{ nullosztómentessége} \Rightarrow d = c \text{ vagy } g(d) = 0.$$

$$\text{Ind. feltétel} \Rightarrow g \text{ különböző gyökeinek száma} \leq n - 1.$$

$\Rightarrow$ ha c nem gyöke g -nek, akkor is f -nek max. n különböző gyöke van



Lemma(polinomok egyezősége)

Ha két, legfeljebb n -edfokú polinom (nullpolinomot is beleértve) $n + 1$ különböző helyen ugyanazt az értéket veszi fel, akkor megegyezik.

Biz

Tfh f és g ilyen polinom, de különbözőek $\Rightarrow$

$f - g$ polinom foka $\leq n$ és legalább $n + 1$ gyöke van



Lemma(polinomfüggvények különbözősége)

Ha a tartóhalmaz végtelen, akkor két különböző polinomhoz nem tartozik ugyanaz a polinomfüggvény.

Biz

Ha így lenne $f - g$ polinomnak végtelen sok gyöke lenne.



Def**Horner-elrendezés**

$f(c) = ?$

n szorzással és n összeadással megkapjuk !

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

$$f(c) = a_0 + a_1c + \dots + a_nc^n = a_nc^n + \dots + a_1c + a_0 =$$

$$= (a_nc^{n-1} + \dots + a_1)c + a_0 = ((a_nc^{n-2} + \dots + a_2)c + a_1)c + a_0 =$$

$$= ((\dots(a_nc + a_{n-1})c + a_{n-2})c + \dots + a_1)c + a_0.$$

Példa

$$f(x) = 5x^3 - 7x^2 + x - 8 = ((5x - 7)x + 1)x - 8.$$

c	5	-7	1	-8	$f(c)$
3		5	8	25	67

Gyökök száma

Függ R -től !

Keressük az $f(x) = x^2 + 1$ polinom gyökeit

1. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ –ben nincs gyöke
2. $\mathbb{C}[x]$ –ben a gyökök száma kettő: i és $-i$
3. $\mathbb{Z}_2[x]$ –ben egy gyöke van: 1
4. $\mathbb{Z}_3[x]$ –ben nincs gyöke .
5. $\mathbb{Z}_5[x]$ –ben két gyöke van: 2 és 3 .

Def

Legyen R egységelemes integritási tartomány, és

$$f \rightarrow f' = a_1 + 2a_2x + \dots + n a_n x^{n-1}$$

$R[x]$ -nek önmagába való leképezése a következő feltételekkel:

1. $c' = 0$, ha c konstans polinom,

2. $(f + g)' = f' + g'$,

3. $(f \cdot g)' = f'g + fg'$,

4. $(e \cdot x)' = e$.

Az f' polinom az f **(algebrai) deriváltpolinomja** .

Def

Legyen R egységelemes integritási tartomány, és $f \in R[x]^*$. Azt mondjuk, hogy $c \in R$ az $f(x)$ **n -szeres gyöke** ($n \in \mathbb{N}^+$), ha

$$(x - c)^n \mid f(x) \text{ és } (x - c)^{n+1} \nmid f(x).$$

Jel:

$$(x - c)^n \parallel f(x).$$

Tétel(többszörös gyökök)

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $c \in R$, $n \in \mathbb{N}^+$

Ha c az $f(x)$ -nek n -szeres gyöke,

akkor c az $f'(x)$ -nek **legalább** $(n - 1)$ -szeres gyöke, és

pontosan $(n - 1)$ -szeres gyök abban az esetben, ha $\text{char}(R) \nmid n$.

Biz

$$= (x - c)^{n-1} \cdot ((x - c) \cdot g'(x) + ng(x)) = (x - c)^{n-1} \cdot h(x).$$

Tehát c legalább $(n-1)$ -szeres gyöke $f'(x)$ -nek és

$$h(c) = (c - c) \cdot g'(c) + ng(c) = ng(c) = \underbrace{g(c) + \dots + g(c)}_{n \text{ db}}.$$

$$(x - c)^n \mid f(x) \Rightarrow g(c) \neq 0.$$

Ha $\text{char}(R) \nmid n \Rightarrow$ az összeg sosem 0.

**Ész**

Fordítva nem igaz pl :

$$f(x) = x^n + 1, \quad f'(x) = nx^{n-1} \Rightarrow$$

$f'(x)$ –nek a 0 $(n - 1)$ –szeres gyöke, $f(x)$ –nek nem .

Ész

test fölötti polinomok euklidészi gyűrűt alkotnak

$\Rightarrow$

felbonthatatlanok és a prímek egybeesnek.

$\forall$ nemnulla konstans polinom egység.

$\forall$ elsőfokú polinom felbonthatatlan.

Komplex eset

Algebra alaptétele $\Rightarrow$

$f \in \mathbb{C}[x] :$

$$f(x) = a_n (x - c_1)^{\alpha_1} \cdot (x - c_2)^{\alpha_2} \cdot \dots \cdot (x - c_k)^{\alpha_k}$$

ahol $c_j \in \mathbb{C}$, $c_i \neq c_j$, ha $i \neq j$ és

$$\alpha_1 + \alpha_2 + \dots + \alpha_k = n = \deg f.$$

$\Rightarrow$

$\mathbb{C}$ fölött az irreducibilis polinomok pontosan az elsőfokúak.

Valós eset

Ész

Ha $f \in \mathbb{R}[x]$, $c \in \mathbb{C}$ és $f(c) = 0$, akkor

$$f(\bar{c}) = 0 \quad \text{is teljesül.}$$

Legyen $c \in \mathbb{C} \setminus \mathbb{R}$ gyöke $f \in \mathbb{R}[x]$ -nek $\Rightarrow$

$$x - c \mid f(x) \quad \text{és} \quad x - \bar{c} \mid f(x),$$

felbonthatatlanok és nem asszociáltak $\Rightarrow$

$$g(x) = (x - c) \cdot (x - \bar{c}) \mid f(x) .$$

$$g(x) = x^2 - 2\operatorname{Re}(c)x + |c|^2 \in \mathbb{R}[x] .$$

$$\Rightarrow \exists h(x) \in \mathbb{R}[x] :$$

$$f(x) = g(x) h(x),$$

$$\text{ahol } \deg(h) = \deg(f) - 2 .$$

$$\Rightarrow$$

$\forall f \in \mathbb{R}[x]$ legfeljebb 2-fokú polinomok szorzatára bontható $\mathbb{R}$ felett.

$$\Rightarrow$$

Azok a másodfokú polinomok felbonthatatlanok, amelyeknek nincs valós gyökük.

Racionális eset

Tétel(Gauss-tétel)

Legyen R tetszőleges Gauss – gyűrű és K a hányadosteste.

1. Ha egy $f \in R[x]$ polinom előállítható két nem konstans g, h polinom szorzataként $K[x]$ -ben, akkor $R[x]$ -ben is előállítható két g^*, h^* polinom szorzataként, úgy hogy

g és g^* , illetve h és h^* asszociáltak $K[x]$ -ben.

2. $R[x]$ is Gauss-gyűrű.

Def

Legyen R Gauss-gyűrű. $R[x]$ egy elemét **primitív polinomnak** nevezzük, ha együtthatóinak legnagyobb közös osztója az egységelem.

Tétel (Schönemann-Eisenstein-tétel)

Ha az R Gauss-gyűrű feletti legalább elsőfokú f primitív polinomhoz van olyan $p \in R$ prímelem, amely nem osztója a főegyütthatónak, de osztója minden más együtthatónak, p^2 viszont nem osztója a konstans tagnak, akkor f irreducibilis. Hasonlóan, ha az R Gauss-gyűrű feletti legalább elsőfokú f primitív polinomhoz van olyan $p \in R$ prímelem, amely nem osztója a konstans tagnak, de osztója minden más együtthatónak, p^2 viszont nem osztója a főegyütthatónak, akkor f irreducibilis.

Legyen tehát $f = x^n + p$, ahol p prím, n pozitív egész.

$\Rightarrow f$ irreducibilis R felett és

a Gauss – tétel miatt R hányadosteste felett is irreducibilis.

$$f(x) = 6x^2 + 12x + 12 = 2 \cdot 3 \cdot (x^2 + 2x + 2)$$

$\mathbb{Q}[x]$ -ben irreducibilis

$\mathbb{Z}[x]$ -ben nem irreducibilis

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

$$g(x) = 6 \cdot f = 2x^2 + 3x + 18$$

$\mathbb{Q}[x]$ -beliek és $f \sim g$, $f \notin \mathbb{Z}[x]$

$\mathbb{Z}$ euklidészi gyűrű $\Rightarrow$

$\mathbb{Z}$ Gauss - gyűrű $\Rightarrow$

$\mathbb{Z}[x]$ Gauss - gyűrű

$\mathbb{Z}[x]$ nem alkot euklidészi gyűrűt, különben

$$(x, 2) = 1 \Rightarrow$$

$$1 = u2 + vx$$



$\mathbb{Z}[x]$ nem alkot főideálgyűrűt:

$$J = \{f(x) \mid f(x) \in \mathbb{Z}[x] \text{ és } f(0) \equiv 0 \pmod{2}\} =$$

$$= \langle 2, x \rangle \subset \mathbb{Z}[x].$$

