Diszkrét matematika 2

7. előadás
Polinomok

Mérai László
merai@inf.elte.hu
https://sites.google.com/view/laszlomerai

Komputeralgebra Tanszék

2023 ősz

Emlékeztető: Polinomok legnagyobb közös osztója

Definíció

Két polinom f és g legnagyobb közös osztója, $h = (f, g) = \mathrm{lnko}(f, g)$, ha

- közös osztó: $h \mid f$ és $h \mid g$;
- legnagyobb: ha $q \mid f$ és $q \mid g \Rightarrow q \mid h$;
- h főegyütthatója 1.

Példa

$$(x - 1, x + 1) = 1 \quad \text{és} \quad (x^2 + 2x + 1, 50x^2 - 50) = x + 1.$$

Megjegyzés:

- A legnagyobb közös osztó kiszámítható az euklideszi algoritmussal.

Emlékeztető: Polinomok legnagyobb közös osztójának kiszámítása, euklidészi algoritmus

Feltehető, hogy $\deg f, \deg g \geq 1$. Végezzük el a következő maradékos osztásokat:

$$\begin{aligned}
f &= q_1 g + r_1 & \qquad \deg r_1 &< \deg g \\
g &= q_2 r_1 + r_2 & \deg r_2 &< \deg r_1 \\
r_1 &= q_3 r_2 + r_3 & \deg r_3 &< \deg r_2 \\
&\vdots \\
r_{\ell-2} &= q_\ell r_{\ell-1} + r_\ell & \deg r_\ell &< \deg r_{\ell-1} \\
r_{\ell-1} &= q_{\ell+1} r_\ell
\end{aligned}$$

Ekkor $(f, g) = r_\ell$.

Emlékeztető: Polinomok legnagyobb közös osztójának kiszámítása, euklidészi algoritmus

Példa

Legyen $f = x^4 + x^3 + x^2 + 2x + 1 \in \mathbb{Z}_5[x]$ és $g = x^4 + x^3 + 4x^2 + 1 \in \mathbb{Z}_5[x]$. $(f, g) = ?$

$$f = g + (2x^2 + 2x)$$

$$g = (3x^2 + 2)(2x^2 + 2x) + (x + 1)$$

$$2x^2 + 2x = 2x(x + 1),$$

i	q_i	r_i
-1	$-$	f
0	$-$	g
1	1	$2x^2 + 2x$
2	$3x^2 + 2$	$x + 1$
3	$2x$	0

tehát $(f, g) = x + 1$.

Azonban az euklideszi algoritmus ennél többre is képes!

Bővített euklidészi algoritmus

Tétel

Minden f, g polinomok esetén léteznek u, v polinomok, hogy $(f, g) = uf + vg$.

Bizonyítás. Legyenek q_i, r_i az euklideszi algoritmussal megkapott polinomok.

- Legyen $u_{-1} = 1$, $u_0 = 0$ és $i \geq 1$ esetén legyen $u_i = u_{i-2} - q_i u_{i-1}$.
- Hasonlóan, legyen $v_{-1} = 0$, $v_0 = 1$ és $i \geq 1$ esetén legyen $v_i = v_{i-2} - q_i v_{i-1}$.

Ekkor $u_i f + v_i g = r_i$, speciálisan $u_\ell f + v_\ell g = r_\ell = (f, g)$.

Példa Legyen $f = x^4 + x^3 + x^2 + 2x + 1 \in \mathbb{Z}_5[x]$ és $g = x^4 + x^3 + 4x^2 + 1 \in \mathbb{Z}_5[x]$. Ekkor

i	r_i	q_i	u_i	v_i	$r_i = u_i f + v_i g$
-1	f	$-$	1	0	$f = 1 \cdot f + 0 \cdot g$
0	g	$-$	0	1	$g = 0 \cdot f + 1 \cdot g$
1	$2x^2 + 2x$	1	1	-1	$2x^2 + 2x = 1 \cdot f - 1 \cdot g$
2	$x + 1$	$3x^2 + 2$	$2x^2 + 3$	$3x^2 + 3$	$x + 1 = (2x^2 + 3) \cdot f + (3x^2 + 3) \cdot g$

Többszörös gyökök

Emlékeztető

Egy f polinomnak legfeljebb $\deg f$ gyöke lehet.

Azonban ez messze nem éles:
$f = x^{10}$ polinomnak foka $\deg f = 10$, de gyökök száma 1.

Definíció

- Egy f polinomnak az x_1 érték gyöke, ha $(x - x_1) \mid f$.
- Egy f polinomnak az x_1 érték k-szoros gyöke, ha $(x - x_1)^k \mid f$ de $(x - x_1)^{k+1} \nmid f$.
- Egy f polinomnak az x_1 érték többszörös gyöke, ha legalább kétszeres gyöke.

Példa Az $f = (x-1)(x+2)^2(x-i)^3 \in \mathbb{C}[x]$ polinomnak az

- $x_1 = 1$ egyszeres gyöke,
- $x_2 = -2$ kétszeres gyöke, többszörös gyök,
- $x_3 = i$ háromszoros gyöke, többszörös gyök,
- $x_4 = \sqrt{2}$ nem gyöke (nullaszoros gyöke).

Többszörös gyökök

Emlékeztető

Egy f polinomnak legfeljebb $\deg f$ gyöke lehet.

Azonban ez messze nem éles:
$f = x^{10}$ polinomnak foka $\deg f = 10$, de gyökök száma 1.

Definíció

- Egy f polinomnak az x_1 érték gyöke, ha $(x - x_1) \mid f$.
- Egy f polinomnak az x_1 érték k-szoros gyöke, ha $(x - x_1)^k \mid f$ de $(x - x_1)^{k+1} \nmid f$.
- Egy f polinomnak az x_1 érték többszörös gyöke, ha legalább kétszeres gyöke.

Hasonlóan bizonyítható:

Tétel (Biz: HF)

Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$. Egy $f \in \mathbb{K}[x]$ polinomnak multiplicitással számolva legfeljebb $\deg f$ gyöke lehet.

Formális derivált

A célunk algoritmust adni a többszörös gyökök megtalálására.

Definíció

Polinomokra definiáljuk a f' formális deriváltat a következő módon:

- $(x^n)' = nx^{n-1}$
- $(cf)' = cf'$
- $(f+g)' = f' + g'$

Tétel

Az így definiált formális derivált teljesíti a szorzat szabályt:

$$(fg)' = f'g + fg'.$$

Megjegyzés: Ez egy formális deriválás, hasonlóság az analitikus deriválthoz csak a véletlen műve.
Vannak más formális deriváltak is, amik eltérnek az analitikustól.

Formális derivált

Formális derivált: $(x^n)' = nx^{n-1}, \quad (cf)' = cf', \quad (f+g)' = f' + g'.$

Tétel (Szorzat szabály) $(fg)' = f'g + fg'.$

Bizonyítás: Legyen $f = c_n x^n + \cdots + c_0$ és $g = d_m x^m + \cdots + d_0$. Ekkor

$$(fg)' = \Big((c_n x^n + \cdots + c_0)(d_m x^m + \cdots + d_0)\Big)' = \left(\sum_{i,j} c_i d_j x^{i+j}\right)' = \sum_{i,j} \left(c_i d_j x^{i+j}\right)'.$$

Itt

$$\left(c_i d_j x^{i+j}\right)' = (i+j) c_i d_j x^{i+j-1} = i c_i x^{i-1} \cdot d_j x^j + c_i x^i \cdot j d_j x^{j-1} = (c_i x^i)' d_j x^j + c_i x^i (d_j x^j)'$$

$\square$

Példa

$$\left(x^5 + x^4 + x^3 + x^2 + x + 1\right)' = 5x^4 + 4x^3 + 3x^2 + 2x + 1$$

Formális derivált és többszörös gyökök

Tétel

Egy adott f polinomnak az x_1 érték többszörös gyöke, ha mind f-nek, mind f'-nek gyöke. Speciálisan f többszörös gyökei az (f,f') gyökei.

Bizonyítás.
Legyen x_1 az f-nek többszörös gyöke, azaz $f = (x-x_1)^2 \cdot g$ valamely g polinomra. Ekkor a szorzat szabály szerint

$$\begin{aligned} f' = \left((x-x_1)^2 \cdot g\right)' &= \left((x-x_1)^2\right)' \cdot g + (x-x_1)^2 \cdot g' \\ &= 2(x-x_1) \cdot g + (x-x_1)^2 \cdot g' = (x-x_1) \cdot \left(2g + (x-x_1) \cdot g'\right). \end{aligned}$$

□

Következmény

Az f polinomnak nincs többszörös gyöke, ha $(f,f') = 1$.

Formális derivált és többszörös gyökök

Tétel

Egy adott f polinomnak az x_1 érték többszörös gyöke, ha mind f-nek, mind f'-nek gyöke. Speciálisan f többszörös gyökei az (f, f') gyökei.

Példa

Legyen $f = x^4 + 3x^3 + 4x^2 + 3x + 1 \in \mathbb{Z}_5[x]$. Ekkor $f' = 4x^3 + 4x^2 + 3x + 3$.
Az (f, f') kiszámolható az euklideszi algoritmussal:

i	r_i	q_i
-1	f	$-$
0	f'	$-$
1	$2x+2$	$4x+3$
2	0	$2x^2+4$

Mivel $(f, f') = x + 1$, így f-nek $x_1 = 4$ többszörös gyöke.

Polinomok felbontása

Emlékeztető:

- $\mathbb{C}$ felett az $ax^2 + bx + c = 0$ mindig megoldható, azaz az $f = ax^2 + bx + c \in \mathbb{C}[x]$ polinomnak mindig van gyöke.
- $\mathbb{C}$ felett az $ax^3 + bx^2 + cx + d = 0$ $\mathbb{C}$ felett mindig megoldható, azaz az $f = ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$ polinomnak mindig van gyöke.

Általában:

Algebra alaptétele

Legyen $f \in \mathbb{C}[x]$ egy pozitív fokú polinom: $\deg f \geq 1$. Ekkor f-nek van gyöke.

Polinomok felbontása

Algebra alaptétele

Legyen $f \in \mathbb{C}[x]$ egy pozitív fokú polinom: $\deg f \geq 1$. Ekkor f-nek van gyöke.

A gyöktényezőket egyenként kiemelve kapjuk a következő állítást.

Következmény

Legyen $f \in \mathbb{C}[x]$ egy n-ed fokú polinom. Ekkor f felírható a következő formában

$$f = a_n(x - x_1) \cdots (x - x_n).$$

Figyelem, az állítás nem igaz $\mathbb{R}[x]$-ben: az $f = x^2 + 2x + 3$ polinomnak nincs $\mathbb{R}$-ben gyöke: $f(a) = (a+1)^2 + 1 > 0$ minden $a \in \mathbb{R}$ esetén.

Azonban az állítás majdnem igaz $\mathbb{R}[x]$, $\mathbb{Q}[x]$ és $\mathbb{Z}_p[x]$ esetén is.