Diszkrét matematika 2

6. előadás
Polinomok

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

Komputeralgebra Tanszék

2023 ősz

Polinomok maradékos osztása

Tétel

Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$ és $f, g \in \mathbb{K}[x]$, $g \neq 0$. Ekkor léteznek olyan $q, r \in \mathbb{K}[x]$ polinomok, hogy

$$f = q \cdot g + r \quad \deg r < \deg g.$$

Példa

Legyen $f = x^3 + x + 1$ és $g = 2x^2 + x + 1$. Ekkor

$$f = \left(\frac{1}{2}x - \frac{1}{4}\right) g + \left(-\frac{3}{4}x - \frac{3}{4}\right)$$

Polinomok foka és gyökök száma

Tétel

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

Bizonyítás. A bizonyítás $\deg f$ szerinti teljes indukcióval.

- Ha $\deg f = 0$, azaz $f = c_0$, $c_0 \neq 0$, akkor f-nek nincs gyöke.
- Legyen $\deg f \geq 1$. Ha f-nek nincs gyöke, akkor igaz az állítás. Ellenkező esetben legyen $x_1 \in \mathbb{K}$ egy gyöke. Maradékos osztás tétele szerint

$$f = q \cdot (x - x_1) + r, \quad \deg r < 1, \quad \text{azaz } r \in \mathbb{K}.$$

Mivel $f(x_1) = 0 = q(x_1) \cdot (x_1 - x_1) + r$, így $r = 0$: $f = q \cdot (x - x_1)$, $\deg q = n - 1$. Ha $x_2 \neq x_1$ egy másik gyöke f-nek, akkor

$$0 = f(x_2) = q(x_2) \cdot (x_2 - x_1) \Longrightarrow q(x_2) = 0.$$

Mivel q-nek legfeljebb $\deg q = n - 1$ gyöke van, így f-nek legfeljebb $n - 1 + 1 = n$ gyöke lehet.

□

Polinomok foka és gyökök száma

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

Figyelem, a tétel $\mathbb{Z}_8[x]$-ben nem igaz:

$$f = x^2 + 2x \in \mathbb{Z}_8[x] \quad \text{esetén} \quad f(0) = f(2) = f(4) = f(6) = 0.$$

U.i.: Az $x_1 = 0$ gyöke a polinomnak. $(x - x_1) = (x - 0) = x$ tagot kiemelve kapjuk, hogy $f = x \cdot (x + 2)$. Azonban pl. $x_1 = 4$ szintén gyöke f-nek, mert $4 \cdot 6 \equiv 0 \mod 8$.

Következmény (A gyöktényező kiemelhetősége)

Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$. Legyen $f \in \mathbb{K}[x]$ és $x_0 \in \mathbb{K}$ egy gyöke. Ekkor f felírható az $f = (x - x_1) \cdot g$ formában valamely $g \in \mathbb{K}[x]$ polinommal.

Hasonlóan, az állítás $\mathbb{Z}_8[x]$-ben nem igaz.

Horner elrendezés

Legyen $f = c_n x^n + \cdots + c_0$. A polinomfüggvény $f(a)$ kiértékelése naiv módon: $f(a) = c_n a^n + \cdots + c_0$: n szorzás és $n-2$ hatványozás.

Horner elrendezés

a	c_n	c_{n-1}	$\ldots$	c_0
	$b_n = c_n$	$b_{n-1} = ab_n + c_{n-1}$	$\ldots$	$f(a) = ab_1 + c_0$

Példa

Legyen $f = 2x^4 + 3x^2 + 2x + 4 \in \mathbb{Z}_5[x]$ és számoljuk ki $f(2)$-t:

a	c_4	c_3	c_2	c_1	c_0
2	2	0	3	2	4
	2	4	1	4	2

Tehát $f(2) = 2$.

- A Horner elrendezés az $f = (((c_n x + c_{n-1})\, x + c_{n-2})\, x + \ldots)\, x + c_0$ felírás.
- A Horner elrendezés n szorzást és 0 hatványozást használ.

Horner elrendezés és maradékos osztás

Legyen $f = c_n x^n + \cdots + c_0$ és tekintsük az a-hoz tartozó Horner elrendezést:

a	c_n	c_{n-1}	$\ldots$	c_0
	$b_n = c_n$	$b_{n-1} = ab_n + c_{n-1}$	$\ldots$	$f(a) = ab_1 + c_0$

Ez valójában az $x - a$ lineáris polinommal való maradékos osztás:

$$f = (x - a) \cdot \left(b_n x^{n-1} + \cdots + b_1\right) + f(a).$$

Bizonyítás. (HF) Visszaszorzással, felhasználva, hogy $c_i = b_i - ab_{i+1}$. □

Példa

Legyen $f = 2x^4 + 3x^2 + 2x + 4 \in \mathbb{Z}_5[x]$ és számoljuk ki $f(2)$-t:

a	c_4	c_3	c_2	c_1	c_0
2	2	0	3	2	4
	2	4	1	4	2

Tehát $f(2) = 2$ és $f = (x - 2) \cdot \left(2x^3 + 4x^2 + x + 4\right) + 2$

Polinomok legnagyobb közös osztója

Definíció

Legyenek f, g polinomok. f osztja g-t, $f \mid g$, ha létezik h polinom, hogy $f \cdot h = g$.

Példa

- $x+1 \mid x^2+2x+1$, mert $x^2+2x+1 = (x+1)(x+1)$.
- $50x+50 \mid x^2+2x+1$, mert $x^2+2x+1 = (50x+50)\left(\frac{1}{50}x+\frac{1}{50}\right)$

Definíció

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

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

Polinomok legnagyobb közös osztójának kiszámítása, euklidészi algoritmus

Tétel

Bármely két f, g polinomnak létezik legnagyobb közös osztója, és az meghatározható az euklideszi algoritmussal.

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

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

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

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 $(f, g) = x + 1$.

Közös gyökök

Emlékeztető Az x_1 érték gyöke f-nak, ha az $x - x_1$ gyöktényező osztja f-et, $x - x_1 \mid f$

Példa

Az $f = (x-1)\cdot(x-2)\cdot(x-3)$ polinomnak az $1, 2, 3$ értékek a gyökei.

Állítás: Legyen $f, g \in \mathbb{K}$ ($\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$). Ekkor az f és g közös gyökei a $h = \text{lnko}(f, g)$ polinom gyökei.

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 $(f, g) = x + 1$. Azaz csak az $x_1 = -1 \equiv 4 \mod 5$ lesz a közös gyök:

a	0	1	2	3	4
$f(a)$	1	3	2	4	0

a	0	1	2	3	4
$g(a)$	1	2	1	0	0

Példa

Legyen $f = (x-1)\cdot(x-\sqrt{2})\cdot(x-3i) \in \mathbb{C}[x]$ és $g = x\cdot(x-\sqrt{2})\cdot(x-3i)$.
Ekkor $h = \text{lnko}(f, g) = (x-\sqrt{2})\cdot(x-3i) \in \mathbb{C}[x]$