Diszkrét matematika 2

5. előadás
Polinomok

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

Komputeralgebra Tanszék

2023 ősz

Polinomok és alkalmazásuk

A polinomok $x^2 + 2x + 1$, $x^5 + \frac{3}{2}x^2 - ix + i + \sqrt{2}$, ... típusú kifejezések.

Alkalmazásuk:

- Numerikus módszerek: bonyolult függvények közelítése

$$\sin(x) \approx x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!}, \qquad |x| < 1 \qquad \text{hiba} < 10^{-7}$$

$$e^x \approx 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} + \frac{x^7}{7!}, \qquad |x| < 1 \qquad \text{hiba} < 10^{-3}$$

- Hibajavító kódok: Adatátvitel során sérült jel rekonstrukciója

kódszavak $\longleftrightarrow$ polinomok

Polinomok és alkalmazásuk

A polinomok $x^2 + 2x + 1$, $x^5 + \frac{3}{2}x^2 - ix + i + \sqrt{2}$, ... típusú kifejezések.

Alkalmazásuk:

- Numerikus módszerek: bonyolult függvények közelítése
- Hibajavító kódok: Adatátvitel során sérült jel rekonstrukciója
- Komputeralgebra, szimbolikus számítások: határozott integrálok, differenciálegyenletek (pontos) megoldása

$$\int x^2 \mathrm{d}x = \frac{x^3}{3} + C$$

- Robotika: Robotkarok pontos mozgásának leírása

Polinomok formális bevezetése

Jelölés: legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_p\}$

Definíció

A $\mathbb{K}$ fölötti polinomok halmaza $\mathbb{K}[x]$ az x és $\mathbb{K}$ elemei által az $+, -, \cdot$ segítségével alkotott formális kifejezések :

$$\mathbb{K}[x] = \{c_n x^n + \cdots + c_0 : n \geq 0, c_n, \ldots, c_0 \in \mathbb{K}\}\,.$$

Adott polinom $f = c_n x^n + \cdots + c_0$ együtthatói a $c_n, \ldots, c_0$ számok,míg $c_n \neq 0$ esetén f foka $\deg f = n$ és főegyütthatója c_n. .

Példa

- $f = x^2 + 2x + 1 \in \mathbb{C}[x]$, $\deg f = 2$
- $g = x^5 + \frac{3}{2}x^2 - ix + i + \sqrt{2} \in \mathbb{C}[x]$, $\deg g = 5$
- $h = 3x^2 + 2x + 1 \in \mathbb{Z}_3[x]$, $\deg h = 1$ (ugyanis $3 \equiv 0 \mod 3$)

Polinomok formális bevezetése

Polinomok: $\mathbb{K}[x] = \{c_n x^n + \cdots + c_0 : n \geq 0, c_n, \ldots, c_0 \in \mathbb{K}\}$

- Alapvető tulajdonságok: $f, g \in \mathbb{K}[x]$:

$$f \pm g \in \mathbb{K}[x] \quad \text{és} \quad f \cdot g \in \mathbb{K}[x].$$

- Polinomok reprezentációja számítógépen :
A polinomokat véges hosszú sorozatokkal reprezentálhatjuk. Legyen $\mathbb{K}^* = \bigcup_{n \geq 0} \mathbb{K}^n$ és

$$f = c_n x^n + \cdots + c_0 \leftrightarrow \mathbf{f} = (c_0, c_1, \ldots, c_n) \in \mathbb{K}^*.$$

Ekkor $\mathbf{f} \pm \mathbf{h}$ koordinátánként (kiegészítve 0 komponensekkel). Szorzás:

$$(c_0, c_1, \ldots, c_n) \cdot (d_0, d_1, \ldots, d_m) = (c_0 d_0, c_0 d_1 + c_1 d_0, \ldots)$$

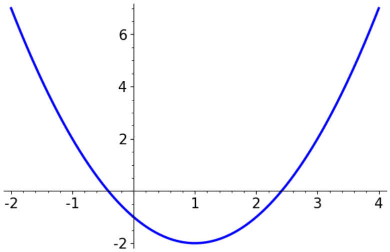
Polinomok és polinomfüggvények

Adott $f = c_n x^n + \cdots + c_0 \in \mathbb{K}[x]$ polinomhoz definiálhatjuk a hozzá tartózó polinomfüggvényt:

$$z \xrightarrow{f} f(z) = c_n z^n + \cdots + z_0 \in \mathbb{K}$$

Egy f polinomnak az x_0 érték a gyöke, ha a megfelelő polinomfüggvény ott a 0 értéket veszi fel:

$$x_0 \xrightarrow{f} f(x_0) = 0.$$



Az $f = x^2 - 2x - 1 \in \mathbb{R}[x]$ polinomhoz tartozó polinomfüggvény.

Polinomok és polinomfüggvények

Figyelem: A polinom és polinomfüggvény nem azonosak!
Az

$$f = 0 \in \mathbb{Z}_2[x] \quad \text{és} \quad g = x^2 - x \in \mathbb{Z}_2[x]$$

polinomok nem azonosak, $f \neq g$, de a hozzájuk tartozó polinomfüggvények azok:

$$f(0) = f(1) = 0 \quad \text{és} \quad g(0) = g(1) = 0.$$

Általában: adott p prímszám esetén az

$$f = 0 \in \mathbb{Z}_p[x] \quad \text{és} \quad g = x^p - x \in \mathbb{Z}_p[x]$$

polinomfüggvényei azonosak:

$$x^p - x = x(x^{p-1} - 1) \equiv 0 \mod p$$

u.i.: $p \mid x$ esetén triviális, $p \nmid x$ esetén Euler-Fermat tétel.
Konvenció: Adott f esetén legyen $f(x)$ a hozzá tartozó polinomfüggvény.

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

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

A bizonyítás konstruktív, algoritmust ad a q és r polinomok kiszámítására.

Polinomok maradékos osztása

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

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

Bizonyítás. A bizonyítás analóg az egész számok esetéhez, $\deg f$ szerinti teljes indukcióval bizonyítjuk.

- Ha $\deg f < \deg g$, akkor legyen $q = 0$, $r = f$.
- Tegyük fel, hogy ha $\deg f < n$, akkor igaz az állítás. Legyen most

$$f = c_n x^n + \cdots + c_0 \quad \text{és} \quad g = d_m x^m + \cdots + d_0, \quad c_n, d_m \neq 0, n \geq m.$$

Legyen $\tilde{f} = f - \frac{c_n}{d_m} x^{n-m} g$. Ekkor $\deg \tilde{f} < n$. Indukció szerint legyen

$$\tilde{f} = f - \frac{c_n}{d_m} x^{n-m} g = \tilde{q} \cdot g + \tilde{r} \quad \deg \tilde{r} < \deg g.$$

Ekkor

$$f = \left(\tilde{q} + \frac{c_n}{d_m} x^{n-m} \right) g + \tilde{r} \quad \deg \tilde{r} < \deg g.$$

$\square$

Polinomok maradékos osztása

Példa Legyen
$$f = x^3 + x + 1 \quad \text{és} \quad g = 2x^2 + x + 1.$$

1. Legyen $f_1 = f - \frac{1}{2}xg = -\frac{1}{2}x^2 - \frac{1}{2}x + x + 1$
2. Legyen $f_2 = f_1 - \frac{-1}{4}g = -\frac{3}{4}x - \frac{3}{4}$.
3. Tehát $r = -\frac{3}{4}x - \frac{3}{4}$ és $q = \frac{1}{2}x - \frac{1}{4}$.

Az algoritmus során polinomokat összeadunk, kivonunk, skalárral szorzunk ill. g főegyüthatójával osztunk.

A tétel $\mathbb{Z}[x]$-ben és $\mathbb{Z}_8[x]$-ben nem igaz. Azonban, 1 együtthatójú g polinommal itt is lehet maradékosan osztani.