Diszkrét matematika 2

8. előadás
Polinomok

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

Komputeralgebra Tanszék

2023 ősz

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 $ax^3 + bx^2 + cx + d = 0$ 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.

Irreducibilis polinomok

Az irreducibilis polinomok azt a szerepet játszák, mint a prímszámok $\mathbb{Z}$-ben, vagy a gyöktényezők $\mathbb{C}[x]$-ben.

Definíció

Egy f polinom irreducibilis, ha nem bontható szorzatra nem-triviális módon, azaz

$$f = g \cdot h \quad \Longrightarrow \quad \deg g = \deg f \quad \text{vagy} \quad \deg h = \deg f.$$

Példa

- Az elsőfokú polinomok irreducibilisek.
- $\mathbb{C}[x]$-ben pontosan az $a(x - x_1)$, $a, x_1 \in \mathbb{C}$, $a \neq 0$ polinomok az irreducibilisek.
- $f = x^2 + 2x + 3$ irreducibilis $\mathbb{R}[x]$-ben (nincs gyöke), de nem az $\mathbb{C}[x]$-ben.

Tétel (NB)

Egy f polinom pontosan akkor irreducibilis, ha prím tulajdonságú , azaz

$$f \mid g \cdot h \quad \Longrightarrow \quad f \mid g \quad \text{vagy} \quad f \mid h.$$

Számelmélet alaptétele polinomokra

Emlékeztető: minden $n \in \mathbb{Z}$, $n \neq 0$ szám felírható $n = \pm p_1 \cdots p_\ell$ alakban, ahol a felírás sorrendtől eltekintve egyértelmű.

Tétel

Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$. Ekkor minden $f \in \mathbb{K}[x]$ polinom felírható

$$f = a \cdot f_1 \cdots f_\ell, \quad a \in \mathbb{K},\ a \neq 0,\ f_1, \ldots, f_\ell \in \mathbb{K}[x]$$

alakban, ahol $f_1 \ldots, f_\ell$ egy főegyütthatós irreducibilis polinomok és a felírás sorrendtől eltekintve egyértelmű.

A bizonyítás az egész számokhoz hasonlóan történik.

Számelmélet alaptétele polinomokra

Minden $f \in \mathbb{K}[x]$ polinom sorrendtől eltekintve egyértelműen felírható

$$f = af_1 \cdots f_\ell, \quad a \in \mathbb{K},\ a \neq 0,\ f_1, \ldots, f_\ell \in \mathbb{K}[x]$$

alakban ahol $f_1 \ldots, f_\ell$ egy főegyütthatós irreducibilis polinomok.

Bizonyítás.

- Felírás létezése. Indukció $\deg f$ szerint. Ha $\deg f = 1$, akkor f irreducibilis. Legyen $\deg f > 1$. Ha f irreducibilis, akkor felírható egytényezős szorzatként. Ha f nem irreducibilis, akkor felírható $f = g \cdot h$ alakban, ahol $\deg g, \deg h < \deg f$. Legyen

  $$g = bg_1 \cdots g_k \quad \text{és} \quad h = ch_1 \cdots h_m$$

  g és h egy felbontása irreducibilisek szorzatára. Ekkor az $f = bcg_1 \cdots g_k \cdot h_1 \cdots h_m$ egy felbontás.

Számelmélet alaptétele polinomokra

Minden $f \in \mathbb{K}[x]$ polinom sorrendtől eltekintve egyértelműen felírható

$$f = af_1 \cdots f_\ell, \quad a \in \mathbb{K},\ a \neq 0,\ f_1, \ldots, f_\ell \in \mathbb{K}[x]$$

alakban ahol $f_1 \ldots, f_\ell$ egy főegyüttható irreducibilis polinomok.

Bizonyítás.

- Felírás egyértelműsége. Legyen
$$f = af_1 \cdots f_\ell = bg_1 \cdots g_k$$
Mivel mindegyik f_i, g_j polinom egy főegyüttható, $a = b$.

  Mivel f_1 irreducibilis és osztja a bal oldalt, így osztja a jobb oldalt is. Speciálisan osztania kell az egyik g_j polinomot is. Feltehetjük, hogy $f_1 = g_1$.

  Egyszerűsítve kapjuk továbbá, hogy
$$f_2 \cdots f_\ell = g_2 \cdots g_k$$
Az eljárást folytatva kapjuk az egyértelműséget.

□

Példa irreducibilis polinomokra

Példa nem irreducibilis polinomra:
Ha $\deg f > 1$ és f-nek van gyöke, akkor f nem irreducibilis: $f = (x - x_1) \cdot g$.

Példa irreducibilis polinomra:

- $\mathbb{K} = \mathbb{C}$: Algebra alaptétele szerint pontosan az elsőfokú polinomok az irreducibilisek.
- $\mathbb{K} = \mathbb{R}$: Minden legalább harmadfokú polinom nem irreducibilis. (HF)
- $\mathbb{K} = \mathbb{Q}$: Rengeteg irreducibilis polinom van: $f = x^n - p$ (NB)
- $\mathbb{K} = \mathbb{Z}_p$ Rengeteg irreducibilis polinom van:
  - $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$, $f = x^3 + x + 1 \in \mathbb{Z}_2[x]$, $f = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$,...
  - $f = x^2 + 1 \in \mathbb{Z}_3[x]$, $f = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$, $f = x^4 + 2x^2 + 2 \in \mathbb{Z}_3[x]$,...

Példa irreducibilis polinomokra $\mathbb{Z}_2$ fölött

- Elsőfokú polinomok
  - Az elsőfokú polinomok irreducibilisek: $x, x+1$
- Másodfokú polinomok
  - Az elsőfokú polinomok többszörösei nem irreducibilisek:

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

  - A többi másodfokú polinom irreducibilis: $x^2 + x + 1$
- Harmadfokú polinomok
  - Az első- és másodfokú polinomok többszörösei nem irreducibilisek:

$$x^3, \quad x^2(x+1) = x^3 + x^2, \quad x(x+1)^2 = x^3 + x, \quad (x+1)^3 = x^3 + x^2 + x + 1,$$
$$x(x^2 + x + 1) = x^3 + x^2 + x, \quad (x+1)(x^2 + x + 1) = x^3 + 1$$

  - A többi harmadfokú polinom irreducibilis: $x^3 + x^2 + 1$, $x^3 + x + 1$

Kongruenciák polinomokra

Emlékeztető: $a \equiv b \mod n$, ha $n \mid a - b$.

Példa

- $2 \equiv 5 \equiv 8 \equiv -1 \equiv \ldots \mod 3$
- $1 \equiv 8 \equiv 15 \equiv \ldots \mod 7$

Definíció

Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$ és legyen $h \in \mathbb{K}[x]$ egy nem-nulla polinom. Ekkor $f, g \in \mathbb{K}[x]$ polinomokra:

$$f \equiv g \mod h \quad \text{ha} \quad h \mid f - g.$$

Példa

- $\mathbb{R}$ fölött $x^2 \equiv -1 \mod x^2 + 1$.
- $\mathbb{Z}_2$ fölött $x^2 + x \equiv 1 \mod x^2 + x + 1$.
- $\mathbb{C}$ fölött $x^5 + (1+i)x^4 - 3x^2 + \sqrt{2}x + 1 \equiv -2x^2 + (1 + \sqrt{2} + i)x + 1 \mod x^3 - 1$.

Kongruenciák polinomokra

Emlékeztető: $f \equiv g \mod h$ ha $h \mid f - g$.
A kongruencia polinomokra, ugyanazon tuljadonságokkal rendelkezik, mint egész számok körében:

Tétel (NB)

A kongruencia equivalencia reláció, azaz azaz: $f, g, h \in \mathbb{K}[x]$ esetén

- reflexív: $f \equiv f \mod h$;
- tranzitív: $f \equiv g \mod h$, $g \equiv k \mod h \Longrightarrow f \equiv k \mod h$;
- szimmetrikus: $f \equiv g \mod h$, $\Longrightarrow g \equiv f \mod h$.

Példa

Legyen $x^2 + x + 1 \in \mathbb{Z}_2[x]$: Ekkor

- $x^3 + x + 1 \equiv x^3 + x + 1 \mod x^2 + x + 1$;
- $x^3 + x + 1 \equiv x^3 + x^2 \mod x^2 + x + 1$, $x^3 + x^2 \equiv x^5 + x^4 + x^2 \mod x^2 + x + 1$;
  $\Longrightarrow x^3 + x + 1 \equiv x^5 + x^4 + x^2 \mod x^2 + x + 1$;
- $x^3 + x^2 \equiv x^5 + x^4 + x^2 \mod x^2 + x + 1 \Longrightarrow x^5 + x^4 + x^2 \equiv x^3 + x^2 \mod x^2 + x + 1$.

Kongruenciák polinomokra

Emlékeztető: $f \equiv g \mod h$ ha $h \mid f - g$.
A kongruencia polinomokra, ugyanazon tuljadonságokkal rendelkezik, mint egész számok körében:

Tétel (NB)

A kongruencia kompatibilis az összeadással és szorzással,
azaz: $f, g, h, k, l \in \mathbb{K}[x]$ esetén

- $f \equiv g \mod h, k \equiv l \mod h \Longrightarrow f + k \equiv g + l \mod h$;
- $f \equiv g \mod h, k \equiv l \mod h \Longrightarrow f \cdot k \equiv g \cdot l \mod h$.

Példa

Legyen $x^2 + 1 \in \mathbb{R}[x]$: Ekkor

- $x^2 \equiv -1 \mod x^2 + 1, \quad x^4 + x^3 \equiv -x + 1 \mod x^2 + 1;$
  $\Longrightarrow x^4 + x^3 + x^2 \equiv -x \mod x^2 + 1;$
- $-x^3 - x^2 \equiv x + 1 \mod x^2 + 1, \quad x^4 + x^3 \equiv -x + 1 \mod x^2 + 1;$
  $\Longrightarrow (-x^3 - x^2)(x^4 + x^3) \equiv (x + 1)(-x + 1) = -x^2 + 1 \equiv 2 \mod x^2 + 1.$