Okruhy polynomů

Základní myšlenky

1. Nahraďte čísla polynomy.
2. Dokažte větu o dělení se zbytkem.
3. Eukleidův algoritmus, Bezoutova rovnost.
4. Místo $\mathbb{Z}_m$ získáme nová čísla: zbytky po dělení polynomem.
5. Získáme tak nové okruhy, nová tělesa.
6. Lze očekávat: co šlo v $\mathbb{Z}_m$, půjde i pro nová "čísla".
   Nové očekávané aplikace: nové lineární kódy, šifrovací protokoly...
   Neočekávané aplikace: nemožnost některých konstrukcí, neexistence některých algoritmů.

Setkání s polymorfismem: základní algoritmy budou stejné pro čísla i pro polynomy.

Definice

Ať $\mathbb{K}$ je těleso. Polynom nad $\mathbb{K}$ v neurčité x je buď

1. zápis
$$p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_0$$
kde $n \geq 0$, $a_i \in \mathbb{K}$ (koeficienty), $a_n \neq 0$.

   Značení: $\deg(p(x)) = n$.

nebo

2. $p(x) = 0$.

   Značení: $\deg(p(x)) = -\infty$.

Množinu všech takových polynomů značíme $\mathbb{K}[x]$.

Pozor!

Značce x říkáme neurčitá, nikoli proměnná.

Polynom je zápis, nikoli funkce!

Konvence

V této přednášce značí $\mathbb{K}$ vždy těleso.
Řekneme-li polynom, myslíme tím polynom nad $\mathbb{K}$.

Základní operace s polynomy

Například pro $p(x) = 3x^2 + 4x + 2$, $q(x) = 6x^3 + 3x + 5$ v $\mathbb{Z}_7[x]$.

1. Sčítání:

$$p(x) + q(x) = 6x^3 + 3x^2 + 7x + 7 = 6x^3 + 3x^2$$

   Platí: $\deg(p(x) + q(x)) \leq \max(\deg(p(x)), \deg(q(x)))$.

2. Násobení:

$$p(x) \cdot q(x) = 4x^5 + 3x^3 + 6x^2 + 5x + 3$$

   Platí: $\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$.

Věta

$\langle \mathbb{K}[x], +, \cdot, 0, 1 \rangle$ je komutativní okruh s jednotkou.

Věta o dělení se zbytkem pro polynomy

Ať $a(x)$ a $b(x)$ jsou dva nenulové polynomy v $\mathbb{K}[x]$. Pak existují jednoznačně určené polynomy $q(x)$, $r(x)$ tak, že $\deg(r(x)) < \deg(b(x))$ a platí rovnost $a(x) = b(x) \cdot q(x) + r(x)$.

Příklad

$a(x) = 2x^3 - 4x + 1$, $b(x) = 3x + 2$. Vydělte se zbytkem

1. v $\mathbb{K} = \mathbb{R}$.
2. v $\mathbb{K} = \mathbb{Z}_5$.

Polymorfní algoritmus!

Definice

Prvek $a \in \mathbb{K}$ je kořen polynomu $p(x)$, pokud platí rovnost $p(a) = 0$.

Poznámka

1. V $\mathbb{C}$: polynom stupně n má přesně n kořenů (i s násobnostmi) — Fundamentální věta algebry.
2. Polynom stupně n nemusí mít žádný kořen: např. $x^2 + x + 1 \in \mathbb{Z}_2[x]$.

Poznámka

Neexistence kořenů a faktorizace spolu nesouvisí!
Např.
$$x^4 + x^2 + 1 = (x^2 + x + 1) \cdot (x^2 + x + 1)$$
nad $\mathbb{Z}_2$.

Definice

Řekneme, že polynom $a(x)$ dělí polynom $b(x)$ (značíme $a(x) \mid b(x)$), pokud existuje polynom $n(x)$ takový, že $b(x) = n(x) \cdot a(x)$.

Pokud $a(x)$ dělí $b(x)$, pak polynom $a(x)$ nazveme dělitelem polynomu $b(x)$.

Pozor!

Může se stát, že $a(x) \mid b(x)$ a současně $b(x) \mid a(x)$. Takovým polynomům říkáme asociované. Značení $a(x) \sim b(x)$.

Tvrzení

1. $\sim$ je ekvivalence na $\mathbb{K}[x]$.
2. $a(x) \sim b(x)$ iff v $\mathbb{K}$ existuje $r \neq 0$ tak, že $a(x) = r \cdot b(x)$.

Tvrzení

Ať a je prvek $\mathbb{K}$. Hodnota $p(a)$ je zbytek po dělení $p(x)$ polynomem $x - a$. Takže a je kořen polynomu $p(x)$ právě tehdy, když polynom $x - a$ dělí polynom $p(x)$.

Důsledek

Polynom $p(x)$ stupně $n \geq 0$ má v tělese $\mathbb{K}$ nanejvýš n různých kořenů (i s násobnostmi).

Důsledek

V tělese $\mathbb{K}$ jsou následující podmínky ekvivalentní:

1. $\mathbb{K}$ má nekonečný počet prvků.
2. Nad $\mathbb{K}$ není zapotřebí rozlišovat mezi polynomy jako výrazy a polynomy jako funkcemi.

Definice

Nekonstantnímu polynomu $p(x)$ říkáme ireducibilní, pokud je $p(x)$ dělitelný pouze polynomy (asociovanými s) 1 a $p(x)$.

Tvrzení

Ať p je prvočíslo. Pro každé přirozené číslo $n \geq 2$ existuje ireducibilní polynom stupně n nad $\mathbb{Z}_p$. Množina ireducibilních polynomů nad $\mathbb{Z}_p$ je tedy nekonečná.

Poznámka

Ireducibilní polynomy budou hrát roli prvočísel. Předchozí tvrzení říká, že nad $\mathbb{Z}_p$ jich máme dost (srovnejte s nekonečností množiny prvočísel).

Definice

Řekneme, že polynom $d(x)$ je největším společným dělitelem polynomů $a(x)$, $b(x)$ (značení $d(x) = \gcd(a(x), b(x))$), pokud jsou splněny následující dvě podmínky:

1. Polynom $d(x)$ je společným dělitelem polynomů $a(x)$, $b(x)$, tj. platí, $d(x) \mid a(x)$ a současně $d(x) \mid b(x)$.
2. Polynom $d(x)$ je největším ze všech společných dělitelů polynomů $a(x)$, $b(x)$, tj. platí následující: je-li $c(x)$ takový polynom, pro který platí $c(x) \mid a(x)$ a současně $c(x) \mid b(x)$, potom $c(x) \mid d(x)$.

Pokud $\gcd(a(x), b(x))$ je asociován s 1, řekneme, že polynomy $a(x)$, $b(x)$ jsou nesoudělné.

Věta

Mějme polynomy $a(x), b(x)$. Pak $\mathrm{gcd}(a(x), b(x))$ existuje a je určen jednoznačně až na násobek konstantním polynomem.

Věta (Bezoutova rovnost pro polynomy

Mějme polynomy $a(x), b(x)$. Pak existují polynomy $p(x), q(x)$ takové, že

$$\mathrm{gcd}(a(x), b(x)) = a(x) \cdot p(x) + b(x) \cdot q(x)\,.$$

Rozšířený Eukleidův algoritmus pro polynomy

Spočtěte $\gcd$ a Bezoutovu rovnost pro x^5+1 a x^2+1 v $\mathbb{Z}_5[x]$.

$a(x)$	$b(x)$	$q(x)$	$r(x)$	$\alpha_2(x)$	$\alpha_1(x)$	$\beta_2(x)$	$\beta_1(x)$
x^5+1	x^2+1			1	0	0	1
x^5+1	x^2+1	x^3+4x	$x+1$	0	1	1	$4x^3+x$
x^2+1	$x+1$	$x+4$	2	1	$4x+1$	$4x^3+x$	$x^4+4x^3+4x^2+x+1$
$x+1$	2	$3x+3$	0				

Platí $\gcd(a(x), b(x)) = 2$ a Bezoutova rovnost má tvar

$$2 = (4x+1)\cdot(x^5+1)+(x^4+4x^3+4x^2+x+1)\cdot(x^2+1) \quad \text{v } \mathbb{Z}_5[x]$$

neboli (polynom 2 je asociován s 1, protože $1 = 2\cdot 3$ v $\mathbb{Z}_5[x]$)

$$1 = (2x+3)\cdot(x^5+1)+(3x^4+2x^3+2x^2+3x+3)\cdot(x^2+1) \quad \text{v } \mathbb{Z}_5[x]$$

Polynomy x^5+1 a x^2+1 jsou v $\mathbb{Z}_5[x]$ nesoudělné.

Tvrzení

Každý nekonstantní polynom z $\mathbb{K}[x]$ lze vyjádřit jako součin ireducibilních polynomů.

Tvrzení

Pokud ireducibilní polynom $m(x)$ dělí součin polynomů $a(x) \cdot b(x)$, pak $m(x)$ dělí $a(x)$ nebo $b(x)$.

Věta

Každý nekonstantní polynom z $\mathbb{K}[x]$ lze jednoznačně vyjádřit (až na pořadí faktorů a násobení konstantou) jako součin ireducibilních faktorů (polynomů).