Okruhy polynómov

22. apríla 2024

Definícia polynómu

$$p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

- $a_i \in R$, R je komutatívny okruh s jednotkou
- $a_n, a_{n-1}, \ldots, a_0 \in R$ = *koeficienty* polynómu p
- n je *stupeň* polynómu (ak $a_n \neq 0$)
- a_n je *vedúci koeficient* (ak $a_n \neq 0$)
- Polynómy sa rovnajú, ak majú rovnaké koeficienty.

Rovnosť polynómov

Definícia

Dva polynómy považujeme za rovnaké, ak majú rovnaké koeficienty, t.j. ak $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, $q = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$ a $n \geq m$, tak $p = q$ práve vtedy, keď

$$a_i = b_i \qquad \text{pre } i = 0, 1, \ldots, m$$

a $a_i = 0$ pre $i = m + 1, \ldots, n$.

$$0x^3 + 1x^2 + 2x + 1 = 1x^2 + 2x + 1$$

Operácie

Pre $p = x^2 + 2x + 1$ a $q = 2x + 1$:

$$p + q = (x^2 + 2x + 1) + (2x + 1) = x^2 + 2x + 2x + 1 + 1 = x^2 + 4x + 2$$

Operácie

Pre $p = x^2 + 2x + 1$ a $q = 2x + 1$:

$$(x^2 + 2x + 1)(2x + 1) = x^2 \cdot 2x + 2x \cdot 2x + 1 \cdot 2x + x^2 \cdot 1 + 2x \cdot 1 + 1 \cdot 1$$

$$(x^2 + 2x + 1)(2x + 1) = 2x^2 \cdot x + 4x \cdot x + 2 \cdot x + 1x^2 + 2x + 1$$

$$(x^2 + 2x + 1)(2x + 1) = 2x^3 + 4x^2 + 2x + 1x^2 + 2x + 1$$

$$(x^2 + 2x + 1)(2x + 1) = 2x^3 + 5x^2 + 4x + 1$$

Operácie

Súčet polynómov p a q je

$$p + q = \sum_{i=0}^{n} (a_i + b_i)x^i.$$

Súčin polynómov p a q je polynóm $r = \sum_{i=0}^{2n} c_i x^i$, kde

$$c_k = \sum_{j=0}^{k} a_j b_{k-j}.$$

$(R[x], +, \cdot)$ je komutatívny okruh s jednotkou.

Násobenie a stupeň

Tvrdenie

Ak R je obor integrity, tak pre ľubovoľné nenulové polynómy $f, g \in R[x]$ platí

$$\mathrm{st}(fg) = \mathrm{st}(f) + \mathrm{st}(g)$$

a okruh $R[x]$ polynómov nad okruhom R je obor integrity.

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

$$c_{n+m} = a_n b_m$$

Veta o delení so zvyškom

Veta (Veta o delení so zvyškom)

Nech F je pole, $f(x), g(x) \in F[x]$ a $g(x) \neq 0$. Potom existujú $q(x), r(x) \in F[x]$ také, že

$$f(x) = q(x) \cdot g(x) + r(x)$$

a $\operatorname{st} r(x) < \operatorname{st} g(x)$.
Navyše, $q(x)$ a $r(x)$ sú týmito podmienkami jednoznačne určené.

$q(x)$ = podiel
$r(x)$ = zvyšok po delení

Veta o delení so zvyškom

Veta

Nech a, b sú celé čísla, $b > 0$. Potom existujú celé čísla q a r také, že

$$a = q \cdot b + r \qquad a \qquad 0 \leq r < b.$$

Navyše, q a r sú týmito podmienkami jednoznačne určené.

Dosadzovací homomorfizmus

Definícia

Nech R je komutatívny okruh s jednotkou. *Polynomickou funkciou* nad R budeme rozumieť ľubovoľnú funkciu $f\colon R \to R$ určenú predpisom

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

pre nejaké $n \in \mathbb{N}$ a $a_1 \dots a_n \in R$.

Okruh polynomických funkcií: $(F\langle x\rangle, +, \cdot)$
polynóm: $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$
funkcia: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$

$$\varphi\colon F[x] \to F\langle x\rangle$$

Dosadzovací homomorfizmus

Ak $b \in R$, dá sa b dosadiť do polynómu $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x]$.

$$f_b\colon R[x] \to R$$

$$f_b\colon f \mapsto a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0$$

Polynomické funkcie

Tvrdenie

Ak F je nekonečné pole tak polynomická funkcia $f\colon F \to F$

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

sa rovná nulovej funkcii práve vtedy, keď $a_0 = a_1 = \cdots = a_n = 0$, t.j. vtedy, keď sú všetky koeficienty nulové.

Polynomické funkcie

polynomické funkcie $\neq$ polynómy

Príklad

- $F = \mathbb{Z}_2$
- ako polynómy: $x^2 + x \neq 0$
- ako funkcie: $x^2 + x = 0$