Polynómy a okruh $F[x]$

1. februára 2023

Polynómy ako funkcie

Funkcie $f : F \to F$ tvaru

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

kde $a_0, \ldots, a_n \in F$.

- Ak F je nekonečné pole, takýto pohľad je v poriadku.
- Pri konečných poliach treba niektoré veci robiť inak.

Terminológia

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

- Stupeň $\operatorname{st} f(x) = n$, ak $a_n \neq 0$. Pre nulový polynóm položíme $\operatorname{st} f(x) = -\infty$.
- $a_0, \ldots, a_n$ voláme *koeficienty*
- Výraz $a_n x^n$ voláme *vedúci člen* polynómu $f(x)$ a a_n sa nazýva *vedúci koeficient*.
- Ak $a_n = 1$, tak polynóm $f(x)$ je *normovaný* alebo *monický*.

Operácie s polynómami

- Polynómy vieme sčitovať a násobiť.
- Dostaneme tak komutatívny okruh s jednotkou.
- Je to aj obor integrity.

$$\operatorname{st} f(x)g(x) = \operatorname{st} f(x) + \operatorname{st} g(x) \tag{1}$$

Veta o delení so zvyškom

Tvrdenie (Veta o delení so zvyškom)

Nech $f(x), g(x) \in F[x]$ *a* $g(x) \neq 0$. *Potom existujú celé polynómy* $q(x), r(x) \in F[x]$ *také, že platí*

$$f(x) = q(x) \cdot g(x) + r(x), \qquad \operatorname{st} r(x) < \operatorname{st} g(x).$$

Navyše polynómy $q(x)$ *a* r *sú týmito podmienkami jednoznačne určené.*
Polynóm $q(x)$ *budeme volať podiel a polynóm* $r(x)$ *zvyšok po delení polynómu* $f(x)$ *polynómom* $g(x)$. *Budeme používať označenie* $r(x) = f(x) \bmod g(x)$.

Deliteľnosť v $F[x]$

Definícia

Nech F je pole a $f(x), g(x) \in F[x]$. Hovoríme, že $f(x)$ *delí* $g(x)$ a označujeme $f(x) \mid g(x)$, ak existuje polynóm $h(x) \in F[x]$ taký, že

$$g(x) = f(x)h(x).$$

V opačnom prípade používame označenie $f(x) \nmid g(x)$.

$$f(x) \mid g(x) \qquad \Leftrightarrow \qquad r(x) = 0$$

Deliteľnosť v $F[x]$

Tvrdenie

Nech F je pole, $f(x), g(x), h(x) \in F[x]$. Potom platí:

(i) $1 \mid f(x)$, $f(x) \mid 0$

(ii) *Ak* $0 \mid f(x)$, *tak* $f(x) = 0$.

(iii) $f(x) \mid f(x)$

(iv) *Ak* $f(x) \mid g(x)$ *a* $g(x) \mid h(x)$, *tak* $f(x) \mid h(x)$.

(v) *Ak* $f(x) \mid g(x)$ *aj* $g(x) \mid f(x)$, *tak existuje* $c \in F$, $c \neq 0$ *také, že* $f(x) = cg(x)$; *a obrátene.*

$f(x) \mid g(x) \wedge g(x) \mid f(x) \Leftrightarrow f(x) = c \cdot g(x)$ *pre nejaké* $c \in F \setminus \{0\}$

Deliteľnosť v $F[x]$

$$f(x) \mid g(x), f(x) \mid h(x) \Rightarrow f(x) \mid g(x) \pm h(x)$$
$$f(x) \mid g(x) \Rightarrow f(x) \mid g(x)h(x)$$

Korene polynómov

Dosadenie a zvyšok

$$f(c) = a_n c^n + \cdots + a_1 c + a_0.$$

Môžeme si všimnúť, že hodnota $f(c)$ prirodzene súvisí s delením polynómom tvaru $x - c$.

Tvrdenie

Nech F je pole, $f(x) \in F[x]$ a $c \in F$. Označme r zvyšok po delení polynómu $f(x)$. Potom platí $f(c) = r$.

Korene polynómov

Dosadenie a zvyšok

Definícia

Nech F je pole a $f(x) \in F[x]$. Prvok $c \in F$ je *koreň polynómu* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ ak platí $f(c) = a_n c^n + \cdots + a_1 c + a_0 = 0$.

Tvrdenie

Nech F je pole, $f(x) \in F[x]$ a $c \in F$. Potom c je koreňom polynómu $f(x)$ práve vtedy, keď $(x - c) \mid f(x)$, t.j. keď existuje polynóm $g(x)$ taký, že

$$f(x) = (x - c)g(x).$$

Korene polynómov

Dosadenie a zvyšok

Definícia

Nech F je pole, $f(x) \in F[x]$ a $c \in F$. Hovoríme, že c je *k-násobný koreň* polynómu $f(x)$ ak

$$(x - c)^k \mid f(x).$$

Veta

Nech $f(x) \in F[x]$ je nenulový polynóm nad poľom F. Potom počet koreňov polynómu $f(x)$ v F je nanajvýš $\operatorname{st} f(x)$.

Nulová funkcia musí mať nulové koeficienty

Ak F je nekonečné pole, tak z

$$(\forall c \in F) f(c) = 0$$

vyplýva $a_0 = a_1 = \cdots = a_n = 0$.

Nefunguje to v konečných poliach

$f, g : \mathbb{Z}_2 \to \mathbb{Z}_2$

$$f = x^2 + x$$
$$g = 0$$

Nefunguje to v konečných poliach

Veta

Nech $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ *pričom* $a_n \neq 0$ *a všetky koeficienty sú celé čísla. Ak racionálne číslo* $\frac{p}{q}$ *je koreňom polynómu* $f(x)$*, pričom* $\gcd(p, q) = 1$*, tak platí*

$$p \mid a_0, \qquad q \mid a_n.$$

Dôsledok

Ak $f(x)$ *je monický polynóm s celočíselnými koeficientami a* α *je nejaký racionálny koreň polynóm* $f(x)$*, tak platí* $\alpha \in \mathbb{Z}$*.*

Deliteľnosť a ideály

- $f(x) \mid g(x)$
- $g(x) \in (f(x))$
- $(g(x)) \subseteq (f(x))$

Iba hlavné ideály

Tvrdenie

Nech F je pole a $I \subseteq F[x]$ je ideál v okruhu $(F[x], +, \cdot)$. Potom existuje polynóm $a(x) \in F[x]$ taký, že

$$I = (a(x)) = \{a(x)f(x); f(x) \in F[x]\}.$$

Ak navyše pridáme podmienku, že polynóm $a(x)$ je monický alebo nulový, tak je polynóm $a(x)$ ideálom I jednoznačne určený.

Najväčší spoločný deliteľ

Definícia

Nech F je pole a $f(x), g(x) \in F[x]$. Hovoríme, že polynóm $d(x) \in F[x]$ je *najväčší spoločný deliteľ* polynómov $f(x)$ a $g(x)$, ak platí

- $d(x) \mid f(x)$, $d(x) \mid g(x)$
- Pre ľubovoľný polynóm $c(x) \in F[x]$ taký, že $c(x) \mid f(x)$ a $c(x) \mid g(x)$ platí aj $c(x) \mid d(x)$.

$$c(x) \mid f(x) \wedge c(x) \mid g(x) \Rightarrow c(x) \mid d(x)$$

Najväčší spoločný deliteľ

- Takto definovaný n.s.d nie je určený jednoznačne.
- Monický n.s.d označíme

$$d(x) = \gcd(f(x), g(x)).$$

Najväčší spoločný deliteľ

Tvrdenie

Nech F je pole a $f(x), g(x), d(x) \in F[x]$. Potom množina

$$I = \{u(x)f(x) + v(x)g(x); u(x), v(x) \in F[x]\}$$

je ideál v okruhu $F[x]$.
Polynóm $d(x)$ je najväčší spoločný deliteľ polynómov $f(x)$ a $g(x)$ práve vtedy, keď $(d(x)) = I$.

$$(d(x)) = \{u(x)f(x) + v(x)g(x); u(x), v(x) \in F[x]\}$$

Bézoutova identita

Dôsledok

Nech F je pole a $f(x), g(x) \in F[x]$. Ak $d(x) = \gcd(f(x), g(x))$, tak existujú polynómy $u(x), v(x) \in F[x]$ také, že

$$d(x) = u(x)f(x) + v(x)g(x).$$

Kongruencie

Definícia

Nech F je pole a $a(x), b(x), f(x) \in F[x]$. Hovoríme, že polynómy $a(x)$ a $b(x)$ sú *kongruentné modulo* $f(x)$ ak platí

$$f(x) \mid a(x) - b(x).$$

Pre takúto situáciu používame označenie $a(x) \equiv b(x) \pmod{f(x)}$.

$$a(x) \equiv b(x) \pmod{f(x)} \quad \Leftrightarrow \quad f(x) \mid a(x) - b(x)$$

Kongruencie

Tvrdenie

Nech $f(x), a(x), b(x), c(x) \in F[x]$. *Potom platí:*

(i) $a(x) \equiv a(x) \pmod{f(x)}$

(ii) *Ak* $a(x) \equiv b(x) \pmod{f(x)}$, *tak aj* $b(x) \equiv a(x) \pmod{f(x)}$.

(iii) *Ak* $a(x) \equiv b(x) \pmod{f(x)}$ *a* $b(x) \equiv c(x) \pmod{f(x)}$, *tak aj* $a(x) \equiv c(x) \pmod{f(x)}$.

Kongruencie

Ak $a(x) \equiv c(x) \pmod{f(x)}$, $b(x) \equiv d(x) \pmod{f(x)}$, tak platí

$$\begin{aligned} a(x) + c(x) &\equiv b(x) + d(x) \pmod{f(x)} \\ a(x) \cdot c(x) &\equiv b(x) \cdot d(x) \pmod{f(x)} \end{aligned} \tag{2}$$