

Faktorový okruh $F[x]/(h(x))$

14. novembra 2024

Okruh $F(x)/(h(x))$

Veta

Nech F je pole a $h(x) \in F[x]$ je polynóm nad poľom F stupňa $n \geq 1$. Pre reláciu ekvivalencie „byť kongruentné modulo $h(x)$ “ na množine polynómov $F[x]$ označme triedy ekvivalencie ako

$$\overline{f(x)} = \{g(x) \in F[x]; f(x) \equiv g(x) \pmod{h(x)}\}.$$

Množinu týchto tried ekvivalencie označme ako $F(x)/(h(x))$. Pre každé $f(x) \in F[x]$ existuje práve jeden polynóm $r(x)$ taký, že $f(x) \equiv r(x) \pmod{h(x)}$ a súčasne $\text{st } f(x) < \text{st } h(x)$. (T.j. každá trieda je jednoznačne reprezentovaná polynómom stupňa menšieho než n .)

Okruh $F(x)/(h(x))$

Veta

Predpisy

$$\begin{aligned}\overline{f(x)} + \overline{g(x)} &= \overline{f(x) + g(x)} \\ \overline{f(x)} \cdot \overline{g(x)} &= \overline{f(x) \cdot g(x)}\end{aligned}\tag{1}$$

určujú dobre definované binárne operácie na množine $F(x)/(h(x))$ a $(F(x)/(h(x)), +, \cdot)$ s týmito operáciami tvorí komutatívny okruh s jednotkou. Tento okruh voláme faktorový okruh $F[x]$ podľa $h(x)$. Navyše platí, že triedy konštantných polynómov, t.j. množina $\{\overline{c}; c \in F\}$, určujú podokruh, ktorý je izomorfný s poľom F .

Príklady

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$$

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$$

Príklad $\mathbb{R}(x)/(x^2 + 1)$

$$\mathbb{R}[x]/(x^2 + 1) = \{\overline{ax + b}; a, b \in \mathbb{R}\}$$

$$\overline{ax + b} + \overline{cx + d} = \overline{(a + c)x + (b + d)}$$

$$\overline{ax + b} \cdot \overline{cx + d} = \overline{(ad + bc)x + (bd - ac)}$$

$$\begin{aligned}(ax + b)(cx + d) &= acx^2 + (ad + bc)x + bd \\ &= ac(x^2 + 1) + (ad + bc)x + (bd - ac)\end{aligned}$$

Príklad $\mathbb{R}(x)/(x^2 + 1)$

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$$

$$\overline{ax + b} \cdot \overline{cx + d} = \overline{(ad + bc)x + (bd - ac)}$$
$$(ai + b) \cdot (ci + d) = (ad + bc)i + (bd - ac)$$

Príklad $\mathbb{Q}[x]/(x^2 - 2)$

$$\mathbb{Q}[x]/(x^2 - 2) = \{\overline{ax + b}; a, b \in \mathbb{Q}\}$$

$$\begin{aligned}(ax + b)(cx + d) &\equiv acx^2 + (ab + cd)x + bd \\ &\equiv 2ac + (ab + cd)x + bd \\ &\equiv (ab + cd)x + (bd + 2ac)\end{aligned}$$

$$\overline{ax + b} \cdot \overline{cx + d} = \overline{(ab + cd)x + (bd + 2ac)}$$

Príklad $\mathbb{Q}[x]/(x^2 - 2)$

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$$

$$(b + a\sqrt{2})(d + c\sqrt{2}) = (bd + 2ac) + (ab + cd)\sqrt{2}$$
$$\overline{b + ax} \cdot \overline{d + cx} = \overline{(bd + 2ac) + (ab + cd)x}$$

Ireducibilné polynómy

Definícia

Nekonštantný polynóm $p(x) \in F[x]$ sa nazýva *ireducibilný polynóm* ak pre ľubovoľné $f(x), g(x) \in F[x]$ také, že

$$f(x) \cdot g(x) = p(x)$$

je niektorý z polynómov $f(x), g(x)$ konštantný polynóm.

Ireducibilné polynómy

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$$

- ▶ Nad $\mathbb{R}$ sú $x^2 \pm \sqrt{2}x + 1$ ireducibilné.
- ▶ Nad $\mathbb{C}$ sa dajú rozložiť.
- ▶ Nad $\mathbb{Q}$ je polynóm $x^4 + 1$ ireducibilný.

Ireducibilné polynómy

Tvrdenie

*Nech F je pole a $f(x) \in F[x]$ je polynóm stupňa 2 alebo 3.
Polynóm $f(x)$ je ireducibilný práve vtedy, keď nemá korene.*

Ireducibilné polynómy

$$p(x) \mid g(x)h(x) \quad \Rightarrow \quad p(x) \mid g(x) \vee p(x) \mid h(x) \quad (2)$$

Tvrdenie

Nech $p(x), f(x) \in F[x]$ a $p(x)$ je ireducibilný. Potom $p(x) \mid f(x)$ alebo $\gcd(p(x), f(x)) = 1$.

Pole $F(x)/(p(x))$

Veta

Nech F je pole a $p(x) \in F[x]$ je ireducibilný polynóm nad F .

Potom okruh $F[x]/(p(x))$ je pole.

Navyše toto pole obsahuje podpole izomorfné s poľom F , konkrétne platí, že zobrazenie

$$\varphi: F \rightarrow F(x)/(p(x))$$

$$\varphi: c \mapsto \bar{c}$$

je injektívny homomorfizmus.

$p(x)$ má koreň v $F(x)/(p(x))$

Tvrdenie

*Nech F je pole a $p(x) \in F[x]$ je ireducibilný polynóm nad F .
Ak $L = F[x]/(p(x))$ chápeme ako nadpole poľa F , tak $u = \bar{x}$ je koreň polynómu $p(x)$ v tomto poli.*

$p(x)$ má koreň v $F(x)/(p(x))$

Ak $p(x) = a_n x^n + \cdots + a_1 x + a_0$, tak dostaneme

$$\begin{aligned}
 p(\bar{x}) &= a_n \bar{x}^n + \cdots + a_1 \bar{x} + a_0 \\
 &= \overline{a_n x^n} + \cdots + \overline{a_1 x} + \overline{a_0} \\
 &= \overline{a_n x^n + \cdots + a_1 x + a_0} \\
 &= \overline{p(x)} \\
 &= \bar{0} = 0
 \end{aligned}$$

Štvorprvkové pole

$$\mathbb{Z}_2[x]/(x^2 + x + 1)$$

- ▶ $x^2 + x + 1$ nemá korene v $\mathbb{Z}_2$
- ▶ Je to teda ireducibilný polynóm
- ▶ $\mathbb{Z}_2/(x^2 + x + 1) = \{\overline{ax + b}; a, b \in \mathbb{Z}_2\}$ je štvorprvkové pole.

Štvorprvkové pole

$$\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, u, u + 1\}$$

+	0	1	u	$u + 1$
0	0	1	u	$u + 1$
1	1	0	$u + 1$	u
u	u	$u + 1$	0	1
$u + 1$	$u + 1$	u	1	0

.	0	1	u	$u + 1$
0	0	0	0	0
1	0	1	u	$u + 1$
u	0	u	$u + 1$	1
$u + 1$	0	$u + 1$	1	u