Rozšírenia polí

17. mája 2020

Rozšírenia polí

$$\mathbb{C} = \{a + bi; a, b \in \mathbb{R}\}$$
$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$$

Tieto dva príklady sú podobné:

- K poľu $\mathbb{R}$ sme pridali koreň polynómu $x^2 + 1$.
- K poľu $\mathbb{Q}$ sme pridali koreň polynómu $x^2 - 2$.

Rozšírenia polí

Definícia

Ak K, F sú polia a súčasne F je podokruhom K, tak hovoríme, že K je *rozšírením* poľa F.

Stupeň rozšírenia

Definícia

Ak K je rozšírenie poľa F také, že K je konečnorozmerný vektorový priestor nad F, tak K nazývame *konečné rozšírenie* poľa F. Dimenziu $d_F(K)$ poľa K ako vektorového priestoru nad F nazývame *stupeň rozšírenia* a označujeme $[K : F]$.

$$[K : F] = d_F(K)$$

Pridanie koreňa

$$[\mathbb{C} : \mathbb{R}] = 2$$

$$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$$

Tieto dva príklady sú podobné:

- K poľu $\mathbb{R}$ sme pridali koreň polynómu $x^2 + 1$.
- K poľu $\mathbb{Q}$ sme pridali koreň polynómu $x^2 - 2$.

Pridanie koreňa

Veta

Nech F je pole a $p(x)$ je ireducibilný polynóm v $F[x]$. Potom existuje rozšírenie poľa F, v ktorom $p(x)$ má koreň.

$$K = F[x]/(p(x))$$

$$p(\overline{x}) \stackrel{(*)}{=} \overline{p(x)} = p(x) + (p(x)) = 0 + (p(x))$$

Pridanie koreňa

$$
\begin{aligned}
\overline{p(x)} &= \overline{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\
&= \overline{a_n x^n} + \overline{a_{n-1}x^{n-1}} + \cdots + \overline{a_1 x} + \overline{a_0} \\
&= \overline{a_n} \cdot \overline{x}^n + \overline{a_{n-1}} \cdot \overline{x}^{n-1} + \cdots + \overline{a_1} \cdot \overline{x} + \overline{a_0} \\
&\overset{(\triangle)}{=} a_n \overline{x}^n + a_{n-1}\overline{x}^{n-1} + \cdots + a_1 \overline{x} + a_0 \\
&= p(\overline{x})
\end{aligned}
$$

Pridanie koreňa

Veta

Nech $p(x) \in F[x]$ je ireducibilný polynóm a $K = F[x]/(p(x))$. Nech $n = \operatorname{st} p$. Označme $u = x + (p(x)) = \varphi(x)$ (kde $\varphi\colon F[x] \to K$ označuje kanonický homomorfizmus). Potom $1, u, \dots, u^{n-1}$ je báza K ako vektorového priestoru nad F, čiže

$$K = \{a_{n-1}u^{n-1} + \cdots + a_1 u + a_0; a_0, \dots, a_{n-1} \in F\}.$$

Dôsledok

Ak $p(x) \in F[x]$ je ireducibilný polynóm stupňa n, tak $K = F[x]/(p(x))$ je konečné rozšírenie F a stupeň rozšírenia $[K : F]$ je tiež rovný n.

$$[K : F] = \operatorname{st} p(x)$$

Príklady konečných rozšírení

$$GF_4 = \mathbb{Z}_2[x]/(x^2 + x + 1)$$

$$(au + b) + (cu + d) = (a + b)u + (b + d)$$

$$\begin{aligned}(au + b)(cu + d) &= acu^2 + (bc + ad)u + bd \\ &= ac(u + 1) + (bc + ad)u + bd \\ &= (ac + bc + ad)u + (ac + bd)\end{aligned}$$

Príklady konečných rozšírení

$+$	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

$\cdot$	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

Príklady konečných rozšírení

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

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

$$(ax+b)(cx+d)+(p(x)) = (cb+ad)x+(bd-ac)+(p(x)),$$
$$(au+b)(cu+d) = (cb+ad)u+(bd-ac).$$

Príklady konečných rozšírení

$$(au + b)(cu + d) = (cb + ad)u + (bd - ac)$$

$$(ai + b)(ci + d) = (bc + ad)i + (bd - ac)$$

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

Jednoduché rozšírenie

Definícia

Ak K je rozšírenie F a $u_1, \dots, u_n \in K$, tak symbolom $F(u_1, \dots, u_n)$ označujeme podpole generované množinou $F \cup \{u_1, \dots, u_n\}$. (T.j. najmenšie podpole, ktoré obsahuje túto množinu, čiže prienik všetkých podpolí, ktoré ju obsahujú.) V prípade, že existuje $u \in K$ také, že $K = F(u)$ hovoríme o *jednoduchom rozšírení.*

Pridanie koreňa

Veta

Nech F je pole, $p(x) \in F[x]$ je ireducibilný polynóm nad F a K je rozšírenie F, ktoré obsahuje koreň u polynómu $p(x)$. Potom

$$F(u) \cong F[x]/(p(x)).$$

$\overline{\varphi}_u \colon F[x]/(p(x)) \to F(u)$

$$\overline{\varphi_u} \colon a(x) + (p(x)) \mapsto a(u)$$

Izomorfizmus medzi rozšíreniami

izomorfizmus $\varphi\colon F \to F'$

$$\hat{\varphi}\colon \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \varphi(a_i) x^i$$

Izomorfizmus medzi rozšíreniami

Veta

Nech $\varphi\colon F \to F'$ *je izomorfizmus polí. Nech* $p(x)$ *je ireducibilný polynóm nad* F *a* $p'(x) \in F[x]$ *je polynóm* $\hat{\varphi}(p)$ *(čiže polynóm, ktorý získame použitím izomorfizmu* $\varphi\colon F \to F'$ *na všetky koeficienty polynómu* $f(x)$*). Potom* $p'(x)$ *je tiež ireducibilný polynóm (nad* F'*).*
Nech u *je koreň* $p(x)$ *(v nejakom nadpoli* F*) a* v *je koreň* $p'(x)$ *(v nejakom nadpoli* F'*). Potom existuje izomorfizmus*

$$\sigma\colon F(u) \to F'(v),$$

ktorý zobrazí u *na* v *a rozširuje* φ*, t.j.* $\sigma(u) = v$ *a* $\sigma|_F = \varphi$*.*