Minimálny polynóm

5. decembra 2022

Minimálny polynóm

Algebraické prvky

Definícia

Nech K je rozšírenie poľa F a $u \in K$. Hovoríme, že prvok $u \in F$ je *algebraický* nad F, ak existuje polynóm $f(x) \in F[x]$ taký, že u je jeho koreňom.

$$(\exists f(x) \in F[x]) f(u) = 0$$

Ak prvok $u \in K$ nie je algebraický, tak hovoríme, že u je transcendentný prvok.

Minimálny polynóm

Minimálny polynóm

Definícia

Nech K je rozšírenie poľa F a $u \in K$ je algebraický prvok nad F. Polynóm $m(x)$ sa nazýva *minimálny polynóm* prvku u, ak je to nenulový monický polynóm najnižšieho možného stupňa, ktorého koreňom je u.

Ak potrebujeme zdôrazniť z akého prvku sme minimálny polynóm dostali, použijeme označenie $m_u(x)$.

Minimálny polynóm

Minimálny polynóm

$$I = \{f(x) \in F[x]; f(u) = 0\}$$

Tvrdenie

Nech K je rozšírenie poľa F a $u \in K$ je algebraický prvok nad F. Potom existuje minimálny polynóm $m(x)$ prvku u. Tento polynóm je prvkom u určený jednoznačne.
Navyše pre ľubovoľný polynóm $f(x) \in F[x]$ platí, že u je koreňom polynómu $f(x)$ práve vtedy, keď $m(x) \mid f(x)$.

$$f(u) = 0 \Leftrightarrow m(x) \mid f(x) \tag{1}$$

Minimálny polynóm

Minimálny polynóm

Dôsledok

Nech K je rozšírenie poľa F, $u \in K$ je algebraický prvok nad F a $m(x)$ je jeho minimálny polynóm.
Potom pre ľubovoľné polynómy $f(x), g(x) \in F[x]$ platí $f(u) = g(u)$ práve vtedy, keď $f(x) \equiv g(x) \pmod{m(x)}$.

$$f(u) = g(u) \Leftrightarrow f(x) \equiv g(x) \pmod{m(x)} \tag{2}$$

Minimálny polynóm

Minimálny polynóm

Príklad

$F = \mathbb{Q}$

- Pre $u = \sqrt{2}$ máme

$$m_u(x) = x^2 - 2.$$

- Pre $u = \sqrt[3]{2}$ máme

$$m_u(x) = x^3 - 2$$

.

Minimálny polynóm

Minimálny polynóm je ireducibilný

Tvrdenie

Nech $m_u(x)$ je minimálny polynóm prvku u nad poľom F. Potom $m(x)$ je ireducibilný v $F[x]$.

Minimálny polynóm

$F(u) \cong F[x]/(m(x))$

Veta

Nech K je nadpole poľa F. Nech prvok $u \in K$ je algebraický nad F a jeho minimálny polynóm $m(x)$ má stupeň n. Potom

$$\begin{aligned} F(u) &= \{a_{n-1}u^{n-1} + \cdots + a_1 u + a_0; a_0, \ldots, a_{n-1} \in F\} \\ &= \{f(u); f(x) \in F[x], \operatorname{st} f(x) < n\}. \end{aligned}$$

Navyše predpis

$$\varphi\colon \overline{f(x)} \mapsto f(u)$$

určuje dobre definované zobrazenie $\varphi\colon F[x]/(m(x)) \to F(u)$ Teda platí

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

Minimálny polynóm

$F(u) \cong F[x]/(m(x))$

$$\varphi(\overline{f(x)+g(x)}) = f(u)+g(u) = \varphi(\overline{f(x)}) + \varphi(\overline{g(x)})$$

$$\varphi(\overline{f(x)\cdot g(x)}) = f(u)\cdot g(u) = \varphi(\overline{f(x)}) \cdot \varphi(\overline{g(x)})$$

$$\begin{aligned} \varphi(\overline{f(x)}) = \varphi(\overline{g(x)}) &\Rightarrow f(u) = g(u) \\ &\Rightarrow f \equiv g \pmod{m} \\ &\Rightarrow \overline{f(x)} = \overline{g(x)} \end{aligned}$$

Minimálny polynóm

$\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(\sqrt[3]{2})$

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$$
$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}; a, b, c \in \mathbb{Q}\}$$

Minimálny polynóm

Stupeň $[u : F]$

Tvrdenie

Nech K je rozšírenie poľa F, $u \in K$ je algebraický prvok nad poľom F. Potom stupeň rozšírenia $F(u)$ nad poľom F je rovný stupňu jeho minimálneho polynómu.

$$[F(u) : F] = \deg m_u(x).$$

Toto číslo budeme tiež nazývať stupeň prvku u nad F a označovať $[u : F]$.