

Minimálny polynóm

21. novembra 2024

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

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

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

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

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

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 $f(x) \equiv g(x) \pmod{m(x)}$.

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

Minimálny polynóm

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

$$\begin{aligned} f(u) = g(u) &\Leftrightarrow f(u) - g(u) = 0 \\ &\Leftrightarrow m(x) \mid f(x) - g(x) \\ &\Leftrightarrow f(x) \equiv g(x) \pmod{m(x)} \end{aligned}$$

Minimálny polynóm je ireducibilný

Tvrdenie

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

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

Definícia

Nech K je pole, F je jeho podpole a $u_1, \dots, u_k \in F$.

Symbolom $F(u_1, \dots, u_k)$ označujeme najmenšie podpole poľa K obsahujúce $F \cup \{u_1, \dots, u_k\}$.

V prípade jediného prvku budeme používať označenie $F(u)$.

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

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

$$\begin{aligned} F(u) &= \{a_{n-1}u^{n-1} + \cdots + a_1u + a_0; a_0, \dots, a_{n-1} \in F\} \\ &= \{f(u); f(x) \in F[x], \text{st } f(x) < n\}. \end{aligned}$$

Navyše predpis

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

určuje dobre definované zobrazenie $\varphi: F[x]/(m(x)) \rightarrow F(u)$. Teda platí

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

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

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

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

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

Pole $F(u)$

Definícia

Nech K je pole, F je jeho podpole a $u_1, \dots, u_k \in F$.

Symbolom $F(u_1, \dots, u_k)$ označujeme najmenšie podpole poľa K obsahujúce $F \cup \{u_1, \dots, u_k\}$.

V prípade jediného prvku budeme používať označenie $F(u)$.

Prienik podpolí

Úloha

Nech K je pole a $\{F_i; i \in I\}$ je nejaký neprázdny systém podpolí poľa K . Dokážte, že potom aj prienik

$$F = \bigcap_{i \in I} F_i$$

je podpole poľa K .

Ukážte, že pre ľubovoľnú podmnožinu $M \subseteq K$ existuje najmenšie podpole F poľa K také, že $M \subseteq F$. (Vďaka takémuto argumentu vieme, že existuje podpole $F(u_1, \dots, u_k)$, ktoré sme zaviedli v predošlej definícii.)

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

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

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

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 $[u : F]$.