Struktura konečných těles 1.

Konečná tělesa

24. dubna 2020

Obsah přednášky

3.1 Podtělesa: Popíšeme strukturu podtěles konečného tělesa. Ukážeme, že pro každé $m \mid n$ existuje právě jedno podtěleso tělesa $\mathbb{F}_{p^n}$, které má $\mathbb{F}_{p^m}$ prvků. Uspořádání těchto podtěles je dáno uspořádaním dělitelů n relací dělitelnosti.

Obsah přednášky

3.1 Podtělesa: Popíšeme strukturu podtěles konečného tělesa. Ukážeme, že pro každé $m \mid n$ existuje právě jedno podtěleso tělesa $\mathbb{F}_{p^n}$, které má $\mathbb{F}_{p^m}$ prvků. Uspořádání těchto podtěles je dáno uspořádaním dělitelů n relací dělitelnosti.

3.2 Aditivní a multiplikativní grupa: Popíšeme aditivní grupu konečného tělesa a multiplikativní grupu jeho nenulových prvků. Ukážeme, že obě grupu jsou cyklické. Generátor multiplikativní grupy se nazývá primitivní prvek.

Obsah přednášky

3.1 Podtělesa: Popíšeme strukturu podtěles konečného tělesa. Ukážeme, že pro každé $m \mid n$ existuje právě jedno podtěleso tělesa $\mathbb{F}_{p^n}$, které má $\mathbb{F}_{p^m}$ prvků. Uspořádání těchto podtěles je dáno uspořádaním dělitelů n relací dělitelnosti.

3.2 Aditivní a multiplikativní grupa: Popíšeme aditivní grupu konečného tělesa a multiplikativní grupu jeho nenulových prvků. Ukážeme, že obě grupu jsou cyklické. Generátor multiplikativní grupy se nazývá primitivní prvek.

3.3 Minimální polynomy: Zavedeme pojem algebraického prvku nad tělesem a jeho minimálního polynomu. Ukážeme souvislost mezi stupněm minimálního polynomu a dimenzí rozšíření o daný algebraický prvek.

O podtělesech konečných těles

Věta

O podtělesech konečných těles

Věta

- *Podtěleso tělesa $\mathbb{F}_{p^n}$ má p^m prvků pro některé $m \mid n$.*

O podtělesech konečných těles

Věta

- *Podtěleso tělesa $\mathbb{F}_{p^n}$ má p^m prvků pro některé $m \mid n$.*
- *Pro každé $m \mid n$ existuje právě jedno takové podtěleso.*

O podtělesech konečných těles

Věta

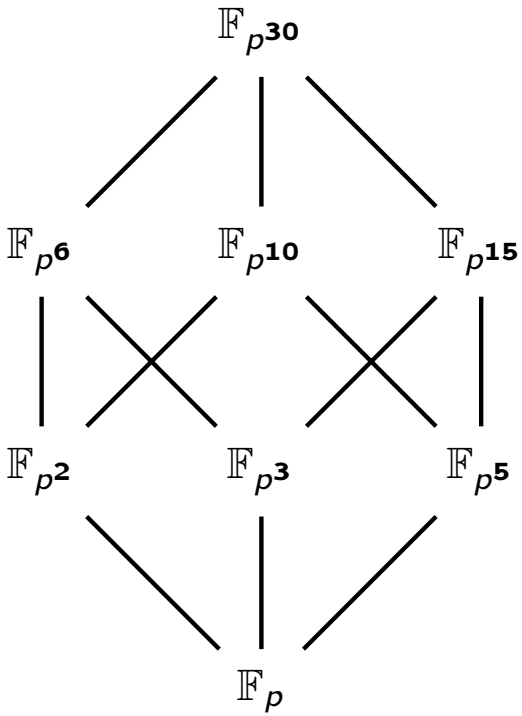
- *Podtěleso tělesa $\mathbb{F}_{p^n}$ má p^m prvků pro některé $m \mid n$.*
- *Pro každé $m \mid n$ existuje právě jedno takové podtěleso.*

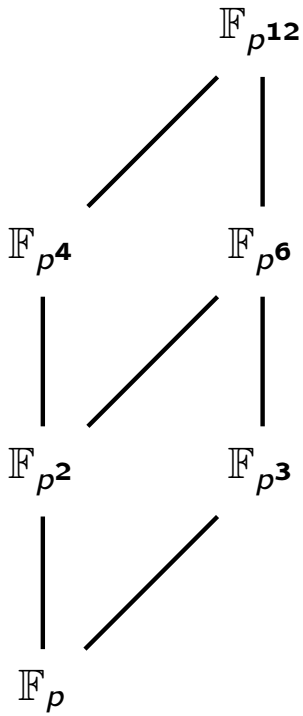
Poznámka

Je-li $\boldsymbol{F}$ p^m-prvkové podtěleso tělesa $\mathbb{F}_{p^n}$, potom

$$\boldsymbol{F} = \left\{ a \in \mathbb{F}_{p^n} \mid a = a^{p^m} \right\}.$$

Struktura podtěles - obrázek





Popis grup a primitvní prvky

Věta

Buď p prvočíslo a $q = p^n$. Potom

Popis grup a primitvní prvky

Věta

Buď p prvočíslo a $q = p^n$. Potom

1. $(\mathbb{F}_q, +) \simeq (\mathbb{Z}_p, +_{\bmod p})^n$.

Popis grup a primitvní prvky

Věta

Buď p prvočíslo a $q = p^n$. Potom

1. $(\mathbb{F}_q, +) \simeq (\mathbb{Z}_p, +_{\bmod p})^n$.
2. $(\mathbb{F}_q^*, \cdot) \simeq (\mathbb{Z}_{q-1}, +_{\bmod q-1})$.

Popis grup a primitvní prvky

Věta

Buď p prvočíslo a $q = p^n$. Potom

1. $(\mathbb{F}_q, +) \simeq (\mathbb{Z}_p, +_{\bmod p})^n$.
2. $(\mathbb{F}_q^*, \cdot) \simeq (\mathbb{Z}_{q-1}, +_{\bmod q-1})$.

Definice

Prvek a tělesa $\mathbb{F}_q$ se nazývá *primitivní*, pokud je generátorem cyklické multiplikativní grupy $\mathbb{F}_q^*$.

Popis grup a primitvní prvky

Věta

Buď p prvočíslo a $q = p^n$. Potom

1. $(\mathbb{F}_q, +) \simeq (\mathbb{Z}_p, +_{\bmod p})^n$.
2. $(\mathbb{F}_q^*, \cdot) \simeq (\mathbb{Z}_{q-1}, +_{\bmod q-1})$.

Definice

Prvek a tělesa $\mathbb{F}_q$ se nazývá *primitivní*, pokud je generátorem cyklické multiplikativní grupy $\mathbb{F}_q^*$.

Pozorování

Primitivních prvků tělesa $\mathbb{F}_q$ je tolik, kolik je generátorů cyklické grupy $\mathbb{Z}_{q-1}$. Těch je $\varphi(q-1)$, kde φ značí *Eulerovu funkci*.

Algebraický prvek a minimální polynom

Definice

Buď $\boldsymbol{F} \leq \boldsymbol{E}$ rozšíření těles. Prvek $\alpha \in \boldsymbol{E}$ je *algebraický* nad $\boldsymbol{F}$ je-li pokud $f(\alpha) = 0$ pro nějaký nenulový polynom $f(x) \in \boldsymbol{F}[x]$.

Algebraický prvek a minimální polynom

Definice

Buď $\boldsymbol{F} \leq \boldsymbol{E}$ rozšíření těles. Prvek $\alpha \in \boldsymbol{E}$ je *algebraický* nad $\boldsymbol{F}$ je-li pokud $f(\alpha) = 0$ pro nějaký nenulový polynom $f(x) \in \boldsymbol{F}[x]$.

Definice

Nenulový monický polynom $m(x) \in \boldsymbol{F}[x]$ nejmenšího stupně takový, že $m(\alpha) = 0$ nazýváme *minimální polynom* prvku α.

Vlastnosti minimálního polynomu

- Polynom $m(x)$ je ireducibilní.

Vlastnosti minimálního polynomu

- Polynom $m(x)$ je ireducibilní.
- Ireducibilní monický polynom nad $\boldsymbol{F}$ je minimální polynom libovolného svého kořene.

Vlastnosti minimálního polynomu

- Polynom $m(x)$ je ireducibilní.
- Ireducibilní monický polynom nad $\boldsymbol{F}$ je minimální polynom libovolného svého kořene.
- Pro polynom $f(x) \in \boldsymbol{F}[x]$ platí, že

$$f(x) = 0 \iff m \mid f.$$

Vlastnosti minimálního polynomu

- Polynom $m(x)$ je ireducibilní.
- Ireducibilní monický polynom nad $\boldsymbol{F}$ je minimální polynom libovolného svého kořene.
- Pro polynom $f(x) \in \boldsymbol{F}[x]$ platí, že

$$f(x) = 0 \iff m \mid f.$$

- Platí, že

$$\boldsymbol{F}(\alpha) \simeq \boldsymbol{F}[x]/(m(x)), \text{ a tedy } \quad \dim_{\boldsymbol{F}} \boldsymbol{F}(\alpha) = \deg m(x).$$

Vlastnosti minimálního polynomu

- Polynom $m(x)$ je ireducibilní.
- Ireducibilní monický polynom nad $\boldsymbol{F}$ je minimální polynom libovolného svého kořene.
- Pro polynom $f(x) \in \boldsymbol{F}[x]$ platí, že

$$f(x) = 0 \iff m \mid f.$$

- Platí, že

$$\boldsymbol{F}(\alpha) \simeq \boldsymbol{F}[x]/(m(x)), \text{ a tedy } \quad \dim_{\boldsymbol{F}} \boldsymbol{F}(\alpha) = \deg m(x).$$

- Je-li $\deg m(x) = k$, tvoří prvky $1, \alpha, \ldots, \alpha^{k-1}$ bázi $\boldsymbol{F}(\alpha)$.

Hledání minimálního polynomu

- Buď $\boldsymbol{F} \leq \boldsymbol{E}$ rozšíření těles takové, že $\dim_{\boldsymbol{F}} \boldsymbol{E} = k$ je konečná.

Hledání minimálního polynomu

- Buď $\boldsymbol{F} \leq \boldsymbol{E}$ rozšíření těles takové, že $\dim_{\boldsymbol{F}} \boldsymbol{E} = k$ je konečná.
- Hledáme minimální polynom prvku $\alpha \in \boldsymbol{E}$. Množina $\{1, \alpha, \alpha^2, \ldots, \alpha^k\}$ je lineárně závislá nad $\boldsymbol{F}$.

Hledání minimálního polynomu

- Buď $\boldsymbol{F} \leq \boldsymbol{E}$ rozšíření těles takové, že $\dim_{\boldsymbol{F}} \boldsymbol{E} = k$ je konečná.
- Hledáme minimální polynom prvku $\alpha \in \boldsymbol{E}$. Množina $\{1, \alpha, \alpha^2, \ldots, \alpha^k\}$ je lineárně závislá nad $\boldsymbol{F}$.
- Řešením soustavy rovnic najdeme $b_0, b_1, \ldots, b_k$ takové, že

$$b_k \alpha^k + \cdots + b_1 \alpha + b_0 = 0.$$

Hledání minimálního polynomu

- Buď $\boldsymbol{F} \leq \boldsymbol{E}$ rozšíření těles takové, že $\dim_{\boldsymbol{F}} \boldsymbol{E} = k$ je konečná.
- Hledáme minimální polynom prvku $\alpha \in \boldsymbol{E}$. Množina $\{1, \alpha, \alpha^2, \ldots, \alpha^k\}$ je lineárně závislá nad $\boldsymbol{F}$.
- Řešením soustavy rovnic najdeme $b_0, b_1, \ldots, b_k$ takové, že

$$b_k \alpha^k + \cdots + b_1 \alpha + b_0 = 0.$$

- Prvek α je kořenem polynomu $f(x) = b_k x^k + \cdots + b_1 x + b_0 \in \boldsymbol{F}[x]$.

Hledání minimálního polynomu

- Buď $\boldsymbol{F} \leq \boldsymbol{E}$ rozšíření těles takové, že $\dim_{\boldsymbol{F}} \boldsymbol{E} = k$ je konečná.
- Hledáme minimální polynom prvku $\alpha \in \boldsymbol{E}$. Množina $\{1, \alpha, \alpha^2, \ldots, \alpha^k\}$ je lineárně závislá nad $\boldsymbol{F}$.
- Řešením soustavy rovnic najdeme $b_0, b_1, \ldots, b_k$ takové, že

$$b_k\alpha^k + \cdots + b_1\alpha + b_0 = 0.$$

- Prvek α je kořenem polynomu $f(x) = b_k x^k + \cdots + b_1 x + b_0 \in \boldsymbol{F}[x]$.
- Polynom $m(x)$ je tedy dělitelem polynomu $f(x)$.

Příklad

Příklad

Příklad

- Hledáme minimální polynom prvku $\alpha + 1$ nad tělesem $\mathbb{Z}_5[\alpha]/(\alpha^2 + 1)$.

Příklad

- Hledáme minimální polynom prvku $\alpha + 1$ nad tělesem $\mathbb{Z}_5[\alpha]/(\alpha^2 + 1)$.
- Hledáme a, b tak, že

$$a(\alpha + 1)^2 + b(\alpha + 1) + 1 = 0.$$

Příklad

- Hledáme minimální polynom prvku $\alpha + 1$ nad tělesem $\mathbb{Z}_5[\alpha]/(\alpha^2 + 1)$.
- Hledáme a, b tak, že

$$a(\alpha + 1)^2 + b(\alpha + 1) + 1 = 0.$$

- Po roznásobení dotaneme

$$a(\alpha^2 + 1) + \alpha(2a + b) + (a + b + 1) = 0.$$

Příklad

- Hledáme minimální polynom prvku $\alpha + 1$ nad tělesem $\mathbb{Z}_5[\alpha]/(\alpha^2 + 1)$.
- Hledáme a, b tak, že

$$a(\alpha + 1)^2 + b(\alpha + 1) + 1 = 0.$$

- Po roznásobení dotaneme

$$a(\alpha^2 + 1) + \alpha(2a + b) + (a + b + 1) = 0.$$

- Odtud $2a + b = 0$ a $a + b + 1 = 0$ a tedy $a = 1$, $b = 3$.

Příklad

- Hledáme minimální polynom prvku $\alpha + 1$ nad tělesem $\mathbb{Z}_5[\alpha]/(\alpha^2 + 1)$.
- Hledáme a, b tak, že

$$a(\alpha + 1)^2 + b(\alpha + 1) + 1 = 0.$$

- Po roznásobení dotaneme

$$a(\alpha^2 + 1) + \alpha(2a + b) + (a + b + 1) = 0.$$

- Odtud $2a + b = 0$ a $a + b + 1 = 0$ a tedy $a = 1$, $b = 3$.
- $m(x) = x^2 + 3x + 1$.