Struktura konečných těles 2.

Konečná tělesa

15. května 2020

Obsah přednášky

3.4 Ireducibilní polynomy: Ukážeme, že pro nad konečným polynom existují ireducibilní polynomy libovolných stupňů. Polynom $x^{q^n} - x$ je dělitelný ireducibilním polynomem f stupně m nad konečným tělesem $\mathbb{F}_q$ právě když $m \mid n$. Polynom $x^{q^n} - x$ je součinem všech těchto polynomů. Dále ukážeme, že kořenové rozšíření konečného tělesa je zároveň rozšířením rozkladovým.

Obsah přednášky

3.4 Ireducibilní polynomy: Ukážeme, že pro nad konečným polynom existují ireducibilní polynomy libovolných stupňů. Polynom $x^{q^n} - x$ je dělitelný ireducibilním polynomem f stupňe m nad konečným tělesem $\mathbb{F}_q$ právě když $m \mid n$. Polynom $x^{q^n} - x$ je součinem všech těchto polynomů. Dále ukážeme, že kořenové rozšíření konečného tělesa je zároveň rozšířením rozkladovým.

3.5 Automorfismy konečných těles: Ukážeme, že automorfimy konečného tělesa jsou právě mocniny *Frobeniova automorfismu*.

Obsah přednášky

3.4 Ireducibilní polynomy: Ukážeme, že pro nad konečným polynom existují ireducibilní polynomy libovolných stupňů. Polynom $x^{q^n} - x$ je dělitelný ireducibilním polynomem f stupňe m nad konečným tělesem $\mathbb{F}_q$ právě když $m \mid n$. Polynom $x^{q^n} - x$ je součinem všech těchto polynomů. Dále ukážeme, že kořenové rozšíření konečného tělesa je zároveň rozšířením rozkladovým.

3.5 Automorfismy konečných těles: Ukážeme, že automorfimy konečného tělesa jsou právě mocniny *Frobeniova automorfismu*.

3.6 Maticová reprezentace: Ukážeme, jak reprezentovat prvky konečného tělesa pomocí matic.

Existence ireducibilních polynomů a rozklad $x^{q^n} - x$

Věta

Buď $\mathbb{F}_q$ libovolné konečné těleso. Pro každé přirozené číslo n existuje ireducibilní polynom stupně n nad $\mathbb{F}_q$.

Existence ireducibilních polynomů a rozklad $x^{q^n} - x$

Věta

Buď $\mathbb{F}_q$ libovolné konečné těleso. Pro každé přirozené číslo n existuje ireducibilní polynom stupně n nad $\mathbb{F}_q$.

Tvrzení

Buď $f(x) \in \mathbb{F}_q[x]$ ireducibilní polynom. Potom

$$f(x) \mid (x^{q^n} - x) \iff \deg f \mid n.$$

Existence ireducibilních polynomů a rozklad $x^{q^n} - x$

Věta

Buď $\mathbb{F}_q$ libovolné konečné těleso. Pro každé přirozené číslo n existuje ireducibilní polynom stupně n nad $\mathbb{F}_q$.

Tvrzení

Buď $f(x) \in \mathbb{F}_q[x]$ ireducibilní polynom. Potom

$$f(x) \mid (x^{q^n} - x) \iff \deg f \mid n.$$

Důsledek

Polynom $x^{q^n} - x$ je roven součinu všech monických ireducibilních polynomů f nad $\mathbb{F}_q$ takových, že $\deg f \mid n$.

Kořeny ireducibilních polynomů

Věta

Buď $f(x)$ ireducibilní polynom stupně m nad tělesem $\mathbb{F}_q$. Potom platí:

Kořeny ireducibilních polynomů

Věta

Buď $f(x)$ ireducibilní polynom stupně m nad tělesem $\mathbb{F}_q$. Potom platí:

- *Polynom $f(x)$ má v tělese $\mathbb{F}_{q^m}$ nějaký kořen α.*

Kořeny ireducibilních polynomů

Věta

Buď $f(x)$ ireducibilní polynom stupně m nad tělesem $\mathbb{F}_q$. Potom platí:

- *Polynom $f(x)$ má v tělese $\mathbb{F}_{q^m}$ nějaký kořen α.*
- *Prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ jsou po dvou různé a tvoří právě všechny kořeny polynomu $f(x)$.*

Kořeny ireducibilních polynomů

Věta

Buď $f(x)$ ireducibilní polynom stupně m nad tělesem $\mathbb{F}_q$. Potom platí:

- *Polynom $f(x)$ má v tělese $\mathbb{F}_{q^m}$ nějaký kořen α.*
- *Prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ jsou po dvou různé a tvoří právě všechny kořeny polynomu $f(x)$.*

Důsledek

Kořenové rozšíření konečného tělesa určené ireducibilním polynomem $f(x)$ je rozkladovým nadtělesem tohoto polynomu. Speciálně, těleso $\mathbb{F}_{q^m}$ je rozkladovým nadtělesem libovolného ireducibilního polynomu stupně m nad $\mathbb{F}_q$.

Konjugované a absolutně konjugované prvky

Definice

Jsou-li $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ konečná tělesa a $\alpha \in \mathbb{F}_{q^n}$, potom se prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ nazývají *konjugované*. Je-li q prvočíslo, nazývají se dané prvky *absolutně konjugované*.

Konjugované a absolutně konjugované prvky

Definice

Jsou-li $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ konečná tělesa a $\alpha \in \mathbb{F}_{q^n}$, potom se prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ nazývají *konjugované*. Je-li q prvočíslo, nazývají se dané prvky *absolutně konjugované*.

Tvrzení

Buď $m(x)$ minimální polynom prvku $\alpha \in \mathbb{F}_{q^n}$ nad tělesem $\mathbb{F}_q$. Položme $d = \deg m(x)$. Potom jsou prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots \alpha^{q^{d-1}}$ navzájem různé, jsou všechny kořeny polynomu $m(x)$ a tedy

$$m(x) = (x - \alpha)(x - \alpha^q)(x - \alpha^{q^2}) \cdots (x - \alpha^{q^{d-1}}).$$

Frobeniův automorfismus

Věta

Zobrazení

$$\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$
$$a \mapsto a^p$$

je automorfimem tělesa $\mathbb{F}_{p^n}$.

Frobeniův automorfismus

Věta

Zobrazení

$$\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$
$$a \mapsto a^p$$

je automorfimem tělesa $\mathbb{F}_{p^n}$.

Definice

Zobrazení σ se nazývá *Frobeniův automorfismus* tělesa $\mathbb{F}_{p^n}$.

Frobeniův automorfismus

Věta

Zobrazení

$$\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$
$$a \mapsto a^p$$

je automorfimem tělesa $\mathbb{F}_{p^n}$.

Definice

Zobrazení σ se nazývá *Frobeniův automorfismus* tělesa $\mathbb{F}_{p^n}$.

Věta

Zobrazení $\sigma^0, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ *jsou po dvou různé automorfismy tělesa* $\mathbb{F}_{p^n}$ *a jiné automorfismy tohoto tělese nexistují.*

Vlastnosti

Pozorování

Vlastnosti

Pozorování

- Grupa automorfismů konečného tělesa je cyklická, generovaná Frobeniovým automorfismem.

Vlastnosti

Pozorování

- Grupa automorfismů konečného tělesa je cyklická, generovaná Frobeniovým automorfismem.
- $\mathbb{F}_{p^m}$-automorfismy tělesa $\mathbb{F}_{p^n}$ jsou právě mocniny automorfismu σ^m. Těch je $\frac{n}{m}$.

Vlastnosti

Pozorování

- Grupa automorfismů konečného tělesa je cyklická, generovaná Frobeniovým automorfismem.
- $\mathbb{F}_{p^m}$-automorfismy tělesa $\mathbb{F}_{p^n}$ jsou právě mocniny automorfismu σ^m. Těch je $\frac{n}{m}$.
- Prvky konjugované k $\alpha \in \mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ jsou právě obrazy tohoto prvky při $\mathbb{F}_q$ automorfismech tělesa $\mathbb{F}_{q^n}$.

Vlastnosti

Pozorování

- Grupa automorfismů konečného tělesa je cyklická, generovaná Frobeniovým automorfismem.
- $\mathbb{F}_{p^m}$-automorfismy tělesa $\mathbb{F}_{p^n}$ jsou právě mocniny automorfismu σ^m. Těch je $\frac{n}{m}$.
- Prvky konjugované k $\alpha \in \mathbb{F}_{q^n}$ nad $\mathbb{F}_q$ jsou právě obrazy tohoto prvky při $\mathbb{F}_q$ automorfismech tělesa $\mathbb{F}_{q^n}$.
- Prvky konjugované k primitivnímu prvky jsou primitivní.

Věta Cayleyova-Hamiltonova

Definice (Dosazení matice do poynomu)

Buď $\boldsymbol{A}$ čtvercová matice řádu n a $f(x) = a_m x^m + \cdots a_1 x + a_0$ polynom nad tělesem $\mathbb{F}$. Dosazením matice $\boldsymbol{A}$ do polynomu $f(x)$ dostaneme matici $f(\boldsymbol{A}) = a_m \boldsymbol{A}^m + \cdots + a_1 \boldsymbol{A} + a_0 \boldsymbol{I}$, kde $\boldsymbol{I}$ značí jednotkovou matici řádu n.

Věta Cayleyova-Hamiltonova

Definice (Dosazení matice do poynomu)

Buď $\boldsymbol{A}$ čtvercová matice řádu n a $f(x) = a_m x^m + \cdots a_1 x + a_0$ polynom nad tělesem $\mathbb{F}$. Dosazením matice $\boldsymbol{A}$ do polynomu $f(x)$ dostaneme matici $f(\boldsymbol{A}) = a_m \boldsymbol{A}^m + \cdots + a_1 \boldsymbol{A} + a_0 \boldsymbol{I}$, kde $\boldsymbol{I}$ značí jednotkovou matici řádu n.

Věta (Cayelyova-Hamiltonova věta)

Buď $\boldsymbol{A}$ čtvercová matice řádu n nad tělesem $\mathbb{F}$ a buď $\chi_{\boldsymbol{A}}(\lambda) = \det(\boldsymbol{A} - \lambda \boldsymbol{I})$ její charakteristický polynom. Potom

$$\chi_{\boldsymbol{A}}(\boldsymbol{A}) = \boldsymbol{0}$$

kde $\boldsymbol{0}$ značí nulovou matici řádu n.

Doprovodná matice polynomu

Definice

Nechť $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ je monický polynom nad tělesem $\boldsymbol{F}$. *Doprovodnou maticí* polynomu $f(x)$ rozumíme matici

$$\boldsymbol{A}_f := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & 0 & -a_{n-2} \\ 0 & \dots & 0 & 0 & 1 & -a_{n-1} \end{pmatrix}$$

nad tělesem $\mathbb{F}$ typu $n \times n$ nad $\boldsymbol{F}$.

Vlastnosti doprovodné matice

Lemma

Buď $f(x)$ ireducibilní monický polynom stupně n nad tělesem $\boldsymbol{F}$. Potom je

$$\chi_{\boldsymbol{A}_f}(\lambda) = (-1)^n f(\lambda).$$

Vlastnosti doprovodné matice

Lemma

Buď $f(x)$ ireducibilní monický polynom stupně n nad tělesem $\boldsymbol{F}$. Potom je

$$\chi_{\boldsymbol{A}_f}(\lambda) = (-1)^n f(\lambda).$$

Důsledek

Buď $f(x)$ ireducibilní monický polynomnad tělesem $\boldsymbol{F}$. Potom je

$$f(\boldsymbol{A}_f) = \boldsymbol{0}.$$

Maticová reprezentace

Věta

Buď $f(x)$ ireducibilní monický polynom nad tělesem $\boldsymbol{F}$ a $\boldsymbol{A}_f$ jeho doprovodná matice. Položme

$$\boldsymbol{M} := \{g(\boldsymbol{A}_f) \mid \deg g < \deg f\}.$$

Zobrazení

$$\begin{aligned} \boldsymbol{F}[\alpha]/(f(\alpha)) &\to \boldsymbol{M} \\ g(\alpha) &\mapsto g(\boldsymbol{A}_f) \end{aligned}$$

je izomorfismus těles.

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní .

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen).

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$\boldsymbol{A}_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$\boldsymbol{A}_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prvky tělesa $\mathbb{F}_8$ můžeme ztotožnit s maticemi:

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$\boldsymbol{A}_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prvky tělesa $\mathbb{F}_8$ můžeme ztotožnit s maticemi:

$$\mathbf{0} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$\boldsymbol{A}_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prvky tělesa $\mathbb{F}_8$ můžeme ztotožnit s maticemi:

$$\boldsymbol{0} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \boldsymbol{I} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prvky tělesa $\mathbb{F}_8$ můžeme ztotožnit s maticemi:

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prvky tělesa $\mathbb{F}_8$ můžeme ztotožnit s maticemi:

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$A_f + I = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prvky tělesa $\mathbb{F}_8$ můžeme ztotožnit s maticemi:

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$A_f + I = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad A_f^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prvky tělesa $\mathbb{F}_8$ můžeme ztotožnit s maticemi:

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$A_f + I = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad A_f^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad A_f^2 + I = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prvky tělesa $\mathbb{F}_8$ můžeme ztotožnit s maticemi:

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$A_f + I = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad A_f^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad A_f^2 + I = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$A_f^2 + A_f = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix},$$

Příklad

Příklad

Polynom $f(x) = x^3 + x + 1$ je monický a nad tělesem $\mathbb{F}_2$ ireducibilní (stačí ověřit, že nemá kořen). Podle definice je

$$A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prvky tělesa $\mathbb{F}_8$ můžeme ztotožnit s maticemi:

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$A_f + I = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad A_f^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad A_f^2 + I = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$A_f^2 + A_f = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad A_f^2 + A_f + I = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$