Konečná tělesa

2. Struktura konečných těles

Lemma 2.1. *Nechť* $\mathbf{F}$ *je konečné těleso a* $\mathbf{K}$ *je podtěleso* $\mathbf{F}$*, počet prvků* $\mathbf{K}$ *je* q*. Pak* $\mathbf{F}$ *má* q^m *prvků pro nějaké přirozené číslo* $m \geq 1$*.*

Důkaz. Všimněme si, že $\mathbf{F}$ je vektorový prostor nad $\mathbf{K}$ (je třeba ověřit axiomy vektorového prostoru). Ten má konečnou dimenzi $m \geq 1$ neboť má pouze konečně mnoho prvků a tedy obsahuje konečnou generující množinu. Zvolíme bázi $b_1, \ldots, b_m$ v $\mathbf{F}$. Potom každý prvek $x \in \mathbf{F}$ lze jednoznačně vyjádřit ve tvaru $x = a_1b_1 + a_2b_2 + \ldots + a_mb_m$, kde $a_1, a_2, \ldots, a_m \in \mathbf{K}$. Takových lineárních kombinací je přesně q^m. □

Věta 2.2. *Každé konečné těleso má* p^k *prvků pro nějaké prvočíslo* p *a celé číslo* $k \geq 1$*.*

Důkaz. Označme $\mathbf{K}$ prvotěleso v $\mathbf{F}$. Charakteristika $\mathbf{F}$ je p pro nějaké prvočíslo p, tedy $\mathbf{K}$ má p prvků. Zbytek plyne z Lemma 2.1. □

V dalším se budeme zabývat otázkou, zda pro každé prvočíslo p a celé číslo $k \geq 1$ existuje těleso s p^k prvky. Jestliže ano, kolik takových těles existuje?

Definice. Nechť $\mathbf{E}, \mathbf{F}$ jsou dvě tělesa. Pak vzájemně jednoznačné zobrazení $\mathbf{T} : \mathbf{E} \to \mathbf{F}$ je *izomorfismus*, jestliže pro libovolné dva prvky $a, b \in \mathbf{E}$ platí:

$$\mathbf{T}(a + b) = \mathbf{T}(a) + \mathbf{T}(b)$$

$$\mathbf{T}(a \cdot b) = \mathbf{T}(a).\mathbf{T}(b)$$

Pokud pro nějaké těleso $\mathbf{K}$ platí $\mathbf{K} \subseteq \mathbf{E} \cap \mathbf{F}$, pak izomorfismus $\mathbf{T} : \mathbf{E} \to \mathbf{F}$ se nazývá $\mathbf{K}$-*izomorfismus*, jestliže pro každé $a \in \mathbf{K}$ platí $\mathbf{T}(a) = a$.

Příklad. Nechť $\mathbf{F}$ je těleso charakteristiky $p > 0$ a $\mathbf{K}$ je prvotěleso $\mathbf{F}$. Pak zobrazení $\mathbf{T} : \mathbb{Z}_p \to \mathbf{K}$ definované předpisem

$$\mathbf{T}(k) = \underbrace{1 + 1 + \ldots + 1}_{k} = k \cdot 1$$

je izomorfismus. Je třeba ověřit podmínky z definice izomorfizmu.

Příklad. Nechť $\mathbf{K}$ je těleso a $p(x) \in \mathbf{K}[x]$ je ireducibilní polynom stupně n. Pak množina polynomů z $\mathbf{K}[x]$ stupně menšího než n s operacemi sčítání a násobení modulo $p(x)$ je opět těleso jak jsme si připomněli v minulé přednášce. Označíme jej $\mathbf{E}$. Pro ty, co mají rádi ideály a faktorové okruhy (důkazy s nimi jsou jednodušší!) připomeňme, že $\mathbf{E} \simeq \mathbf{K}[x]/(p)$.

Nechť $p(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, kde $a_i \in \mathbf{K}$. Prvky $\mathbf{E}$ jsou polynomy $x, x^3 - x + 1 + 1, \ldots$, mezi nimi jsou i konstanty $a \in \mathbf{K}$. S konstantami se v obou tělesech $\mathbf{K}$ a $\mathbf{E}$ počítá stejně. Tedy $\mathbf{K} \subseteq \mathbf{E}$ je podtěleso tělesa $\mathbf{E}$.

Polynom $p(x)$ nemá v $\mathbf{K}$ žádný kořen, pokud $n > 1$.

Poznámka. Nechť $f(x) \in \mathbf{K}[x]$ a $a \in \mathbf{K}$ je kořen $f(x)$. Potom $(x - a)|f(x)$.

Důkaz. Libovolný polynom $f(x)$ můžeme napsat ve tvaru $f(x) = q(x)\cdot(x-a)+r(x)$, kde $\deg r(x) < \deg(x-a) = 1$, takže $r(x)$ je konstantní polynom. Protože a je kořen $f(x)$, po dosazení do $f(x)$ dostáváme $0 = f(a) = q(a)\cdot(a-a)+r(a) = r(a)$. Protože je $r(x)$ konstantní polynom a $r(a) = 0$, platí $r(x) = 0$ a tedy $(x - a)|f(x)$. □

Příklad. Uvažujme polynom $p(z) = a_n z^n + \ldots + a_1 z + a_0 \in K[z]$. Dosadíme-li $z = x \in E$, pak je hodnota $p(x)$ nějaký prvek tělesa $\mathbf{E}$, konrétně je to $p(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbf{E}$. Protože $p(x) \equiv 0 \bmod p(x)$, platí $p(x) = 0 \in \mathbf{E}$. Polynom $p(z)$ má tedy v tělese $\mathbf{E}$ aspoň jeden kořen.

Definice. Nechť $\mathbf{K}$ je těleso a $p(x) \in \mathbf{K}[x]$ je polynom ireducibilní nad $\mathbf{K}$. Potom těleso $\mathbf{E} \supseteq \mathbf{K}$ se nazývá *kořenové rozšíření* $\mathbf{K}$ určené polynomem $p(x)$, jestliže v $\mathbf{E}$ existuje nějaký kořen θ polynomu $p(x)$ a každé podtěleso $\mathbf{E}$, které obsahuje současně $\mathbf{K}$ a θ, se rovná $\mathbf{E}$.

Věta 2.3 (O existenci a jednoznačnosti kořenového rozšíření tělesa $\mathbf{K}$ určeného ireducibilním polynomem $p(x) \in \mathbf{K}[x]$)**.** *Nechť $\mathbf{K}$ je těleso a $p(x) \in \mathbf{K}[x]$ je polynom ireducibilní nad $\mathbf{K}$. Potom existuje kořenové rozšíření $\mathbf{E}$ tělesa $\mathbf{K}$ určené polynomem $p(x)$. Kořenové rozšíření je určeno jednoznačně až na $\mathbf{K}$-izomorfismus.*

Důkaz. (1) Nejprve dokážeme existenci kořenového rozšíření. Víme, že těleso $\mathbf{E}$ obsahující všechny polynomy stupně menšího než je stupeň $p(x)$ s operacemi sčítání a násobění modulo $p(x)$ je těleso obsahující $\mathbf{K}$ jako podtěleso, a ukázali jsme si, že v něm existuje aspoň jeden kořen polynomu $p(x)$. Nechť $f(x) = b_m x^m + \ldots + b_1 x + b_0 \in \mathbf{K}[x]$, přičemž m je menší než je stupeň $p(x)$. Pak takový polynom musí ležet v libovolném podtělese $\mathbf{E}$ obsahujícím x a $\mathbf{K}$.

(2) Zbývá dokázat jednoznačnost. Nechť $\mathbf{F} \supseteq \mathbf{K}$ je nějaké kořenové rozšíření $\mathbf{K}$ obsahující kořen θ polynomu $p(x)$. Definujme zobrazení $\mathbf{T} : \mathbf{E} \to \mathbf{F}$ předpisem $\mathbf{T}(f(x)) = f(\theta)$, kde $f(x) = b_m x^m + \ldots + b_1 x + b_0$ a $f(\theta) = b_m \theta^m + \ldots + b_1 \theta + b_0$.

Chceme dokázat, že $\mathbf{T}$ je $\mathbf{K}$-izomorfismus. Jestliže $a \in \mathbf{K}$, potom $\mathbf{T}(a) = a$.

Dokážeme, že $\mathbf{T}$ je homomorfismus. Nechť $f(x), g(x) \in \mathbf{E}$ jsou libovolné dva prvky, $f(x) = b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$ a $g(x) = c_{m-1} x^{m-1} + \ldots + c_1 x + c_0$. Potom platí platí

$$\mathbf{T}(f(x)) = \sum_{i=0}^{m-1} b_i \theta^i, \qquad \mathbf{T}(g(x)) = \sum_{i=0}^{m-1} c_i \theta^i$$

$$\mathbf{T}((f+g)(x)) = \sum_{i=0}^{m-1} (b_i + c_i)\theta^i = \sum_{i=0}^{m-1} b_i \theta^i + \sum_{i=0}^{m-1} c_i \theta^i = \\ = \mathbf{T}(f(x)) + \mathbf{T}(g(x))$$

Podobně (důkaz ale vyžaduje více počítání!)

$$\mathbf{T}(fg(x)) = \mathbf{T}(f(x)) \cdot \mathbf{T}(g(x)).$$

Nyní dokážeme, že $\mathbf{T}$ je prosté zobrazení. Nechť $f(x), g(x) \in \mathbf{E}$ jsou navzájem různé polynomy z $\mathbf{E}$ takové, že $\mathbf{T}(f(x)) = \mathbf{T}(g(x))$. Pak $\sum_{i=0}^{m-1} b_i \theta^i = \sum_{i=0}^{m-1} c_i \theta^i$, t.j. $\sum_{i=0}^{m-1} (b_i - c_i)\theta^i = 0$. Takže θ je kořen polynomu $0 \neq g(x) = (b_{m-1} - c_{m-1})x^{m-1} + \ldots + (b_1 - c_1)x + (b_0 - c_0) \in \mathbf{K}[x]$, který musí mít stupeň aspoň 1. Prvek θ je ale také kořenem polynomu $p(x) \in \mathbf{K}[x]$. Tedy θ je kořen polynomu $d(x) := \mathrm{NSD}(g(x), p(x)) \in \mathbf{K}[x]$. Pak $d(x) | p(x)$ v $\mathbf{K}[x]$, přičemž $1 \leq \deg d(x) < \deg p(x)$. To je však spor s předpokladem, že $p(x)$ je ireducibilní v $\mathbf{K}[x]$.

Zbývá dokázat, že $\mathbf{T}$ je na $\mathbf{F}$. $\Im\mathbf{T}$ je podtěleso $\mathbf{F}$ obsahující $\mathbf{K}$ a θ. Protože $\mathbf{F}$ je kořenové rozšíření $\mathbf{K}$ určené $p(x)$, platí $\Im\mathbf{T} = \mathbf{F}$.

Jsou-li nyní $\mathbf{F}, \mathbf{G}$ dvě kořenová rozšíření $\mathbf{K}$ určená polynomem $p(x)$, pak existují $\mathbf{K}$-izomorfismy $\mathbf{T} : \mathbf{E} \to \mathbf{F}$ a $\mathbf{U} : \mathbf{E} \to \mathbf{G}$. Potom $\mathbf{U}\mathbf{T}^{-1} : \mathbf{F} \to \mathbf{G}$ je $\mathbf{K}$-izomorfismus $\mathbf{F}$ a $\mathbf{G}$.

□

Poznámka. Jsou-li $\mathbf{F}$ a $\mathbf{G}$ dvě kořenová rozšíření tělesa $\mathbf{K}$ určená ireducibilním polynomem $p(x) \in \mathbf{K}[x]$ a označíme-li $\theta \in \mathbf{F}$ a $\sigma \in \mathbf{G}$ kořeny plynomu $p(x)$, pak $\mathbf{K}$-izomorfizmus $\mathbf{U}\mathbf{T}^{-1} : \mathbf{F} \to \mathbf{G}$ z posledního odstavce důkazu předchozí věty má vlastnost

$$\mathbf{U}\mathbf{T}^{-1}(\theta) = \mathbf{U}(x) = \sigma.$$

Lemma 2.4. *Nechť $\mathbf{F}$ je těleso charakteristiky $p > 0$. Pak pro libovolné $a, b \in \mathbf{F}$ a libovolné celé číslo $k > 0$ platí*

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

Důkaz. Důkaz provedeme indukcí dle k.

(1) Nechť $k = 1$. Podle binomické věty platí $(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + \binom{p}{p-1}ab^{p-1} + b^p$. Protože $p|\binom{p}{i}$ pro $i \in \{1, 2, \ldots, p-1\}$, platí v tělese $\mathbf{F}$, že $\binom{p}{i}.1 = 0$. Tedy také $\binom{p}{i}a^{p-i}b^i = 0$ v $\mathbf{F}$ a proto $(a+b)^p = a^p + b^p$.

(2) Předpokládejme platnost tvrzení pro $k-1$, tedy $(a+b)^{p^{k-1}} = a^{p^{k-1}} + b^{p^{k-1}}$. Potom platí $(a+b)^{p^k} = ((a+b)^{p^{k-1}})^p = (a^{p^{k-1}} + b^{p^{k-1}})^p = a^{p^k} + b^{p^k}$.

□

Lemma 2.5. *Nechť $\mathbf{F}$ je konečné těleso s q prvky. Potom pro každé $a \in \mathbf{F}$ platí $a^q = a$.*

Důkaz. Pro $a = 0$ lemma platí. Nechť $a \neq 0$, pak vezmeme multiplikativní grupu $\mathbf{F}$. Ta má $q-1$ prvků. Protože řád libovolného prvku konečné grupy je dělitelem počtu prvků této grupy, tak platí $a^{q-1} = 1$. □