Konečná tělesa

Poznámka. Konečným tělesem rozumíme těleso mající konečně mnoho prvků. V Algebře I jsme dokázali, že pro každé konečné těleso K platí, že jeho multiplikativní grupa $(K^\times, \cdot)$ je cyklická.

Příklad. Pro libovolné prvočíslo p je okruh $\mathbb{Z}_p$ zbytkových tříd modulo p konečné těleso charakteristiky p.

Poznámka. Charakteristika libovolného tělesa je nula nebo prvočíslo. Protože každé těleso charakteristiky nula obsahuje podtěleso izomorfní s $\mathbb{Q}$, má každé konečné těleso prvočíselnou charakteristiku.
Připomeňme, že každé těleso K charakteristiky $p \neq 0$ obsahuje podtěleso izomorfní s tělesem $\mathbb{Z}_p$. Můžeme tedy prvky tohoto podtělesa ztotožnit s prvky tělesa $\mathbb{Z}_p$ a považovat $\mathbb{Z}_p$ za podtěleso tělesa K.

Počet prvků konečného tělesa

Věta 1. *Nechť K je libovolné konečné těleso charakteristiky p. Pak K je jednoduchým rozšířením tělesa $\mathbb{Z}_p$ a pro jeho počet prvků platí $|K| = p^m$, kde $m = [K : \mathbb{Z}_p]$.*

Důkaz. Označíme-li c generátor cyklické grupy $(K^\times, \cdot)$, platí $K = \mathbb{Z}_p(c)$. Pak $1, c, c^2, \ldots, c^{m-1}$ je báze vektorového prostoru K nad $\mathbb{Z}_p$, a libovolný prvek tělesa K lze napsat ve tvaru $r(c)$ pro jediný polynom $r \in \mathbb{Z}_p[x]$ stupně $\operatorname{st} r < m$.
Takových polynomů je právě p^m, protože každý z m koeficientů může nabývat libovolné z p hodnot.

Věta 2. *Nechť K je libovolné konečné těleso mající p^m prvků. Pak každý prvek $c \in K$ je kořenem polynomu $x^{p^m} - x \in \mathbb{Z}_p[x]$.*

Důkaz. Jistě je kořenem 0. Každý prvek $c \in K$, $c \neq 0$, je prvkem grupy $(K^\times, \cdot)$ mající $p^m - 1$ prvků. Z Lagrangeovy věty plyne $c^{p^m-1} = 1$, a tedy $c^{p^m} = c$.

Věta 3. *Nechť p je libovolné prvočíslo a m přirozené číslo. Pak rozkladové těleso T polynomu $h = x^{p^m} - x \in \mathbb{Z}_p[x]$ nad $\mathbb{Z}_p$ má právě p^m prvků.*

Důkaz. Nechť $K = \{t \in T; t^{p^m} = t\}$ je množina všech kořenů polynomu h v T. Derivace $h' = p^m x^{p^m-1} - 1 = -1$ je nesoudělná s polynomem h, a tedy h nemá žádný násobný kořen, proto $|K| = p^m$. Ukážeme, že K je podtěleso tělesa T. Zřejmě $0, 1 \in K$.

Protože umocňujeme v komutativním okruhu na prvočíselnou charakteristiku p, z Algebry I víme, že pro libovolné prvky $a, b \in T$ platí $(a+b)^p = a^p + b^p$. Odtud indukcí $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ pro libovolné $n \in \mathbb{N}$. Pro libovolné prvky $k, h \in K$ platí $k^{p^m} = k$, $h^{p^m} = h$, a tedy $(k+h)^{p^m} = k^{p^m} + h^{p^m} = k + h$, což znamená $k + h \in K$. Speciálně $-1 = \underbrace{1 + \cdots + 1}_{p-1} \in K$.

Podobně $(k \cdot h)^{p^m} = k^{p^m} \cdot h^{p^m} = k \cdot h$, odkud $k \cdot h \in K$. Speciálně $-k = (-1) \cdot k \in K$. Je-li $k \neq 0$, pak $(k^{-1})^{p^m} = (k^{p^m})^{-1} = k^{-1}$, a tedy $k^{-1} \in K$. Tedy K je těleso o p^m prvcích.
Rozkladové těleso je nejmenší těleso obsahující všechny kořeny daného polynomu, platí tedy $T = K$.

Konstrukce konečného tělesa o daném prvků

Důsledek. *Nechť p je libovolné prvočíslo a m přirozené číslo. Pak existuje alespoň jeden normovaný ireducibilní polynom $f \in \mathbb{Z}_p[x]$ stupně* $\operatorname{st} f = m$.

Důkaz. Těleso T z věty 3 má p^m prvků, tedy $[T : \mathbb{Z}_p] = m$. Podle věty 1 jde o jednoduché rozšíření $T = \mathbb{Z}_p(c)$, minimální polynom prvku c nad $\mathbb{Z}_p$ má stupeň m a je normovaný a ireducibilní.

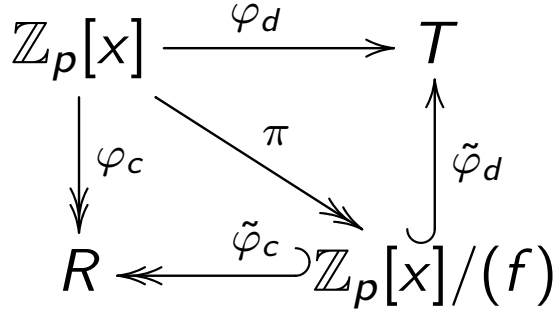
Poznámka. Chceme-li sestrojit těleso o p^m prvcích, stačí nalézt normovaný ireducibilní polynom $f \in \mathbb{Z}_p[x]$ stupně $\operatorname{st} f = m$.
Hledaným tělesem je pak faktorokruh $R = \mathbb{Z}_p[x]/(f)$.
Pro prvek $c = x + (f)$ pak platí $R = \mathbb{Z}_p(c)$ a minimálním polynomem prvku c je polynom f.

Příklad. Sestrojme těleso o 16 prvcích.
Polynom $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$ je ireducibilní, tedy faktorokruh $R = \mathbb{Z}_2[x]/(f)$ je těleso a $|R| = 2^4$. Označíme-li $c = x + (f)$, je $R = \mathbb{Z}_2(c) = \{a_3c^3 + a_2c^2 + a_1c + a_0;\ a_0, a_1, a_2, a_3 \in \mathbb{Z}_2\}$. Při násobení prvků využíváme toho, že c je kořenem polynomu f, tedy platí $c^4 = c + 1$.

Konečné těleso je jednoznačně určeno svým počtem prvků (až na izomorfismus)

Věta 4. Libovolná konečná tělesa o stejném počtu prvků jsou izomorfní.

Důkaz. Nechť R je libovolné těleso mající p^m prvků a nechť T je rozkladové těleso polynomu $h = x^{p^m} - x \in \mathbb{Z}_p[x]$ nad $\mathbb{Z}_p$ z věty 3. Ukážeme, že $R \cong T$. Podle věty 1 existuje $c \in R$ tak, že $R = \mathbb{Z}_p(c)$. Označme f minimální polynom prvku c nad $\mathbb{Z}_p$. Podle věty 2 je c kořenem polynomu h, tedy $f \mid h$ v $\mathbb{Z}_p[x]$. Protože h je v $T[x]$ součinem lineárních činitelů, existuje v T kořen d polynomu f. Máme homomorfismy okruhů $\varphi_c : \mathbb{Z}_p[x] \to R$ a $\varphi_d : \mathbb{Z}_p[x] \to T$, kde pro libovolné $g \in \mathbb{Z}_p[x]$ je $\varphi_c(g) = g(c) \in R$ a $\varphi_d(g) = g(d) \in T$. Platí $\ker \varphi_c = \ker \varphi_d = (f)$. Z hlavní věty o faktorokruzích dostáváme diagram:



Protože $|R| = |T| \in \mathbb{N}$, je injekce $\tilde{\varphi}_d \circ (\tilde{\varphi}_c)^{-1} : R \to T$ bijekcí, tedy $R \cong T$.

Podtělesa konečného tělesa

Věta 5. *Nechť konečné těleso K charakteristiky p má p^m prvků a nechť R je podtěleso tělesa K. Pak R má p^d prvků, kde $d \mid m$.*

Důkaz. Podle věty 1 platí
$m = [K : \mathbb{Z}_p] = [K : R] \cdot [R : \mathbb{Z}_p] = [K : R] \cdot d$.

Věta 6. *Nechť K je konečné těleso charakteristiky p mající p^m prvků a nechť přirozené číslo $d \mid m$. Pak existuje jediné podtěleso R tělesa K mající p^d prvků.*

Důkaz. Podle vět 3 a 4 jsou všechny prvky tělesa K jednoduchými kořeny polynomu $x^{p^m} - x$. Z $d \mid m$ plyne $(p^d - 1) \mid (p^m - 1)$, neboť $(p^d - 1)(p^{m-d} + p^{m-2d} + \cdots + p^d + 1) = p^m - 1$. Analogicky $(x^{p^d-1} - 1) \mid (x^{p^m-1} - 1)$ v $\mathbb{Z}_p[x]$, a tedy $(x^{p^d} - x) \mid (x^{p^m} - x)$. Proto K obsahuje p^d kořenů polynomu $x^{p^d} - x$, které podle důkazu věty 3 tvoří podtěleso R tělesa K. Naopak každý prvek podtělesa o p^d prvcích musí být podle věty 2 kořenem polynomu $x^{p^d} - x$, je tedy R jediné podtěleso tělesa K o p^d prvcích.

Rozklad polynomu $x^{p^m} - x \in \mathbb{Z}_p[x]$ na ireducibilní činitele

Věta 7. Nechť p je prvočíslo, $m \in \mathbb{N}$. Polynom $h = x^{p^m} - x \in \mathbb{Z}_p[x]$ je roven součinu všech normovaných ireducibilních polynomů v $\mathbb{Z}_p[x]$, jejichž stupeň $d \mid m$.

Důkaz. Podle věty 3 má polynom h pouze jednoduché kořeny, v jeho rozkladu na součin normovaných ireducibilních polynomů v $\mathbb{Z}_p[x]$ má proto každý činitel jen jednoduché kořeny a žádný činitel se neopakuje. Nechť f je libovolný činitel v tomto rozkladu, $d = \operatorname{st} f$. Rozkladové těleso T polynomu h obsahuje všech d jeho kořenů, přitom f je minimálním polynomem svému libovolnému kořenu $c \in T$, proto $d = [\mathbb{Z}_p(c) : \mathbb{Z}_p]$, podle věty 5 tedy $d \mid m$.

Nechť naopak je $g \in \mathbb{Z}_p[x]$ libovolný normovaný ireducibilní polynom stupně $d \mid m$. Pak $\mathbb{Z}_p[x]/(g)$ je konečné těleso o p^d prvcích, ve kterém má polynom g kořen, podle vět 6 a 4 je toto těleso izomorfní s podtělesem tělesa T, proto má g také kořen $c \in T$. Minimálním polynomem prvku c je g, a tedy $g \mid h$.

Počty normovaných ireducibilních polynomů

Věta 8. *Označme $m_{p,d}$ počet normovaných ireducibilních polynomů v $\mathbb{Z}_p[x]$ stupně d. Pak pro libovolné $m \in \mathbb{N}$ platí* $\sum_{d|m} d \cdot m_{p,d} = p^m$.

Důkaz. Stačí porovnat stupně v rozkladu polynomu $h = x^{p^m} - x \in \mathbb{Z}_p[x]$ podle věty 7. Stupeň součinu všech $m_{p,d}$ normovaných ireducibilních polynomů stupně d je $d \cdot m_{p,d}$.

Poznámka. Pomocí věty 8 můžeme počty $m_{p,d}$ určit rekurentně vzhledem k d:

$m_{p,1} = p,$

$m_{p,1} + 2m_{p,2} = p^2 \quad \Rightarrow \quad m_{p,2} = \frac{1}{2}(p^2 - p),$

$m_{p,1} + 3m_{p,3} = p^3 \quad \Rightarrow \quad m_{p,3} = \frac{1}{3}(p^3 - p),$

$m_{p,1} + 2m_{p,2} + 4m_{p,4} = p^4 \quad \Rightarrow \quad m_{p,4} = \frac{1}{4}(p^4 - p^2),$

$m_{p,1} + 5m_{p,5} = p^5 \quad \Rightarrow \quad m_{p,5} = \frac{1}{5}(p^5 - p),$

$m_{p,1} + 2m_{p,2} + 3m_{p,3} + 6m_{p,6} = p^6 \quad \Rightarrow \quad m_{p,6} = \frac{1}{6}(p^6 - p^3 - p^2 + p)$

$\vdots$

Frobeniův automorfismus

Věta 9. *Nechť konečné těleso K charakteristiky p má p^m prvků. Pak zobrazení $\varphi : K \to K$, určené předpisem $\varphi(a) = a^p$ pro každé $a \in K$, je izomorfismus okruhů, je to tedy automorfismus tělesa K.*

Důkaz. Zřejmě $\varphi(1) = 1$. Pro každé $a, b \in K$ je
$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$,
$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$, neboť umocňujeme v komutativním okruhu na prvočíselnou charakteristiku. Je tedy φ homomorfismus okruhů. Protože jde z tělesa do tělesa, je injektivní. Protože je mezi konečnými množinami o stejném počtu prvků, je i surjektivní.

Definice. Izomorfismus φ se nazývá Frobeniův automorfismus.

Poznámka. Množina všech automorfismů tělesa K tvoří grupu vzhledem k operaci skládání. V této grupě má Frobeniův automorfismus φ řád m. Indukcí vůči k dostaneme $\varphi^k(a) = a^{p^k}$. Věta 2 zaručí $\varphi^m = \mathrm{id}_K$, podle věty 3 pro libovolné $d \mid m$ je $\{a \in T;\, \varphi^d(a) = a\}$ podtěleso tělesa T o p^d prvcích. Je možné dokázat, že φ je generátor grupy všech automorfismů tělesa K.

Grupa automorfismů konečného tělesa

Věta 10. Nechť konečné těleso K charakteristiky p má p^m prvků. Pak grupa všech automorfismů tělesa K je cyklická grupa řádu m, generovaná Frobeniovým automorfismem.

Důkaz. Z předchozí poznámky víme, že Frobeniův automorfismus generuje v grupě všech automorfismů tělesa K cyklickou podgrupu řádu m. Stačí tedy ukázat, že automorfismů tělesa K je nejvýše m. Podle věty 1 je $K = \mathbb{Z}_p(c)$, přičemž minimální polynom f prvku c nad $\mathbb{Z}_p$ má stupeň m. Ukážeme, že libovolný automorfismus $\psi : K \to K$ je jednoznačně určen svou hodnotou na prvku c, označme $d = \psi(c)$. Platí $K = \mathbb{Z}_p(c) = \{a_{m-1}c^{m-1} + a_{m-2}c^{m-2} + \cdots + a_1 c + a_0;\ a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_p\}$. Libovolný prvek $a \in \mathbb{Z}_p$ je součtem několika jedniček, proto $\psi(a) = a$, tedy $\psi(a_{m-1}c^{m-1} + a_{m-2}c^{m-2} + \cdots + a_1 c + a_0) = a_{m-1}d^{m-1} + a_{m-2}d^{m-2} + \cdots + a_1 d + a_0$. Podobně $f(d) = f(\psi(c)) = \psi(f(c)) = \psi(0) = 0$, tedy d je kořen polynomu f. Ovšem polynom v tělese nemůže mít kořenů více než je jeho stupeň.