1. Konečná tělesa

1.1. Konečná tělesa

▶ 1.1.1. Věta (Wedderburn). Libovolné konečné těleso je komutativní.

▶ 1.1.2. Věta. Libovolné konečné těleso T má řád p^n, kde $p \in \mathbb{P}$ a $n \in \mathbb{N}$, přičemž $p = \operatorname{ch} T$ a $n = \dim_{Z_p} T$.

◦ *Důkaz.* T je vektorový prostor nad tělesem Z_p (až na izomorfie) a $\dim_{Z_p} T = n$, a tedy $T \ni \alpha = \sum_{i=1}^{n} \alpha_i u_i$, kde $\alpha_i \in Z_p$ a $(u_i)_{i=1}^{n}$ je báze T. Počet n-tic $(\alpha_1, \ldots, \alpha_n)$ je p^n a z jednoznačnosti vyjádření prvku v bázi dostáváme, že prvků T je také p^n. □

▶ 1.1.3. Lemma (binomická věta). Nechť R je asociativní a komutativní okruh s jednotkou, nechť $a, b \in R^\bullet$ a $n \in \mathbb{N}$. Pak platí:

$$(a+b)^n = a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i b^{n-i} + b^n.$$

▶ 1.1.4. Lemma. V tělese charakteristiky $p \in \mathbb{P}$ platí:

$$(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m}.$$

◦ *Důkaz.* Nechť nejprve $m = 1$. Důkaz provedeme matematickou indukcí podle m.

($m = 1$, $a + b$) Chceme ukázat, že $\sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} = 0$. Zjevně platí, že $p \mid p! = \binom{p}{i} i!(p-i)!$. Neboť p je prvočíslo, musí dělit alespoň jeden z činitelů. Neboť pro $0 < i < p$ je $i < p$ a $p - i < p$, platí $p \mid \binom{p}{i}$, tedy $\binom{p}{i}$ je násobkem charakteristiky, a tedy $\binom{p}{i} a^i b^{p-i} = 0$.

($m = 1$, $a - b$) Pro $p = 2$ je $(a-b)^2 = a^2 - 2ab + b^2 = a^2 - b^2 = a^2 - b^2 + 2b^2 = a^2 + b^2$ Pro p liché je $(a-b)^p = (a + (-b))^p = a^p + (-b)^p = a^p - b^p$.

($m \to m+1$) $(a \pm b)^{p^{m+1}} = \left((a \pm b)^{p^m}\right)^p = \left(a^{p^m} \pm b^{p^m}\right)^p = \left(a^{p^m}\right)^p \pm \left(b^{p^m}\right)^p = a^{p^{m+1}} \pm b^{p^{m+1}}$.

□

▶ 1.1.5. Lemma. V konečném tělese řádu q platí pro všechny prvky $a^q = a$.

◦ *Důkaz.* Nechť $|U| = q$, lib. $a \in U$, $a \neq 0$. Pak $a \in U_*$, $|U_*| = q - 1$ a podle Lagrangeovy věty řád a dělí $q - 1$, a tedy $a^{q-1} = 1$. Potom též $a^q = a$, což platí i pro $a = 0$, tedy pro všechny prvky. □

▶ 1.1.6. Věta. K libovolným číslu $p \in \mathbb{P}$ a $n \in \mathbb{N}$ existuje až na izomorfismus právě jedno těleso řádu p^n. Takové těleso značíme $\mathrm{GF}(p^n)$ (Galoisova tělesa).

◦ *Důkaz.* Položme $q := p^n$ a definujme $P := x^q - x \in Z_p[x]$. Nechť U je rozkladové těleso polynomu P a nechť $U_0 = \{\alpha \in U \mid P(\alpha) = 0\} = \{\alpha \in U \mid \alpha^q = \alpha\}$. Dále $P' = qx^{q-1} - 1x^0 = pp^{n-1}x^{q-1} - 1x^0 = -1x^0$, tedy derivace nemá kořen, a tedy všechny kořeny P jsou 1násobné.

Ukážeme, že U_0 je těleso, tedy že je uzavřené v tělese U. Mějme $\alpha, \beta \in U_0$. Pak $(\alpha - \beta)^q = (\alpha - \beta)^{p^n} = \alpha^q - \beta^q = \alpha - \beta$, tedy $\alpha - \beta \in U_0$. Nechť navíc $\beta \neq 0$, pak $(\alpha\beta^{-1})^q = \alpha^q \left(\beta^q\right)^{-1} = \alpha\beta^{-1}$, tedy $\alpha\beta^{-1} \in U_0$. Tedy jsme nalezli těleso o p^n prvcích.

Jednoznačnost nedokazujeme. □

► 1.1.7. Lemma. Buď $G = (M, \cdot)$ grupa a nechť $a, b \in M$ komutují, tj. $ab = ba$, a označme $m = |a|$, $n = |b|$ a $r = |ab|$ řády prvků a, b a ab. Pak $r \mid mn$, a tedy $r \leq mn$. A jsou-li m, n nesoudělná, je $r = mn$.

◦ *Důkaz.* Platí $(ab)^{mn} = (a^m)^n (b^n)^m = 1^n 1^m = 1$, tedy $r \mid mn$.

Pro nesoudělná m, n je $1 = (ab)^{mr} = (a^m)^r b^{mr} = b^{mr} \Rightarrow n \mid mr \Rightarrow n \mid r$. Podobně také $m \mid r$, tedy $mn \mid r$. □

► 1.1.8. Věta. Buď $G = (M, \cdot)$ grupa a nechť $a, b \in M$ komutují, tj. $ab = ba$, a označme $m = |a|$, $n = |b|$ řády prvků a a b. Potom $(\exists c \in M)(|c| = \nu(m, n))$.

◦ *Důkaz.* Položme $m = p_1^{k_1} \cdots p_r^{k_r}\, p_{r+1}^{k_{r+1}} \cdots p_{r+s}^{k_{r+s}}$ a $n = p_1^{\ell_1} \cdots p_r^{\ell_r}\, p_{r+1}^{\ell_r+1} \cdots p_{r+s}^{\ell_r+s}$, přičemž $k_i \geq \ell_i$ pro $i \in \widehat{r}$ a $k_i < \ell_i$ jinak.

Dále označme $\bar{m} = p_1^{k_1} \cdots p_r^{k_r}$ a $\bar{n} = p_{r+1}^{\ell_r+1} \cdots p_{r+s}^{\ell_r+s}$. Zjevně $\delta(\bar{m}, \bar{n}) = 1$. Označme $\bar{a} = a^{\frac{m}{\bar{m}}}$ a $\bar{b} = b^{\frac{n}{\bar{n}}}$. Pak $|\bar{a}| = \bar{m}$ a $\left|\bar{b}\right| = \bar{n}$. Dále $\bar{a}$ a $\bar{b}$ komutují a mají nesoudělné řády, označme $c = \bar{a}\bar{b}$, pak $|c| = \bar{m}\bar{n} = \nu(m, n)$. □

► 1.1.9. Věta. Multiplikativní grupa libovolného konečného tělesa T je cyklická.

◦ *Důkaz.* Označme $q = p^n = |T|$ počet prvků tělesa T, tedy $T = \mathrm{GF}(q)$ Víme, že $|T_*| = q - 1$. Vezměme libovolné $a \in T_*^\bullet$

Nechť $|a| = q - 1$, pak $\langle a \rangle = T_*$ a jsme hotovi. Nechť tedy $m = |a| < q - 1$. Mějme libovolné b takové, že pro $n = |b|$ platí $n \mid m$. Tedy víme, že $b^m = 1$, a tedy b je kořenem polynomu $x^n - 1 \in Z_p[x]$, který má nejvýše m kořenů. A neboť $m < q - 1$, existuje alespoň jeden prvek b takový, že pro $n = |b|$ platí $n \nmid m$. Víme, že T_* je komutativní, tedy $(\exists c)(|c| = \nu(m, n))$ a neboť $n \nmid m$, je $\nu(m, n) > m$.

Po konečně mnoha krocích musíme nezbytně dojít k číslu $q - 1$. □

► 1.1.10. Definice. Primitivním prvkem konečného tělesa T je libovolný generátor jeho multiplikativní grupy.

► 1.1.11. Důsledek. Libovolné konečné těleso má primitivní prvek.

► 1.1.12. Poznámka. Mějme $Z_p[x]$ a $P \in Z_p[x]$ ireducibilní stupně n. Pak $Z_p[x] \,/\, I_P$ je těleso o p^n prvcích a v následující větě ukážeme, že takto lze zkonstruovat všechna konečná tělesa.

► 1.1.13. Příklad. Prozkoumejme GF(9).

$9 = 3^2$, tedy $Z_3 = \{0, 1, 2\}$ a $P = x^2 + x + 2$, P nemá v Z_3 kořen, tedy je ireducibilní.

Platí $x^2 + x + 2 \equiv_P \theta$, tedy $x^2 \equiv_P -x - 2 \equiv_P 2x + 1$ a $2x^2 = x + 2$.

Prvky jsou $\{0, x^0 \equiv 1,\ x^1 \equiv x,\ x^2 \equiv 2x + 1,\ x^3 \equiv 2x^2 + x \equiv 2x + 2,\ x^4 \equiv 2,\ x^5 \equiv 2x,\ x^6 \equiv x + 2,\ x^7 \equiv x^2 + 2x \equiv x + 1\}$. Pro kontrolu spočítáme, že $x^8 \equiv x^2 + x \equiv 1 = x^0$.

Tedy $\overline{x}$ je primitivním prvkem GF(9). Vždy existuje P, aby $\overline{x}$ bylo primitivním prvkem příslušného konečného tělesa. Takové P nazýváme primitivní polynom.

► 1.1.14. Věta. K libovolným $p \in \mathbb{P}$ a $n \in \mathbb{N}$ existuje $P \in Z_p[x]$ takový, že $\operatorname{st} P = n$ a P je ireducibilní nad Z_p.

◦ *Důkaz.* Už víme, že existuje $U = \mathrm{GF}(p^n)$, platí $\operatorname{ch} U = p$ a Z_p je prvotěleso U. Nechť α je primitivní prvek U. Ukážeme, že $U = Z_p(\alpha)$.

(⊆) Pokud $x = 0$, je $x \in Z_p(\alpha)$, pokud $x \neq 0$, je $x = \alpha^k$, tedy $x \in Z_p(\alpha)$.

(⊇) Platí $Z_p \cup \{\alpha\} \subseteq U$ a $Z_p(\alpha)$ je nejmenší takové, tedy $Z_p(\alpha) \subseteq U$.

Nutně $\alpha \neq 0$, tedy $\alpha \in U_*$ a $\alpha^{q-1} = 1$, kde $q = p^n$. Tedy α je kořenem polynomu $x^{q-1} - 1 \in Z_p[x]$ a α je algebraický nad Z_p. Nechť M_α je minimální polynom prvku α nad Z_p. Pak M_α je ireducibilní a je $\operatorname{st} M_\alpha = \operatorname{st} \alpha = \dim_{Z_p} Z_p(\alpha) = \dim_{Z_p} U = n$.

Hledaným polynomem je tedy minimální polynom primitivního prvku tělesa GF(q). □

• 1.2. Eulerova funkce ϕ

► 1.2.1. Definice. $\phi : \mathbb{N} \to \mathbb{N}$, $\phi(n)$ je počet čísel z $\widehat{n}$, která jsou s n nesoudělná.

► 1.2.2. Příklad. $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$.

► 1.2.3. Věta. Buďte $p, q \in \mathbb{P}$, $n, m \in \mathbb{N}$. Pak

(1) $\phi(p) = p - 1$;

(2) $\phi(p^n) = p^n - p^{n-1} = p^n \left(1 - \frac{1}{p}\right)$;

(3) $p \neq q$, pak $\phi(pq) = \phi(p)\phi(q)$;

(4) $\delta(m, n) = 1$, pak $\phi(mn) = \phi(m)\phi(n)$.

◦ *Důkaz.*

(1) Speciální případ (2).

(2) S p^n jsou soudělné právě všechny násobky p, kterých je v $\widehat{p^n}$ právě p^n/p.

(3) S pq jsou nesoudělné právě všechny násobky p a q, kterých je v $\widehat{pq}$ právě $q + p - 1$.

(4) Bez důkazu.

□

► 1.2.4. Lemma. Nechť $k, \ell, m \in \mathbb{N}$. Pak pokud $\delta(k,m) = \delta(\ell,m) = 1$, platí $\delta(k\ell, m) = 1$.

◦ *Důkaz.* Existují $u, v_{1,2} \in \mathbb{Z}$ tak, že $u_1 k + v_1 m = 1$ a $u_2 \ell + v_2 m = 1$. Vynásobením rovností dostaneme $(u_1 u_2)kl + (u_1 v_2 k + v_1 u_2 \ell + v_1 v_2 m)m = 1$. □

► 1.2.5. Věta. Mějme $m \in \mathbb{N}$, $m \geq 2$. Uvažujme Z_m a definujme $G_m^\bullet := \left\{\overline{k} \;\middle|\; \delta(k,m) = 1\right\} \subseteq Z_m^\bullet$. Pak G_m s operací násobení tříd je grupa o $\phi(m)$ prvcích.

◦ *Důkaz.* Součin tříd pomocí předchozího lemmatu zůstane v G. Taktéž $\delta(1,m) = 1$, tedy G má jednotku $\overline{1}$.

Pokud $\overline{k} \in G^\bullet$, pak $(\exists u, v)(uk + vm = 1)$, tedy $\overline{u}\overline{k} + \overline{v}\underbrace{\overline{m}}_{\overline{0}} = \overline{u}\overline{k} = \overline{1}$ a $\left(\overline{k}\right)^{-1} = \overline{u}$. A z definice Eulerovy funkce plyne, že $|G_m| = \phi(m)$. □

► 1.2.6. Věta (Euler, Fermat). Buďte $m \in \mathbb{N}$, $m \geq 2$ a nechť $k \in \widehat{m}$ je nesoudělné s m. Pak $k^{\phi(m)} \equiv_m 1$.

◦ *Důkaz.* Pro $\overline{k} \in G_m^\bullet$ je $\left(\overline{k}\right)^{\phi(m)} = \overline{1}$, tedy $k^{\phi(m)} \equiv_m 1$. □

► 1.2.7. Věta (Malá Fermatova věta). Je-li $p \in \mathbb{P}$ a $k \in \widehat{p-1}$, pak $k^{p-1} \equiv_p 1$

◦ *Důkaz.* Speciální případ Eulerovy-Fermatovy věty pro $p \in \mathbb{P}$, a tedy $\phi(p) = p - 1$. □

► 1.2.8. Věta (Velká Fermatova věta). Pro $n \in \mathbb{N}$, $n > 2$ neexistují přirozená a, b, c taková, že $a^n + b^n = c^n$.