6 Konečná tělesa

V této kapitole budeme pod pojmem těleso mít na mysli vždy konečné komutativní těleso, tedy množinu s dvěma binárními operacemi $(T, +, \cdot)$, kde $(T, +)$ je komutativní grupa s neutrálním prvkem 0, $(T - \{0\}, \cdot)$ je komutativní grupa s neutrálním prvkem 1, přičemž $1 \neq 0$, a násobení je distributivní vůči sčítání.

Charakteristika tělesa

6.1 Definice Nechť $(T, +, \cdot, 0, 1)$ je konečné těleso. Nejmenší přirozené číslo $r > 0$ takové, že $\underbrace{1 + 1 + \ldots + 1}_{r\text{-krát}} = 0$, se nazývá *charakteristika tělesa* T. Značíme $\operatorname{char} T$.
(Charakteristika tělesa je vlastně řád prvku 1 v grupě $(T, +)$ - viz následující kapitola.)

6.2 Tvrzení *Charakteristika konečného tělesa je vždy prvočíslo.*

Důkaz Kdyby $\operatorname{char} T = r$ bylo složené číslo, $r = ab$ pro $1 < a \leq b < r$, pak by bylo platilo:

$$0 = \underbrace{1 + 1 + \ldots + 1}_{r\text{-krát}} = \underbrace{\underbrace{(1 + 1 + \ldots + 1)}_{a\text{-krát}} + \ldots + \underbrace{(1 + 1 + \ldots + 1)}_{a\text{-krát}}}_{b\text{-krát}} = \underbrace{(1 + 1 + \ldots + 1)}_{a\text{-krát}} \cdot \underbrace{(1 + 1 + \ldots + 1)}_{b\text{-krát}}$$

(Při úpravách používáme toho, že sčítání je asociativní, 1 je neutrální prvek vůči násobení, násobení je distributivní vůči sčítání.) Protože těleso nemá dělitele nuly, musí být buď $\underbrace{1 + 1 + \ldots + 1}_{a\text{-krát}} = 0$ nebo $\underbrace{1 + 1 + \ldots + 1}_{b\text{-krát}} = 0$, což je spor s tím, že r je nejmenší takové číslo. Tudíž r je prvočíslo. ⊠

6.3 Příklad Zřejmě $\operatorname{char} \mathbb{Z}_p = p$. Nechť $T = \mathbb{Z}_p[x]/q(x)$, kde $q(x)$ je ireducibilní nad $\mathbb{Z}_p$, pak $\operatorname{char} T = p$.
Aneb každé rozšíření T tělesa $\mathbb{Z}_p$ vytvořené jako faktorový okruh polynomů nad $\mathbb{Z}_p$ modulo ireducibilní polynom, má charakteristiku p.

6.4 Ukážeme, že $\operatorname{char} T = p$ právě, když těleso T je rozšířením tělesa $\mathbb{Z}_p$. V následující části opět 1 značí neutrální prvek vůči násobení a 0 značí neutrální prvek vůči sčítání v tělese T.
Množina

$$P = \{1,\ 1 + 1,\ 1 + 1 + 1, \ldots, \underbrace{1 + 1 + \ldots + 1}_{p\text{-krát}} = 0\}$$

má p různých prvků a tvoří podgrupu grupy $(T, +)$ generovanou prvkem 1. Množina P je uzavřená i vůči násobení (součin dvou prvků z P se dá přepsat podle distributivního zákona na součet 1, což je prvek z P), a snadno se odvodí, že P tvoří podtěleso tělesa T.
Podle tvrzení o řádech prvků je $k \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{k\text{-krát}} = 0$ právě, když $p \mid k$, tedy v tělese P se počítá stejně jako v tělese $\mathbb{Z}_p$. Zobrazení

$$\underbrace{1 + 1 + \ldots + 1}_{k\text{-krát}} \longleftrightarrow k$$

je tudíž tělesový izomorfismus, skrze který můžeme ztotožnit těleso $(P, +, \cdot)$ s tělesem $(\mathbb{Z}_p, +, \cdot)$ a psát $\mathbb{Z}_p \subseteq T$. Těleso T charakteristiky p lze považovat za rozšíření tělesa $\mathbb{Z}_p$.

6.5 Tvrzení *Každé konečné těleso má p^k prvků, pro nějaké prvočíslo p a nějaké přirozené číslo k.*

Důkaz Těleso T charakteristiky p lze považovat za lineární prostor nad tělesem $\mathbb{Z}_p$ (násobení skaláry ze $\mathbb{Z}_p$ je realizováno jako násobení v tělese T, neboť $\mathbb{Z}_p \subseteq T$). Jelikož je T konečné těleso, tak musí mít jakožto lineární prostor konečnou bázi, označme $\dim T = k$. Každý prvek z lineárního prostoru T je lineární kombinací k bázických prvků s koeficienty ze $\mathbb{Z}_p$, těchto kombinací je právě p^k. ⊠

Aneb na šestiprvkové množině není možné definovat operace sčítání a násobení tak, aby byly splněny vlastnosti požadované pro komutativní těleso.

6.6 Tvrzení *Nechť T je těleso charakteristiky p. Pak pro každé $a, b \in T$ platí:* $(a+b)^p = a^p + b^p$

Důkaz Podle binomické věty je

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}\, b^k$$

Přitom $\binom{p}{0} = \binom{p}{p} = 1$ a pro $1 \le k \le (p-1)$ je $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p\cdot(p-1)\cdot\ldots\cdot(p-k+1)}{1\cdot2\cdot3\cdot\ldots\cdot k}$. V čitateli je součin k po sobě jdoucích přirozených čísel a ten je vždy dělitelný číslem $k!$. Zlomek lze zkrátit tak, že ve jmenovateli bude 1, přičemž p je prvočíslo, takže p v čitateli zůstane. Pro $1 \le k \le (p-1)$ je tedy $\binom{p}{k} = p \cdot l$, pro $l \in \mathbb{N}$. V tělese charakteristiky p je $\binom{p}{k} = p \cdot l = 0$, všechny mezičleny vypadnou a zůstane $(a+b)^p = a^p + b^p$. ⊠

6.7 Důsledek *Nechť T je těleso charakteristiky p, a nechť $m \in \mathbb{N}$.*
1. Pro každé $a, b, \in T$ je $(a+b)^{(p^m)} = a^{(p^m)} + b^{(p^m)}$.
2. Pro všechny $a_1, \ldots, a_n \in T$ je $(a_1 + a_2 + \ldots + a_n)^{(p^m)} = a_1^{(p^m)} + a_2^{(p^m)} + \ldots + a_n^{(p^m)}$.

Důkaz Lze dokázat z předchocího tvrzení konečnou indukcí dle m, resp. dle n. ⊠

6.8 Tvrzení *Pro polynomy nad $\mathbb{Z}_p$ platí:*
1. $x^p - 1 = (x-1)^p$, tedy prvek $1 \in \mathbb{Z}_p$ je p-násobný kořen polynomu $x^P - 1$.
2. $x^{(p^m)} - 1 = (x-1)^{(p^m)}$, tedy prvek $1 \in \mathbb{Z}_p$ je p^m-násobný kořen polynomu $x^{(p^m)} - 1$.
3. $x^{p-1} - 1 = (x-1)(x-2)\ldots(x-(p-1))$, tedy všechny prvky $0 \ne a \in \mathbb{Z}_p$ jsou kořenem polynomu $x^{p-1} - 1$.

Důkaz
1. Protože $\operatorname{char} \mathbb{Z}_p = p$, lze dokázat obdobně jako v předchozím tvrzení, že $(x-1)^P = x^p + (-1)^p$. Ale $(-1)^p = -1$, neboť prvočíslo p je liché (kromě $p = 2$, ale v $\mathbb{Z}_2$ je $-1 = 1$).
3. Z Malé Fermatovy věty každé $0 \ne a \in \mathbb{Z}_p$ splňuje $a^{p-1} = 1$ v $\mathbb{Z}_p$, je tedy kořenem polynomu $x^{p-1} - 1$. ⊠

Primitivní prvek tělesa

Nejdříve bude třeba připomenout některé výsledky z teorie konečných grup, jako např. pojmy řád prvku v grupě, generátor cyklické grupy, Lagrageovu větu a Eulerovu větu pro konečné grupy. Tyto výsledky ponecháme většinou bez důkazu.

6.9 Věta (Eulerova) *Nechť $(G, \circ, 1)$ je konečná grupa o n prvcích. Pro každé $a \in G$ platí: $a^n = 1$ v G.*

Důkaz (pro komutativní grupu G) Levá translace prvkem $a \in G$ definovaná předpisem $l_a : G \to G : l_a(x) = a \circ x$ je v grupě vzájemně jednoznačné zobrazení. Tudíž součin všech prvků z grupy $G = \{x_1, x_2, \ldots, x_n\}$ je možné napsat dvěma způsoby:

$$s = \prod_{i=1}^{n} x_i = \prod_{i=1}^{n} (a \circ x_i)$$

Díky komutativitě dostáváme

$$s = a^n \circ \prod_{i=1}^{n} x_i = a^n \circ s,$$

a vynásobíme-li rovnost prvkem s^{-1}, který v grupě existuje, získáme dokazovaný vztah $1 = a^n$. ⊠

6.10 Věta (Malá Fermatova) *Pro každé $a \ne 0$ je $a^{p-1} = 1$ v $\mathbb{Z}_p$.*

6.11 Věta (Euler-Fermatova) *Pro každé a nesoudělné s n je $a^{\varphi(n)} = 1$ v $\mathbb{Z}_n$.*

6.12 Uvědomme si, že obě tyto věty jsou speciální verzí Eulerovy věty pro grupu invertibilních prvků v $\mathbb{Z}_n$. Grupu invertibilních prvků v monoidu $(\mathbb{Z}_n, \cdot)$ značíme $\mathbb{Z}_n^*$ a invertibilní jsou právě prvky nesoudělné s n:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n; a \text{ je nesoudělné s } n\}$$

Počet prvků této grupy $|\mathbb{Z}_n^*| = \varphi(n)$, kde φ je Eulerova funkce:

$$\varphi : \mathbb{N} \to \mathbb{N} : \varphi(n) = \text{ počet čísel mezi 0 až (n-1) nesoudělných s n}$$

Pro výpočet Eulerovy funkce platí následující vzorce, na základě kterých umíme spočítat $\varphi(n)$, kdykoli známe prvočíselný rozklad čísla n.

- $\varphi(p) = p - 1$ pro p prvočíslo
- $\varphi(p^k) = p^k - p^{k-1}$ pro p prvočíslo a k přirozené číslo
- $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$ pro n, m navzájem nesoudělná přirozená čísla

Například $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8, \}$, $|\mathbb{Z}_9^*| = \varphi(9) = 6$, všechny prvky $a \in \mathbb{Z}_9$ splňují $a^6 = 1$ v $\mathbb{Z}_9$. Ovšem číslo 6 není vždy ten nejmenší exponent, na který je třeba umocnit, aby vyšlo 1, třeba $8^2 = 1$ a $4^3 = 1$ v $\mathbb{Z}_9$. Tento fakt vede k následující definici.

6.13 Definice Nechť $(G, \circ)$ je konečná grupa s neutrálním prvkem 1, $a \in G$. Nejmenší přirozené číslo $r > 0$ takové, že $a^r = \underbrace{a \circ a \circ \ldots \circ a}_{r\text{-krát}} = 1$ se nazývá *řád prvku* a v grupě G. Značíme $\mathrm{r}(a) = r$.

Takové $r > 0$, že $a^r = 1$, v grupě G určitě existuje. V konečné grupě se musí výsledky mocnin opakovat, $a^k = a^l$ pro nějaké $k < l$. Vynásobíme-li rovnost inverzním prvkem k prvku a^k, který v grupě musí existovat, dostaneme $1 = a^{l-k}$. Definice pojmu řád prvku a je smysluplná.

6.14 Tvrzení *Nechť $(G, \circ, 1)$ je konečná grupa, $a \in G$. Je-li $\mathrm{r}(a) = r$, pak množina $P = \{a, a^2, a^3, \ldots, a^r = 1\}$ tvoří r-prvkovou podgrupu grupy G, tzv. cyklickou podgrupu generovanou prvkem a, značíme ji $P = \langle a \rangle$.*

6.15 Věta (Lagrangeova) *Počet prvků libovolné podgrupy P (v grupě G) je dělitelem počtu prvků grupy G.*

6.16 Důsledek *Řád prvku a v grupě G je dělitelem počtu prvků grupy G.*

6.17 Definice Grupa $(G, \circ, 1)$ o n prvcích se nazývá *cyklická grupa*, pokud $G = \langle a \rangle = \{a, a^2, a^3, \ldots, a^n = 1\}$. Prvek a je tzv. *generátor* grupy G.

6.18 Tvrzení *Prvek a je generátor grupy $(G, \circ, 1)$ o n prvcích právě, když $\mathrm{r}(a) = n$. To nastane právě, když je splněna kterákoliv z následujících podmínek:*

- *$a^r \neq 1$ pro každé $r < n$, kde $r \mid n$*
- *$a^r \neq 1$ pro každé $r = \frac{n}{p}$, kde p je prvočíslo a $p \mid n$*

6.19 Příklad Chceme najít generátor grupy $\mathbb{Z}_{19}^*$, která má $\varphi(19) = 18$ prvků. Možné řády jsou dělitelé čísla $18 = 2 \cdot 3^2$, přičemž maximální dělitelé jsou 6 a 9. Zkusíme $a = 2$ a spočteme $2^6 = 7 \neq 1$ a $2^9 = -1 \neq 1$. Prvek 2 tedy je generátor a grupa $\mathbb{Z}_{19}^*$ je cyklická.

6.20 Tvrzení *Nechť $(G, \circ, 1)$ je konečná grupa, $a \in G$. Pak $a^k = 1$ v grupě G právě, když $r(a) \mid k$.*

6.21 Tvrzení *Nechť $r(a) = r$ v grupě G, pak $r(a^k) = \frac{r}{\gcd(k,r)}$ v grupě G.*
Speciálně, pokud $r(a) = ks$, pak $r(a^k) = s$.

6.22 Nechť $G = \langle a \rangle$ je cyklická grupa o n prvcích. Nechť $r \mid n$, tehdy a jen tehdy platí:

1. V grupě G lze nalézt prvek řádu r, například prvek $b = a^k$, kde $n = kr$.
2. Prvků řádu r je v grupě G celkem $\varphi(r)$ a jsou tvaru b^j pro všechna j nesoudělná s r, $0 \leq j < r$.

3. Rovnice $x^r = 1$ má v grupě G právě r řešení - jsou to všechny prvky z podgrupy $\langle b\rangle$ generované prvkem řádu r. (Tyto prvky jsou tvaru b^i, $0 \le i < r$, tudíž řeší danou rovnici: $(b^i)^r = (b^r)^i = 1^i = 1$, a fakt, že v cyklické grupě žádná další řešení nejsou, plyne z následujícího bodu.)
4. V grupě G je právě jedna podgrupa o r prvcích a to podgrupa $P_r = \langle b\rangle$, kde $b = a^k$ pro $k = \frac{n}{r}$.

Pro obecné r (tedy i když $r \nmid n$ platí:

1. Rovnice $x^r = 1$ má právě $d = \gcd(r, n)$ řešení v grupě G (a to všechny prvky z podgrupy P_d, aneb rovnice se redukuje na $x^d = 1$).

A teď už zpět ke konečným tělesům:

6.23 Věta *Nechť $(T, +, \cdot, 0, 1)$ je konečné těleso o n prvcích. Grupa invertibilních prvků v tělese, tedy grupa $(T^* = T - \{0\}, \cdot)$, je vždy cyklická.*

Důkaz První část důkazu se opírá o vlastnosti řádů prvků. Řád prvku je dělitelem počtu prvků grupy, tedy $r(a) \,|\, (n-1)$. Chceme najít prvek, jehož řád je $n-1$. Označíme jako m největší řád prvků v grupě T^*. Dokážeme, že pak řád libovolného prvku v T^* dělí toto m (což dá trochu práce - musíme dokázat, že existuje-li v grupě prvek řádu r a prvek řádu s, pak v ní existuje i prvek řádu $\mathrm{lcm}(r, s)$). Tudíž každý prvek v T^* splňuje $a^m = 1$ a je kořenem polynomu $x^m - 1$. Druhá část důkazu se opírá o fakt, že v tělese může mít polynom nejvýše tolik kořenů, kolik je jeho stupeň. Odtud $m = n-1$ a každý prvek, který má tento řád m, je generátorem grupy T^*. ☒

6.24 Definice Nechť $(T, +, \cdot, 0, 1)$ je konečné těleso, jakýkoliv generátor grupy $(T^* = T - \{0\}, \cdot)$ se nazývá *primitivní prvek* tělesa T.

6.25 Tvrzení *Nechť T je konečné těleso o n prvcích. Polynom $x^r - 1$ má v tělese T celkem r různých kořenů právě, když $r \,|\, (n-1)$.*

Důkaz Grupa $(T^*, \cdot)$ je cyklická grupa o $(n-1)$ prvcích. V ní existuje prvek β řádu r právě, když $r \,|\, (n-1)$. Tento prvek je kořen polynomu $x^r - 1$, neboť splňuje $\beta^r = 1$. Podgrupa generovaná prvkem β má r prvků tvaru β^i, $1 \le i \le r$, a každý z nich je kořenem polynomu $x^r - 1$, neboť $(\beta^i)^r = (\beta^r)^i = 1^i = 1$. Více kořenů polynom stupně r mít v tělese nemůže. (Aneb kořeny polynomu $x^r - 1$ jsou právě všechna řešení rovnice $x^r = 1$ v cyklické grupě T^*.) Pokud $r \nmid (n-1)$, pak má rovnice $x^r = 1$ v cyklické grupě pouze $\gcd(r, n-1) < r$ řešení, tedy polynomu $x^r - 1$ má méně než r kořenů. ☒

6.26 Věta Fermatova: *Nechť T je konečné těleso o n prvcích. Pak každý prvek tělesa je kořenem polynomu $x^n - x$, tj. pro každý $a \in T$ platí $a^n = a$.*

Důkaz Každý nenulový prvek tělesa T je kořenem polynomu $x^{n-1} - 1$, neboť je tvaru α^i pro primitivní prvek α tělesa T ($r(\alpha) = n-1$) - viz předchozí tvrzení. Tudíž každý (i nulový) prvek je kořenem polynomu $x^n - x$. ☒

6.27 Důsledek *Nechť T je konečné těleso charakteristiky p (aneb rozšíření tělesa $\mathbb{Z}_p$), a prvek $a \in T$. Pak vztah $a^p = a$ platí v tělese T právě, když $a \in \mathbb{Z}_p$.*

Důkaz Prvky $a \in \mathbb{Z}_p$ tento vztah splňují dle Fermatovy věty, tvoří tedy celkem p kořenů polynomu $x^p - x$. A více kořenů tento polynom stupně p v tělese T mít nemůže. ☒

6.28 Příklad Těleso $GF(8)$ sestrojené jako $T = \mathbb{Z}_2[x]/q(x)$, kde $q(x) = x^3 + x + 1$ je ireducibilní nad $\mathbb{Z}_2$, je těleso $T = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$.
$|T^*| = 7$, možné řády prvků $r \,|\, 7$, tedy kromě $a = 1$ (který má řád r(1) = 1) je každý nenulový prvek primitivním prvkem tělesa T. Použijeme prvek α a napíšeme každý nenulový prvek v T jako mocninu prvku α.

$$\alpha^1 = \alpha,\ \alpha^2 = \alpha^2,\ \alpha^3 = \alpha + 1,\ \alpha^4 = \alpha^2 + \alpha,\ \alpha^5 = \alpha^2 + \alpha + 1,\ \alpha^6 = \alpha^2 + 1,\ \alpha^7 = 1.$$

Tuto tabulku můžeme použít pro násobení v tělese T. Např.

$$(\alpha^2 + 1) \cdot (\alpha^2 + \alpha) = \alpha^6 \cdot \alpha^4 = \alpha^{10} = \alpha^7 \cdot \alpha^3 = 1 \cdot \alpha^3 = \alpha + 1$$

6.29 Třetí pohled na násobení v konečném tělese T o n prvcích: Nalezneme primitivní prvek β tělesa T a vytvoříme tabulku délky $(n-1)$, v níž je každý nenulový prvek napsán jako mocnina primitivního prvku β. Pak můžeme prvky násobit jako mocniny $\beta^k \cdot \beta^l = \beta^{k+l}$, přičemž v exponentu počítáme modulo $\mathrm{r}(\beta) = n-1$.

6.30 Příklad Těleso $GF(9)$ sestrojené jako $T = \mathbb{Z}_3[x]/q(x)$, kde $q(x) = x^2+1$ je ireducibilní nad $\mathbb{Z}_3$, je těleso komplexních čísel nad $\mathbb{Z}_3$, $T = \{a\,i + b,\ a, b \in \mathbb{Z}_3,\ i^2 = -1\}$.
$|T^*| = 8$, možné řády prvků $r \mid 8$. Přitom $i^4 = 1$, tedy $\mathrm{r}(i) = 4$, ale $(i+1)^4 \neq 1$, tedy $\mathrm{r}(i+1) = 8$ a $(i+1)$ je primitivním prvkem tělesa T.
Polynom $x^4 - 1$ má v tělese T všechny čtyři kořeny a jsou to prvky ± 1 a $\pm i$ tedy prvky podgrupy $\langle i \rangle$.

6.31 Poznámka Vždy lze setrojit těleso $GF(p^k)$ tak, aby kořen ireducibilního polynomu byl zároveň primitivním prvkem v tomto tělese. Aneb pro konstrukci tělesa $T = \mathbb{Z}_p[x]/q(x)$, lze zvolit ireducibilní polynom $q(x)$ stupně k tak, aby - napíšeme-li prvky tělesa T jako polynomy v proměnné z a počítáme dle pravidla $q(z) = 0$ - prvek z byl primitivním prvkem tělesa T.

6.32 Příklad Těleso $GF(9)$ sestrojené jako $T = \mathbb{Z}_3[x]/q(x)$, kde $q(x) = x^2 + x + 2$ je ireducibilní nad $\mathbb{Z}_3$, aneb těleso $T = \{a\,z + b,\ a, b \in \mathbb{Z}_3,\ z^2 = 2z + 1\}$.
$z^4 = (2z+1)^2 = z^2 + z + 1 = 2 \neq 1$, tedy $\mathrm{r}(z) = 8$ a z je primitivním prvkem tělesa T.

7 Polynomy nad $\mathbb{Z}_p$ a jejich kořeny v tělese T charakteristiky p

Těleso T charakteristiky p lze považovat za rozšíření tělesa $\mathbb{Z}_p$, tj. $\mathbb{Z}_p \subset T$. Pak každý polynom nad $\mathbb{Z}_p$ lze přirozeně považovat za polynom nad T a lze hledat jeho kořeny v tělese T. V předchozí kapitole jsme se dozvěděli, že každý prvek tělesa je kořenem polynomu $x^n - x$, kde $n = |T|$ (Fermatova věta), a že polynom $x^r - 1$ má v tělese r různých kořenů právě, když $r|n$, a jsou tvaru β^i, kde β je prvek řádu r. Nyní budeme zkoumat libovolné celočíselné polynomy s koeficienty v $\mathbb{Z}_p$ a jejich kořeny v tělese T.

7.1 Tvrzení *Nechť $q(x)$ je celočíselný polynom nad $\mathbb{Z}_p$ a nechť T je těleso charakteristiky p. Má-li polynom $q(x)$ kořen c v tělese T, pak má také kořen c^p v tělese T.*

Důkaz Označme $q(x) = a_n\, x^n + \ldots + a_1\, x + a_0$, kde $a_i \in \mathbb{Z}_p$. Víme, že c je kořen polynomu $q(x)$, tedy $q(c) = 0$. Potom $0 = 0^p = [q(c)]^p = a_n^p\, (c^n)^p + \ldots + a_1^p\, c^p + a_0^p$, neboť $\operatorname{char} T = p$. V důsledku Malé Fermatovy věty platí pro všechny prvky ze $\mathbb{Z}_p$, že $a_i^p = a_i$. Můžeme tedy dále upravit naši rovnost $0 = a_n\, (c^p)^n + \ldots + a_1\, c^p + a_0 = q(c^p)$ a dostáváme, že c^p je také kořen polynomu $q(x)$. ⊠

7.2 Důsledek *Nechť $q(x)$ je celočíselný polynom nad $\mathbb{Z}_p$ a nechť T je těleso charakteristiky p. Má-li polynom $q(x)$ kořen c v tělese T, pak má také kořeny $c^p, c^{(p^2)}, c^{(p^3)}, \ldots$ v tělese T.*

Tvorba kořenů se zastaví nejpozději po k krocích, kde $|T| = p^k$. Pro prvek c z tělesa T totiž platí $c^{(p^k)} = c$ podle Fermatovy věty.

7.3 Poznámka Podobnou situaci s kořeny v nadtělese známe u reálných polynomů a jejich komplexních kořenů. I zde je jistý vztah mezi kořeny, konkrétně má-li reálný polynom komplexní kořen $c = \alpha + \beta i$, pak musí mít i komplexně sdružený kořen $\bar{c} = \alpha - \beta i$.

7.4 Příklad Mějme těleso $GF(8)$ vyrobené takto: $T = \mathbb{Z}_2[x]/q(x)$, kde $q(x) = x^3 + x + 1$ je ireducibilní polynom nad $\mathbb{Z}_2$. Prvky tělesa označíme jako polynomy v proměnné α, tedy $T = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$. Polynom $q(x) = x^3 + x + 1$ je ireducibilní nad $\mathbb{Z}_2$, nemá tedy žádný kořen v tělese $\mathbb{Z}_2$.
V tělese T ale platí, že $q(\alpha) = \alpha^3 + \alpha + 1 = 0$, protože polynom $q(x)$ má nulový zbytek po dělení $q(x)$. Prvek α je tedy kořenem polynomu $q(x)$ v tělese T. Charakteristika tělesa $\operatorname{char} T = 2$, další kořeny polynomu $q(x)$ jsou α^2, $\alpha^4 = \alpha^2 + \alpha$ - můžeme to ověřit dosazením. Více kořenů není, neboť polynom stupně 3 může mít v tělese nejvýše tři kořeny - skutečně vyrábění dalších kořenů umocňováním na druhou se už zacyklí, $\alpha^8 = \alpha$, protože $|T| = 8$.

7.5 Tvrzení *Nechť $q(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$ stupně k. Pak v tělese $GF(p^k)$ tvaru $T = \mathbb{Z}_p[x]/q(x)$ má polynom $q(x)$ celkem k různých kořenů a polynom $q(x)$ se rozkládá na součin lineárních polynomů nad T.*

Důkaz $T = \{a_{k-1}\, z^{k-1} + \ldots + a_1\, z + a_0,\ a_i \in \mathbb{Z}_p, q(z) = 0\}$ Jedním kořenem polynomu $q(x)$ je prvek z a další kořeny vzniknou umocňováním na $\operatorname{char} T = p$, tedy z^p, z^{p^2}, …, $z^{p^{k-1}}$ jsou také kořeny polynomu $q(x)$. Zbývá dokázat, že jsou navzájem různé. To vyplývá z následujícího pojmu "minimální polynom". Pokud by se výroba kořenů zacyklila dříve než u $z^{(p^k)} = z$, pak by minimální polynom pro kořen z byl polynom nad $\mathbb{Z}_p$ stupně menšího než k a tento minimální polynom by dělil beze zbytku polynom $q(x)$, což by byl spor s ireducibilitou polynomu $q(x)$ nad $\mathbb{Z}_p$. ⊠

7.6 Definice Nechť T je konečné těleso charakteristiky p a prvek $c \in T$. *Minimální polynom nad $\mathbb{Z}_p$ pro prvek c* je nenulový celočíselný polynom nad $\mathbb{Z}_p$ co nejmenšího stupně, který má kořen c v tělese T. Označíme jej $m_c(x)$.

Takový polynom vždy existuje, neboť prvek $c \in T$ je dle Fermatovy věty kořenem celočíselného polynomu $x^{(p^k)} - x$, kde $p^k = |T|$. Mezi všemi nenulovými celočíselnými polynomy nad $\mathbb{Z}_p$ s kořenem $c \in T$ lze najít nějaký nejmenšího stupně. Zřejmě jeho konstantní násobek bude mít kořen c a bude téhož stupně - ukážeme, že minimální polynomy pro prvek c jsou navzájem asociované a jako $m_c(x)$ budeme značit ten, který má vedoucí koeficient roven 1 (monický minimální polynom pro prvek c).

7.7 Tvrzení *Nechť T je konečné těleso charakteristiky p a nechť c c^p, $c^{(p^2)}$, ..., $c^{(p^l)}$ jsou všechny různé prvky vzniklé umocňování prvku $c \in T$ na p-tou. Pak minimální polynom pro prvek c je polynom:*

$$m_c(x) = (x - c)(x - c^p) \cdot \ldots \cdot (x - c^{(p^l)})$$

Důkaz Každý celočíselný polynom nad $\mathbb{Z}_p$ musí mít s kořenem $c \in T$ také všechny tyto kořeny tvaru $c^{(p^i)}$. Jejich přidání je tedy nutné, dokážeme, že je i postačující. Označme a_i koeficienty výše vytvořeného polynomu $m_c(x)$. Spočítáme dvěma způsoby polynom $(m_c(x))^p$. Jelikož $\operatorname{char} T = p$, platí:

$$(m_c(x))^p = (\sum_{i=0}^{m} a_i x^i)^p = \sum_{i=0}^{m} a_i^p (x^p)^i$$

$$(m_c(x))^p = (x - c)^p (x - c^p)^p \cdot \ldots \cdot (x - c^{(p^l)})^p =$$

$$= (x^p - c^p)(x^p - c^{(p^2)}) \cdot \ldots \cdot (x^p - c^{(p^{l+1})}) = m_c(x^p) = \sum_{i=0}^{m} a_i (x^p)^i$$

Využili jsme toho, že $c^{p^{l+1}} = c$. Z rovnosti polynomů plyne, že $a_i^p = a_i$ pro všechna $0 \leq i \leq m$. To je možné jen, když všechna $a_i \in \mathbb{Z}_p$, polynom $m_c(x)$ je tedy celočíselný.

⊠

7.8 Tvrzení *Nechť $m_c(x)$ je minimální polynom nad $\mathbb{Z}_p$ pro prvek $c \in T$, $\operatorname{char} T = p$. Pak platí:*

1. *$m_c(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$*
2. *polynom $f(x)$ nad $\mathbb{Z}_p$ má kořen $c \in T$ právě, když $m_c(x) | f(x)$ nad $\mathbb{Z}_p$*

Důkaz 1) Kdyby $m_c(x) = a(x)b(x)$ byl netriviální rozklad nad $\mathbb{Z}_p$, pak by prvek c musel být kořenem polynomu $a(x)$ nebo $b(x)$ (neboť těleso nemá dělitele nuly), což by byl spor s tím, že $m_c(x)$ je celočíselný polynom nejmenšího stupně s kořenem c.
2) Celočíselný polynom $f(x)$ nad $\mathbb{Z}_p$ musí mít s kořenem $c \in T$ také všechny kořeny tvaru $c^{(p^i)}$, musí být tedy dělitelný všemi lineárními polynomy tvary $(x - c^{(p^i)})$. Proto je $f(x)$ dělitelný polynomem $m_c(x)$. ⊠

7.9 Důsledky

1. $f(x)$ je minimální polynom pro prvek c právě, když $f(x)$ je ireducibilní nad $\mathbb{Z}_p$ a $f(c) = 0$ v tělese T.
2. Monický $m_c(x)$ je určen jednoznačně.
3. $m_c(x) | (x^n - 1)$ právě, když $r(c) | n$.

Důkaz 1) $f(x)$ musí být dělitelný polynomem $m_c(x)$, ale protože $f(x)$ je ireducibilní nad $\mathbb{Z}_p$, tak $f(x) = a\, m_c(x)$ pro $a \in \mathbb{Z}_p$, tudíž $f(x)$ je také minimálním polynomem pro prvek c.
2) Minimální polynomy pro c se musí dělit navzájem (být asociované), monický je tedy jen jeden.
3) $m_c(x) | (x^n - 1)$ právě, když c je kořenem polynomu $x^n - 1$, aneb $c^n = 1$ v T. To nastane právě, když $r(c) | n$ - $r(c)$ je řád prvku c v grupě T^*. ⊠

7.10 Příklad Těleso $GF(8)$ sestrojené jako $T = \mathbb{Z}_2[x]/q(x)$, kde $q(x) = x^3 + x + 1$ je ireducibilní nad $\mathbb{Z}_2$, aneb $T = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$. Najdeme minimální polynomy pro všechny prvky.

Minimální polynom pro prvky ze $\mathbb{Z}_2$ jsou lineární: $m_0(x) = x$, $m_1(x) = x - 1$.
Minimální polynom pro kořen α je polynom $q(x) = x^3 + x + 1$, neboť $q(\alpha) = 0$ v tělese T a $q(x)$ je ireducibilní nad $\mathbb{Z}_2$. Tento polynom je také minimálním polynomem pro prvky α^2 a $\alpha^4 = \alpha^2 + \alpha$.
Najdeme minimální polynom pro kořen $\alpha + 1$ v tělese T. Další nutné kořeny jsou $(\alpha + 1)^2 = \alpha^2 + 1$, $(\alpha + 1)^4 = \alpha^2 + \alpha + 1$ a minimální polynom (pro tyto tři prvky) bude:

$$m_{\alpha+1}(x) = (x - (\alpha + 1))(x - (\alpha^2 + 1))(x - (\alpha^2 + \alpha + 1)) = x^3 + x^2 + 1$$

Můžeme to ověřit roznásobením, anebo odvodit následující úvahou: Víme, že má vyjít ireducibilní polynom stupně 3. Tyto polynomy jsou nad $\mathbb{Z}_2$ pouze dva, x^3+x+1 a x^3+x^2+1. První je roven polynomu $q(x) = m_\alpha(x)$ a nemá kořen $\alpha + 1$, takže $m_{\alpha+1}(x) = x^3 + x^2 + 1$.

Podle Fermatovy věty je každý prvek tělesa $GF(8)$ kořenem polynomu $x^8 - x$, tudíž minimální polynom každého prvku musí dělit polynom $x^8 - x$. A skutečně, rozložíme-li tento polynom na ireducibilní polynomy nad $\mathbb{Z}_2$, získáme $x^8 - x = x(x^7 - 1) = x(x - 1)(x^3 + x^2 + 1)(x^3 + x + 1)$.

Minimálních polynomů se využívá k důkazu faktu, že každé konečné komutativní těleso je Galoisovo.

7.11 Věta *Nechť T je konečné komutativní těleso charakteristiky p. Pak T je izomorfní s Galoisovým tělesem $\mathbb{Z}_p[x]/q(x)$, kde $q(x)$ je minimální polynom pro primitivní prvek tělesa T.*

Důkaz Hlavní myšlenka důkazu (detaily ponecháme čtenáři): Buď α primitivní prvek tělesa T a $m_\alpha(x)$ jeho minimální polynom, $\mathrm{st}(m_\alpha) = k$. Pak každý nenulový prvek tělesa T je tvaru $\beta = \alpha^i$. Podělíme-li se zbytkem polynom x^i polynomem $m_\alpha(x)$ v $\mathbb{Z}_p[x]$, dostaneme $x^i = q(x)m_\alpha(x) + t(x)$ a $st(t(x)) < k$. Můžeme tedy každý prvek zapsat ve tvaru polynomu v proměnné α stupně nejvýše $k - 1$, $\beta = \alpha^i = 0 + t(\alpha)$.
Přitom různé polynomy v proměnné α stupně nejvýše $k - 1$ určují různé prvky tělesa T: kdyby $t_1(\alpha) = t_2(\alpha)$, pak by $(t_1 - t_2)(\alpha) = 0$, ale α nemůže být kořenem žádného polynomu stupně menšího než k kromě nulového polynomu, tudíž $t_1(x) = t_2(x)$. Máme tedy vzájemně jednoznačné zobrazení mezi nenulovými prvky tělesa T a nenulovými polynomy nad $\mathbb{Z}_p$ stupně nejvýše $k - 1$. Prvku 0 přiřadíme nulový polynom.
Toto zobrazení je tělesovým izomorfismem mezi tělesem T a tělesem $\mathbb{Z}_p[x]/m_\alpha(x)$ - sčítání a násobení je respektováno, protože těleso T má charakteristiku p a protože je v něm $m_\alpha(\alpha) = 0$, 0 a 1 jsou respektovány zřejmě. ⊠