Konečná tělesa

4. přednáška z algebraického kódování

Obsah

Komutativní těleso

Definice

Množina se dvěma operacemi $(T, +, \cdot)$ se nazývá *komutativní těleso*, jestliže

1. $(T, +)$ je komutativní grupa (neutrální prvek značíme 0);
2. $(T - \{0\}, \cdot)$ je komutativní grupa (neutrální prvek značíme 1);
3. násobení je distributivní vůči sčítání.

V této přednášce nás budou zajímat konečná komutativní tělesa. Budeme mluvit jednoduše o konečných tělesech, protože lze dokázat, že všechna konečná tělesa jsou komutativní.

Galoisova tělesa

Připomenutí

Na minulé přednášce jsme zkonstruovali Galoisova tělesa $GF(p^k)$:

- $T = \mathbb{Z}_p[x]/q(x)$, kde $q(x)$ je ireducibilní nad $\mathbb{Z}_p$ stupně k;
- T má p^k prvků;
- T je rozšířením tělesa $\mathbb{Z}_p$.
  Pokud ztotožníme každé $a \in \mathbb{Z}_p$ se zbytkovou třídou $[a] \in T$, pak bude $(\mathbb{Z}_p, +, \cdot)$ podtěleso tělesa $(T, +, \cdot)$.

Cílem dnešní přednášky bude ukázat, že jiná konečná tělesa než Galoisova neexistují. Cestou se dozvíme mnoho důležitého o konečných tělesech.

Charakteristika tělesa

Definice

Nechť $(T, +, \cdot, 0, 1)$ je konečné těleso. Nejmenší přirozené $r > 0$ takové, že

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

se nazývá *charakteristika tělesa* T. Značíme $\mathrm{char}(T)$.

Poznámka

Charakteristika tělesa je vlastně řád prvku 1 v grupě $(T, +)$.

Příklad

- $\mathrm{char}(\mathbb{Z}_p) = p$
- $\mathrm{char}(GF(p^k)) = p$

Charakteristika tělesa

Tvrzení

Každé konečné těleso T má $\mathrm{char}(T) = p$ pro nějaké prvočíslo p.

Nechť T je konečné těleso, $\mathrm{char}(T) = p$. Nechť 1 značí neutrální prvek vůči násobení a 0 značí neutrální prvek vůči sčítání v T. Množina

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

tvoří podtěleso tělesa T (tzv. *prvotěleso* tělesa T).
Navíc těleso $(P, +, \cdot)$ je izomorfní s tělesem $(\mathbb{Z}_p, +, \cdot)$, můžeme je tedy ztotožnit a psát $\mathbb{Z}_p \subseteq T$.
Těleso T charakteristiky p lze považovat za rozšíření tělesa $\mathbb{Z}_p$.

Charakteristika tělesa

Těleso charakteristiky p jako lineární prostor nad $\mathbb{Z}_p$

Nechť T je konečné těleso, $\mathrm{char}(T) = p$, aneb $\mathbb{Z}_p \subseteq T$.
Pak T tvoří lineární prostor nad $\mathbb{Z}_p$ (násobení skaláry ze $\mathbb{Z}_p$ je realizováno jako násobení v tělese T).

Jelikož má T konečně prvků, musí mít tento lineární prostor konečnou dimenzi, $\dim T = k$. Každý vektor má jednoznačně určené souřadnice vůči pevně zvolené bázi, tudíž $T \cong \mathbb{Z}_p^k$.

Věta

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

Aneb šestiprvkové těleso neexistuje.

Charakteristika tělesa

Tvrzení

Nechť T je těleso, $\mathrm{char}(T) = p$. Pak pro každé $a, b \in T$ platí:

$$(a+b)^p = a^p + b^p$$

Důsledek

Nechť T je těleso, $\mathrm{char}(T) = p$, a nechť $m \in \mathbb{N}$.

- Pro každé $a, b, \in T$ je $(a+b)^{(p^m)} = a^{(p^m)} + b^{(p^m)}$.
- Pro všechny $a_1, \ldots, a_n \in T$ je $(a_1 + a_2 + \ldots + a_n)^{(p^m)} = a_1^{(p^m)} + a_2^{(p^m)} + \ldots + a_n^{(p^m)}$.

Charakteristika tělesa

Tvrzení

Pro polynomy nad $\mathbb{Z}_p$ platí:

- $x^p - 1 = (x-1)^p$, tedy $1 \in \mathbb{Z}_p$ je p-násobný kořen.
- $x^{(p^m)} - 1 = (x-1)^{(p^m)}$, tedy $1 \in \mathbb{Z}_p$ je p^m-násobný kořen. Obojí plyne z faktu, že $\mathrm{char}(\mathbb{Z}_p) = p$.
- $x^{p-1} - 1 = (x-1)(x-2)\dots(x-(p-1))$, tedy všechny prvky $0 \neq a \in \mathbb{Z}_p$ jsou kořenem. Toto je důsledkem Malé Fermatovy věty.

Výše uvedené polynomy se tedy v $\mathbb{Z}_p[x]$ rozkládají na kořenové činitele.

Kořeny polynomu

Věta - počet kořenů polynomu v tělese

Nechť T je těleso. Polynom $m(x) \in T[x]$ stupně $k \geq 0$ má v tělese T nejvýše k kořenů.

Poznámka

Důkaz se opírá o fakt, že těleso nemá dělitele nuly.

Polynom stupně k nad okruhem, který má dělitele nuly, může mít v tomto okruhu i více než k kořenů. Dá se pak rozložit různými způsoby na polynomy nižších stupňů.

Např. $m(x) = x^2 - 1$ má čtyři kořeny v okruhu $\mathbb{Z}_8$, a to $1, 3, 5, 7$.
V $\mathbb{Z}_8[x]$ platí $x^2 - 1 = (x-1)(x+1) = (x-3)(x+3)$.

Primitivní prvek tělesa

Věta

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

Definice

Generátor grupy $(T^*, \cdot)$ se nazývá *primitivní prvek* tělesa T.

Poznámka

Důkaz se opírá o fakt, že v tělese může mít polynom nejvýše tolik kořenů, kolik je jeho stupeň.

Grupa invertibilních prvků v okruhu cyklická být nemusí.
Např. ve čtyřprvkové grupě $\mathbb{Z}_8^*$ mají všechny prvky řád $r \leq 2$.

Primitivní prvek tělesa

Příklad

Těleso $GF(8)$ sestrojené jako $T = \mathbb{Z}_2[x]/(x^3 + x + 1)$ 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 $r \mid 7$, tedy každý nenulový prvek $a \neq 1$ je primitivním prvkem tělesa T.
Použijme jako primitivní prvek α a napišme každý nenulový prvek v T jako mocninu prvku α.

α^1	α^2	α^3	α^4	α^5	α^6	α^7
α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$	1

Tuto tabulku můžeme použít pro násobení v tělese T:

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

Primitivní prvek tělesa

Třetí pohled na násobení v konečném tělese

Nechť T je těleso o p^k prvcích s primitivním prvkem β.

Vytvoříme tabulku délky $(p^k - 1)$, v níž je každý nenulový prvek napsán jako mocnina primitivního prvku β.

Prvky násobíme jako mocniny $\beta^k \cdot \beta^l = \beta^{k+l}$, přičemž v exponentu počítáme modulo $\mathrm{r}(\beta) = p^k - 1$.

Primitivní prvek tělesa

Další příklad

Těleso $GF(9)$ sestrojené jako $T = \mathbb{Z}_3[x]/(x^2+1)$ 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 $r \,|\, 8$. Přitom $i^4 = 1$, tedy $\mathrm{r}(i) = 4$.
Ale $(i+1)^4 \neq 1$, tedy $(i+1)$ je primitivním prvkem tělesa T.

Těleso $GF(9)$ sestrojené jako $T = \mathbb{Z}_3[x]/(x^2+x+2)$ je těleso $T = \{a\,z + b,\ a, b \in \mathbb{Z}_3,\ z^2 = 2z + 1\}$.

Zde $z^4 \neq 1$, tedy z je primitivním prvkem tělesa T.

Poznámka

Vždy lze setrojit těleso $GF(p^k)$ tak, aby kořen ireducibilního polynomu byl zároveň primitivním prvkem v tomto tělese.

Kořeny polynomu $x^r - 1$ v tělese

Tvrzení

Nechť T je konečné těleso o p^k prvcích.
Polynom $x^r - 1$ má v tělese T celkem r různých kořenů (rozkládá se v $T[x]$ na kořenové činitele) právě, když $r \mid (p^k - 1)$.

Kořeny jsou tvaru β^i, kde β je prvek řádu r, $1 \leq i \leq r$.

Poznámka

Pokud $r \nmid (p^k - 1)$, pak má polynomu $x^r - 1$ v tělese T pouze $\gcd(r, p^k - 1) < r$ kořenů.

Fermatova věta

Fermatova věta

Nechť T je konečné těleso o p^k prvcích.
Každý prvek tělesa T je kořenem polynomu $x^{(p^k)} - x$, aneb pro každý $a \in T$ platí $a^{(p^k)} = a$.

Poznámka

Každý nenulový prvek tělesa T je kořenem polynomu $x^{(p^k-1)} - 1$.
Důvod: $0 \neq a = \alpha^i$, kde α je primitivní prvek, tedy $r(\alpha) = p^k - 1$.

Oba polynomy výše se v $T[x]$ rozkládají na kořenové činitele.

Důsledek

Nechť T je konečné těleso, $\mathrm{char}(T) = p$, aneb $\mathbb{Z}_p \subseteq T$.
Pak $a^p = a$ pro $a \in T$ právě, když $a \in \mathbb{Z}_p$.

Kořeny polynomů nad $\mathbb{Z}_p$ v tělese T charakteristiky p

Těleso T charakteristiky p lze považovat za rozšíření tělesa $\mathbb{Z}_p$, aneb $\mathbb{Z}_p \subseteq T$. Pak každý polynom nad $\mathbb{Z}_p$ lze považovat za polynom nad T, aneb $\mathbb{Z}_p[x] \subseteq T[x]$.

Budeme hledat kořeny polynomů s koeficienty ze $\mathbb{Z}_p$ v tělese T.

Podobnou situaci známe: komplexní kořeny reálných polynomů. Platí zde:

Má-li reálný polynom komplexní kořen $c = a + bi$, pak musí mít i komplexně sdružený kořen $\bar{c} = a - bi$.

Kořeny polynomů nad $\mathbb{Z}_p$ v tělese T charakteristiky p

Věta

Nechť $a(x)$ je polynom nad $\mathbb{Z}_p$ a nechť T je těleso, $\mathrm{char}(T) = p$. Má-li polynom $a(x)$ kořen c v tělese T, pak má také kořen c^p.

Důsledek

Nechť $a(x)$ je polynom nad $\mathbb{Z}_p$ a nechť T je těleso, $\mathrm{char}(T) = p$. Má-li polynom $a(x)$ kořen c v tělese T, pak má také kořeny $c^p, c^{(p^2)}, c^{(p^3)} \ldots$ atd.

Tvorba kořenů se zastaví nejpozději po k krocích, kde $|T| = p^k$. Podle Fermatovy věty je totiž $c^{(p^k)} = c$.

Kořeny polynomů nad $\mathbb{Z}_p$ v tělese T charakteristiky p

Příklad

Těleso $GF(8)$, $T = \mathbb{Z}_2[x]/(x^3 + x + 1)$, je těleso $T = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$.

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 platí, že $q(\alpha) = \alpha^3 + \alpha + 1 = 0$, prvek α je tedy kořenem polynomu $q(x)$ v tělese T.
Protože $\mathrm{char}(T) = 2$, další kořeny jsou α^2, $\alpha^4 = \alpha^2 + \alpha$.

Více kořenů polynom stupně 3 v tělese mít nemůže. Skutečně vyrábění kořenů se zacyklí: $\alpha^8 = \alpha$, protože $|T| = 8$.

Kořeny polynomů nad $\mathbb{Z}_p$ v tělese T charakteristiky p

Tvrzení

Nechť $q(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$ stupně k.
V tělese $T = \mathbb{Z}_p[x]/q(x)$ má polynom $q(x)$ celkem k různých kořenů. Aneb $q(x)$ se rozkládá v $T[x]$ na součin kořenových činitelů.

Zapíšeme-li prvky v tělese T jako polynomy v proměnné z, pak kořeny polynomu $q(x)$ jsou prvky $z, z^p, z^{(p^2)}, \ldots, z^{(p^{k-1})}$.

Minimální polynom

Definice

Nechť T je konečné těleso, $\mathrm{char}(T) = p$ 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 s kořenem c v tělese T.
Označíme jej $m_c(x)$.

Poznámky

- Minimální polynom pro prvek c existuje, neboť $c \in T$ je dle Fermatovy věty kořenem celočíselného polynomu $x^{(p^k)} - x$, kde $p^k = |T|$.
- Minimální polynom pro prvek c není určen jednoznačně, s každým polynomem splňují danou definici i všechny jeho nenulové konstantní násobky.

Minimální polynom

Tvrzení

Nechť T je konečné těleso, $\mathrm{char}(T) = p$, $c \in T$.
Nechť $c, c^p, c^{(p^2)}, \ldots, c^{(p^l)}$ jsou všechny různé prvky vzniklé postupným umocňování prvku c na p-tou. Pak

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

Tvrzení

- $m_c(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$
- polynom $a(x) \in \mathbb{Z}_p[x]$ má kořen $c \in T$ právě, když $m_c(x) \mid a(x)$ v $\mathbb{Z}_p[x]$

Minimální polynom

Důsledky

- Minimální polynomy pro daný $c \in T$ tvoří třídu navzájem asociovaných polynomů. Monický $m_c(x)$ je určen jednoznačně.
- $m(x)$ je minimální polynom pro prvek c právě, když $m(x)$ je ireducibilní nad $\mathbb{Z}_p$ a $m(c) = 0$ v tělese T.

Tvrzení

Nechť T je konečné těleso, $\mathrm{char}(T) = p$ a nechť $\mathrm{r}(c)$ značí řád prvku c v grupě T^*.
Pak $m_c(x) | (x^n - 1)$ v $\mathbb{Z}_p[x]$ právě, když $\mathrm{r}(c) \mid n$.

Minimální polynom

Příklad

Těleso $GF(8)$, $T = \mathbb{Z}_2[x]/(x^3 + x + 1)$, je těleso
$T = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$.

Minimální polynomy pro $c \in T$:
$m_0(x) = x$, $m_1(x) = x - 1$.

$m_\alpha(x) = q(x) = x^3 + x + 1$, neboť $q(x)$ je ireducibilní a $q(\alpha) = 0$.
$q(x)$ je též minimálním polynomem pro α^2 a pro $\alpha^4 = \alpha^2 + \alpha$.

$m_{\alpha+1}(x)$ musí mít i kořeny $(\alpha + 1)^2 = \alpha^2 + 1$,
$(\alpha + 1)^4 = \alpha^2 + \alpha + 1$. Vyjde $m_{\alpha+1}(x) = x^3 + x^2 + 1$.

Řád každého nenulového prvku $\mathrm{r}(c) \mid 7$, tudíž minimální polynom každého nenulového prvku musí dělit $x^7 - 1$.
Skutečně $x^7 - 1 = (x - 1)(x^3 + x^2 + 1)(x^3 + x + 1)$ v $\mathbb{Z}_2[x]$.

Minimální polynom

Poznámka

Předchozí příklad lze zobecnit:

Nechť $q(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$ stupně k.
Uvažujme těleso $T = \mathbb{Z}_p[x]/q(x) = \{a(z), \mathrm{st}(a(z)) < k\}$.
Polynom $q(x)$ je minimálním polynomem pro prvek $z \in T$.
Z Fermatovy věty plyne, že prvek z je také kořenem polynomu $x^{(p^k-1)} - 1$, tudíž tento polynom musí být dělitelný minimálním polynomem pro prvek z.
Každý ireducibilní polynom stupně k nad $\mathbb{Z}_p$ musí dělit polynom $x^{(p^k-1)} - 1$ nad $\mathbb{Z}_p$.

V rozkladu polynomu $x^{(p^k-1)} - 1$ na ireducibilní polynomy nad $\mathbb{Z}_p$ se nacházejí všechny monické ireducibilní polynomy stupně k nad $\mathbb{Z}_p$.

Konečná tělesa jsou Galoisova

Minimálních polynomů se využívá k důkazu faktu, že každé konečné komutativní těleso T je Galoisovo.
Už víme, že těleso T má prvočíselnou charakteristiku p a že lze chápat jako rozšíření tělesa $\mathbb{Z}_p$. Má tedy smysl mluvit o minimálních polynomech jeho prvků nad $\mathbb{Z}_p$.

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.

Konečná tělesa jsou Galoisova

Hlavní myšlenka důkazu

Buď α primitivní prvek tělesa T a $m_\alpha(x)$ jeho minimální polynom, označme $\mathrm{st}(m_\alpha) = k$.
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 v T zapsat ve tvaru polynomu $t(\alpha)$ stupně nejvýše $k-1$, neboť $\beta = \alpha^i = 0 + t(\alpha)$. (Prvku 0 přiřadíme nulový polynom.)
Získáme vzájemně jednoznačné zobrazení mezi T a $\mathbb{Z}_p[x]/m_\alpha(x)$, které je tělesovým izomorfismem.