Katedra
aplikované matematiky

KONEČNÁ TĚLESA

PAVEL JAHODA

Pavel Jahoda
Konečná tělesa

ISBN

Obsah

Kapitola 1

Tělesa

Těleso je algebraická struktura se dvěma binárními operacemi, jež mají „příjemné“ vlastnosti.

Jde o netriviální komutativní okruh, kde ke každému nenulovému prvku existuje inverze vzhledem k násobení.

Definice 1.1. (*Těleso*) Tělesem nazveme uspořádanou trojici $(T, +, \cdot)$, kde T je neprázdná množina a $+$ a $\cdot$ jsou zobrazení splňující následující požadavky

- $(T, +)$ je komutativní grupa, to jest:
  1.) $+ : T \times T \mapsto T$, (uzavřenost)
  2.) $\forall a, b, c \in T : a + (b + c) = (a + b) + c$, (asociativnost)
  3.) $\exists\, 0 \in T\, \forall a \in T : a + 0 = 0 + a = a$, (existence nulového prvku)
  4.) $\forall a \in T\, \exists\, -a \in T\, :\, a + (-a) = (-a) + a = 1$, (existence inverzních prvků vzhledem ke sčítání)
  5.) $\forall a, b \in T : a + b = b + a$, (komutativnost)
- $(T, \cdot)$ je komutativní monoid, to jest:
  1.) $\cdot : T \times T \mapsto T$, (uzavřenost)
  2.) $\forall a, b, c \in T : a \cdot (b \cdot c) = (a \cdot b) \cdot c$, (asociativnost)
  3.) $\exists\, 1 \in T\, \forall a \in T : a \cdot 1 = 1 \cdot a = a$, (existence jednotkového prvku)
  4.) $\forall a, b \in T : a \cdot b = b \cdot a$, (komutativnost)
- $\forall a \in T - \{0\}\, \exists\, a^{-1} \in A\, :\, a \cdot a^{-1} = a^{-1} \cdot a = 1$, (existence inverzních prvků vzhledem k násobení)
- $0 \neq 1$, (netriviálnost)
- Násobení je distributivní zleva i zprava, to jest:
  1.) $\forall a, b, c \in T :\, a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
  2.) $\forall a, b, c \in T :\, (b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

Mezi nejznámější příklady těles patří těleso racionálních čísel $(\mathbb{Q}, +, \cdot)$ a těleso reálných čísel $(\mathbb{R}, +, \cdot)$ (s obvyklým sčítáním a násobením racionálních, respektive reálných čísel). Celá čísla s obvyklým sčítáním a násobením celých čísel těleso netvoří – nenajdeme inverzní prvky vzhledem k násobení (kromě jedničky a mínus jedničky – ty je mají).

1.1 Konečná tělesa

Známým příkladem konečného tělesa je těleso $(\mathbb{Z}_p, +, \cdot)$, kde p je nějaké prvočíslo. Jde o těleso zbytkových tříd modulo p s obvyklým sčítáním a násobením zbytkových tříd. Jako konkrétní příklad uveďme $(\mathbb{Z}_5, +, \cdot)$. Pro jednoduchost označme prvky $\mathbb{Z}_5$ jako $0, 1, 2, 3, 4$ (místo $\overline{0}_5, \ldots, \overline{4}_5$). Sčítání a násobení je potom dáno tabulkami:

$+$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tělesa $(\mathbb{Z}_p, +, \cdot)$ jsou tělesa, která mají p prvků. Nejsou však jedinými konečnými tělesy. Dá se ukázat, že všechna konečná tělesa $(T, +, \cdot)$ splňují podmínku

$$|T| = p^n,$$

kde p je prvočíslo a $n \in \mathbb{N}$. Navíc, pro každé prvočíslo p a přirozené číslo n umíme zkonstruovat konečné těleso o p^n prvcích. Ukažme si na konkrétním příkladě.

1.2 Konstrukce tělesa $GF(3^2)$.

Vyjdeme z okruhu polynomů $(\mathbb{Z}_3[x], +, .)$. Prvky $\mathbb{Z}_3[x]$ jsou polynomy jedné neurčité nad $\mathbb{Z}_3$. Jsou to polynomy ve tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0, \text{ kde } a_i \in \mathbb{Z}_3,$$

Pro jednoduchost zápisu budeme dále místo $\overline{a} \bmod 3$ psát pouze a. Jinak řečeno, místo zbytkových tříd budeme psát jejich libovolného reprezentanta. Například, místo $\overline{1} \bmod 3$ můžeme psát jen 1, ale i -2, nebo 4 ....

Sčítání a násobení polynomů v $\mathbb{Z}_3[x]$ je definováno „přirozeným způsobem.“ Ilustrujme na příkladech:

$$(x^3 + 2x^2 - x + 2) + (2x^3 + 2x^2 - x - 1) = 3x^3 + 4x^2 - 2x + 1 = x^2 + x + 1,$$

$$(x^3 + 2) \cdot (2x^2 - x) = 2x^5 - x^4 + 4x^2 - 2x = 2x^5 + 2x^4 + x^2 + x.$$

Nyní si vybereme nějaký **ireducibilní polynom** $p(x)$ **druhého stupně** nad $\mathbb{Z}_3$ a faktorizujeme $\mathbb{Z}_3[x]$ podle množiny (ideálu) násobků tohoto polynomu - označme ji $[p(x)]$. To jest, vznikne struktura

$$\mathbb{Z}_3[x]/_{[p(x)]} = \{\mathbf{f(x)} + [\mathbf{p(x)}] \mid f(x) \in \mathbb{Z}_3[x]\},$$

kde

$$f(x) + [p(x)] = \{f(x) + k \cdot p(x) \mid k \in \mathbb{Z}_3\}.$$

Všimněme si, že

$$(f(x)+p(x))+[p(x)] = \{f(x)+p(x)+k\cdot p(x) \mid k \in \mathbb{Z}_3\} = \{f(x)+k_1\cdot p(x) \mid k_1 \in \mathbb{Z}_3\} = f(x)+[p(x)$$

Z toho je zřejmé, že $f(x) + [p(x)]$ a $g(x) + [p(x)]$ jsou tytéž prvky množiny $\mathbb{Z}_3[x]/_{[p(x)]}$ právě když se liší pouze o násobek polynomu $p(x)$ - právě když dávají stejný zbytek po dělení polynomem $p(x)$. Jinak řečeno, třídu rozkladu $f(x)+[p(x)]$ můžeme reprezentovat zbytkem z polynomu $f(x)$ po dělení polynomem $p(x)$. Množinu $\mathbb{Z}_3[x]/_{[p(x)]}$ tedy můžeme chápat jako množinu všech možných zbytků, které můžeme obdržet při dělení polynomů z $\mathbb{Z}_3[x]$ polynomem $p(x)$.

Kolik takových zbytků je? To záleží na stupni polynomu $p(x)$. Vezměme konkrétní příklad:

$$p(x) = x^2 + x + 2.$$

Jedná se o ireducibilní polynom nad $\mathbb{Z}_3$. Při dělení tímto polynomem můžeme obdržet jako zbytek libovolný polynom nad $\mathbb{Z}_3$, jehož stupeň je menší než 2. Jde o polynomy:

$$\left.\begin{array}{l} 0x+0 \\ 0x+1 \\ 0x+2 \\ 1x+0 \\ 1x+2 \\ 1x+3 \\ 2x+0 \\ 2x+1 \\ 2x+2 \end{array}\right\} \Rightarrow \text{ počet prvků } \mathbb{Z}_3[x]/_{[p(x)]} \text{ je } 3^2$$

Sčítání a násobení prvků z $\mathbb{Z}_3[x]/_{[p(x)]}$ je opět definováno „přirozeným způsobem“:

$$(f(x) + [p(x)]) + (g(x) + [p(x)]) = (f(x) + g(x)) + [p(x)] \text{ (tři druhy plusů !!! :))}$$

a

$$(f(x) + [p(x)]) \cdot (g(x) + [p(x)]) = (f(x) \cdot g(x)) + [p(x)].$$

Množina $\mathbb{Z}_3[x]/_{[p(x)]}$ s takto definovanými operacemi bude tvořit konečné těleso.

Dá se ukázat, že nezávisí na výběru reprezentantů - místo s prvky $\mathbb{Z}_3[x]/_{[p(x)]}$ (zbytkovými třídami) můžu pracovat s jejich reprezentanty - polynomy nad $\mathbb{Z}_3$ stupně menšího než tři.

Tabulky násobení a sčítání v $\mathbb{Z}_3[x]/_{[p(x)]}$ proto můžeme psát ve tvaru:

$\cdot$	**0**	**1**	**2**	**x**	**x + 1**	**x + 2**	**2x**	**2x + 1**	**2x + 2**
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	$2x+1$	1	$x+1$	$x+2$	$2x+2$	2
x + 1	0	$x+1$	$2x+2$	1	$x+2$	$2x$	2	x	$2x+1$
x + 2	0	$x+2$	$2x+1$	$x+1$	$2x$	2	$2x+2$	1	x
2x	0	$2x$	x	$x+2$	2	$2x+2$	$2x+1$	$x+1$	1
2x + 1	0	$2x+1$	$x+2$	$2x+2$	x	1	$x+1$	2	$2x$
2x + 2	0	$2x+2$	$x+1$	2	$2x+1$	x	1	$2x$	$x+2$

$+$	**0**	**1**	**2**	**x**	**x + 1**	**x + 2**	**2x**	**2x + 1**	**2x + 2**
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
x + 1	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
x + 2	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
2x	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
2x + 1	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
2x + 2	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

Jak bylo řečeno, množinu $\mathbb{Z}_3[x]/_{[p(x)]}$ můžeme chápat jako množinu všech možných zbytků, které můžeme obdržet při dělení polynomů z $\mathbb{Z}_3[x]$ polynomem $p(x)$. Zvolili jsme $p(x) = x^2 + x + 2$. Není to však jediný ireducibilní polynom stupně 2 nad $\mathbb{Z}_3$! Co když zvolíme jiný, například:

$$x^2 + 1 \ ?!$$

Obdržíme jinou strukturu? Zkusme.

Množina zbytků bude jistě stejná - půjde o všechny možné polynomy stupně menšího než dva nad $\mathbb{Z}_3$. Jak bude vypadat jejich tabulka sčítání? Ta se proti

předchozímu případu také nebude lišit – sčítání bude fungovat stejně – nezávisí na volbě polynomu. Tabulky násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$ a $\mathbb{Z}_3[x]/_{[x^2+1]}$ se však lišit budou. Napišme si je pod sebe:

Tabulka násobení v$\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{x}$	$\mathbf{x+1}$	$\mathbf{x+2}$	$\mathbf{2x}$	$\mathbf{2x+1}$	$\mathbf{2x+2}$
$\mathbf{0}$	0	0	0	0	0	0	0	0	0
$\mathbf{1}$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$\mathbf{2}$	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
$\mathbf{x}$	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$\mathbf{x+1}$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$\mathbf{x+2}$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$\mathbf{2x}$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$\mathbf{2x+1}$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$\mathbf{2x+2}$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v$\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{x}$	$\mathbf{x+1}$	$\mathbf{x+2}$	$\mathbf{2x}$	$\mathbf{2x+1}$	$\mathbf{2x+2}$
$\mathbf{0}$	0	0	0	0	0	0	0	0	0
$\mathbf{1}$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$\mathbf{2}$	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
$\mathbf{x}$	0	x	$2x$	$2x+1$	1	$x+1$	$x+2$	$2x+2$	2
$\mathbf{x+1}$	0	$x+1$	$2x+2$	1	$x+2$	$2x$	2	x	$2x+1$
$\mathbf{x+2}$	0	$x+2$	$2x+1$	$x+1$	$2x$	2	$2x+2$	1	x
$\mathbf{2x}$	0	$2x$	x	$x+2$	2	$2x+2$	$2x+1$	$x+1$	1
$\mathbf{2x+1}$	0	$2x+1$	$x+2$	$2x+2$	x	1	$x+1$	2	$2x$
$\mathbf{2x+2}$	0	$2x+2$	$x+1$	2	$2x+1$	x	1	$2x$	$x+2$

Všimněme si, že první tři řádky a také první tři sloupce jsou stejné, jinde se tabulky liší. Ukážeme, že i přesto jde kvalitativně o tytéž struktury.

Přeuspořádejme prvky v tabulce násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$:

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	**0**	**1**	**2**	**x**	**x + 1**	**x + 2**	**2x**	**2x + 1**	**2x + 2**
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	**0**	**1**	**2**	**x + 2**	**x**	**x + 1**	**2x + 1**	**2x + 2**	**2x**
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

1.3 Základní otázky a odpovědi

- **Existují konečná tělesa?**

  Ano, například $(\mathbb{Z}_p, +\cdot)$.

- **Kolik prvků mohou mít konečná tělesa?**

  Každé konečné těleso má p^n prvků, kde p je prvočíslo a n je přirozené číslo.

- **Existuje konečné těleso o p^n prvcích pro každé prvočíslo p a přirozené číslo n?**

Ano. Pro každé $n \in \mathbb{N}$ a pro každé prvočíslo p existuje ireducibilní polynom $p(x) \in \mathbb{Z}_p[x]$, který je stupně n. Jsme tedy schopni zkonstruovat těleso $GF(p^n) = \mathbb{Z}_p[x]/p(x)$. Jde o těleso zbytků po dělení polynomem $p(x)$.

- **Proč by měl být polynom $p(x)$ použitý při konstrukci konečného tělesa ireducibilní?**

  V opačném případě by vzniklá struktura nebyla tělesem. Jednoduchý pčíklad. Pokud bychom se snažili sestrojit $GF(2^2)$ pomocí polynomu

  $$p(x) = x^2 - 1 = (x-1)(x+1) \in \mathbb{Z}_2,$$

  Došlo by k tomu, že

  $$\underbrace{((x-1)+[p(x)])}_{\neq \mathbf{0} = 0+[p]\in\mathbb{Z}_2[x]/_{[p(x)]}} \cdot \underbrace{((x+1)+[p(x)])}_{\neq \mathbf{0} = 0+[p]\in\mathbb{Z}_2[x]/_{[p(x)]}} = \underbrace{((x-1)(x+1)+[p(x)])}_{= \mathbf{0} = 0+[p]\in\mathbb{Z}_2[x]/_{[p(x)]}}.$$

  A k tomu v tělese nesmí dojít! V tělese neexistují netriviální dělitelé nuly!

- **Ireducibilních polynomů stupně n nad $\mathbb{Z}_p[x]$ může být více. Dostanu pro různé ireducibilní polynomy při konstrukci konečného tělesa různá konečná tělesa?**

  Ano, i ne. Prvky těchto těles jsou stejné, tabulky sčítání také, tabulky násobení se však liší. Nicméně tato tělesa jsou izomorfní. To znamená, že při vhodném „přejmenování - označení“ prvků těles bychom obdrželi stejné tabulky násobení.