

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 $\bar{0}_5, \dots, \bar{4}_5$). 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

·	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.

Pr. 2konstruuujeme těleso s 2^2 prvky

(intuitivní představa: číselný rámek, na dvou pozicích máme dvě možnosti: 0 a 1)

$$\begin{bmatrix} 0 & 0 \end{bmatrix}; \begin{bmatrix} 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \end{bmatrix} \Rightarrow 4 \text{ možnosti} \Rightarrow 4 \text{ prvky}$$

zvolíme: $T = \{ \underset{0}{0x+0}; \underset{1}{0x+1}; \underset{x}{1x+0}; \underset{x+1}{1x+1} \}$

Sčítání musí být uzavřené: $(1x+1) + 1x \stackrel{?!}{=} 2x+1 \notin T$?!

Tak co když bychom sčítali koeficienty modulo 2 ?? :

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

- $\Rightarrow$
- 1.) uzavřenost + $\checkmark$
 - 2.) komutativnost + $\checkmark$
 - 3.) asociativita +
plyne a asociativita sčítání na $(\mathbb{Z}_2, +)$
 - 4.) $0 = 0$
 - 5.) $-0 = 0, -1 = 1, -x = x, -(x+1) = x+1$

$\Rightarrow \underline{\underline{(T, +) \text{ je komutativní grupa}}}$

ale jak definovat násobení ?!

Násobení musí být uzavřené $x \cdot (x+1) \stackrel{?!}{=} x^2 + x \notin T$?!

∇ Tj. sou jen polynomy stupně maximálně 1! Co když bychom postupovali analogicky jako u +? Tam jsme odečítali násobky 2 když byl součet větší než 1. Co když bychom když odečítali násobky x^2 ($0 \cdot x^2$, když tam x^2 není a $1 \cdot x^2$, když se ve výsledku x^2 objeví) ?! Zkusme:

Násobíme „modulo x^2 “

•	0	1	X	X+1
0	0	0	0	0
1	0	1	X	X+1
X	0	X	0	X
X+1	0	X+1	X	1

$$\Rightarrow X \cdot X = X^2 = X^2 - X^2 = 0$$

$$X \cdot (X+1) = X^2 + X = X^2 + X - X^2 = X$$

$$(X+1)(X+1) = X^2 + 2X + 1 = X^2 + 1 = 1$$

Problém! Toto by jistě nebylo těleso!

$$\underset{0}{\overset{\neq}{X}} \cdot \underset{0}{\overset{\neq}{X}} = 0 \quad \left(\begin{array}{l} \text{v tělese nesmí být} \\ \text{dělitelé nuly!} \end{array} \right)$$

Příčina: X^2 lze rozložit na součin prvků z T

Násobíme „modulo x^2+1 “

$$\Rightarrow X \cdot X = X^2 = X^2 - (X^2+1) = -1 = 1$$

$$(X+1)(X+1) = X^2 + 2X + 1 = X^2 + 1 = X^2 + 1 - (X^2+1) = 0$$

$\Rightarrow$ Stejný problém, stejná příčina: X^2+1 lze rozložit na součin prvků z T : $X^2+1 = (X+1)(X+1)$

$\Rightarrow$ Potřebujeme násobit „modulo ireducibilní polynom“ stupně 2 (s koeficienty ze $\mathbb{Z}_2$). Zbývá poslední možnost:

Násobíme „modulo $x^2 + x + 1$ “

	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

$$x \cdot x = x^2 = x^2 - (x^2 + x + 1) = -x - 1 = x + 1$$

$$x \cdot (x+1) = x^2 + x - (x^2 + x + 1) = -1 = 1$$

$$(x+1)(x+1) = x^2 + 2x + 1 - (x^2 + x + 1) = x$$

6.) uzavřenost. $\checkmark$

7.) komutativnost. $\checkmark$

8.) asociativnost. ?! dá se dokázat (DÚ)

9.) $e = 1$

$$10.) \bar{1}^1 = 1, \quad \bar{x}^1 = x+1, \quad (x+1)^1 = x$$

12.+13.) distributivita ?! dá se dokázat (DÚ)

$\Rightarrow$ T takto definovaným sčítáním a násobením tvoří těleso o 2^2 prvcích

Obecně: mmmm Takto můžeme vždy rekonstruovat těleso o p^n prvcích, kde p je prvočíslo.

$$T = \{ a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0 \mid a_{n-1}, \dots, a_0 \in \mathbb{Z}_p \}$$

Sčítáme „koeficienty modulo p .“

Násobíme polynomy „modulo nějaký ireducibilní polynom“ stupně n (dá se dokázat, že takový vždy existuje).

Př: Proveďte operace s polynomy ze $\mathbb{Z}_3[x]$.

$$1.) (x^3 - 2x^2 + 6x + 3) + (5x^2 - 2x + 1) = x^3 + \underset{0}{3}x^2 + \underset{1}{4}x + \underset{1}{4} = \underline{\underline{x^3 + x + 1}}$$

$$2.) (x^2 + 2x - 1)(x + 2) = x^3 + 2x^2 + 2x^2 + 4x - x - 2 = \underline{\underline{x^3 + x^2 + 1}}$$

3.) Určete zbytek po dělení:

$$\begin{aligned} (x^4 - 2x^3 - x^2 + 2x - 1) : (x^2 + x + 2) &= x^2 \\ - (x^4 + x^3 + 2x^2) & \\ 0x^4 - \underset{-0x^3}{3x^3} + \underset{0x^2}{3x^2} + 2x - 1 &= (2x - 1) \end{aligned}$$

$$\Rightarrow \underline{\underline{x^4 - 2x^3 - x^2 + 2x - 1 = x^2(x^2 + x + 2) + (2x - 1)}}$$

4.) Určete zbytek po dělení:

$$\begin{aligned} (x^5 + 2x^4 - x^2 + x + 2) : (x^2 + x + 2) &= x^3 + x^2 \\ - (x^5 + x^4 + 2x^3) & \\ x^4 - 2x^3 - x^2 + x + 2 & \\ - (x^4 + x^3 + 2x^2) & \\ \quad \quad \quad (x + 2) & \end{aligned}$$

$$\Rightarrow \underline{\underline{(x^5 + 2x^4 - x^2 + x + 2) = (x^3 + x^2)(x^2 + x + 2) + (x + 2)}}$$

Př: Určete množinu všech polynomů ze $\mathbb{Z}_3[x]$, které při dělení polynome $x^2 + x + 2$ dávají zbytek $x + 2$.

$$= \{ f(x) \in \mathbb{Z}_3[x] \mid f(x) = g(x)(x^2 + x + 2) + (x + 2), \text{ kde } g(x) \in \mathbb{Z}_3[x] \} =$$

$$= \{ (x + 2) + g(x)(x^2 + x + 2) \mid g(x) \in \mathbb{Z}_3[x] \} = \quad / \text{ označme } [x^2 + x + 2] = \underbrace{\{ g(x)(x^2 + x + 2) \mid g(x) \in \mathbb{Z}_3[x] \}}_{\text{množina všech násobků polynomu } g(x)}$$

$$= \underline{\underline{(x + 2) + [x^2 + x + 2]}}$$

↑
sčítání komplexů

Obdobně můžeme polynomy ze $\mathbb{Z}[x]$, které po dělení polynome $x^2 + x + 2$ dávají zb. $2x - 1$: $\underline{\underline{(2x - 1) + [x^2 + x + 2]}}$

Př. Nalezněte všechny možné zbytky po dělení polynomu ze $\mathbb{Z}_3[x]$ polynomem x^2+x+2 . Kolik jich je?

Jsou to všechny polynomy ze $\mathbb{Z}[x]$, jejichž stupeň je menší, než 2:

$$\underline{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2.}$$

Tj. jsou to polynomy $ax+b$, kde $a \in \{0,1,2\}, b \in \{0,1,2\} \Rightarrow$ je jich 3^2 .

Př. Dokažte, že $([x^2+x+2], +, \cdot)$ je ideál v okruhu $(\mathbb{Z}_3[x], +, \cdot)$.

Důkaz: $[x^2+x+2] = \{g(x)(x^2+x+2) \mid g(x) \in \mathbb{Z}_3[x]\} \subseteq \mathbb{Z}_3[x]$

1.) $([x^2+x+2], +, \cdot)$ je okruh:

I.) $([x^2+x+2], +)$ je komutativní grupa: (sčítání je komutativní, neboť je komutativní na $\mathbb{Z}_3[x]$)

$$\alpha) \forall g_1(x)(x^2+x+2), g_2(x)(x^2+x+2) \in [x^2+x+2] : g_1(x)(x^2+x+2) + g_2(x)(x^2+x+2) = \\ = (g_1(x) + g_2(x))(x^2+x+2) \in [x^2+x+2]$$

$\beta)$ sčítání polynomů z $[x^2+x+2]$ je asociativní, neboť sčítání polynomů ze $\mathbb{Z}_3[x]$ je asociativní (je to okruh).

$\gamma)$ nulový prvek = polynom $0x+0$

$$\delta) -(ax+b) = (-a)x + (-b) \quad (a, b \in \mathbb{Z}_3 = \text{grupa} \Rightarrow \exists -a, -b)$$

II.) násobení polynomů ze $[x^2+x+2]$ je asociativní, neboť nás. polynomů ze $\mathbb{Z}_3[x]$ je asociativní (je to okruh).

III.) Platí distributivní zákon zleva i zprava (v $[x^2+x+2]$), neboť platí v $\mathbb{Z}_3[x]$ (je to okruh)

$$2.) \forall r(x) \in \mathbb{Z}_3[x] \quad \forall i(x) \in [x^2+x+2] : r(x) \cdot i(x) = r(x) \cdot g(x)(x^2+x+2) = \underbrace{r(x) \cdot g(x)}_{\in \mathbb{Z}_3[x]}(x^2+x+2) \in [x^2+x+2]$$

□

Pr. 11: Určete faktorový okruh $\mathbb{Z}_3[x]/[x^2+x+2]$ a tabulky operací na tomto okruhu.

$$\mathbb{Z}_3[x]/[x^2+x+2] = \{f(x) + [x^2+x+2] \mid f(x) \in \mathbb{Z}_3[x]\}$$

polynom $f(x)$ lze podělit polynomem x^2+x+2 se zbytkem :

$$f(x) = q(x)(x^2+x+2) + (ax+b) \quad (q(x) \in \mathbb{Z}_3[x])$$

$$\begin{aligned} \Rightarrow f(x) + [x^2+x+2] &= \{ \underbrace{q(x)(x^2+x+2)}_{f(x)} + (ax+b) + q(x)(x^2+x+2) \mid q(x) \in \mathbb{Z}_3[x] \} = \\ &= \{ (ax+b) + \underbrace{(q(x)+q(x))}_{g^*(x)}(x^2+x+2) \mid g^*(x) \in \mathbb{Z}_3[x] \} = \\ &= (ax+b) + [x^2+x+1] \end{aligned}$$

$$\Rightarrow \mathbb{Z}_3[x]/[x^2+x+2] = \{ (ax+b) + [x^2+x+1] \mid a, b \in \mathbb{Z}_3 \}$$

$\Rightarrow$ Prvky $\mathbb{Z}_3[x]/[x^2+x+2]$ jsou zbytkové třídy modulo x^2+x+2 .

Povšimněte si označení $(ax+b) + [x^2+x+1] = \overline{ax+b}$, takže

$$\underline{\underline{\mathbb{Z}_3[x]/[x^2+x+2] = \{ \overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2} \}}}$$

Tabulky sčítání a násobení v $\mathbb{Z}_3[x]/[x^2+x+2]$:

+	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	$x + 1$

·	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	$2x$	$x + 2$

Př: Je $\mathbb{Z}_3[x]/[x^2+x+2]$ těleso?

je to jistě okruh. Navíc $\forall f(x) \in \mathbb{Z}_3[x]$:

$$\begin{aligned} 1.) \quad & (f(x) + [x^2+x+2]) \cdot (1 + [x^2+x+2]) = f(x) + [x^2+x+2] \\ & (1 + [x^2+x+2]) \cdot (f(x) + [x^2+x+2]) = f(x) + [x^2+x+2] \end{aligned}$$

$1 + [x^2+x+2]$ je jednotkový prvek v okruhu.

2.) Násobení v $\mathbb{Z}_3[x]/[x^2+x+2]$ je komutativní, neboť násobení v $\mathbb{Z}_3[x]$ je komutativní.

3.) Každý prvek ze $\mathbb{Z}_3[x]/[x^2+x+2]$ má prvek inverzní vzhledem k násobení (viz. tabulka násobení).

4.) nulový prvek = $(0x+0) + [x^2+x+2] \neq (0x+1) + [x^2+x+2] = \text{jednotkový prvek}$

- 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 příklad. Pokud bychom se snažili sestavit $GF(2^2)$ 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.