Těleso

Definice: *Těleso* je množina T spolu se dvěma *komutativními* binárními operacemi $+$ a $\cdot$, kde $(T, +)$ a $(T \setminus 0, \cdot)$ jsou (Abelovské) grupy a navíc $\forall a, b, c \in T : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Jinými slovy, musejí být splněny následující axiomy:

- $\forall a, b \in T : a + b = b + a$
- $\forall a, b, c \in T : (a + b) + c = a + (b + c)$
- $\exists 0 \in T\ \forall a \in T : a + 0 = a$
- $\forall a \in T\ \exists -a \in T : a + (-a) = 0$
- $\forall a, b \in T : a \cdot b = b \cdot a$ . . . včetně 0 !
- $\forall a, b, c \in T \setminus 0 : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\exists 1 \in T \setminus 0\ \forall a \in T \setminus 0 : a \cdot 1 = a$ . . . znamená $1 \neq 0$
- $\forall a \in T \setminus 0\ \exists a^{-1} \in T \setminus 0 : a \cdot a^{-1} = 1$
- $\forall a, b, c \in T : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Symbol součinu $\cdot$ se často vynechává a má přednost před $+$.

Ukázky

$(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$, stručně $\mathbb{Q},\mathbb{R},\mathbb{C}$, jsou tělesa.

$\mathbb{Z}_p$ zbytkové třídy modulo *prvočíslo* p jsou tělesa ($\mathbb{Z}_4$ a $\mathbb{Z}_6$ nejsou!)

$\mathbb{Z}_7$:

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tyto binární operace $+$ a $\cdot$ splňují všechny axiomy.
Jmenovitě opačné a inverzní prvky jsou:

a	0	1	2	3	4	5	6
$-a$	0	6	5	4	3	2	1

a	0	1	2	3	4	5	6
a^{-1}		1	4	5	2	3	6

Množina $\left\{\frac{p(x)}{q(x)}\right\}$ s polynomy p,q s reálnými koeficienty tvoří těleso $\mathbb{R}(x)$ *reálných racionálních funkcí*.

Metavěta

Metavěta: Všechna doposud uvedená tvrzení o soustavách rovnic, maticích a výpočtech nad $\mathbb{R}$ jsou platná i v libovolném tělese T.

Metadůkaz: Předvedené důkazy využívaly z $\mathbb{R}$ jen axiomy tělesa.

Ukázka: Řešení soustavy $\boldsymbol{Ax} = \boldsymbol{b}$ nad $\mathbb{Z}_7$:
Převedeme matici soustavy $(\boldsymbol{A}|\boldsymbol{b})$ do odstupňovaného tvaru:

$$\left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 3 & 1 & 2 & 1 & 0 \end{array}\right) \underset{+4\,\mathrm{I}}{\sim} \left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 2 & 4 & 1 & 4 \end{array}\right) \underset{+5\,\mathrm{II}}{\sim} \left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) = (\boldsymbol{A}'|\boldsymbol{b}')$$

Pokud poslední sloupec neobsahuje pivot, vyřešíme $\boldsymbol{A}'\overline{\boldsymbol{x}} = \mathbf{0}$:

$$\begin{array}{rcl} \overline{x}_2 & = & -4\overline{x}_4 - 2\overline{x}_3 \;=\; 3\overline{x}_4 + 5\overline{x}_3 \\ \overline{x}_1 & = & -4\overline{x}_3 - 2\overline{x}_2 \;=\; 3\overline{x}_3 + 5(3\overline{x}_4 + 5\overline{x}_3) \;=\; \overline{x}_4 \end{array}$$

Nahradíme volné proměnné: $\overline{\boldsymbol{x}} = p_1(0,5,1,0)^{\mathsf{T}} + p_2(1,3,0,1)^{\mathsf{T}}$

Přičteme nějaké řešení $\boldsymbol{A}'\boldsymbol{x} = \boldsymbol{b}'$, např. $(4,2,0,0)^{\mathsf{T}}$ a máme:

$$\boldsymbol{x} = (4,2,0,0)^{\mathsf{T}} + p_1(0,5,1,0)^{\mathsf{T}} + p_2(1,3,0,1)^{\mathsf{T}}$$

Metavěta

Metavěta: Všechna doposud uvedená tvrzení o soustavách rovnic, maticích a výpočtech nad $\mathbb{R}$ jsou platná i v libovolném tělese T.

Ukázka: Výpočet inverzní matice nad $\mathbb{Z}_5$:

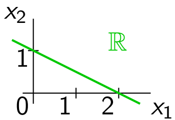
$$(\boldsymbol{A}|\mathbf{I}) = \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 3 & 4 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \begin{array}{c} \\ +2\,\mathrm{I} \\ \\ \end{array} \sim \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 0 & 4 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \begin{array}{c} +2\,\mathrm{III} \\ \mathrm{III} \\ -\mathrm{II} \end{array} \sim$$

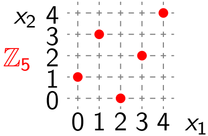
$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 4 & 1 & 0 & 2 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 & 4 & 0 \end{array}\right) \begin{array}{c} +\,\mathrm{III} \\ -\,\mathrm{III} \\ \\ \end{array} \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 4 & 4 & 2 \\ 0 & 1 & 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 3 & 4 & 0 \end{array}\right) = (\mathbf{I}|\boldsymbol{A}^{-1})$$

Zkouška:

$$\begin{array}{ccc|ccc} & & & 4 & 4 & 2 \\ & \boldsymbol{A}\boldsymbol{A}^{-1} = \mathbf{I} & & 2 & 1 & 1 \\ & & & 3 & 4 & 0 \\ \hline 1 & 3 & 2 & 1 & 0 & 0 \\ 3 & 4 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}$$

Pozor: Geometrická interpretace může být jiná! V $\mathbb{R}$ tvoří řešení rovnice $x_1 + 2x_2 = 2$ přímku, zatímco v $\mathbb{Z}_5$ má stejná rovnice jen 5 řešení.





Vlastnosti tělesa

Protože $(T,+)$ a $(T \setminus 0, \cdot)$ jsou grupy, máme už v tělese dokázáno:

- jednoznačnost prvků 0 a 1, … z jednoznačnosti e v grupě,
- jednoznačnost $-a$, a také jednoznačnost a^{-1} pro $a \neq 0$,
- korektnost ekviv. úprav: $c = d \Leftrightarrow ac + b = ad + b$ pro $a \neq 0$,
- řešitelnost rovnic: $ax + b = c \Leftrightarrow x = \frac{c-b}{a}$ pro $a \neq 0$.

Pozorování: Pro každé $a \in T$ platí, že $0a = 0$ a $(-1)a = -a$.

Důkaz:

$$0a = 0a + 0 = 0a + (0a - 0a) = (0+0)a - 0a = 0a - 0a = 0$$

$$\begin{aligned}(-1)a &= (-1)a + 0 = (-1)a + a - a = (-1)a + 1a - a \\ &= (-1+1)a - a = 0a - a = 0 - a = -a\end{aligned}$$

Pozorování: Pokud $ab = 0$, pak $a = 0$ nebo $b = 0$.

Důkaz: Sporem, pokud by $ab = 0$ pro $a, b \neq 0$, pak $\exists a^{-1}, b^{-1}$.
Pak $1 = aa^{-1}bb^{-1} = aba^{-1}b^{-1} = 0a^{-1}b^{-1} = 0$, což je spor.

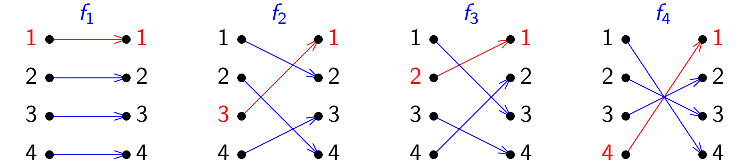
Tělesa z modulární aritmetiky

Věta: $\mathbb{Z}_p$ je těleso, právě když je p prvočíslo.

Důkaz: $\Rightarrow$: Pokud by p bylo složené $p = ab$, pak $ab \equiv 0 \pmod p$, což je spor s pozorováním.

$\Leftarrow$: Většina axiomů plyne z vlastností $+$ a $\cdot$ na $\mathbb{Z}$, kromě existence inverzních prvků a^{-1}, protože $\mathbb{Z}$ není uzavřená na dělení. Cíl: $\forall a \in \{1, \ldots, p-1\}\ \exists a^{-1} \in \{1, \ldots, p-1\} : aa^{-1} \equiv 1 \pmod p$.

Nechť $f_a : \{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ t.ž. $f_a(x) = (ax) \bmod p$. Hledané a^{-1} splňuje $f_a(a^{-1}) = 1$, čili stačí ukázat, že 1 je v oboru hodnot f_a. Dokážeme dokonce, že f_a je surjektivní (neboli „na“).



$f_1(1) = 1 \cdot 1 = 1$ $\quad$ $f_2(3) = 2 \cdot 3 = 1$ $\quad$ $f_3(2) = 3 \cdot 2 = 1$ $\quad$ $f_4(4) = 4 \cdot 4 = 1$

$1^{-1} = 1$ $\quad$ $2^{-1} = 3$ $\quad$ $3^{-1} = 2$ $\quad$ $4^{-1} = 4$

Tělesa z modulární aritmetiky

Věta: $\mathbb{Z}_p$ je těleso, právě když je p prvočíslo.

Důkaz: $\Rightarrow$: Pokud by p bylo složené $p = ab$, pak $ab \equiv 0 \pmod{p}$, což je spor s pozorováním.

$\Leftarrow$: Většina axiomů plyne z vlastností $+$ a $\cdot$ na $\mathbb{Z}$, kromě existence inverzních prvků a^{-1}, protože $\mathbb{Z}$ není uzavřená na dělení. Cíl: $\forall a \in \{1, \dots, p-1\}\ \exists a^{-1} \in \{1, \dots, p-1\} : aa^{-1} \equiv 1 \pmod{p}$.

Nechť $f_a : \{1, \dots, p-1\} \to \{1, \dots, p-1\}$ t.ž. $f_a(x) = (ax) \bmod p$. Hledané a^{-1} splňuje $f_a(a^{-1}) = 1$, čili stačí ukázat, že 1 je v oboru hodnot f_a. Dokážeme dokonce, že f_a je surjektivní (neboli „na“).

Protože f_a zobrazuje konečnou množinu na sebe samu, pak platí, že je surjektivní, právě když je prosté.

Pokud by pro spor f_a nebylo prosté, pak $\exists b, c$ b.ú.n.o. $b > c$ t.ž. $f_a(b) = f_a(c) \Rightarrow 0 = f_a(b) - f_a(c) \equiv ab - ac = a(b-c) \pmod{p}$, což je spor s tím, že p je prvočíslo, neboť $a, b-c \in \{1, \dots, p-1\}$.

Galoisovo těleso

Věta: Těleso o velikosti n existuje právě když n je mocninou prvočísla. Je jednoznačné až na izomorfismus a značí se $\mathrm{GF}(n)$.

Ukázka: Těleso $\mathrm{GF}(4) = \mathrm{GF}(2^2)$. Pro $T = \{0, 1, a, b\}$ definujeme sčítání a součin předpisem:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Tyto operace $+$ a $\cdot$ splňují všechny axiomy.

Jiný pohled na stejné těleso: Vezměme za T všechny polynomy maximálního stupně 1 s koeficienty v $\mathbb{Z}_2$, např. $a = x$, $b = x + 1$. Součin se provádí modulo polynom $x^2 + x + 1$.

$+$	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

$\cdot$	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

Charakteristika tělesa

Definice: V tělese T, pokud $\exists n \in \mathbb{N} : \underbrace{1 + 1 + \cdots + 1}_{n\times} = 0$,

pak nejmenší takové n je *charakteristika* tělesa T.
Jinak má těleso T charakteristiku 0. Značí se $\mathrm{char}(T)$.

Ukázka: $\mathrm{char}(\mathbb{R}) = 0$ a $\mathrm{char}(\mathbb{Z}_p) = p$.

Věta: Charakteristika tělesa je vždy prvočíslo nebo 0.

Důkaz: Sporem, pokud by charakteristika byla složená $n = ab$,
pak $0 = \underbrace{1 + 1 + \cdots + 1}_{n\times} = \underbrace{(1 + 1 + \cdots + 1)}_{a\times}\underbrace{(1 + 1 + \cdots + 1)}_{b\times} \neq 0$,

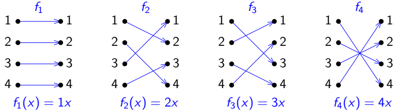
neboť $\underbrace{1 + 1 + \cdots + 1}_{a\times} \neq 0$ a $\underbrace{1 + 1 + \cdots + 1}_{b\times} \neq 0$.

Pozorování: V tělesech charakteristiky 2 je každý prvek opačný sám k sobě a odečítání lze nahradit sčítáním.
Důkaz: $1 + 1 = 0 \;\Rightarrow\; -1 = 1 \;\Rightarrow\; -a = a \;\Rightarrow\; a - b = a + b$.

Malá Fermatova věta

Věta: [Fermat 1640•, Leibnitz 1683+, Euler 1736*]
Pro prvočíslo p a každé $a \in \{1, \ldots, p-1\}$: $a^{p-1} \equiv 1 \pmod p$.

Důkaz: Zobrazení $f_a : x \to ax$ je
v $\mathbb{Z}_p$ bijekcí na $\{1, \ldots, p-1\}$.



Proto v $\mathbb{Z}_p$ platí:

$$\prod_{x=1}^{p-1} x = \prod_{x=1}^{p-1} f_a(x) = \prod_{x=1}^{p-1} ax = a^{p-1} \prod_{x=1}^{p-1} x$$

a po zkrácení $\prod_{x=1}^{p-1} x$ dostaneme $1 = a^{p-1}$.

Důsledky: V $\mathbb{Z}_p$ s prvočíselným p
jakékoli a splňuje $a^p = a$.
Nenulová a mají inverze $a^{-1} = a^{p-2}$.

Pierre de Fermat
1607 – 1665
Obr. Wikipedie

•bez důkazu, +nepublikováno, *publikováno

Kvíz — řešení

Je-li u některých otázek více možností správných, vyberte všechny.

1. Rozhodněte, které z následujících podmnožin $\mathbb{R}$, resp. $\mathbb{C}$ tvoří těleso vzhledem k obvyklým operacím sčítání a násobení:
   a) $\{a\sqrt{2} : a \in \mathbb{Q}\}$ b) $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
   c) $\{a + bi\sqrt{2} : a, b \in \mathbb{Q}\}$ d) $\{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Q}\}$
2. Pravda nebo lež?
   Pokud jsou $(R, +, \cdot)$, $(S, +, \cdot)$ a $(T, +, \cdot)$ tělesa,
   kde $R \subseteq T$ a $S \subseteq T$, potom je $(R \cap S, +, \cdot)$ také těleso.
   (Na podmnožinách jsou $+$ a $\cdot$ odvozené zúžením z $(T, +, \cdot)$.)
3. Kolik prvků ze $\mathbb{Z}_{12}$ nemá inverzi vzhledem k násobení?
   a) 0 b) 1 c) 2 d) 4 e) 7 f) 8 g) 11 h) 12
4. Řešením rovnice $ax + b = 1$ na $\mathrm{GF}(4)$ je
   a) $x = 0$ b) $x = 1$ c) $x = a$ d) $x = b$ e) $\emptyset$
5. Pravda nebo lež?
   Protože $9 \notin \mathbb{Z}_7$, je každá matice řádu 9 nad $\mathbb{Z}_7$ singulární.

Komentář k řešení kvízu

1. a) 1 není racionální násobek $\sqrt{2}$, b) a c) třeba ověřit uzavřenost na $+$ a $\cdot$, a také existenci inverzí, např.:
$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$, nebo
$(a+b\mathrm{i}\sqrt{2})^{-1} = \frac{(a-b\mathrm{i}\sqrt{2})}{(a+b\mathrm{i}\sqrt{2})(a-b\mathrm{i}\sqrt{2})} = \frac{a}{a^2+2b^2} - \frac{b}{a^2+2b^2}\mathrm{i}\sqrt{2}$
d) $\sqrt{2}\cdot\sqrt{3} = \sqrt{6} \notin \{a+b\sqrt{2}+c\sqrt{3} : a,b,c \in \mathbb{Q}\}$.
Kdyby $\sqrt{6} = a+b\sqrt{2}+c\sqrt{3}$, pak $\sqrt{3}(\sqrt{2}-c) = a+b\sqrt{2} \Rightarrow 3(2+c^2-2\sqrt{2}c) = a^2+2b^2+2\sqrt{2}ab$.
Z koeficientů u $\sqrt{2}$ je $c = -\frac{ab}{3}$. Pak $6+\frac{a^2b^2}{3} = a^2+2b^2 \Rightarrow (a^2-6)(b^2-3) = 0$, spor s $a,b \in \mathbb{Q}$.
2. Z jednoznačnosti 0 a 1 v T plyne, že $0,1 \in R\cap S$. Potom už stačí ověřit existenci obou inverzí, např. pro $a \in R\cap S$ máme $a \in R \wedge a \in S \Rightarrow -a \in R \wedge -a \in S \Rightarrow -a \in R\cap S$ (i pro a^{-1}).
3. Násobky 2 a 3 (prvočíselných dělitelů 12) mají při dělení 12 zbytek dělitelný 2 nebo 3. Jsou to čísla $0,2,3,4,6,8,9$ a 10. Násobky zbylých mohou dát 1: $1^2 = 5^2 = 7^2 = 11^2 = 1$ v $\mathbb{Z}_{12}$.
4. Z $ax+b=1$ vyjádříme: $x = a^{-1}(1-b) = a^{-1}a = 1$.
5. Např. $\mathbf{I}_9$, čili jednotková matice řádu 9, je regulární i v $\mathbb{Z}_7$.

Otázky k porozumění tématu přednášky

- Existuje nějaká struktura $(S, +, \cdot)$ splňující distributivní axiom, kde $(S, +)$ i $(S, \cdot)$ jsou grupy se stejným neutrálním prvkem?
- Které axiomy z definice tělesa byly využity v důkazech tvrzení:
  - Přičtení i-tého řádku k j-tému je ekvivalentní řádková úprava.
  - Každé řešení soustavy lze získat zpětnou substitucí.
  - Hodnost matice je definována jednoznačně.
  - Maticový součin je asociativní.
  - $\boldsymbol{A}^{-1}\boldsymbol{A} = \mathbf{I}_n$.

  a které axiomy v těchto důkazech potřeba nebyly?
- Platí v tělesech vztah $a^m \cdot a^n = a^{m+n}$?
  Pokud ano, pro jaké možné exponenty m a n?
- Mějme čtvercovou matici $\boldsymbol{A}$ s prvky z množiny $\{0, 1, 2\}$. Jak se může měnit regularita $\boldsymbol{A}$, pokud její obsah interpretujeme nad různými tělesy, jako např. $\mathbb{R}, \mathbb{Q}, \mathbb{Z}_3, \mathbb{Z}_5$, apod.?