Těleso

Co říkala paní učitelka o vlastnostech sčítání a násobení reálných čísel:

- 1.) $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ (uzavřenost sčítání)
- 2.) $\forall a,b \in \mathbb{R} : a+b = b+a$ (komutativnost sčítání)
- 3.) $\forall a,b,c \in \mathbb{R} : a+(b+c) = (a+b)+c$ (asociativnost sčítání)
- 4.) $\exists\, o \in \mathbb{R}\ \forall x \in \mathbb{R} : o+x = x+o = x$ (∃ neutrální prvek při sčítání $o=0$)
- 5.) $\forall x \in \mathbb{R}\ \exists\, x^* \in \mathbb{R} : x+x^* = x^*+x = o$ (každý prvek má prvek inverzní $x^* = -x$)

→ $(\mathbb{R}, +)$ je komutativní grupa

- 6.) $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ (uzavřenost násobení)
- 7.) $\forall a,b \in \mathbb{R} : a \cdot b = b \cdot a$ (komutativnost násobení)
- 8.) $\forall a,b,c \in \mathbb{R} : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociativnost násobení)
- 9.) $\exists\, e \in \mathbb{R}\ \forall x \in \mathbb{R} : e \cdot x = x \cdot e = x$ (∃ neutrální prvek při násobení $e = 1$)

→ $(\mathbb{R}, \cdot)$ je komutativní monoid

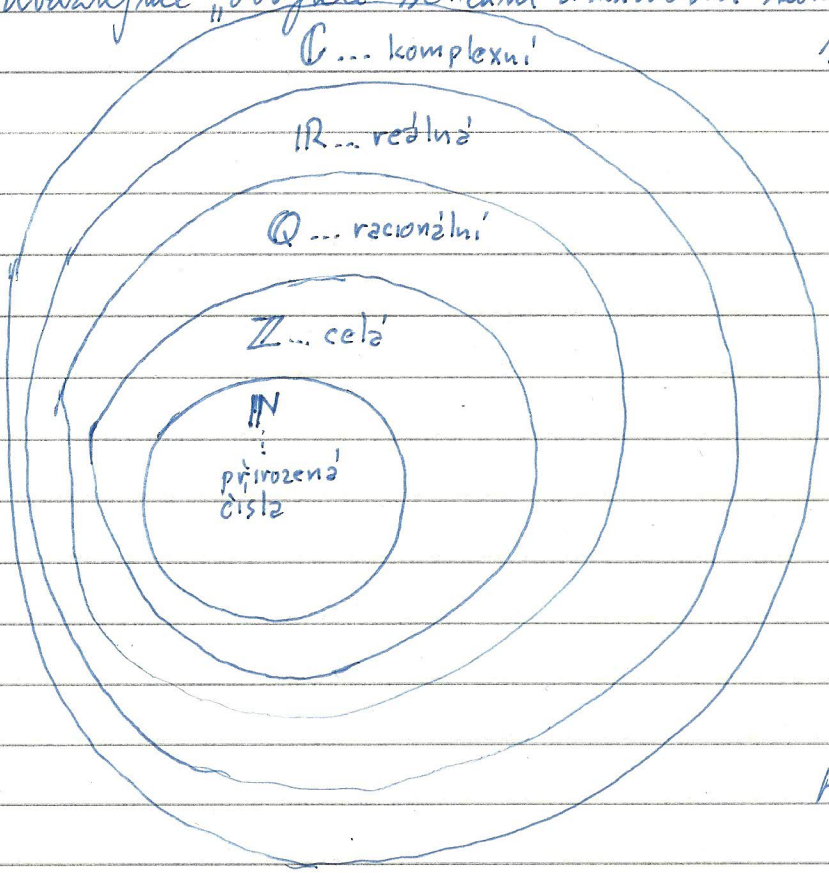
- 10.) $\forall x \in \mathbb{R} - \{o\}\ \exists\, x' \in \mathbb{R} : x \cdot x' = x' \cdot x = e$ (každý nenulový prvek má prvek inverzní vzhledem k násobení $x' = \frac{1}{x} = x^{-1}$)
- 11.) $e \neq o$ (netriviálnost)
- 12.) $\forall a,b,c \in \mathbb{R} : a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ (distributivnost zleva)
- 13.) $\forall a,b,c \in \mathbb{R} : (a+b) \cdot c = (a \cdot c) + (b \cdot c)$ (distributivnost zprava)

$\Rightarrow (\mathbb{R}, +, \cdot)$ je těleso

Definice (Těleso): Uspořádanou trojici $(T,+,\cdot)$ nazveme tělesem právě tehdy, když

- $(T,+)$ je komutativní grupa
- $(T,\cdot)$ je komutativní monoid
- $\forall x \in T-\{o\}\ \exists\ \bar{x}^{-1} \in T : x\cdot\bar{x}^{-1} = \bar{x}^{-1}\cdot x = e$, kde o je neutrální prvek při sčítání a e při násobení
- $o \neq e$
- Násobení je distributivní zleva i zprava.

Př.: Uvažujme „obvyklé" sčítání a násobení komplexních čísel =>



1.) $(\mathbb{N},+,\cdot)$ není těleso, neboť např. $0 \notin \mathbb{N}$, nebo prvek $2 \in \mathbb{N}$ nemá inverzní prvek při sčítání ($-2 \in \mathbb{Z}$ ale ne do $\mathbb{N}$)

2.) • $(\mathbb{Z},+)$ je komutativní grupa
• $(\mathbb{Z},\cdot)$ je komutat. monoid
• $1 \neq 0$
• násobení je distributivní zleva i zprava

ALE! např. $2 \in \mathbb{Z}$ nemá inverzní prvek vzhledem k násobení ($\frac{1}{2} \notin \mathbb{Z}$).
$\Rightarrow (\mathbb{Z},+,\cdot)$ není těleso

3.) $(\mathbb{Q},+,\cdot)$ je těleso ($\frac{p}{q} \in \mathbb{Q}-\{0\} \Rightarrow \left(\frac{p}{q}\right)^{-1} = \frac{q}{p} \in \mathbb{Q}$)
4.) $(\mathbb{R},+,\cdot)$ je těleso
5.) $(\mathbb{C},+,\cdot)$ je těleso

6.) $(\mathbb{R}-\mathbb{Q},+,\cdot)$ není těleso : $\underbrace{\sqrt{2}}_{\in \mathbb{R}-\mathbb{Q}} \cdot \underbrace{\sqrt{2}}_{\in \mathbb{R}-\mathbb{Q}} = 2 \notin \mathbb{R}-\mathbb{Q}$

Př. Zkonstruujeme těleso $(\mathbb{P}, +, \cdot)$, kde $\mathbb{P} \not\subseteq \mathbb{C}$ (neobsahuje „čísla") a bude mít jen konečný počet prvků.

$\mathbb{P} = \{$ Jeník, Dušan, Tonik $\}$ ... množina prasátek

Operace sčítání prasátek a násobení prasátek definujme následovně:

+	J	D	T
J	D	T	J
D	T	J	D
T	J	D	T

Tab. 1.

⇒ např.: D + D = J

·	J	D	T
J	J	D	T
D	D	J	T
T	T	T	T

Tab. 2.

- $(P, +)$ je komutativní grupa:

1.) uzavřenost +: Všechny prvky v Tab. 1 patří do $\mathbb{P}$ ⇒ $+ : \mathbb{P} \times \mathbb{P} \to \mathbb{P}$

2.) komutativnost +: Tabulka je symetrická podle diagonály ⇒ $\forall a, b \in \mathbb{P} : a + b = b + a$

3.) asociativnost +: a) $J + (D + T) = J + D = T$
$(J + D) + T = T + T = T$
b) ⋮ ověřit ostatní možnosti, za DÚ
⇒ $\forall a, b, c \in \mathbb{P} : a + (b + c) = (a + b) + c$

4.) neutrální prvek při +: $\exists \sigma = T \in \mathbb{P}$: $T + J = J + T = J$
$T + D = D + T = D$
$T + T = T + T = T$ (T je nulový prvek)

5.) inverzní prvky při +: existují pro každý prvek z $\mathbb{P}$:
$-T = T$, neboť $T + T = T$ $(= \sigma)$
$-D = J$, neboť $D + J = T$
$-J = D$, neboť $J + D = T$

6.) uzavřenost ·: Všechny prvky v Tab. 2. patří do $\mathbb{P}$ ⇒ $\cdot : \mathbb{P} \times \mathbb{P} \to \mathbb{P}$

7.) komutativnost ·: Tab. 2. je symetrická podle diagonály, proto
$\forall a, b \in \mathbb{P} : a \cdot b = b \cdot a$

8.) asociativnost $\cdot$: a) $J\cdot(D\cdot T) = J\cdot T = T$
$(J\cdot D)\cdot T = D\cdot T = T$ ⟫
b) $D\cdot(J\cdot J) = \dots$
ověřit další možnosti za DÚ
⟹ $\forall a,b,c\in\mathbb{P}: a\cdot(b\cdot c)=(a\cdot b)\cdot c$

9.) neutrální prvek při $\cdot$: $\exists e = J \in T$:
$J\cdot J = J = J\cdot J$
$J\cdot D = D = D\cdot J$
$J\cdot T = T = T\cdot J$
(⟹ J je jedničkou v $\mathbb{P}$)

10.) každý nenulový prvek má inverzi vzhledem k násobení (nenulové jsou J a D)
$J^{-1} = J$, neboť $J\cdot J = J = e$
$D^{-1} = D$, neboť $D\cdot D = J = e$
(T inverzní prvek nemá, ale to nevadí, neboť T je nula!)

11.) $T \neq J$, tzn. $0 \neq e$

12.) distributivita zleva : a) $J\cdot(D+T) = J\cdot D = D$
$J\cdot D + J\cdot T = D + T = D$ ⟫
b) ⋮ další možnosti ověřit za DÚ
⟹ $\forall a,b,c\in\mathbb{P}$: $a\cdot(b+c) = a\cdot b + a\cdot c$

13.) distributivita zprava : a) $(J+D)\cdot T = T\cdot T = T$
$J\cdot T + D\cdot T = T + T = T$ ⟫
b) ⋮ další možnosti ověřit za DÚ

⟹ $(\{\text{Jenik}, \text{Dušan}, \text{Tonik}\}, +, \cdot)$ tvoří těleso !

Základní vlastnosti

Předpokládejme, že $(T, +, \cdot)$ je těleso $\Rightarrow$

$\forall a \in T$:

$$a = e \cdot a = (e + o)a = e \cdot a + o a = a + o \cdot a \Rightarrow$$

$$-a + a = -a + a + o \cdot a \Rightarrow$$

$$o = o \cdot a \quad (\cdot \text{ je komutativní} \Rightarrow a \cdot o = o) \Rightarrow$$

$$\boxed{\forall a \in T : o \cdot a = a \cdot o = o}$$

Navíc $\forall a, b \in T - \{o\}$: $\exists \bar{a}^1 \in T$. Předpokládejme, že

$$a \cdot b = o$$

$$\Rightarrow b = e \cdot b = \bar{a}^1 \cdot a \cdot b = \bar{a}^1 \cdot o = o \Rightarrow \text{SPOR s } b \in T - \{\bar{o}\} \Rightarrow$$

$$\boxed{\forall a, b \in T - \{o\} : a \cdot b \neq o}$$

Předpokládejme, že $\bar{o}^1$ je inverzní prvek k o vzhledem k násobení $\Rightarrow$

$$o \cdot \bar{o}^1 = e \quad \wedge \quad o \cdot \bar{o}^1 = o \text{ (viz výše)}$$

$$\Rightarrow \quad e = o \quad \Rightarrow \text{spor!} \text{ (s definičním axiomem } o \neq e)$$

$$\Rightarrow \boxed{\bar{o}^{-1} \text{ neexistuje}}$$

Př. Zkonstruujeme těleso o 2^2 prvcích

(intuitivní představa: Číselný rámeček, na dvou pozicích máme dvě možnosti: 0 a 1)

$\boxed{0}\boxed{0}$; $\boxed{0}\boxed{1}$, $\boxed{1}\boxed{0}$, $\boxed{1}\boxed{1}$ ⇒ 4 možnosti ⇒ 4 prvky

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

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

Tak co kdyby 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

⇒

1.) uzavřenost + ✓

2.) komutativnost + ✓

3.) asociativita +
plyne z asociativity sčítání na $(\mathbb{Z}_2, +, \cdot)$

4.) $-0 = 0$

5.) $-0=0$, $-1=1$, $-x=x$, $-(x+1)=x+1$

⇒ $(T,+)$ je komutativní grupa

Ale jak definovat násobení ?!

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

↯ Tj. jsou jen polynomy stupně maximálně 1! Co kdyby bychom postupovali analogicky jako u +? Tam jsme odečítali násobky 2 když byl součet větší než 1. Co kdyby bychom tady 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

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

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

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

Problém! Toto by jistě nebylo těleso!:

$X \cdot X = 0$ (v tělese nesmí být dělitelé nuly!)
$X \neq 0 \quad X \neq 0$

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

Násobíme „modulo x^2+1"

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

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

$\Rightarrow$ 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 . V

7.) komutativnost . V

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

9.) $e = 1$

10.) $\bar{1}^1 = 1$, $\bar{X}^1 = X+1$, $(X+1)^{-1} = X$

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

⇒ T takto definovaným sčítáním a násobením tvoří těleso o 2^2 prvcích

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

$$T = \{ a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1 x + a_0 \mid a_{n-1}, \dots, a_0 \in \mathbb{Z}_p \}$$

Sčítáme „koeficienty modulo p."

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