▶ AXIOMATICKÉ ZAVEDENÍ ČÍSEL

Množina je **soubor objektů**. Pokud objekt x patří do množiny M, píšeme $x \in M$. Jestliže x nepatří do M, pak píšeme $x \notin M$. Množina M je neprázdná, píšeme $M \neq \emptyset$, pokud obsahuje aspoň jeden prvek. Symbol $\emptyset$ značí prázdnou množinu.

[Axiomatické zavedení reálných čísel] Předpokládáme (definitoricky), že existuje neprázdná množina $\mathbb{R}$, na které existují dvě operace $+, \cdot$ a relace uspořádání $<$ tak, že platí axiomy (A1) – (A4) (o sčítání)
(M1) – (M4) (o násobení)
D (spojující násobení a sčítání)
(O1) – (O4) (o uspořádání)
(Arch) (Archimedův axiom úplnosti)

Takovouto strukturu $(\mathbb{R}, +, \cdot, <)$ budeme nazývat **množina reálných čísel**, značíme $\mathbb{R}$.

Axiomy budeme zavádět postupně. Jejich postupné zavedení nám umožní oddělit a zavést jiné číselné množiny.

Nejdříve zavedeme axiomy pro sčítání a násobení. Předpokládáme, že na $\mathbb{R}$ jsou dvě operace $+$ a $\cdot$ tak, že ($+ : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ a $\cdot : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$) platí:

(A1) $(\forall x, y, z \in \mathbb{R}) : (x+y)+z = x+(y+z)$ ASOCIATIVITA

(A2) $(\forall x, y \in \mathbb{R}) : x+y = y+x$ KOMUTATIVITA

(A3) $\exists\ 0 \in \mathbb{R}$ (prvek) $x+0 = 0+x = x$ EXISTENCE NEUTRÁLNÍHO PRVKU

(A4) $(\forall x \in \mathbb{R})(\exists$ prvek opačný $-x)$ $x+(-x) = 0$ EXISTENCE INVERZNÍHO PRVKU.

Poznámka pod čarou: Axiomy (A1) – (A4) říkají, že $(\mathbb{R}, +)$ je **Abelova** (neboli komutativní) **grupa**.

(M1) $(\forall x,y,z \in \mathbb{R})\quad (x\cdot y)\cdot z = x\cdot(y\cdot z)$ ASOCIATIVITA

(M2) $(\forall x,y \in \mathbb{R})\quad x\cdot y = y\cdot x$ KOMUTATIVITA

(M3) $\exists$ prvek, označíme $1 \in \mathbb{R}$, tak, že EXISTENCE NEUTRÁLNÍHO PRVKU

$$x\cdot 1 = 1\cdot x = x$$

(M4) $(\forall x \in \mathbb{R}, x \neq 0)$ ($\exists$ prvek označme jej x^{-1} nebo $\frac{1}{x}$) $x\cdot x^{-1} = 1$ EXISTENCE INVERZNÍHO PRVKU

Obě operace spojuje distributivní axiom:

(D) $(\forall x,y,z \in \mathbb{R})\quad (x+y)\cdot z = x\cdot y + y\cdot z$ DISTRIBUTIVITA

<u>Definice</u> (z algebry) Množina, jejíž objekty splňují $\boxed{\text{(A1)–(A4) a (M1)–(M4) a také (D)}}$ se nazývá <u>těleso</u> (angl. field)

Z definice axiomů plyne, že těleso musí obsahovat alespoň dva různé prvky: $0 \neq 1$ (neutrální prvky vzhledem k sčítání a násobení).

<u>Příklad 1</u> (tělesa, které má právě dva prvky 0, 1). Buď $\mathbb{F}_2 = \{0,1\}$, kde operace + a $\bullet$ jsou dány tabulkami:

+	0	1
0	0	1
1	1	0

$\bullet$	0	1
0	0	0
1	0	1

Na příkladu vidíme, že

- axiomy tělesa ani nezaručují, že $1+1 \neq 0$
- ani přirozená čísla nemusí být podmnožinou číselného tělesa.

<u>Příklad 2</u> Definujme $\mathbb{C} \stackrel{\text{df.}}{=} \{z = (z_1, z_2);\ z_1, z_2 \in \mathbb{R}\}$ a zavedme na $\mathbb{C}$ operace $\oplus$ a $*$ takto: $\forall z, u \in \mathbb{C}$

$$z \oplus u \stackrel{\text{df.}}{=} (z_1+u_1, z_2+u_2)$$

$$z * u = (z_1, z_2) * (u_1, u_2) \stackrel{\text{df.}}{=} (z_1u_1 - z_2u_2,\ z_1u_2 + z_2u_1)$$

<u>Cvičení</u> (DÚ) Ukažte, že $(\mathbb{C}, \oplus, *)$ je těleso.

Terminologie: Je-li $z = (z_1, z_2)$, pak z_1 .... reálná část z, z_2 .... imaginární část z. Je-li $x \in \mathbb{R}$, pak ztotožňujeme $x = (x, 0)$ a také reálnou osu s $\mathbb{R}$ a chápeme $\mathbb{R} \subset \mathbb{C}$.

Speciálně: $0=(0,0)$ a $1=(1,0)$. Definujme $\boxed{i=(0,1)}$ IMAGINÁRNÍ JEDNOTKA

<u>Tvrzení</u> $(\forall z\in\mathbb{C})$ $z=(z_1,z_2)$ lze psát ve tvaru $z=z_1+iz_2$.

Dk
$$\left.\begin{array}{l} z_1=(z_1,0) \\ iz_2=(0,1)*(z_2,0)=(0,z_2) \end{array}\right\}\Rightarrow z_1+iz_2=(z_1,0)+(0,z_2)=(z_1,z_2)$$

<u>Tvrzení</u> $i^2=-1$

Dk $i^2=i*i=(0,1)*(0,1)=(-1,0)=-1$.

Nyní přidáme k $\mathbb{R}$ další 4 axiomy: předpokládáme existenci binární relace $>$, která dává uspořádání reálných čísel a splňuje:

(O 1) Nastává právě jedna z relací pro $\forall x\in\mathbb{R}$: $x>0$, $x=0$ nebo $-x>0$.

(píšeme: $x>y \overset{\text{df.}}{=} x-y>0$, $x=y \overset{\text{df.}}{=} x-y=0$, ...)

(O 2) Je-li $x>y$, pak pro každé $z\in\mathbb{R}$: $x+z>y+z$

(odsud plyne $1+1\neq 0$) $\boxed{\text{Úmluva } 1>0}$

(O 3) Je-li $x>0$ a $y>0$, pak $xy>0$

(O 4) Je-li $x>y$ a $y>z$, pak $x>z$.

Zavedeme označení:
$\mathbb{R}^+=\{x\in\mathbb{R};\ x>0\}$ kladná čísla
$\mathbb{R}^-=\{x\in\mathbb{R};\ -x>0\}$ záporná čísla
$x\le y \overset{\text{df.}}{=} y>x$ nebo $y=x$

<u>Cvičení</u> Z axiomů plyne:
Je-li $x<y$ a $z>0$, pak $xz<yz$
Je-li $x<y$ a $z<0$, pak $xz>yz$.

<u>Tvrzení 1</u> (důležité) Buďte $a,b\in\mathbb{R}$ splňující $(\forall\varepsilon>0)(a\le b+\varepsilon)$. Pak $a\le b$.

Dk Sporem: Nechť ($a\le b+\varepsilon$ pro $\forall\varepsilon>0$) $\wedge$ $b<a$. Uvaž $\varepsilon=\frac{a-b}{2}$.

Pak $b+\varepsilon=b+\frac{a-b}{2}=\frac{a}{2}+\frac{b}{2}<\frac{a}{2}+\frac{a}{2}=a$. Tedy

z podtrženého $b+\varepsilon<a$ což je $\lightning$ s předpokladem.

<u>Def.</u> Řekneme, že podmnožina $P\subset\mathbb{R}$ je induktivní množina pokud platí:
- $1\in P$
- $x\in P \Rightarrow x+1\in P$

Příklady: $\mathbb{R}$, $\mathbb{R}_+$ jsou induktivní množiny

Def. (Přirozená čísla $\mathbb{N}$) Nejmenší induktivní množina v $\mathbb{R}$, ozn. $\mathbb{N}$.

Tvr. $\mathbb{N} = \{1, \underbrace{1+1}_{2}, \underbrace{2+1}_{3}, \dots\}$

Def.
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
- $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-m;\ m \in \mathbb{N}\} = \{\pm k;\ k \in \mathbb{N}\} \cup \{0\}$
  celá čísla (integers)
- $\mathbb{Q} = \{x;\ x = \frac{p}{q}$ kde $p \in \mathbb{Z}$ a $q \in \mathbb{N}\}$

Cvičení
- $\mathbb{Q}$ splňuje všechny axiomy (A1)-(A4), (M1)-(M4), D a (O1)-(O4).
- Jsou-li $a, b \in \mathbb{Q}$, pak $\frac{a+b}{2} \in \mathbb{Q}$. Navíc $\frac{a+b}{2}$ leží mezi a a b. Odsud plyne:
  Je-li dáno racionální číslo, pak nelze mluvit o nejbližším větším racionálním čísle.

- $\mathbb{R} \setminus \mathbb{Q}$ iracionální čísla

Tvrzení 2 Je-li $m \in \mathbb{N}$ takové, že m nelze zapsat ve tvaru $m = k^2$, pak $\sqrt{m}$ je iracionální.

Dk vynecháme. Pro $m=2$ se důkaz dělá na SŠ. Důkaz si najdete ve zdrojích/literatuře. $\blacksquare$

- Čísla $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \dots$, ale i π, e^{π}, e jsou iracionální.
- Ukážeme si později, že množina $\mathbb{R} \setminus \mathbb{Q}$ obsahuje "řádově více prvků" než množina $\mathbb{Q}$.
- Iracionální čísla vznikla přirozeně při hledání řešení rovnice $x^2=2$.

Uspořádání $<$, $\leq$ nám umožňují zavést pojem intervalu.

Buď $a, b \in \mathbb{R}$, $a<b$.

$(a,b) =^{df} \{x \in \mathbb{R};\ a < x < b\}$ — OTEVŘENÝ INTERVAL

$\langle a,b \rangle =^{df} \{x \in \mathbb{R};\ a \leq x \leq b\}$ — UZAVŘENÝ INTERVAL (užívá $[a,b] := \langle a,b\rangle$)

$(a,b\rangle =^{df} \{x \in \mathbb{R};\ a < x \leq b\}$

$\langle a,b) = \{x \in \mathbb{R};\ a \leq x < b\}$

(polouzavřené intervaly)

Zavádíme také symboly $+\infty$ a $-\infty$ (nepatří do $\mathbb{R}$):

$(a,+\infty) = \{x \in \mathbb{R};\ x > a\}$ a podobně $\langle a,+\infty)$

$(-\infty,a) = \{x \in \mathbb{R};\ x < a\}$ a podobně $(-\infty,a\rangle$

Např: $\mathbb{R} = (-\infty,\infty)$ a $\{a\}$ je degenerovaný uzavřený interval (bod a).

<u>Geometrická interpretace $\mathbb{R}$</u> $\mathbb{R}$ ztotožníme s přímkou, na které zvolíme dva různé body 0 a 1. Zpravidla $0<1$. Tím zvolíme (definujeme) měřítko a orientaci. Uspořádání $x<y$ má pak jednoduchou interpretaci: y je napravo od x.

Budujeme axiomatickou teorii reálných čísel. Zbývá nám zformulovat <u>axiom úplnosti</u>, který by měl oddělit reálná čísla od racionálních. K formulaci axiomu úplnosti budeme potřebovat pojmy: horní/dolní závora (neboli mez) a supremum/infimum

<u>Def.</u>
- Buď S podmnožina $\mathbb{R}$. Je-li $b\in\mathbb{R}$ takové, že pro všechna $x\in S$ platí $x\leq b$, pak b je <u>horní závora S</u> a říkáme, že S je <u>omezená shora</u>
- Podobně: dolní závora S, omezenost zdola.
- Množina S je <u>omezená</u> $\overset{df}{\equiv}$ (S je omezená shora) $\wedge$ (S je omezená zdola).

<u>Cvičení!</u>
- Je-li b horní závora, pak každé číslo větší než b je také horní závora.
- Je-li b <u>horní závora S</u> a $b\in S$, pak b je <u>maximum S</u> (neboli maximální prvek S) $b=\max\{x;\ x\in S\}=\max\limits_{x\in S}\{x\}$

<u>Def.</u> Množina S je neomezená shora, nemá-li horní závoru.

<u>Příklady</u> (i) $\mathbb{R}^+=(0,+\infty)$ je neomezená shora, je však omezená zdola, 0 je dolní závora (a také jakékoliv číslo menší než nula je dolní závora). 0 však není minimem $\mathbb{R}^+$, neboť $0\notin\mathbb{R}^+$.

(ii) $S=\langle 0,1\rangle$ je omezená shora i omezená zdola, je tedy omezená, dolní závora $0\in S$, horní závora $1\in S$. tedy $0=\min S$ a $1=\max S$.

(iii) $S=(0,1)$ 1 je nejmenší horní závora, $1\notin S$

(iv) $S=\{\frac{1}{n},\ n\in\mathbb{N}\}$ je omezená, $1\in S$ je horní závora, $0\notin S$ je největší dolní závora.

Def. Číslo $b \in \mathbb{R}$ je <u>supremum</u> S pokud b je nejmenší horní závora S, tzn., (i) b je horní závora S

(ii) žádné číslo menší než b není horní závora S.

Píšeme $\boxed{b = \sup S}$ Je-li $b \in S$, pak $\sup S = \max S$.

Číslo $b \in \mathbb{R}$ je <u>infimum</u> S, pokud b je největší dolní závora S.

Píšeme $\boxed{b = \inf S.}$ Je-li $b \in S$, pak $\inf S = \min S$.

$\boxed{\text{Axiom ÚPLNOSTI}}$ Každá neprázdná shora omezená podmnožina $S \subset \mathbb{R}$ má supremum.

<u>Důsledek</u> Každá neprázdná zdola omezená množina $S \subset \mathbb{R}$ má infimum.

Dk K S sestrojme množinu $-S \stackrel{df}{=} \{x \in \mathbb{R};\ -x \in S\}$. Pak $-S$ je omezená shora. Má supremum b. Položme $a := -b$. Pak a je infimum S, neb vlastnosti plynou z vlastností suprema b.

<u>Tvrzení 3</u> (Aproximační vlastnost) Buď $S \neq \emptyset$, $S \subseteq \mathbb{R}$, $b := \sup S$. Pak pro $(\forall a < b)(\exists x \in S)$ $\quad a < x \leq b$.

Dk Z definice suprema plyne $x \leq b$ pro $\forall x \in S$. Kdyby $(\exists a < b)$ $(\forall x \in S)$ $x \leq a$, pak b není supremum S (nejmenší horní závora), neboť a by byla horní závora a $a < b$, což je spor $\square$

<u>Tvrzení 4</u> (Aditivní vlastnost suprema) Buď $A, B \subset \mathbb{R}$, $A \neq \emptyset$, $B \neq \emptyset$, $a = \sup A$, $b = \sup B$. Definujme $C \stackrel{df}{=} \{x + y;\ x \in A, y \in B\}$

Potom $\boxed{\sup C = a + b \left(= \sup A + \sup B\right)}$

Dk Rovnost dokážeme tak, že platí $\boxed{\sup C \leq a + b}$ a také $\boxed{a + b \leq \sup C + 2\varepsilon \quad \forall \varepsilon > 0}$, což s pomocí Tvrzení 1 dá důkaz Tvrzení 4.

$\boxed{\leq}$ pro $(\forall x \in A)(\forall y \in B)$ $\quad x + y \leq a + b$. Tedy $a + b$ je horní závora C a $\sup C \leq a + b$.

$\boxed{\geq}$ Buď ε libovolné, ale pevné. Z Tvrzení 3 plyne existence $x_0 \in A$ a $y_0 \in B$: $\quad \begin{cases} a - \varepsilon < x_0 \leq a \\ b - \varepsilon < y_0 \leq b \end{cases}$

Sečtením: $\quad a + b - 2\varepsilon < x_0 + y_0 \leq \sup C$

Tedy $a + b \leq \sup C + 2\varepsilon$ a dle Tvrz. 1: $a + b \leq \sup C$. $\square$