

PŘEDNÁŠKA 1, 14. 2. 2022
MNOŽINY, FUNKCE, REÁLNÁ ČÍSLA

- *Co analyzuje matematická analýza?* Nekonečné procesy a operace. Podívejme se na dva paradoxy.

$$S = 1 - 1 + \frac{1}{2} - \frac{1}{2} + \frac{1}{3} - \frac{1}{3} + \dots + \underbrace{\frac{1}{n} - \frac{1}{n}}_{=0} + \dots = 0,$$

ale i, po zpřeházení sčítanců,

$$S = 1 + \frac{1}{2} - 1 + \frac{1}{3} + \frac{1}{4} - \frac{1}{2} + \dots + \underbrace{\frac{1}{2n-1} + \frac{1}{2n} - \frac{1}{n}}_{=\frac{1}{2n(2n-1)} > 0} + \dots > 0?$$

Dále tu je nekonečná tabulka s položkami $-1, 0$ a 1

1	-1	0	0	0	...	$\sum = 0$
0	1	-1	0	0	...	$\sum = 0$
0	0	1	-1	0	...	$\sum = 0$
0	0	0	1	-1	...	$\sum = 0$?
0	0	0	0	1	...	$\sum = 0$
\vdots	\vdots	\vdots	\vdots	\vdots	\ddots	\vdots
$\sum = 1$	$\sum = 0$	$\sum = 0$	$\sum = 0$	$\sum = 0$...	$\sum = 1 \setminus 0$

a odlišnými celkovými součty po řádcích a po sloupcích.

- *Opakování logického a množinového značení.* Logické spojky: $\varphi \vee \psi \dots$ nebo, $\varphi \wedge \psi \dots$ a zároveň, $\varphi \Rightarrow \psi \dots$ implikace, $\varphi \Leftrightarrow \psi \dots$ ekvivalence, $\neg \varphi \dots$ negace. Např. vždy platí, že

$$\neg(\varphi \vee \psi) \Leftrightarrow \neg\varphi \wedge \neg\psi.$$

Důležité jsou i závorky a vazebná síla spojek. Kvantifikátory: $\forall x : \varphi(x) \dots$ pro každé x platí, že $\varphi(x)$, $\exists x : \varphi(x) \dots$ existuje takové x , že platí $\varphi(x)$. Např. vždy platí, že

$$\neg(\exists x : \varphi(x)) \iff \forall x : \neg\varphi(x).$$

Pomocí \emptyset značíme prázdnou množinu a značení $x \in A$ znamená, že množina x je prvkem množiny A . Množinu M zapíšeme výčtem jejích prvků, např.

$$M = \{a, b, 2, \{\emptyset, \{\emptyset\}\}, \{a\}\}$$

(kolik jich M má?), nebo pomocí nějaké jejich vlastnosti, např. pro $\mathbb{N} := \{1, 2, 3, \dots\}$ je

$$M = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N} : n = 2 \cdot m\}$$

množina (všech) sudých přirozených čísel.

Vztahy mezi množinami: $A \subset B \stackrel{\text{def}}{\iff} \forall x : x \in A \Rightarrow x \in B$
 \dots A je podmnožinou B , $\neg\exists x : x \in A \wedge x \in B \dots$ A a B jsou disjunktní, $A = B \iff (\forall x : x \in A \iff x \in B)$ je *axiom extenzionality* určující rovnost dvou množin.

Operace s množinami: $A \cup B := \{x \mid x \in A \vee x \in B\}$ je jejich sjednocení, $A \cap B := \{x \in A \mid x \in B\}$ je jejich průnik, $\bigcup A := \{x \mid \exists b \in A : x \in b\}$ je suma množiny A , $\bigcap A := \{x \mid \forall b \in A : x \in b\}$ je průnik množiny A , $A \setminus B := \{x \in A \mid x \notin B\}$ je (množinový) rozdíl množin A a B a

$$\mathcal{P}(A) := \{X \mid X \subset A\}$$

je potence (potenční množina) množiny A .

• *Uspořádané dvojice a funkce.* Pro každé dvě množiny A a B je množina

$$(A, B) := \{\{B, A\}, \{A\}\}$$

(*uspořádanou*) dvojicí množin A a B . Vždy platí, že

$$(A, B) = (A', B') \iff A = A' \wedge B = B' .$$

Uspořádanou trojici množin A , B a C lze definovat jako

$$(A, B, C) := (A, (B, C))$$

a podobně lze definovat usp. čtveřici (A, B, C, D) atd., ale lepší je vzít

$$(A, B, C) := \{(1, A), (2, B), (3, C)\}$$

atd. *Kartézský součin* množin A a B je množina

$$A \times B := \{(a, b) \mid a \in A, b \in B\} .$$

Každá množina $C \subset A \times B$ je (*binární*) *relace* mezi A a B . Místo $(a, b) \in C$ píšeme $a C b$, např. $2 < 5$. Pokud $A = B$, mluvíme o relaci na množině A .

Definice 1 (funkce) *Funkce (též zobrazení) f z množiny A do množiny B je každá taková uspořádaná trojice*

$$(A, B, f) ,$$

že $f \subset A \times B$ a pro každé $a \in A$ existuje právě jedno $b \in B$, že $a f b$. Píšeme, že $f: A \rightarrow B$ a $f(a) = b$.

Množina A je *definiční obor* funkce f a B je její *obor hodnot*. Prvek b je *hodnota* funkce f na jejím *argumentu* a . Pro $C \subset A$, resp. $C \subset B$, je

$$f[C] := \{f(a) \mid a \in C\} \subset B , \text{ resp.} \\ f^{-1}[C] := \{a \in A \mid f(a) \in C\} \subset A ,$$

obraz množiny C funkcí f , resp. *vzor* množiny C funkcí f .

• *Rodinky funkcí a operace s funkcemi. Posloupnost* (v množině X) je funkce

$$a: \mathbb{N} \rightarrow X .$$

Píšeme $(a_n) = (a_1, a_2, \dots) \subset X$ a $a_n := a(n)$, kde $n \in \mathbb{N} (= \{1, 2, \dots\})$. *Slovo* (nad abecedou X) je funkce

$$u: [n] \rightarrow X$$

pro nějaké $n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$, kde $[n] := \{1, 2, \dots, n\}$ a $[0] := \emptyset$. Pro $n = 0$ i $u = \emptyset$. Píšeme $u = a_1 a_2 \dots a_n$, kde $a_i := u(i)$ pro $i \in [n]$. (*Binární*) *operace* (na množině X) je funkce

$$o: X \times X \rightarrow X .$$

Místo $o((a, b)) = c$ píšeme $a o b = c$, např. $1 + 1 = 2$.

Funkce $f: X \rightarrow Y$ je *prostá* (též *injektivní, injekce*), pokud pro každé $a, b \in X$ máme, že $a \neq b \Rightarrow f(a) \neq f(b)$. Je *na* (též *surjektivní, surjekce*), pokud $f[X] = Y$. Je *vzájemně jednoznačná* (též *bijektivní, bijekce*), je-li prostá a na. Je *konstantní*, když existuje takové $c \in Y$, že $f(a) = c$ pro každé $a \in X$. Funkce $f: X \rightarrow X$ je *identická*, když $f(a) = a$ pro každé $a \in X$.

Je-li $f: X \rightarrow Y$ prostá funkce, její *inverzní funkce* (též *inverz*) je funkce $f^{-1}: f[X] \rightarrow X$ daná předpisem $f^{-1}(y) = x \iff f(x) = y$. Pro dvě (navazující) funkce

$$g: X \rightarrow Y \text{ a } f: Y \rightarrow Z$$

je odpovídající *složená funkce* (též *složenina*) funkce

$$f \circ g = f(g): X \rightarrow Z$$

daná předpisem $f(g)(a) := f(g(a))$, $a \in X$.

- *Lineární uspořádání, infima a suprema.*

Definice 2 (lineární uspořádání) *Relace $<$ na množině A , která je $(a, b, c \in A)$*

1. *ireflexivní: $\forall a : a \not< a$,*
2. *tranzitivní: $\forall a, b, c : a < b \wedge b < c \Rightarrow a < c$,*
3. *trichotomická: $\forall a, b : a < b \vee b < a \vee a = b$,*

se nazývá lineárním uspořádáním na množině A .

Všimněte si, že z 1 a 2 plyne, že v 3 vždy nastává právě jedna možnost. Značení $a \leq b$ znamená, že $a < b \vee a = b$. Dále $a > b$ znamená, že $b < a$, a podobně pro $a \geq b$. Lineární uspořádání na A označujeme jako $(A, <)$ nebo jako $(A, <_A)$.

Nechť $(A, <)$ je lineární uspořádání na A a $B \subset A$. Řekneme, že B je *shora omezená*, když pro nějaké $a \in A$ je $b \leq a$ pro každé $b \in B$. Prvek a pak je *horní mez* množiny B . Podobně se definují omezenost zdola a dolní meze. Množinu horních (resp. dolních) mezí množiny B označíme jako $H(B)$ (resp. $D(B)$). *Maximum* (též *největší prvek*) množiny B , které nemusí existovat, je takový prvek $b \in B$, že $\forall b' \in B : b' \leq b$. Podobně se definuje *minimum* (*nejmenší prvek*) množiny B . Tyto prvky značíme jako $\max(B)$ a $\min(B)$.

Definice 3 (supremum a infimum) *Nechť $(A, <)$ je lineární uspořádání na A a nechť $B \subset A$. Pokud $H(B) \neq \emptyset$ a existuje $\min(H(B))$, nazveme tento prvek supremem množiny B a označíme ho jako*

$$\sup(B) := \min(H(B)) .$$

Pokud $D(B) \neq \emptyset$ a existuje $\max(D(B))$, nazveme tento prvek infimem množiny B a označíme ho jako

$$\inf(B) := \max(D(B)) .$$

Například ve standardním lin. uspořádání reálných čísel $\min((0, 1))$ neexistuje, $\min([0, 1)) = 0$, $\inf((0, 1)) = \inf([0, 1)) = 0$ a $\sup(\mathbb{N})$ neexistuje, protože $H(\mathbb{N}) = \emptyset$.

- *Uspořádaná tělesa.* Potřebujeme je pro definici reálných čísel.

Definice 4 (uspořádané těleso) *Uspořádaným tělesem F rozumíme algebraickou strukturu*

$$F = (F, 0_F, 1_F, +_F, \cdot_F, <_F)$$

na množině F se dvěma různými význačnými prvky 0_F a 1_F v F , se dvěma operacemi $+_F$ a \cdot_F na F , s lineárním uspořádáním $<_F$ na F a takovou, že se splňují následující axiomy ($a, b, c \in F$).

1. $\forall a : a +_F 0_F = a \wedge a \cdot_F 1_F = a$ (prvek 0_F je neutrální v $+_F$ a prvek 1_F v \cdot_F).
2. *Obě operace $+_F$ a \cdot_F jsou asociativní a komutativní.*
3. $\forall a, b, c : a \cdot_F (b +_F c) = (a \cdot_F b) +_F (a \cdot_F c)$ (platí distributivní zákon).
4. $\forall a \exists b : a +_F b = 0_F, \forall a \neq 0_F \exists b : a \cdot_F b = 1_F$ (existují inverzní prvky).
5. $\forall a, b, c : a <_F b \Rightarrow a +_F c <_F b +_F c, \forall a, b : a, b >_F 0_F \Rightarrow a \cdot_F b >_F 0_F$ ($<_F$ respektuje obě operace).

Axiomy 1–4 jsou axiomy *tělesa*. Příkladem uspořádaného tělesa jsou *zlomky* (též *racionální čísla*) \mathbb{Q} :

$$\mathbb{Q} := \{m/n \mid m, n \in \mathbb{Z}, n \neq 0\},$$

kde $\mathbb{Z} := \{\dots, -1, 0, 1, \dots\}$ jsou *celá čísla*. Další příklad? Třeba

$$\mathbb{Q}(\sqrt{2}) := \{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\}.$$

Obě uspořádaná tělesa se liší, rovnice $x^2 = 2$ nemá řešení v \mathbb{Q} (jak ukážeme v následující pasáži), ale je řešitelná v $\mathbb{Q}(\sqrt{2})$.

- *Neúplnost uspořádaného tělesa \mathbb{Q} .*

Definice 5 (úplnost) *Uspořádané těleso je úplné, pokud jeho každá neprázdná a shora omezená podmnožina má supremum.*

Ukážeme, že uspořádané těleso \mathbb{Q} úplné není, plyne to z následující věty. Pro její důkaz si připomeneme *princip indukce*, že každá neprázdná podmnožina $X \subset \mathbb{N}$ má minimum.

Věta 6 ($\sqrt{2} \notin \mathbb{Q}$) *Rovnice*

$$x^2 = 2$$

nemá v oboru zlomků řešení.

Důkaz. Pro spor necht' $(a/b)^2 = 2$ pro nějaké $a, b \in \mathbb{N}$. Tedy

$$a^2 = 2b^2$$

a podle principu indukce můžeme předpokládat, že číslo a v této rovnici je minimální. Číslo a^2 je sudé, tedy i a je sudé a $a = 2c$ pro nějaké $c \in \mathbb{N}$. Pak ale

$$(2c)^2 = 2b^2 \rightsquigarrow 4c^2 = 2b^2 \rightsquigarrow b^2 = 2c^2 .$$

Protože $b < a$, dostali jsme řešení vysazené rovnice s číslem nalevo menším než a , což je spor. □

Důsledek 7 (neúplnost \mathbb{Q}) *Uspořádané těleso*

$$\mathbb{Q} = (\mathbb{Q}, 0, 1, +, \cdot, <)$$

racionálních čísel není úplné.

Důkaz. Ukážeme, že množina zlomků

$$X := \{r \in \mathbb{Q} \mid r^2 < 2\}$$

je neprázdná a shora omezená, ale nemá supremum. První dvě vlastnosti jsou jasné, $1 \in X$ a $x < 2$ pro každé $x \in X$.

Pro spor vezmeme zlomek $s := \sup(X)$. Když $s^2 > 2$, existuje zlomek $r > 0$, že $s - r > 0$ a stále $(s - r)^2 > 2$. Pak ale $s - r > x$ pro každé $x \in X$ a máme spor s tím, že s je nejmenší horní mez množiny X . Když $s^2 < 2$, existuje zlomek $r > 0$, že stále $(s + r)^2 < 2$. Tedy $s + r \in X$ a máme spor s tím, že s je horní mez množiny X . Podle trichotomie uspořádání musí být, že $s^2 = 2$. To je ale podle předchozí věty nemožné. \square

- *Úplné uspořádané těleso \mathbb{R} .*

Věta 8 (existence \mathbb{R}) *Existuje jediné (viz věta 9) úplné uspořádané těleso*

$$\mathbb{R} = (\mathbb{R}, 0_{\mathbb{R}}, 1_{\mathbb{R}}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, <_{\mathbb{R}}).$$

Nazýváme ho tělesem reálných čísel.

Připomínáme vlastnost/axiom úplnosti: je-li $X \subset \mathbb{R}$ neprázdná množina a existuje-li nějaké $y \in \mathbb{R}$, že $x \leq_{\mathbb{R}} y$ pro každé $x \in X$, potom má množina takových čísel y nejmenší prvek. Index \mathbb{R} budeme u neutrálních prvků, operací a uspořádání vynechávat. Každé uspořádané těleso obsahuje jako své prvotěleso (nejmenší podtěleso) kopii racionálních čísel \mathbb{Q} .

Vysvětlíme, jak úplnost uspořádaného tělesa ho činí v jistém smyslu jednoznačným. Bijekce $f: F \rightarrow G$ mezi dvěma usp. tělesy

je jejich *izomorfismus*, pokud $f(0_F) = 0_G$, $f(1_F) = 1_G$ a pro každé $x, y \in F$ je

$$f(x +_F y) = f(x) +_G f(y), \quad f(x \cdot_F y) = f(x) \cdot_G f(y)$$

a

$$x <_F y \iff f(x) <_G f(y).$$

Věta 9 (jednoznačnost \mathbb{R}) Každá dvě úplná uspořádaná tělesa jsou izomorfní.

Důsledek 10 ($\sqrt{2} \in \mathbb{R}$) Rovnice

$$x^2 = 2$$

má v oboru reálných čísel řešení.

Důkaz. Vezmeme podobnou množinu jako v důkazu důsledku 7, tedy

$$X := \{a \in \mathbb{R} \mid a^2 < 2\}.$$

Podle věty 8 existuje supremum $s := \sup(X) \in \mathbb{R}$. Stejně argumenty jako v onom důkazu ukazují, že nenastává ani $s^2 < 2$ ani $s^2 > 2$. Tedy $s^2 = 2$. \square

V pozdější přednášce dokážeme dalekosáhlé zobecnění předchozího výsledku. Spojitost funkce v následujícím tvrzení znamená (později to definujeme přesně), že malá změna argumentu funkce způsobí malou změnu hodnoty.

Tvrzení 11 (Bolzano–Cauchyova věta) *Nechť $a \leq b$ jsou reálná čísla a*

$$f: [a, b] \rightarrow \mathbb{R}$$

je taková spojitá funkce, že $f(a)f(b) \leq 0$. Potom existuje číslo $c \in [a, b]$, že $f(c) = 0$.

- *Spočetné a nespočetné množiny, nespočetnost \mathbb{R} .* Množina X je nekonečná, když existuje prostá funkce $f: \mathbb{N} \rightarrow X$. Když X není nekonečná, je konečná. Dá se dokázat, že pro každou konečnou množinu X existuje surjekce $f: \mathbb{N} \rightarrow X$.

Definice 12 ((ne)spočetné množiny) *Pojmenujeme následující druhy množin X .*

- 1. X je spočetná, když existuje bijekce $f: \mathbb{N} \rightarrow X$.*
- 2. X je nejvýše spočetná, je-li konečná nebo spočetná.*
- 3. X je nespočetná, když není nejvýše spočetná.*

Věta 13 (spočetnost \mathbb{Q}) *Množina zlomků je spočetná.*

Důkaz. Pro zlomek $\frac{m}{n} \in \mathbb{Q}$ v základním tvaru, to jest když $n > 0$ a když čísel $m \in \mathbb{Z}$ a jmenovatel n jsou nesoudělná čísla (tj. největší číslo $k \in \mathbb{N}$ dělicí současně m i n je $k = 1$), definujeme normu $\|\frac{m}{n}\| := |m| + n \in \mathbb{N}$ a množiny

$$Z_j := \{z_{1,j} < z_{2,j} < \cdots < z_{k_j,j} \mid z_{i,j} \in \mathbb{Q}, \|z_{i,j}\| = j\}, j \in \mathbb{N}.$$

Například

$$Z_5 = \left\{ -\frac{4}{1} < -\frac{3}{2} < -\frac{2}{3} < -\frac{1}{4} < \frac{1}{4} < \frac{2}{3} < \frac{3}{2} < \frac{4}{1} \right\} \text{ a } k_5 = 8 .$$

Zde $\frac{0}{5} \notin Z_5$, protože čísla 0 a 5 nejsou nesoudělná. Patrně $j \neq j' \Rightarrow Z_j$ a $Z_{j'}$ jsou disjunktní, každá Z_j je konečná (a $\neq \emptyset$) a $\bigcup_{j \in \mathbb{N}} Z_j = \mathbb{Q}$. Zobrazení $f: \mathbb{N} \rightarrow \mathbb{Q}$ definujeme jako

$$f(1) = z_{1,1}, f(2) = z_{2,1}, \dots, f(k_1) = z_{k_1,1}, f(k_1 + 1) = z_{1,2}, \dots$$

— hodnoty funkce f nejprve projdou k_1 seřazených zlomků v Z_1 , pak k_2 seřazených zlomků v Z_2 , a tak dál. Obecná hodnota je pro $j \in \mathbb{N}$ rovna

$$f(k_1 + k_2 + \dots + k_{j-1} + i) = z_{i,j}, \quad i \in [k_j],$$

kde pro $j = 1$ tento argument funkce f definujeme jako i . Lehce se vidí, že f je bijekce. \square

Dokážeme nespočetnost \mathbb{R} . Odvodíme ji jako důsledek základního výsledku o množinách, který ukazuje, že potence $\mathcal{P}(X)$ je podstatně větší množina než X .

Věta 14 (Cantorova) *Pro žádnou množinu X neexistuje surjekce*

$$f: X \rightarrow \mathcal{P}(X)$$

z ní na její potenci.

Důkaz. Pro spor buď X množina a $f: X \rightarrow \mathcal{P}(X)$ buď surjekce. Uvážíme podmnožinu

$$Y := \{x \in X \mid x \notin f(x)\} \subset X .$$

Protože f je na, existuje takové $y \in X$, že $f(y) = Y$. Pokud $y \in Y$, podle definice množiny Y platí, že $y \notin f(y) = Y$. Pokud $y \notin Y = f(y)$, má y vlastnost prvků množiny Y a $y \in Y$. V obou případech to je spor. \square

Jako $\{0, 1\}^{\mathbb{N}}$ označíme množinu (všech) posloupností $(a_n) \subset \{0, 1\}$.

Důsledek 15 (o 0-1 posloupnostech) Surjekce

$$f: \mathbb{N} \rightarrow \{0, 1\}^{\mathbb{N}}$$

neexistuje.

Důkaz. Zobrazení $g: \{0, 1\}^{\mathbb{N}} \rightarrow \mathcal{P}(\mathbb{N})$, $g((a_n)) := \{n \in \mathbb{N} \mid a_n = 1\}$, je patrně bijekce. Kdyby existovala uvedená surjekce f , složenina $g \circ f$ by byla funkce z \mathbb{N} na $\mathcal{P}(\mathbb{N})$ popírající větu 14. \square

Důsledek 16 (nespočetnost \mathbb{R}) Množina reálných čísel je nespočetná.

Důkaz. Opět dokážeme o něco víc, neexistenci surjekce $f: \mathbb{N} \rightarrow \mathbb{R}$. Reálná čísla si teď představujeme jako nekonečné desetinné rozvoje a vezmeme množinu

$$X := \{0.a_1a_2\dots \mid a_n \in \{0, 1\}\} \subset \mathbb{R}$$

těch, co mají za desetinnou tečkou jen nuly a jedničky. Zřejmě máme bijekci $g: X \rightarrow \{0, 1\}^{\mathbb{N}}$. Kdyby uvedená surjekce f existovala, snadno z ní získáme surjekci $f_0: \mathbb{N} \rightarrow X$ (položíme $f_0(n) := f(n)$ pro $f(n) \in X$, jinak $f_0(n) := 0.000\dots$). Pak by ale složenina $g \circ f_0$ šla z \mathbb{N} na $\{0, 1\}^{\mathbb{N}}$ a popírala by důsledek 15. \square

- *Trochu o \mathbb{C} .* Připomeneme komplexní čísla a jednu jejich stěžejní vlastnost. Je dobře známo, že

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}, \quad i = \sqrt{-1},$$

a že \mathbb{C} s neutrálními prvky $0_{\mathbb{C}} := 0 + 0i$ a $1_{\mathbb{C}} := 1 + 0i$ a operacemi

$$(a + bi) +_{\mathbb{C}} (c + di) := (a +_{\mathbb{R}} c) + (b +_{\mathbb{R}} d)i$$

a

$$(a + bi) \cdot_{\mathbb{C}} (c + di) := (a \cdot_{\mathbb{R}} c -_{\mathbb{R}} b \cdot_{\mathbb{R}} d) + (a \cdot_{\mathbb{R}} d +_{\mathbb{R}} b \cdot_{\mathbb{R}} c)i$$

tvorí těleso. To má následující důležitou vlastnost, platí pro něj takzvaná Základní věta algebry.

Věta 17 (ZVA) *Každý nekonstantní komplexní polynom $p(z)$ v $\mathbb{C}[z]$ (tj. s komplexními koeficienty) má kořen, takové číslo $z_0 \in \mathbb{C}$, že*

$$p(z_0) = 0.$$

DĚKUJI ZA POZORNOST