Přednáška 2, 10. října 2014

Číselné obory. Dobře známe číselné obory

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}\,.$$

Zde $\mathbb{N} = \{1, 2, \dots\}$ jsou *přirozená čísla*, $\mathbb{Z} = \mathbb{N} \cup \{0, -1, -2, \dots\}$ *celá čísla* (symbol pro ně pochází z německého die Zahlen), $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$ jsou *racionální čísla* čili *zlomky*, $\mathbb{R}$ *reálná čísla* a $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ s $i^2 = -1$ jsou čísla *komplexní*, jimiž se dále podrobně zabývat nebudeme.

Co je $\mathbb{R}$ řeknu za chvíli. Prvky množiny $\mathbb{Q}$ jsou přesně řečeno třídy vzájemně ekvivalentních zlomků, přičemž $\frac{a}{b}$ a $\frac{c}{d}$ jsou ekvivalentní, právě když $ad - bc = 0$. Každá taková třída má jako reprezentanta *zlomek* $\frac{a}{b}$ *v základním tvaru*, v němž $b > 0$ a čitatel a a jmenovatel b jsou nesoudělná čísla. Rozšíření číselného oboru do většího je vždy motivováno řešitelností rovnic. Rovnice $5 + x = 3$ nemá řešení v $\mathbb{N}$, ale v $\mathbb{Z}$ již ano ($x = -2$), $5x = 3$ ho nemá v $\mathbb{Z}$, ale má ho ve $\mathbb{Q}$ ($x = \frac{3}{5}$), $x^2 = 3$ je neřešitelná ve $\mathbb{Q}$, ale řešitelná v $\mathbb{R}$ ($x = \sqrt{3}$) a $x^2 = -3$ v $\mathbb{R}$ nemá řešení, ale v $\mathbb{C}$ ho má ($x = i\sqrt{3}$).

Ze čtyř hořejších inkluzí je zcela přesná jen první, $\mathbb{N} \subset \mathbb{Z}$, zbylým třem rozumíme jako vnořením, kdy skutečnou inkluzi dostaneme změnou formátu prvku: číslo $z \in \mathbb{Z}$ je prvek $\mathbb{Q}$, když ho napíšeme jako $\frac{z}{1}$, zlomek $\alpha \in \mathbb{Q}$ je prvkem $\mathbb{R}$ po napsání v desetinném zápisu (při pojetí $\mathbb{R}$ jako desetinných rozvojů), např. $\frac{1}{9} = 0.11111\dots$, a číslo $a \in \mathbb{R}$ je prvek $\mathbb{C}$, když ho napíšeme jako $a + 0i$.

Na všech uvedených číselných oborech máme aritmetické operace sčítání $+$ a násobení $\cdot$, spolu s binární relací $<$ uspořádání (na $\mathbb{C}$ relace $<$ není). Vzhledem k oběma operacím $(\mathbb{Z}, +, \cdot)$ tvoří to, čemu algebraici říkají *okruh*: obě operace jsou asociativní a komutativní, platí distributivita, obě mají neutrální prvky a sice 0 a 1, a při sčítání má každý prvek inverz. $(\mathbb{Q}, +, \cdot, <)$ je *uspořádané těleso*: je to okruh a navíc každý nenulový prvek má při násobení inverz a relace $<$ splňuje: (i) $a < b, b < c \Rightarrow a < c$, (ii) ze tří možností $a < b, a = b, a > b$ vždy nastává právě jedna, (iii) $a < b \Rightarrow a + c < b + c$ a (iv) $a < b, c > 0 \Rightarrow ac < bc$. Rovněž $(\mathbb{R}, +, \cdot, <)$ je uspořádané těleso. Co má $\mathbb{R}$ navíc proti $\mathbb{Q}$ je (1) úplnost (má ucpány díry, které jsou ve $\mathbb{Q}$) a (2) nespočetnost (je mnohem početnější než $\mathbb{Q}$). Obé bude vysvětleno dále. Je třeba říci, že přechod od oboru $\mathbb{Q}$ k oboru $\mathbb{R}$ je ve srovnání s ostatními třemi přechody skok na naprosto odlišnou úroveň.

Reálná čísla jako nekonečné desetinné rozvoje. Jedno z možných pojetí množiny $\mathbb{R}$ je to, že reálná čísla jsou nekonečné desetinné rozvoje, jako

třeba

$$0 = -0.000\ldots,\ -5089.33506\ldots,\ +40.125000\ldots \quad \text{či} \quad -\pi = -3.141592\ldots\ .$$

(Později se zmíním o dvou dalších — a známějších — zavedeních reálných čísel, o Cantorových fundamentálních posloupnostech a Dedekindových řezech.) Reálné číslo a je tedy oznaménkovaná nekonečná posloupnost *cifer* a_n s $n = 0, 1, 2, \ldots$,

$$a = \pm a_0.a_1a_2a_3\ldots\ ,$$

kde $a_0 \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$ a pro $n > 0$, $a_n \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Např. třetí z čísel nahoře má znaménko $+$ a cifry $a_0 = 40$, $a_1 = 1$, $a_2 = 2$, $a_3 = 5$ a $a_n = 0$ pro $n \geq 4$ (je to vlastně $\frac{321}{8}$). Konvence zápisu je, že znaménko $+$ se nepíše a nekonečný úsek nul vynechává, takže píšeme jen 40.125. Číslo nula, jehož všechny cifry jsou 0, může mít obě znaménka, $-0.000\ldots$ a $+0.000\ldots$ ztotožňujeme.

Tento zápis je skoro vždy jednoznačný, ale, jak známo, některá reálná čísla mají zápisy dva: kromě $-0.000\cdots = +0.000\ldots$ též

$$-40.125000\ldots = -40.124999\ldots,\ 1.000\ldots = 0.999\ldots$$

a podobně. Nastává to přesně pro nenulové *končící desetinné rozvoje* $a = \pm a_0.a_1a_2\ldots$, v nichž pro nějaké $k \in \mathbb{N}_0$ je $a_k > 0$, ale $a_{k+1} = a_{k+2} = \cdots = 0$. Pak $b = \pm b_0.b_1b_2\ldots$ (totéž znaménko jako v a), kde $b_n = a_n$ pro $n < k$, $b_k = a_k - 1$ a $b_n = 9$ pro $n > k$, je totéž reálné číslo jako a. Jak tedy rozumět rovnostem jako $1 = 0.999\ldots$? Samozřejmě, že napravo a nalevo od $=$ máme dosti různé věci, nekonečné slovo a jednopísmenné slovo. Z hlediska operací $+$ a $\cdot$ v $\mathbb{R}$ i porovnávání $<$ to ale pro nás je totéž reálné číslo. Stejný „paradox“ se objevuje už v $\mathbb{Q}$, kde vesele píšeme $\frac{12}{4} = \frac{-6}{-2}$ a podobně, i když napravo a nalevo od $=$ jsou dost odlišné dvojice celých čísel, a myslíme tím, že z hlediska aritmetických operací a porovnávání v $\mathbb{Q}$ hrají roli téhož racionálního čísla.

Připomenu, jak reálná čísla porovnáváme relací $<$, což jistě každý ví. Nechť $\alpha, \beta \in \mathbb{R}$ jsou různá čísla (speciálně nemáme zápisy jako $\alpha = 1.000\ldots$ a $\beta = 0.999\ldots$). Pro jednoduchost buďte obě čísla kladná, se znaménkem $+$, obecný případ se na tento snadno převede (rozmyslete si jak). Pak

$$\alpha < \beta \iff \exists k \in \mathbb{N}_0 :\ \alpha_j = \beta_j \text{ pro } 0 \leq j < k, \text{ ale } \alpha_k < \beta_k\ .$$

Nejde o nic jiného než o *lexikografické* (slovníkové) uspořádání podle cifer.

Úloha: *dokažte, že když $\alpha, \beta \in \mathbb{R}$ jsou různá čísla, která mohou mít dva zápisy, pak výsledek jejich porovnání — buď $\alpha < \beta$ anebo $\alpha > \beta$ — je týž bez ohledu na volbu zápisu (tedy nikdy se nestane něco jako, že v jednom zápisu $\alpha = 1.000\ldots > 0.9997589\cdots = \beta$ a ve druhém $\alpha = 0.999\ldots < 0.9997589\cdots = \beta$, což v tomto příkladu skutečně pravda není).*

Jak se taková reálná čísla sčítají a násobí? Stručně řečeno, máme-li spočítat $\alpha \circ \beta$, kde $\alpha = \pm\alpha_0.\alpha_1\alpha_2\ldots$ a $\beta = \pm\beta_0.\beta_1\beta_2\ldots$ jsou dvě reálná čísla a $\circ$ je sčítání nebo násobení, usekáváme jejich zápisy po n-té cifře (tj. další cifry nahradíme nulami, znaménka samozřejmě neměníme), $n = 0, 1, 2, \ldots$, a počítáme posloupnost částečných součtů či součinů (rozmyslete si, že tyto částečné součty či součiny počítáme vlastně v rámci $\mathbb{Q}$)

$$\pm\alpha_0 \circ \pm\beta_0,\ \pm\alpha_0.\alpha_1 \circ \pm\beta_0.\beta_1,\ \pm\alpha_0.\alpha_1\alpha_2 \circ \pm\beta_0.\beta_1\beta_2,\ \ldots\ .$$

Dá se ukázat, že pro každé $k \in \mathbb{N}_0$ se k-tá cifra výsledků pro dostatečně velké n přestane měnit, stabilizuje se, a totéž nastane pro znaménko. Tím je výsledek operace $\alpha \circ \beta$ dobře a jednoznačně definován. Například pro $\alpha = +1.000\ldots$ a $\beta = -0.999\ldots$ (tj. $\alpha = -\beta$) částečné součty pro $\alpha+\beta$ vycházejí

$$+1,\ +0.1,\ +0.01,\ +0.001$$

a tak dál, takže vskutku $\alpha + \beta = +0.000\cdots = 0$. Vlastnosti aritmetických operací a uspořádání na $\mathbb{R}$ podrobně dokazovat a odvozovat nebudu, není to tak lehké, jak se člověku na začátku zdá. Dá se ale dokázat následující věta.

Věta (aritmetika $\mathbb{R}$). *$(\mathbb{R}, +, \cdot, <)$, kde $\mathbb{R}$ je množina oznaménkovaných nekonečných desetinných rozvojů, tvoří uspořádané těleso (po aplikaci ztotožnění $-0.000\cdots = +0.000\ldots$ a všech ztotožnění typu $1.000\ldots = 0.999\ldots$).*

Jako příklad asociativity sčítání v $\mathbb{R}$ máme třeba (vypočteno výše popsaným postupem):

$$(-0.999\cdots + 1) + 0.999\cdots = +0.000\cdots + 0.999\cdots = 0.999\ldots\ ,$$

což je totéž jako

$$-0.999\cdots + (1 + 0.999\ldots) = -0.999\cdots + 1.999\cdots = 1.000\ldots\ .$$

Suprema a infima, úplnost $\mathbb{R}$. Když $X \subset \mathbb{R}$ a $c \in X$, pak $c = \min(X)$, c je *minimum* nebo též *nejmenší prvek* X, pokud $c \leq a$ pro každé $a \in X$.

Podobně se definuje $\max(X)$, *maximum* nebo *největší prvek* X. Číslo $c \in \mathbb{R}$ je *horní mez* množiny $X \subset \mathbb{R}$, když $c \geq a$ pro každé $a \in X$. Podobně se definuje *dolní mez*. Když $X \subset \mathbb{R}$ a $c \in \mathbb{R}$, pak c je *supremum* množiny X, $c = \sup(X)$, když

$$c = \min(\{\text{horní meze množiny } X\}) \ ,$$

tedy c je nejmenší horní mez X. Supremum X nemusí v X ležet a když existuje, je určeno jednoznačně. Ještě jednou řečeno, $c = \sup(X)$, právě když

1. pro každé $a \in X$ je $a \leq c$ (tj. c je horní mez X) a
2. pro každé $d \in \mathbb{R}$, $d < c$, existuje $a \in X$, že $a > d$ (tj. c nelze nijak zmenšit na d, aby zůstalo horní mezí, c je nejmenší horní mez X).

Podobně se definuje *infimum* množiny $X \subset \mathbb{R}$:

$$\inf(X) = \max(\{\text{dolní meze množiny } X\}) \ ,$$

je to největší dolní mez množiny X. Úplně stejně definujeme supremum a infimum pro podmnožiny $\mathbb{Q}$ v uspořádání $(\mathbb{Q}, <)$ (a obecně v každé lineárně nebo i částečně uspořádané množině). Množina $X \subset \mathbb{R}$ je *shora omezená*, má-li alespoň jednu horní mez. Podobně se definuje *omezenost zdola*. Následující výsledek je základní vlastnost reálných čísel, kterou racionální čísla nemají.

Věta (úplnost $\mathbb{R}$). *Každá neprázdná a shora omezená množina reálných čísel má supremum.*

Podobně má každá neprázdná a zdola omezená množina reálných čísel infimum. Před důkazem věty uvedu pár příkladů. Když $X = \emptyset$, rovná se množina horních mezí X celému $\mathbb{R}$ (pro každé $c \in \mathbb{R}$ platí implikace $a \in X \Rightarrow a \leq c$). Nejmenší horní mez tedy neexistuje a $\sup(\emptyset)$ též neexistuje. Když $X = \mathbb{N}$, množina horních mezí X je prázdná, protože X není shora mezená, a $\sup(\mathbb{N})$ neexistuje. Věta říká, že prázdnost X a neomezenost X shora jsou jediné dvě překážky pro existenci suprema. V rámci $\mathbb{R}$,

$$\sup([0,1]) = \sup([0,1)) = \sup([0,1) \cap \mathbb{Q}) = 1 \ .$$

V rámci číselného oboru $\mathbb{Q}$ věta o supremu neplatí:

Tvrzení (neúplnost $\mathbb{Q}$). *Množina $X = \{\alpha \in \mathbb{Q} \mid \alpha > 0, \alpha^2 < 2\} \subset \mathbb{Q}$ je neprázdná a shora omezená, ale nemá v $\mathbb{Q}$ supremum.*

Důkaz. Jistě $1 \in X$ a $a < 2$ pro každé $a \in X$, což dokazuje první část. Nechť $c \in \mathbb{Q}$ je libovolné pevné číslo. Ukážu, že není supremem množiny X. Když $c \leq 0$, jistě není horní mezí X, a proto nechť $c > 0$.

1. Nechť $c^2 < 2$. Pak existuje $\beta \in \mathbb{Q}$, $\beta > 0$, že stále $(c+\beta)^2 < 2$. Pak ale $c + \beta \in X$ a $c + \beta > c$, takže c není horní mezí X. (Potřebujeme, aby číslo $\beta > 0$ splňovalo, že $2c\beta + \beta^2 < 2 - c^2$. Protože pro $0 < \beta < 1$ je $\beta^2 < \beta$, číslo $\beta = (2-c^2)/(2c+2) < 1$ vyhovuje — rozmyslete si proč.)

2. Nechť $c^2 = 2$. Jak jsme na minulé přednášce dokázali, tento případ nenastává.

3. Nechť $c^2 > 2$. Podobně jako v 1. případu existuje $\beta \in \mathbb{Q}$, $0 < \beta < c$, že stále $(c-\beta)^2 > 2$. Pro každé $a \in X$ máme $a^2 < 2 < (c-\beta)^2$, tedy $a < c - \beta$. Takže $c - \beta$ je horní mez X a vzhledem k $c - \beta < c$ není číslo c nejmenší horní mez. (Odhad, jak malé β stačí vzít, je zde přenechán čtenáři jako úloha.)

Žádné $c \in \mathbb{Q}$ tedy není supremem naší množiny X. □

Důkaz věty o úplnosti $\mathbb{R}$. Nechť $X \subset \mathbb{R}$ je libovolná neprázdná a shora omezená množina reálných čísel. Budu postupně definovat cifry jistého čísla $c \in \mathbb{R}$, které se ukáže být supremem X. Bez újmy na obecnosti jsou všechna čísla v X kladná (obecný případ se na tento snadno převede). Položím $X_0 = X$ a pro $n = 0, 1, 2, \ldots$ postupně definuju cifry c_n a množiny $X_n \subset X$,

$$c_n := \max(\{\alpha_n \mid \alpha \in X_n\}) \quad \text{a} \quad X_{n+1} := \{\alpha \in X_n \mid \alpha_n = c_n\} .$$

Tvrdím, že číslo

$$c = +c_0.c_1c_2\ldots$$

je dobře definované a je supremem X. Protože je X shora omezená, je shora omezená (a tedy konečná) i množina cifer $\{\alpha_0 \mid \alpha \in X_0\} \subset \mathbb{N}_0$ a cifra c_0 je dobře definovaná. Pro $n > 0$ už beru maximum z nějaké podmnožiny $\{0, 1, \ldots, 9\}$ a jediným problémem by bylo, kdyby $X_n = \emptyset$. Z definice těchto množin ale snadno indukcí plyne, že jsou všechny neprázdné. Číslo c je tedy korektně definované.

Ukažme, že c je horní mez X. Nechť $\alpha \in X = X_0$. Z definice c_0 plyne, že $\alpha_0 \leq c_0$. Když $\alpha_0 < c_0$, pak $\alpha < c$. Když $\alpha_0 = c_0$, pak z definice c_1 a X_1 plyne, že $\alpha \in X_1$ a $\alpha_1 \leq c_1$. Když $\alpha_1 < c_1$, pak $\alpha < c$. Když $\alpha_1 = c_1$, pak z definice c_2 a X_2 plyne, že $\alpha \in X_2$ a $\alpha_2 \leq c_2$. A tak dále. Když pro nějaké

$n \in \mathbb{N}_0$ (poprvé) nastane $\alpha_n < c_n$, pak $\alpha < c$. Když pro každé $n \in \mathbb{N}_0$ stále $\alpha_n = c_n$, pak $\alpha = c$ (a v tomto případu je $c = \alpha = \max(X)$).

Ukažme, že c je nejmenší horní mez X. Nechť $d \in \mathbb{R}$ je libovolné číslo s $d < c$. Lze předpokládat, že $d > 0$. Podle definice uspořádání na $\mathbb{R}$ existuje takové $n \in \mathbb{N}_0$, že $d_j = c_j$ pro každé $0 \leq j < n$, ale $d_n < c_n$. Vezmeme $\alpha \in X_n$, že $\alpha_n = c_n$. Z definice množiny X_n plyne, že $\alpha_j = c_j$ pro každé $0 \leq j \leq n$. To ale znamená, že $d < \alpha \in X$. Takže c je nejmenší horní mez X. □

Důsledek (existence $\sqrt{2}$ v $\mathbb{R}$). *Rovnice $x^2 = 2$ má v oboru $\mathbb{R}$ řešení.*

Důkaz. Položme, v oboru $\mathbb{R}$,

$$c := \sup(\{a \in \mathbb{R} \mid a > 0, a^2 < 2\}) .$$

Supremum je korektně definované, protože daná množina je neprázdná a shora omezená (obsahuje číslo 1 a její každý prvek je menší než např. 2). Stejně jako v předešlém tvrzení se ukáže, že případy $c^2 > 2$ a $c^2 < 2$ jsou nemožné, protože při nich c není supremem dané množiny. Nutně $c^2 = 2$ a c je řešení dané rovnice. □