Teorie množin

Pojďme se podívat, proč chceme nadefinovat pěknou teorii množin.

Nejprve si nadefinujme množiny naivním způsobem, tedy množina je něco, co obsahuje nějaké prvky.

A díky tomu nám vznikly nové paradoxy. Pojďme se na ně podívat.

Russelův paradox.

Pokud množina x obsahuje sama sebe ($x \in x$), pak je x zvláštní, jinak je obyčejné.

Předpokládejme množinu $O = \{\text{všechny obyčejné množiny}\}$.

Pakliže $O \in O$, potom je O zvláštní, tedy potom $O \notin O$. Naopak, když $O \notin O$, potom je O obyčejná, a tedy $O \in O$. Tím dostáváme spor.

Viníkem tohoto paradoxu je právě definice $O = \{\text{všechny obyčejné množiny}\}$.

Berryho paradox.

Mějme n jako nejmenší kladné celé číslo, které nemůžeme definovat použitím nejvýše 100 znaky.

Každá neprázdná množina přirozených čísel obsahuje nejmenší prvek. Potom $n = \min D$ a $D = \{x \in \mathbb{N} \mid x \text{ nemůžeme def.}\dots\}$.

Pojďme se podívat na důsledky Russelova paradoxu. Například holič holí právě ty muže, kteří se neholí sami. Kdo holí holiče? Podobně *Halting problém* nelze algoritmicky rozhodnout.

Věta (*Banach-Tarski***).** Mějme B jednotkovou kouli v $\mathbb{R}^d$. Jestliže máme $B = B_1 \cup B_2 \cup \ldots \cup b_n$ rozklad a $B'_1, B'_2, \ldots, B'_n$ s nimi kongruentními, sjednocením $\bigcup B_i$ získáme 2 stejné množiny B.

Tato věta platí, jestliže předpokládáme, že rovněž platí axiom výběru. Je dokonce s ním ekvivalentní.

Pojďme se podívat na různá nekonečna. V roce kolem 1870 Cantor dokázal, že reálných čísel je více, než přirozených čísel. Dále rovněž dokázal, že algebraických čísel (čísel takových, co jsou kořeny přirozených polynomů) je stejně mnoho, jako přirozených čísel.

Tímto jsme získali nekonstruktivní důkaz existence transcendentních (nealgebraických) čísel.

Dále kolem 1850 poprvé Bolzano uvažoval o množinách.

Tímto se dostáváme první definici množin:

Definice. Množina je skupina definitivních, různých objektů naší intuice nebo myšlenky.

Tato definice není však moc pěkně matematická. Nebojme se však, kolem roku 1900 přišel Frege a jeho

Definice: *Neomezená abstrakce.* Množina je $\{x \mid P(x)\}$ pro vlastnost P.

Takovou definici už krásně získáváme různé množiny: $\{x \mid x \neq x\} = \emptyset$, $\{x \mid x = a \vee x = b\} = \{a, b\}$ nebo $\{x \mid x \subseteq y\} = P(y)$ potenční množina. A další.

Množina $\{x \mid x \notin x\}$ je ale spor. Proto bychom potřebovali naši definici ještě zlepšit!

A tak v roce 1908 přišel Zermelo s axiomatickou teorií množin, zvanou Zermelo-Frankelovou. V ní jsou množiny definované tentokráte *omezenou* abstrakcí.

1 Axiomatická teorie množin

Definice. Jazykem teorie množin bude binární relační symbol $\in$ s rovností.

Kromě symbolů jazyka si rovněž zavedeme zkratky jako $\emptyset, \subset, \subseteq, \notin$ a podobně.

Axiom existence

Existuje množina bez prvků.

$$(\exists x)(\forall y)\neg(y \in x)$$

Axiom extenzionality

Množiny jsou jednoznačně určeny svými prvky.

$$(\forall X)(\forall Y)((\forall x)(x \in X \Leftrightarrow x \in Y) \Rightarrow X = Y)$$

Opačná implikace platí díky definici rovnosti z logiky.

Věta. Existuje právě jedna množina bez prvků, dále zvána prázdná množina a značena $\emptyset$.

Důkaz. Axiom existence implikuje, že existuje X bez prvků.
Dále mějme Y rovněž bez prvků. Potom díky axiomu extenzionality nutně platí, že $X = Y$.

Schéma axiomu vydělení

Mějme $P(x)$ predikátovou formuli prvního řádu, kde x je volná proměnná. Potom

$$(\forall A)(\exists B)((\forall x)(x \in B \Leftrightarrow x \in A \wedge P(x))).$$

Věta. Množina B z axiomu vydělení je pro danou formuli $P(x)$ a množinu A jednoznačně určená.

Důkaz. Předpokládejme, že $(\exists B)_1, (\exists B)_2$ splňující axiom vydělení. Všimněme si, že $\forall x : x \in B_1 \Leftrightarrow x \in B_2$. Potom díky axiomu extenzionality $B_1 = B_2$. ♡

Díky této větě lze množina B z axiomu vydělení napsat jako $B = \{x \in A \mid P(x)\}$.

Věta (*Existence průniku*). $(\forall P)(\forall Q)(\exists R)((\forall X)(x \in R \Leftrightarrow (x \in P \wedge x \in Q)))$. Dále je R jednoznačně určená a $R = P \cap Q$.

Důkaz. $R = \{x \in P \mid x \in Q\}$. Tedy věta je instance axiomu vydělení pro $P(x) = x \in Q$ a $A = P$. ♡

Tyto axiomy se tímto vyhnuly Russelovu paradoxu. Z axiomů vůbec nevyplývá, že $\{x \mid x \notin x\}$ je množina.
Podobně jsme zabránili Berryho paradoxu, protože $P(x)$ je predikátová formule s jazykem $\in, =$ a logickými symboly.
Zatím nám však axiomy garantují existenci jen jedné množiny, a to $\emptyset$.

Axiom dvojice

K libovolným dvěma množinám A, B existuje množina $\{A, B\}$.

$$(\forall A)(\forall B)(\exists C)(\forall x)(x \in C \Leftrightarrow x = A \vee x = B)$$

Ale pozor, potřeba axiomu dvojice i extenzionality ke zdůvodnění existence $C = \{A, B\}$.

Poznámka: Můžeme mít množiny $A = B$, potom $C = \{A, B\} = \{A\}$ bude jednoprvková množina.

Příklad.

1. $\{\emptyset\} \neq \emptyset$
2. $\{\emptyset, \{\emptyset\}\}$
3. $\{\{\{\{\emptyset\}\}\}\}$

Axiom sjednocení

Ke každé množině S existuje množina U všech prvků x, které náleží nějakému prvku S.

$$(\forall S)(\exists U)(\forall x)(x \in U \Leftrightarrow (\exists A \in S)(x \in A))$$

Tento axiom budeme značit jako $U = \bigcup S$, obvykle však $U = \bigcup_{A \in S} A$.
Znova si můžeme všimnout, že axiom extenzionality nám zaručuje, že je množina U jednoznačná.

Příklad. $\bigcup \{\emptyset, \{\emptyset\}\} = \emptyset \cup \{\emptyset\} = \{\emptyset\}$

Definice. Sjednocení množin $A \cup B = \bigcup \{A, B\}$. Toto sjednocení existuje díky axiomu sjednocení a dvojice. Dále je toto sjednocení jednoznačné díky axiomu extenzionality.

Jestliže $Z = A \cup B$, potom $(\forall x)(x \in Z \Leftrightarrow x \in A \vee x \in B)$.
Pojďme si zavést další značení. $A \subseteq B$ znamená, že $x \in A \Rightarrow x \in B$.

Axiom potence

Pro každou množinu S existuje množina P obsahující všechny podmnožiny S.

$$(\forall S)(\exists P)(\forall x)(x \in P \Leftrightarrow x \subseteq S)$$

Množinu P budeme dále značit jako $P(S)$ a říka se jí potenční množina. Jak nás již nepřekvapí, tato množina je znova jednoznačná.

Příklad. otenční množina $P(\emptyset) = \{\emptyset\}, P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

Můžeme si dále všimnout, že $(\forall X)(\emptyset \subseteq X)$.

2 Základní množinové operace

- $A \cap B = \{x \in (A \cup B) \mid x \in A \wedge x \in B\} \ldots$ je dobře definovaná množina díky axiomu vydělení. $(A \cup B)$ je rovněž dobře definovaná množina.
- $A \setminus B = \{x \in (A \cup B) \mid x \in A \wedge x \notin B\}$.
- $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Tyto operátory nám umožňují vytvořit již jakoukoliv množinu.

Průnik a sjednocení jsou navzájem distributivní: $A \cap (B \cup C) = (A \cap B) \cup (B \cap C)$.

Důkaz. Chceme ukázat, že jsou podmnožinou i nadmnožinou. Pokud $x \in A \cap (B \cup C)$, potom $x \in A \wedge x \in B \cup C \Rightarrow x \in A \wedge (x \in B \vee x \in C)$.

Nyní využijeme distributivity logických operací a dostáváme $(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$. To již implikuje $\subseteq$. Směr $\supseteq$ je analogický. ♡

Definice. $\bigcap S$ budou prvky, které se nacházejí v každé množině uvnitř S a $\bigcap S = \{x \mid (\forall A \in S)(x \in A)\}$

Taková definice je ale problematická, protože $\bigcap \emptyset = \{x \mid \ldots\}$ je vždy pravdivé, a tak by nám vznikla množina všech množin. Proto dodáme podmínku, že $S \neq \emptyset$ a poté zvolíme $B \in S$ tak, že $\bigcap S = \{x \in B \mid \ldots\}$.

Taková definice je nyní korektní díky axiomu vydělení.

Stále je ale otázka, co je $\bigcap \emptyset$. Tím bude prázdná množina.

3 Relace a funkce

Pojďme si zavést pojem uspořádané dvojice. Od takové množiny chceme, aby nám zachovávala pořadí prvků.

Definice: *Uspořádaná dvojice.* $(a, b) = \{\{a\}, \{a, b\}\}$.

Věta. $(a, b) = (a', b') \Leftrightarrow a = a' \wedge b = b'$.

Důkaz. Zpětná implikace vychází ze základní logiky. Nyní se podívejme na dopřednou implikaci. Máme dvě možnosti.

Jestliže $a = b$, potom $(a, b) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$. Pokud $(a, b) = (a', b')$, potom (a', b') je singleton a $\{a\} = \{a'\}$. Tedy $a = a' (b = b')$.

Jinak $a \neq b$, potom (a, b) obsahuje dva různé prvky. Tedy (a', b') rovněž obsahuje dva různé prvky. Tedy $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$, tudíž $\{a\} = \{a'\}$ a $\{a, b\} = \{a', b'\}$. Díky extenzionalitě $a = a'$ a $b = b'$. ♡

Nyní, když máme uspořádané dvojice, pojďme je nějak využít!

Definice: *Binární relace.* Binární relace je množina uspořádaných dvojic.

Příklad. $R = \left\{(m, n) \in \mathbb{N}^2 \mid m/n\right\}$ (Nemáme ale definice $\mathbb{N}, \mathbb{N}^2$, dělitelnosti)

Tyto relace nejsou jen takové množiny dvojic. Ty něco musí znamenat. Pojďme si k nim něco dalšího užitečného nadefinovat.

Definice.

1. Definiční obor R je $\operatorname{dom} R = \{m \mid (\exists n)((m, n) \in R)\}$.
2. Obor hodnot R je $\operatorname{ran} R = \{n \mid (\exists m)((m, n) \in R\})$.
3. Obor $R = \operatorname{dom} R \cup \operatorname{ran} R$.

Tyto definice jsou korektní, pokud umíme ukázat existenci množiny S takové, že $\exists n : (m,n) \in R \Rightarrow x \in S$.

Tato vlastnost platí obecně pro $\{x \mid P(x)\}$, tedy pokud existuje S taková, že $\forall x P(x) \Rightarrow x \in S$, jedná se o množinu, jelikož poté umíme takovou definici přepsat na $\{x \in S \mid P(x)\}$.

Věta. $(m,n) \in R \Rightarrow m,n \in \bigcup\bigcup R$.

Důkaz. Víme, že $\{\{m\},\{m,n\}\} \in R$, potom $\{m,n\} \in \bigcup R$, a tudíž $m \in \bigcup\bigcup R \wedge n \in \bigcup\bigcup R$. ♡

Pro binární relaci R můžeme $(x,y) \in R$ rovněž zapsat jako $x\ R\ y$,

Definice. Obraz množiny A je $R[A] = \{y \in \operatorname{ran} R \mid x\ R\ y\}$ pro nějaké $x \in A$.

Vzor množiny A je $R^{-1}[A] = \{x \in \operatorname{dom} R \mid \exists y \in A : x\ R\ y\}$.

Inverze R je $R^{-1} = \{z \mid z = (x,y) \Rightarrow (y,x) \in R\}$, tedy množina všech „obrácených"dvojic.

Inverzi můžeme zapisovat zkratkou jako $\{(x,y) \mid (y,x) \in R\}$. Znova ale potřebujeme S, kde $(y,x) \in R \Rightarrow (x,y) \in S$. Tedy chceme $S = \operatorname{ran} R \times \operatorname{dom} R$.

Definice: *Kartézský součin.* Množina $A \times B = \{z \mid \exists a \in A\ \exists b \in B : z = (a,b)\}$.

Znova budeme používat zkratku $\{(a,b) \mid a \in A, b \in B\}$. Tato definice tentokrát je ale velmi problematická, nevíme ani, zda je korektní. Nezoufejme však.

Věta. $A \times B$ je množina.

Důkaz. $(a,b) \in P(P(\{a,b\}))$. Tedy $a,b \in A \cup B \Rightarrow (a,b) \in P(P(A \cup B))$. Potom $\{a,b\} \subseteq A \cup B$.

To tedy znamená, že $A \times B = \{z \in P(P(A \cup B)) \mid \exists a \in A\ \exists b \in B : z = (a,b)\}$. Víme, že $P(P(A \cup B))$ je množinou díky axiomům, proto je kartézský součin množinou díky vydělení. ♡

Jak zapsat uspořádané n-tice? $(a,b,c) = ((a,b),c)$. Můžeme ale n-tice mít? Chceme funkci $x : \{1,2,\ldots,n\} \to \mathbb{R}$, kde $n \in \mathbb{N}$.

Nyní bychom rádi měli definováno, co to jsou v řeči množin přirozená čísla. Dejme si pozor na rozdíl významu vzhledem k jazyku množin nebo metajazyku (tak, jak je známe my).

4 Funkce

Definice. Relace f je funkce pokud $f(a,b_1) \wedge f(a,b_2)$ implikuje $b_1 = b_2$.

Tedy funkce je taková relace, že každý prvek vlevo je v relaci s právě jedním prvkem vpravo. K funkci máme potom dobře definované $\operatorname{dom} f, \operatorname{ran} f$.

Definice. B^A je množina všech funkcí z A do B, tedy $\{f \subseteq A \times B \mid f \text{ funkce}, \operatorname{dom} f = A, \operatorname{ran} f = B\}$.

Často se užívá notace $\mathcal{S} = \{S_i \mid i \in I\}$ (případně místo S_i se používá $S(i)$). V té je S funkce s definičním oborem I.

Dále si můžeme zavést notaci $\bigcup \mathcal{S} = \bigcup_{i \in i} S_i = \bigcup_{i \in i} S(i)$. Rovněž $\prod_{i \in I} S_i = \{f \mid \operatorname{dom} f = I, \forall i \in I : f(i) \in S_i\}$. V obou případech se jedná o množiny.

Definice. Funkce f,g jsou kompatibilní, pokud $\forall x \in \operatorname{dom} f \cap \operatorname{dom} g : f(x) = g(x)$.

Funkce f rozšiřuje g, pokud $f \supseteq g$.

Můžeme si všimnout, že funkce f,g jsou kompatibilní právě tehdy, když $f \cup g$ je funkce.

Věta. Nechť F je množina funkcí, které jsou po dvou kompatibilní. Potom $\bigcup F$ je funkce, jejíž $\operatorname{dom} \bigcup f = \bigcup \{\operatorname{dom} f \mid f \in F\}$.

Tento průnik rozšiřuje všechny funkce v F.

Důkaz. Abychom zkontrolovali, že je g funkce, předpokládejme, že $(a,b_1),(a,b_2) \in g$. To znamená, že $\exists f_1, f_2 \in F : (a,b_1) \in f_1, (a,b_2) \in f_2$.

V případě, že $f_1 = f_2$, $b_1 = b_2$, jelikož f_1 je funkce. Jinak $b_1 = b_2$, protože f_1 i f_2 jsou navzájem kompatibilní funkce. ♡

5 Přirozená čísla

Chceme namodelovat přirozená čísla, tedy $0,1,\ldots$ jako množiny. Jaké máme možnosti?

Definice.
$0 = \{\} = \emptyset$
$1 = \{0\} = \{\emptyset\}$
$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$
$3 = \{0, 1, 2\} = \dots$

Definice. Následník $\mathsf{S}(x) = x \cup \{x\}$.

Nyní, když máme následníka, můžeme zapsat jakékoliv číslo, například $7 = \mathsf{SSSSSSS}(0)$.

Definice. Množina I je induktivní, pokud $0 \in I$ a $x \in I \Rightarrow \mathsf{S}(x) \in I$.

Nyní je čas k dalšímu axiomu teorie množin.

Axiom nekonečna

Induktivní množina existuje.

Nyní si konečně můžeme definovat přirozená čísla.

Definice. $\mathbb{N} = \{x \in A \mid \forall \text{ induktivní množinu } I : x \in I\}$ kde A je nějaká induktivní množina, která existuje díky axiomu nekonečna.

$\mathbb{N}$ je množinou, protože můžeme udělat následující. Vzít libovolnou induktivní množinu. Vzít všechny její podmnožiny. Axiomem vydělení vzít pouze podmnožiny, které jsou induktivní. Udělat jejich průnik. Nahlédnout, že se jedná o induktivní množinu. Nahlédnout, že tato induktivní množina je do inkluze minimální. Nahlédnout, že ať začneme s libovolnou induktivní množinou, dostaneme nakonec tu stejnou množinu. Tato množina je množinou přirozených čisel.

Věta.

1. $\mathbb{N}$ je induktivní.
2. $\forall I$ induktivní: $\mathbb{N} \in I$

Důkaz. Nejprve ukážeme, že je $\mathbb{N}$ induktivní. Víme, že $0 \in \mathbb{N}$, jelikož je 0 v každém I. Jakmile je $x \in N$, potom je i v každém I díky definici.

Potom $\forall I$ induktivní $\mathsf{S}(x) \in I$, a tedy $\mathsf{S}(x) \in \mathbb{N}$. ♡

Jako zkratku budeme psát, že $\mathsf{S}(n) = n + 1$.

Nadefinujme si uspořádání $\mathbb{N} : m < n$, jestliže $m \in n$.

Věta (*Princip matematické indukce.*). Mějme P jakoukoliv vlastnost množiny. Jestliže $P(0)$ platí a $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n + 1)$. Potom $\forall n \in \mathbb{N} : P(n)$.

Důkaz. Nechť $A = \{n \in \mathbb{N} : P(n)\}$. Toto je induktivní množina: $0 \in A$ díky první podmínce, tedy $P(0)$ platí. Jestliže $n \in A$, pak $P(n)$ rovněž platí. Tudíž díky druhé podmínce $P(n + 1)$ rovněž platí, a proto $n + 1 \in A$.

Vidíme, že A je induktivní, tedy $A \subseteq \mathbb{N}$, ale zároveň podle definice $A \supseteq \mathbb{N}$. ♡

Pojďme se podívat na nějaké vlastnosti. Pro každé přirozené n platí, že $0 \leq n$. Dále, pro každé n, k přirozené platí, že $k < n + 1$ implikuje, že $k < n$ nebo $k = n$.

Důkaz. Využijeme indukci. Podmínka $P(n) : n \geq 0 \Leftrightarrow n > 0 \vee n = 0 \Leftrightarrow \emptyset \in n \vee \emptyset = n$.

$P(0) : 0 \geq 0$ platí, jelikož $0 = 0$. $P(n) \Rightarrow P(n + 1)$. Pokud $n = 0$, potom $n + 1 = \{\emptyset\} \ni \emptyset$. Pokud ne, potom $\emptyset \in n$ a $\mathsf{S}(n) = n \cup \{n\} \ni \emptyset$.

Pro druhou podmínku víme, že $k < n+1$ a $k \in n \cup \{n\}$. To platí právě tehdy, když $k \in n$ nebo $k \in \{n\} \Leftrightarrow k = n$. ♡

Věta. $(\mathbb{N}, <)$ je lineárně uspořádaná množina.

Důkaz. Nejprve ukážeme, že $<$ je tranzitivní, tedy $\forall k, l, m \in \mathbb{N} : k < l \wedge l < m \Rightarrow k < m$. Využijeme indukci: $P(m) : \forall k, l : k < l < m \Rightarrow k < m$.

a) $P(0)$, předpokládejme $l < 0$, potom $l \in \emptyset$, nemožné.

b) $P(m)$, chceme $P(m + 1)$.

   Víme, že pro $l < m + 1$ platí buď $l < m$, potom $k < l < m \Rightarrow k < m$ díky indukčnímu předpokladu. Jinak $l = m$ a $k < l = m$, tedy $k < m$.

Nyní ukážeme antisymetrii $<$. Pokud $x < y \wedge y < x$, potom díky tranzitivitě $x < x$ a tedy $x \in x$. Zatím nemáme žádný axiom, který by toto zakazoval, ale lze jednoduše dokázat indukcí, že to se u čísel stát nemůže.

Nakonec linearitu $<$. $\forall m, n \in \mathbb{N} : m < n \vee m = n \vee m > n$. Neboli $\forall n \in \mathbb{N} : P(n)$, kde $P(n) = \forall m \in \mathbb{N} : \ldots$ Ukážeme indukcí.

a) $P(0) : \forall m \in \mathbb{N} : m < 0 \vee m = 0 \vee m > 0$, to víme.

b) $P(n) \Rightarrow P(n+1)$. V případě $m < n$ máme $m < n < n+1 \wedge$ tranzitivitu. V případě $m = n$ je $n < n+1 \Leftrightarrow n \in n \cup \{n\}$.

Nakonec $m > n \Rightarrow m \geq n+1$, kde platí určitě jedna možnost. Nechť je tato formule $Q(m)$.

a) $Q(0)$ platí.

b) $Q(m) \Rightarrow Q(m+1)$.

Chceme $m+1 > n \Rightarrow m+1 \geq n+1$ a víme, že $m > n \Rightarrow m \geq n+1$. Podle předchozího lemmatu $n < m \vee n = m \Rightarrow m+1 = n+1$. Tedy $m+1 > m \geq n+1$. ♡

Věta. Předpokládejme, že $\forall n \in \mathbb{N} :$

$$(\forall m < n : P(m)) \Rightarrow P(n) \qquad (*)$$

Potom $\forall n \in \mathbb{N} : P(n)$.

Důkaz. Indukcí pro $Q(n) = \forall m < n : P(m)$.

a) $Q(0)$ je pravdivý.

b) $Q(n) \Rightarrow Q(n+1)$. Podmínka $(*)$ říká, že $Q(n) \Rightarrow P(n)$ a $Q(n+1) \Leftrightarrow Q(n) \wedge P(n)$.

A tedy $\forall n \in \mathbb{N} : Q(n)$. ♡

Definice. Nechť $(A, <)$ je uspořádání. Řekněme, že A je *dobře uspořádaná*, jestliže $\forall B \subseteq A : B \neq \emptyset \Rightarrow B$ má nejmenší prvek (tedy prvek, který je menší než libovolný jiný prvek).

Dobré uspořádání nám tedy říká, že každá podmnožina z našeho uspořádání má minimum. Z toho plyne i že je $<$ je lineárním uspořádáním, protože libovolná dvouprvková množina musí mít nejmenší prvek.

Příklad. $(\mathbb{Q}, <)$ *není* dobře uspořádaná množina. Stejně tak není dobře uspořádaná $(\mathbb{Z}, <)$.

Věta. $(\mathbb{N}, <)$ je dobře uspořádaná množina.

Důkaz. Vezměme si $B \subseteq \mathbb{N}$. Předpokládejme pro spor, že B nemá nejmenší prvek. Mějme indukční podmínku $P(n) : \forall m < n : m \notin B$.

a) $P(0)$ platí, žádný prvek pod nulou není.

b) $P(n) \Rightarrow P(n+1)$. Chceme dokázat $\forall m < n+1 : m \notin B$. Víme z definice B, že $\forall m < n : m \notin B$, tedy $P(n)$ platí, nebo pro $m = n : m \notin B$. Pokud $n \in B$, potom $n = m \in B$, spor s neexistencí minima. Proto $n \notin B$.

Z toho dostaneme, že $\forall n \in \mathbb{N} : P(n)$. Pokud $B \neq \emptyset$, mějme $k \in B$. Potom $P(k+1)$ není pravdivý, máme spor. ♡

6 Rekurze

Mějme posloupnosti definované explicitně: $f(n) = n+1$, tedy $f = \{(n, \mathsf{S}(n)) \in \mathbb{N} \times \mathbb{N} \mid n \in \mathbb{N}\}$.

Rovněž máme posloupnosti definované implicitně (rekurzivně). Příkladem je $f(0) = 1, f(n+1) = (n+1) \cdot f(n)$.

Otázka je, zda je implicitně definovaná f v teorii množin dobře definovaná, tedy zda $g(f(n), n)$ existuje.

Rekurzi potřebujeme už třeba k definování jednoduchého $n + n$.

Věta (*o rekurzi*). Mějme A množinu, a její prvek a $g : A \times \mathbb{N} \to A$. Potom existuje jednoznačná funkce $f : \mathbb{N} \to A$ taková, že

1. $f(0) = a$
2. $f(n+1) = g(f(n), n)$.

Důkaz. t je m-krokový výpočet, pokud $t : (m+1) \to A$, $t(0) = a$, $\forall n < m : t(n+1) = g(t(n), n)$. Potom t je množina uspořádaných dvojic $(0, a), \ldots, (m, f(m))$.

Vezměme si $F = \{t \in P(\mathbb{N} \times A) \mid t$ je m-krokový výpočet pro nějaké $m \in \mathbb{N}\}$. Potom $f = \bigcup F$ a je to dobře definovaná množina.

Všimněme si, že jakmile je t m-krokový výpočet, $t \in P(\mathbb{N} \times A)$. Chceme, aby f byla funkce.

Abychom to dokázali, stačí, aby $t, t' \in F$ implikovalo kompatibilitu t, t'.

Podle definice f dostáváme $\exists m, m'$, kde t a t' jsou m-krokový a m'-krokový výpočet.

Můžeme předpokládat že $m \leq m' : \forall n \in m : t(n) = t'(n)$. Nazvěme tuto podmínku $P(m)$ a použijme indukci.

Pro $n = 0$ máme $t(0) = t'(0) = a$. Potom pro $P(n) \Rightarrow P(n+1)$ máme $t(n) = t'(n) \Rightarrow t(n+1) = g(t(n), n) = t'(n+1) = g(t'(n), n)$, tedy $\operatorname{dom} f = \mathbb{N}$ a $\operatorname{ran} f \subseteq A$.

Z podmínky máme $P(m)$: existuje m-krokový výpočet. Dále $P(0) = t(0) = a, t : \{0\} \to A$, tedy $t = \{(0, a)\}$.

Díky $P(m) \Rightarrow P(m+1)$ můžeme rozšířit t. Tedy pokud je t m-krokový výpočet, potom $t \cup (m+1, g(t(m), m))$ je $(m+1)$-krokový výpočet.

Tedy podle indukce $\forall m : P(m)$ říká, že $\forall m \; \exists t : m \in \operatorname{dom} t \Rightarrow m \in \operatorname{dom} f$. A proto f splňuje „rekurzi“:

a) $\forall t \in F : t(0) = a \Rightarrow f(0) = a$

b) díky definici t-krokového výpočtu pro kontrolu b pro $n \in \mathbb{N}$ použijeme jakýkoliv $(n+1)$-krokový výpočet.

Nyní ještě chceme jednoznačnost f. Mějme h splňující „rekurzi“. Podle indukce ukážeme, že $\forall n f(n) = h(n)$.

Vidíme, že $f(0) = h(0) = a$. Dále, pokud $f(n) = h(n)$, potom $f(n+1) = g(f(n), n) = g(h(n), n) = h(n+1)$. Tedy se musí f a g rovnat. ♡

Věta. Mějme $a : P \to A$ a $g : P \times A \times \mathbb{N} \to A$. Potom existuje $f : P \times \mathbb{N} \to A$ taková, že

a) $\forall p \in P : f(p, 0) = a(p)$

b) $\forall n \in \mathbb{N}, p \in P : f(p, n+1) = g(p, f(p, n), n)$.

Důkaz nebudeme provádět. Je stejný, pouze komplikovanější, jelikož je a funkcí místo konstanty.

7 Aritmetika $\mathbb{N}$

Pojďme si nyní vybudovat na našich přirozených čísel celou aritmetiku. Máme zatím k dispozici jen následníka.

Věta. Existuje právě jedna funkce $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ taková, že

a) $+(m, 0) = m$

b) $+(m, n+1) = +(m, n) + 1$

Důkaz. Využijeme rekurzi, kde $A = P = \mathbb{N}$, $a(p) = p$ a $g(p, a, n) = a + 1$. ♡

Nadále budeme pro $+$ používat infixní notaci, tedy $+(m, n)$ budeme značit $m + n$.

Nyní bychom rádi věděli, zda má sčítání tak, jak jsme si ho zavedli, vlastnosti, jaké bychom od něj čekali.

Věta. Sčítání je komutativní.

Důkaz. Mějme $P(n) : \forall m < n : m + n = n + m$. Chceme, že $P(n)$ platí pro každé n, užijme indukci.

Pro $P(0)$ dostáváme $\forall m \in \mathbb{N} : m + 0 = 0 + m$. Chtěli bychom, aby toto platilo, čeká nás další indukce $Q(m) : 0 + m = m$. Pro $Q(0) : 0 + 0 = 0$, to je v pořádku. Potom $Q(m) \Rightarrow Q(m+1)$ znamená, že $0 + (m+1) = (0 + m) + 1 = m + 1$ užitím $Q(m)$.

Pro $P(n) \Rightarrow P(n+1)$ máme $\forall m : m + (n+1) = (n+1) + m$. Využijeme stejnou indukci $Q(m)$. Tedy $Q(0) : 0 + (n+1) = (n+1) + 0$, což jsme už dokázali.

...

... ♡

8 Kardinality množin

Možná by nás jednoho dne zajímalo, jak jsou množiny velké.

Definice. Množiny A, B mají stejnou velikost nebo kardinalitu právě tehdy, když existuje bijekce z A do B.

O množinách, které jsou stejně velké, budeme říkat, že jsou ekvipotentní a $|A| = |B|$.

Věta. Ekvipotentnost má následující vlastnosti:

1) $|A| = |A|$

2) $|A| = |B| \Rightarrow |B| = |A|$

3) $|A| = |B| \wedge |B| = |C| \Rightarrow |A| = |C|$

Důkaz.

1) Zvolíme $id : A \to A$, kde $a \to a$.

2) Víme, že $f : A \to B$ je bijekce, potom $f^{-1} : B \to A$ je také bijekce.

3) Víme, že $f : A \to B$ a $g : B \to C$ jsou bijekce, potom $g \circ f$ je také bijekce. ♡

Relace R : „být ekvipotentní“ je tedy ekvivalence, jelikož předchozí věta ukázala reflexivitu, symetrii i tranzitivitu.

Co je ale dom R? Kdybychom řekli, že to jsou všechny množiny, měli bychom problém. Potřebujeme tedy nějakou množinu, na kterou dom R omezíme.

Proto bychom rádi zavedli koncept *třídy* bez omezení: Pro jakoukoliv vlastnost P je $\{x \mid P(x)\}$ třída, ale ne nutně množina. Třídy můžeme používat jako zkratky ke všem množinám s nějakou vlastností, avšak nemusí být korektně definované.

Díky tomu můžeme definovat třídové *Relace*, které ale nejsou nutně množinovými relacemi, avšak vypovídají nějaké vlastností daných množin.

Máme sice rovnost kardinalit, ale chtěli bychom taky porovnávat nerovnost. Jak na to?

Definice. Velikosti $|A| \leq |B|$, pokud existuje prosté zobrazení z A do B.

Věta.

1) $|A| \leq |A|$

2) $|A| = |B| \leq |C| = |D| \Rightarrow |A| \leq |C| \wedge |B| \leq |D|$

3) $|A| \leq |B| \leq |C| \Rightarrow |A| \leq |C|$

Důkaz analogický k předchozí větě.

Zdálo by se, že se jedná o třídové uspořádání. Avšak nic nevíme o antisymsetrii, která je důležitá pro definování uspořádání.

Věta (*Cantor-Bernstein*). $|X| \leq |Y| \wedge |Y| \leq |X| \Rightarrow |X| = |Y|$.

Důkaz. Mějme $X'' = g[f[X]] \subseteq X' = g[Y] \subseteq X$. Potom $|X| = |X''|$, jelikož $g \circ f$ je prostá funkce na X''.

Lemma. Jestliže $A_1 \subseteq B \subseteq A \wedge |A_1| = |A|$, potom $|A| = |B|$.

Důkaz. Funkce $f : A \to A_1$ je bijekce. Nyní si vezmeme posloupnosti $A_0, A_1, A_2, \ldots$ a $B_0, B_1, B_2, \ldots$, kde $A_0 = A$ a $B_0 = B$ a $A_{n+1} = f[A_n]$ a $B_{n+1} = f[B_n]$.

Dále víme, že $A \supseteq B \Rightarrow f[A] = A_1 \supseteq f[B] = B_1$.

Dále $B_0 \supseteq A_1 \Rightarrow f[B_0] \supseteq f[A_1]$. Tedy vidíme, že $\forall n : A_n \supseteq B_n \supseteq A_{n+1}$. To ukážeme indukcí: $A_0 \supseteq B_0 \supseteq A_1$. Dále $f[A_n] \supseteq f[B_n] \supseteq f[A_{n+1}]$.

Definujme si tedy $C_n = A_n \setminus B_n$. Potom $C = \bigcup_{n=0}^{\infty} C_n$. Nyní si nadefinujme $g(x) = f(x)$ pro $x \in C$, jinak $g(x) = x$.

Dostaneme, že $f|C_n$ je bijekce mezi C_n a C_{n+1}. To znamená, že $f|C$ je bijekce mezi C a $\bigcup_{n=1}^{\infty} C_n$. Nakonec id je bijekce z $A \setminus C$ do $A \setminus C \subseteq B$.

Tudíž g je bijekce mezi A a B. ♡

Díky lemmatu máme $|X''| = |X'| = |X|$. Protože prostá funkce je bijekcí mezi svým definičním oborem a oborem hodnot, $|X'| = |Y|$. ♡

Ukážeme si ještě jiný důkaz stejné věty, který ale není úplně správný.

Důkaz. Představme si bipartitní graf, kde vrcholy jsou $X \cup Y$ a hrany jsou $\{x, f(x) \mid x \in X\} \cup \{y, g(y) \mid y \in Y\}$ pro $f : X \to Y, g : Y \to X$ prosté funkce.

Můžeme si všimnout, že z každého vrcholu právě jedna hrana vychází a nejvýše jedna vchází.

Komponenty souvislosti jsou sudé cykly nebo orientované cesty mezi partitami.

Nyní můžeme nadefinovat bijekce na jednotlivých komponentách tak, že budeme od počátku cesty postupně střídat hrany jako obrazy.

Nakonec spojením každé bijekce na jednotlivé komponentě dostaneme bijekci mezi X a Y. ♡

Takže tím jsme získali kompletní porovnávací systém velikostí množin. Je zatím ale jen relativní.

Velikost množiny A, tedy $|A|$ bude definovaná jako určitá množina X taková, že $|A| = |X|$. Tato množina X se bude nazývat kardinální číslo.

9 Konečné množiny

Definice. Množina A je konečná, pokud $|A| = |n|$ pro nějaké přirozené číslo n. Jinak je A nekonečná.

Lemma. Neexistuje žádná bijekce mezi n do vlastní podmnožiny n.

Důkaz. Matematickou indukcí podle n.

a) $n = 0$: Neexistuje $X \subsetneq \emptyset$, tedy ani bijekce.

b) $n \to n + 1$: Předpokládejme $f : n + 1 \to X \subsetneq (n + 1)$. Můžou nastat dva případy.

Buď $n \notin X$, potom $F|n : n \to X \setminus f(n) \subsetneq n$ není možné z předpokladu.

Nebo $n \in X$, potom $f(k) = n$. Definujme si nové zobrazení $g : n \to n$, kde $g(k) = f(n)$ a $g(x) = f(x)$, jestliže $x \neq k$.

Potom $\operatorname{ran} g = X \setminus \{n\} \neq n$. Taková funkce však nemůže existovat. ♡

Pokud $|S| = |n|$, potom nadefinujeme symbol $|S|$ jako označení n.

Abychom tuto definici zdůvodnit, využijeme následující:

Věta. Pokud $|S| = |m| \wedge |S| = |n|$, potom $m = n$.

Důkaz. Předpokládejme, že $m < n$. Víme, že $|m| = |n|$, tedy existuje bijekce $f : n \to m$. Jenže $m \subsetneq n$. Opačně analogicky. ♡

Pro $m, n \in \mathbb{N}$ jsou ekvivalentní následující: $m < n$, $m \in n$, $m \subsetneq m$.

Víme, že je každé přirozené číslo konečné. Co ale množina všech přirozených čísel?

Věta. Množina $\mathbb{N}$ je nekonečná.

Důkaz. Pokud $f : \mathbb{N} \to n \in \mathbb{N}$ je bijekce, potom $f|n + 1 : n + 1 \to n$ je prostá. Na druhou stranu je prostá (například) identita. Tím jsme dokázali obě nerovnosti mezi velikostmi množin. Podle Cantor-Bernsteinovy věty existuje bijekce, což je spor. ♡

Věta. Mějme X konečnou a funkci f. Potom $f[X]$ je konečná. Navíc, $|f[X]| \leq |X|$.

Důkaz. Nechť $X = \{x_0, \ldots, x_{n-1}\}$. Funkce $x : n \to X$ je bijekce.

Využijeme rekurzi, tedy $k(0) = 0, k(i + 1) =$ nejmenší k takové, že $f(x_k)$ je nový prvek (pokud existuje).

Dále mějme $y_i = f(x_{k(i)})$. Z toho $f[X] = \{y_0, y_1, \ldots, y_l\}$ pro nějaké l.

Vidíme, že k je prostá funkce z $f[X]$ do X, tedy $|f[X]| \leq |X|$. ♡

Věta. Množiny X, Y jsou konečné, potom $X \cup Y$ je rovněž konečná.

Důkaz. $X = \{x_0, \ldots, x_{m-1}\}, Y = \{y_0, \ldots, y_{n-1}\}$. Mějme $f : m + n \to X \cup Y$. Potom $i \to x_i$, pokud $i < m$, jinak $i \to y_{i-m}$. ♡

Věta. Nechť S je konečná a $\forall x \in S$ je x konečná. Potom $\bigcup S$ je konečná.

Důkaz. Matematickou indukcí podle $|S|$.

a) $S = \emptyset, \bigcup S = \emptyset$.

b) $|S| = n + 1$, potom $S = \{T_0, \ldots, T_n\}$ a $\bigcup S = \bigcup T_i \cup T_n$. ♡

Věta. Nechť X je konečná množina. Potom $P(X)$ je taky konečná.

Nyní víme, co je konečné a co není. Jak je to ale s rozlišováním velikostí nekonečných množin?

Definice. Množina S je spočetná, jestliže $|S| = |\mathbb{N}|$.

Stejně tak můžeme říct, že množina S je nejvýše spočetná, pokud $|S| \leq |\mathbb{N}|$.

Dále, jestliže je S spočetná, potom $|S| = \aleph_0$.

Věta. Nechť S je spočetná, A nekonečná a $A \subseteq S$, potom A je spočetná.

Důkaz. Můžeme předpokládat, že $S = \mathbb{N}$. Nadefinujeme si $f : \mathbb{N} \to A$ podle rekurze: $f(n)$ bude nejmenší přirozené číslo v $A \setminus \{f(i) : i < n\}$.

Tedy $f(0) = \min A$, $f(1) = \min A \setminus \{f(0)\}$ a tak dále. Tato definice má dva možné důsledky.

Buď pro nějaké n je $A \setminus \{f(i) \mid i < n\}$ prázdná, potom ale $|A| = n$, tedy je A konečná.

Jinak je $f : \mathbb{N} \to A$ bijekcí. To, že je prostá, vychází přímo z konstrukce. Ukažme tedy, že je na. Víme, že $f(a) \geq a$. V případě, že $f(a) = a$, máme vyhráno, jinak $f(a) > a$, tudíž $a \in \{f(i) \mid i < a\}$. Což nám společně dává bijekci. ♡

Jako důsledek dostáváme, že jestliže je S nejvýše spočetná, potom je konečná nebo spočetná.

Důkaz. Využijeme funkci $f : S \to \mathbb{N}$, která je prostá. Potom $f[S] = A \subseteq \mathbb{N}$ a máme předchozí větu. ♡

Můžeme si všimnout, že konstrukce f v důkazu nám nějak pojmenovala jednotlivé prvky A přirozenými čísly. Tedy spočetné množiny jdou „očíslovat“ přirozenými čísly.

Věta. Nechť X je spočetná, f je funkce s $\operatorname{dom} f \supseteq X$. Potom $f[X]$ je nejvýše spočetná.

Příklad.

1. $A = A_1 \cup A_2, A_1 \cap A_2 = \emptyset, |A_1| = |A_2| = |\mathbb{N}| = |A|$.
   Tedy $\mathbb{Z} = \mathbb{N} \cup \mathbb{Z}^-$.
2. Mějme $A_n = \left\{p_n^k \mid k \in \mathbb{N}\right\}$, kde p_n je n-té prvočíslo. Potom $N \subseteq A_1 \cup A_2 \cup \ldots$, $A_i \cap A_j = \emptyset$ a $|A_n| = \mathbb{N}$.

Věta.

1) Nechť X, Y jsou spočetné. Potom $X \cup Y$ je spočetná.
2) $\forall n \in \mathbb{N}$: Pokud $\forall i < n : X_i$ je spočetná, potom $\bigcup_{i<n} X_i$ je spočetná.

Důkaz. Mějme bijekce $f : X \to \mathbb{N}, g : Y \to \mathbb{N}$. Pro ně si sestavíme $h : X \cup Y \to \mathbb{Z}$. Tedy pro $x \in X : h(x) = f(x)$ a pro $y \in Y : h(y) = -g(y) - 1$. Potom h je prostá, tedy $|X \cup Y| \leq |\mathbb{Z}|$.

Chtěli bychom zjistit, zda $|\mathbb{N}| = |X| \leq |X \cup Y| \leq |\mathbb{Z}| = |\mathbb{N}|$.

Zavedeme si $F : \mathbb{N} \to \mathbb{Z}$, kde $f(2n) = n$ a $F(2n + 1) = -n - 1$. Tím jsme dostali bijekci mezi $\mathbb{Z}$ a $\mathbb{N}$. Rovněž jsme tím ověřili, že $X \cup Y$ je spočetná.

Pro druhou část použijeme indukci podle n. Víme, že $\bigcup_{i<n+1} X_i = \bigcup_{i<n} X_i \cup X_{n+1}$, o čemž víme, že je spočetné. ♡

Nyní jsme dostali, že konečné sjednocení spočetných množin je spočetné. Co takhle spočetné sjednocení?

Věta. Nechť A, B je spočetná. Potom $A \times B$ je spočetná.

Důkaz. Stačí předpokládat, že $A = B = \mathbb{N}$. Zavedeme si $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ s předpisem $f(k, n) = 2^k(2n + 1) - 1$. Nyní chceme zjistit, zda je na a prostá.

Všimněme si, že $\forall m \in zN \setminus \{0\}$ existuje právě jedno k takové, že $m = 2^k$ krát liché číslo. Tedy f je na.

Jestliže $f(k, n) = f(k', n')$, potom z jednoznačnosti předchozího pozorování $k = k', n = n'$ a f je prostá. ♡

Jiná možnost, jak tuto větu dokázat, je vzít si tabulku $\mathbb{N} \times \mathbb{N}$ a postupně číslovat obrácené diagonály, tedy postupně $(0, 0), (0, 1), (1, 0), (0, 2), (1, 1), (2, 0), \ldots$.

Věta. Předpokládejme, že $\forall n \in \mathbb{N} : A_n$ je spočetná a $a_n : N \to A_n$ je daná bijekce. Potom $\bigcup_{i\in\mathbb{N}} A_n$ je spočetná.

Aby tato věta o spočetném sjednocení šla dokázat, potřebujeme mít bijekce a_n předem, nebo použít axiom výběru k jejich získání.

Důkaz. Nechť $g : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ je bijekce. Dále sestavíme $f : \mathbb{N} \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n$, která je na, kde $(n, k) \to a_n(k)$. Opravdu je na: pokud $x \in \bigcup_{n\in\mathbb{N}} A_n$, potom $\exists n \in \mathbb{N} : x \in A_n$ a $k = a_n^{-1}(x)$.

Tím jsme získali funkci $f \circ g : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n$. Nemusí být nutně prostá, avšak z vlastnosti *na* získáváme $|\mathbb{N}| \geq *|\bigcup A_n| \geq |A_0| = |\mathbb{N}|$, kde $X \geq *Y$ znamená, že existuje zobrazení z X na Y. Rozmyslete si, proč pro nejvýše spočetné množiny platí $X \geq *Y \Leftrightarrow X \geq Y$. Platí to i obecně, ale je třeba axiom výběru, abychom našli pravou inverzi k surjekci. ♡

Věta. Nechť A je spočetná. Potom množina všech konečných posloupností $\operatorname{Seq}(A)$ je spočetná.

Důkaz. $\operatorname{Seq}(A) = \bigcup_{n\in\mathbb{N}} A^n$. Chceme spočetnost A^n a rovněž potřebujeme a_n.

A^n je opravdu spočetná, je to konečně mnoho aplikovaný kartézský součin na A.

Nyní sestavíme a_n rekurzí. $a_{n+1} = \mathbb{N} \to A^{n+1}$ pomocí $a_n = \mathbb{N} \to A^n$ a n.

$a_1 : \mathbb{N} \to A$ existuje a je spočetná. Dále $a_{n+1}(k) = (a_n(s), a_1(t))$ kde $g(k) = (s, t)$ je bijekce $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$.

Podle věty o rekurzi získáváme hledané bijekce a máme spočetné sjednocení. ♡

Ze všech těchto vět získáváme, že množiny $\mathbb{Z} \times (\mathbb{N} \setminus \{0\}), \mathbb{Q}$ i množina algebraických čísel jsou spočetné. Množina všech konečných podmnožin $P_{fin}(S)$ je rovněž spočetná, jestliže S je spočetná.

Věta (*Cantor*). $\forall X : |X| < |P(X)|$.

Důkaz. Chceme ukázat, že $|X| \neq |P(X)|$, tedy neexistuje žádná bijekce $f : X \to P(X)$.

Předpokládejme, že bijekce f existuje, zavedeme si $Y = \{y \in X \mid y \notin f(y)\}$.

Jelikož je f bijekce, existuje $y \in X$ taková, že $f(y) = Y$.

Avšak $y \in Y \Rightarrow y \in f(y) \Rightarrow y \notin Y$. Stejně tak $y \notin Y \Rightarrow y \notin f(y) \Rightarrow y \in Y$. A máme spor za sporem. ♡

Jako důsledek získáváme, že $P(\mathbb{N}) > \mathbb{N}$, a tedy $P(\mathbb{N})$ je *ne*spočetná. A tedy $|\mathbb{R}| = |P(\mathbb{N})| = |2^{\mathbb{N}}|$ a reálná čísla jsou nespočetná.

Důkaz. $|P(n)| = |2^{\mathbb{N}}| \dots$ Všechny funkce $\mathbb{N} \to \{0, 1\}$, což je v podstatě indikátor.

Dále ukažme, že $|\mathbb{R}| \leq |P(\mathbb{Q})| = |P(\mathbb{N})|$. Mějme $f : \mathbb{R} \to P(\mathbb{Q})$ takovou, že $x \to \{r \in \mathbb{Q} : r < x\} \subseteq \mathbb{Q}$. Potom ale $x_1 < x_2 \Rightarrow f(x_1) \subsetneq f(x_2)$, tedy f je prostá.

Pokračujme s $|\mathbb{R}| \geq |2^{\mathbb{N}}|$. Mějme $g : 2^{\mathbb{N}} \to \mathbb{R}$ takovou, že $(x_1, x_2, \dots) \to \sum_{k=1}^{\infty} x_k 3^k$. To je prosté zobrazení.

Získáváme tedy obě nerovnosti, a tedy rovnost. ♡

Tím jsme získali, že existuje nespočetné mnoho reálných čísel, která nejsou algebraická.

Velikost reálných čísel nazveme kontinuum.

Nyní víme, že $|\mathbb{N}| < |P(\mathbb{N})|$. Existuje něco mezi? Podle hypotézy kontinua nic takového není. Žádný důkaz ale nemáme.

10 Konstrukce $\mathbb{R}$ – Dedekindovy řezy

K tomu, abychom vybudovali reálná čísla, nejprve použijeme čísla racionální.

Definice. Řezem je dvojice (A, B) taková, že:

1) $\mathbb{Q} = A \cup B$
2) $A \cap B = \emptyset, A \neq \emptyset, B \neq \emptyset$
3) A nemá maximum
4) $a \in A, b \in B \Rightarrow a < b$

Reálná čísla jsou poté $\mathbb{R} = \{(A, B) \mid (A, B) \text{ je řez}\}$

Nadále budeme říkat, že $(A, B) < (A', B')$, jestliže $A \subseteq A'$. To nám dá porovnávací model reálných čísel.

Sčítání dvou reálných čísel bude $(A, B) + (A', B') = (A'', B''), A'' = A + A' = \{a + a' \mid a \in A, a' \in A'\}$.

Podobně můžeme definovat násobení, a podobně.

Věta. $\forall X \subseteq \mathbb{R}, X \neq \emptyset, X$ je omezená, potom existuje $\sup(x)$.

Důkaz. Můžeme napsat $X = \{(A_i, B_i) \mid i \in I\}$. Množiny A a B potom budou $\bigcup_{i \in I} A_i$ a $B = \mathbb{Q} \setminus A$. Chceme ukázat nyní, že $(A, B) = \sup(X)$.

1) Jedná se o horní závoru: $\forall i : (A_i, B_i) \leq (A, B) \Leftrightarrow A_i \subseteq A$.
2) Ze všech je nejmenší: $\forall$ řez (A', B') : Jestliže $A' \subset A$, potom podle definice $\exists i : A_i \nsubseteq A'$. ♡

11 Kardinální čísla

Rádi bychom pro jakoukoliv množinu X definovali $|X|$ jako určitou množinu (kardinál) takový, že:

1) X a $|X|$ mají stejnou kardinalitu.
2) Pokud X a Y jsou stejné kardinality, potom $|X| = |Y|$ jsou stejnou množinou.

Předpokládejme, že je toto možné. Definujme si nyní vlastnosti.

Začněme součtem.

Definice. Předpokládejme, že $|X| = \kappa, |Y| = \lambda$ a $X \cap Y = \emptyset$. Potom $\kappa + \lambda = |X \cup Y|$.

Věta. Součet $\kappa + \lambda$ je dobře definovaný a nezávisí na volbě X a Y.

Důkaz. Mějme $|X| = |X'| = \kappa$ a $|Y| = |Y'| = \lambda$ a předpokládejme, že $X \cap Y = X' \cap Y' = \emptyset$. Chceme, aby $|X \cup Y| = |X' \cup Y'|$.

Mějme funkce $f : X \to X'$, $g : Y \to Y'$, které jsou bijekcemi. Potom $h = f \cup g : X \cup Y \to X' \cup Y'$ je také bijekce. ♡

Vidíme, že součet velikostí disjunktních množin, tedy velikost jejich sjednocení, je dobře definovaná. Uvidíme, že se i chová hezky.

Věta.

1) $\kappa + \lambda = \lambda + \kappa$
2) $(\kappa + \lambda) + \mu = \kappa + (\lambda + \mu)$
3) $\kappa \leq \kappa + \lambda$
4) $\kappa_1 \leq \lambda_1, \kappa_2 \leq \lambda_2 \Rightarrow \kappa_1 + \kappa_2 \leq \lambda_1 + \lambda_2$

Nyní k součinu.

Definice. Předpokládejme, že $|X| = \kappa, |Y| = \lambda$. Potom $\kappa \cdot \lambda = |X \times Y|$.

Věta. Součin je dobře definovaný a nezávisí na volbě množin.

Důkaz. Mějme bijekce $f : X \to X'$ a $g : Y \to Y'$. Potom $h(x, y) = (f(x), g(y))$ je rovněž bijekce $h : X \times Y \to X' \times Y'$. ♡

Znova se podíváme na vlastnosti součinu kardinálů, a to, že jsou hezké.

Věta.

1) $\kappa\lambda = \lambda\kappa$
2) $(\kappa\lambda)\mu = \kappa(\lambda\mu)$
3) $\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$
4) $\kappa \leq \kappa\lambda$ (pokud $\lambda \neq 0$)
5) $\kappa_1 \leq \lambda_1, \kappa_2 \leq \lambda_2 \Rightarrow \kappa_1\kappa_2 \leq \lambda_1\lambda_2$

Důkaz.

1) Vidíme, že $X \times Y \neq Y \times X$. Avšak $f : (x, y) \to (y, x)$ je bijekce.
2) Funkce $g : (X \times Y) \times Z \to X \times (Y \times Z)$ je bijekce.
3) Předpokládejme $|X| = \kappa, Y = 2 = \{0, 1\}$.
   Potom $X \times Y = X \times \{0, 1\} = X \times \{0\}_{=X'} \cup X \times \{1\}_{=X''}$. Tedy $|X| = |X'| = |X''| = \kappa$ a zároveň $X \cup X' = \emptyset$. Tedy $|X \times Y| = 2\kappa = |X'| + |X''| = \kappa + \kappa$. Podobně pro větší množiny.
4) Mějme $|X| = \kappa$, $|Y| = \lambda \neq 0$. Potřebujeme prosté zobrazení $X \to X \times Y$.
   Zvolme tedy $y_0 \in Y$ a definujeme $f(x) = (x, y_0)$. To je naše hledané prosté zobrazení. ♡

Přesuňme se na mocnění.

Definice. Předpokládejme, že $|X| = \kappa, |Y| = \lambda$. Potom definujeme κ^λ jako $|X^Y| = \{f \mid f : Y \to X \text{ je funkce}\}$.

Věta. Mocnina je dobře definovaná.

Důkaz. Předpokládejme bijekce $f : X \to X', g : Y \to Y'$. Potřebujeme bijekci $h : X^Y \to X'^{Y'}$.

Vezměme si funkce $t : Y \to X$. Potom dále mějme $h : t \to t'$ takové, že $t'(y') = f(t(g^{-1}(y'))$.

Podívejme se, že h je prostá. Mějme $t_1, t_2 \in X^Y$ a nechť $h(t_1) = h(t_2)$. Chceme, aby $(\forall y) \in Y : t_1(y) = t_2(y)$. Tedy $h(t_1)(g(y)) = t_1'(g(y)) = f(t_1(y))$ a $h(t_2)(g(y)) = f(t_2(y))$. Jelikož je f bijekce, dostáváme prostotu $t_1(y) = t_2(y)$.

Dále ukážeme, že je na. Předpokládejme $t' \in X'^{Y'}$ a chceme $t \in X^Y$ takové, že $\forall y' \in Y' : t'(y') = f(t(g^{-1}(y')))$. To je ekvivalentní s tím, že $f^{-1}(t'(y')) = t(g^{-1}(y'))$ a to je ekvivalentní s $\forall y \in Y : f^{-1}(t'(g(y)) = t(y)$. Dostáváme, že $y' = g(y)$ a g je bijekce. Tedy h je rovněž na. ♡

Znova následují vlastnosti.

Věta.

1) $\kappa \leq \kappa^\lambda$ pokud $\lambda > 0$
2) $\lambda \leq \kappa^\lambda$ pokud $\kappa > 1$
3) $\kappa_1 \leq \lambda_1, \kappa^\lambda\kappa^\mu$
4) $\kappa^{\lambda\mu} = (\kappa^\lambda)^\mu$
5) $(\kappa\lambda)^\mu = \kappa^\mu\lambda^\mu$

Důkaz.

3) $\kappa^2 = |x^{\{0,1\}}|$, k té máme bijekci s $|X \times X| = \kappa\kappa$-

5) Mějme $|Z| = \mu$. Chceme bijekci $f : X^{Y \times Z} \to (X^Y)^Z$. Mějme t ze vzoru a t' z obrazu. Potom $(t'(z))(y) = t(y, z)$ je naše bijekce.

♡

Věta. Pro potenční množinu platí $|P(X)| = 2^{|X|}$. Dále $2^\kappa > \kappa$ pro každou κ.

Důkaz. Vezměme bijekci $P(X) \to \{0,1\}^X$, tedy množinu na charakteristický vektor. Tedy $|P(x)| = |\{0,1\}^X| = 2^{|X|}$. Druhá část platí automaticky díky Cantorově větě a první části. ♡

Věta. Velikost $\mathbb{R}^\mathbb{R}$, tedy všech funkcí $\mathbb{R} \to \mathbb{R}$ je 2^{2^ω}. Dále velikost $\mathcal{C}(\mathbb{R})$ všech spojitých funkcí $\mathbb{R} \to \mathbb{R}$ je 2^ω.

Důkaz. Spočítáme $|\mathbb{R}^\mathbb{R}|$. To je $|\mathbb{R}|^{|\mathbb{R}|} = (2^\omega)^{(2^\omega)} = 2^{\omega \cdot 2^\omega}$.

Dále viďme, že $\omega \leq 2^\omega$ a $2^\omega \leq 2^\omega$. Proto $\omega \cdot 2^\omega \leq 2^\omega \cdot 2^\omega = 2^{\omega+\omega} = 2^\omega$. Tedy první část platí.

Pro druhou část platí, že spojitá funkce $\mathbb{R} \to \mathbb{R}$ je jednoznačně definovaná jejími hodnatami na $\mathbb{Q}$. Proto $|\mathcal{C}(\mathbb{R})| \leq |\mathbb{R}^\mathbb{Q}|$.

Dále $f \in \mathbb{R}^\mathbb{R}$, potom restrikce $f|\mathbb{Q} \in \mathbb{R}^Q$ je prosté zobrazení. Dále $|\mathbb{R}|^{|\mathbb{Q}|} = 2^\omega$ a proto $|\mathcal{C}(\mathbb{R})| \leq 2^\omega$. Pro $|\mathcal{C}(\mathbb{R})| \geq 2^\omega$ potřebujeme všechny funkce zobrazující do racionálních konstant. To ale nejsou všechny funkce.

♡

12 Ordinální čísla

Narozdíl od kardinálů ordinály neměří velikost, ale místo toho nám říkají pořadí.

Příklad ordinálních čísel jsou přirozená čísla $0, \mathsf{S}(0), \mathsf{S}(\mathsf{S}(0)), \ldots$ až do nekonečna $\omega = \mathbb{N}$.

Vzpomeňme si, jak jsme definovali následníka u přirozených čísel, a aplikujme jej na ω. Dostáváme $\mathsf{S}(\omega) = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\} = \omega + 1$.

Pokračujme ještě dál. $\{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\} = \omega + \omega = \omega \cdot 2$. Ale stále můžeme pokračovat. $\omega + \omega \cup \{\omega \cdot 2\} = \omega + \omega + \omega = \omega \cdot 3$.

Stále toho ještě nemáme dost. $\bigcup_{n \in \omega} \omega \cdot n = \omega \cdot \omega$, podobně dále můžeme mít $\omega \cdot \omega \cdot \omega$, a tak dále...

Jsou takto definovaná ordinální čísla ale definovaná opravdu správně?

Definice. Nechť $(w, <)$ je ostře lineárně uspořádaná množina. Tato množina je dobře uspořádaná právě tehdy, když každá neprázdná podmnožina w má nejmenší prvek.

Příklad.

1) $(\mathbb{Z}, <)$ není dobře uspořádaná množina, jelikož již přímo množina sama nemá nejmenší prvek.
2) $(\mathbb{N}, <)$ je dobře uspořádaná (dokázáno použitím indukce).

Lemma. Nechť $(W, <)$ je dobré uspořádání a S je počáteční segment, tedy $S \subset W, \forall x \in S, \forall y \in W : y < x \Rightarrow y \in S$. Potom $\exists a \in W : S = \{x \in W \mid x < a\}$

Nadále budeme tuto množinu S psát jako $W[a]$.

Důkaz. Podle předpokladu $W \setminus S \neq \emptyset$, proto existuje $a = \min(W \setminus S)$.

Prvek $a \notin S$ a dále $\forall x \in S : x < a$ (jinak $x = a$ nebo $x > a \Rightarrow a \in S$).

Nyní nahlédněme, že $(\forall x) \in W : x < a \Rightarrow x \in S$. Jinak by bylo $x < a, x \notin S$, a proto $x \in W \setminus S$, což je spor. ♡

Pokud máme racionální čísla, toto lemma neplatí, například pro $\left\{x \in \mathbb{Q} \mid x < \sqrt{2}\right\}$. Problém je, že $\sqrt{2}$ není racionální číslo. To tedy i znamená, že racionální čísla nejsou dobře uspořádána.

Lemma. Nechť $(W, <)$ je dobře uspořádaná množina a $f : W \to W$ je rostoucí funkce, tedy $x < y \Rightarrow f(x) < f(y)$. Potom $\forall x \in W : f(x) \geq x$.

Důkaz. Mějme $S = \{x \in W \mid f(x) < x\}$. Chceme, aby byla tato množina prázdná. Předpokládejme tedy opak.

Potom $a = \min S$, tedy $a \in S$, a proto $f(a) < a$. Proto musí i platit $f(f(a)) < f(a)$. Jenže $f(a) \notin S$, jinak bychom měli spor s minimalitou a. Tudíž $f(f(a)) \geq f(a)$ a máme spor. ♡

Důsledek.

1) Žádná dobře uspořádaná množina není izomorfní se svým počátečním segmentem.
2) Každá dobře uspořádaná množina má na sobě právě jeden izomorfismus, a to identitu.
3) Dvě izomorfní dobře uspořádané množiny mají právě jeden izomorfismus mezi sebou.

Důkaz.

1) Předpokládejme zobrazení $f : (W, <) \to (W[a], <)$, které je izomorfní. f proto musí být rostoucí, tedy $\forall x f(x) \geq x, f(a) \geq a \notin W[a]$.
2) Pokud $f : (W, <) \to (W, <)$ je izomorfismus, potom f i f^{-1} jsou rostoucí. Tudíž $f(x) \geq x$ a zároveň $x \geq f(x)$. Spojením podmínek dostáváme $f(x) = x$.
3) Pokud $f_1, f_2 : (W_1, <) \to (W_2, <)$ jsou izomorfní, potom $f_1^{-1} \circ f_2$ je rovněž izomorfismus. Pokud ale $f_1 \neq f_2$, $f_1^{-1} \circ f_2 \neq id$ a máme spor s předchozím bodem. ♡

Věta. Předpokládejme, že W_1, W_2 jsou dobře uspořádané množiny. Potom právě jedno z následujících tvrzení platí:

1) $W_1 \cong W_2$
2) $W_1 \cong W_2[a]$ pro nějaké $a \in W_2$
3) $W_2 \cong W_1[a]$ pro nějaké $a \in W_1$

Důkaz. Ukážeme, že platí nejvýše jedna z podmínek. Předpokládejme například první a druhé tvrzení najednou. Potom ale $W_2 \cong W_2[a]$, tedy spor.

Nyní nechť $f = \{(x, y) \in W_1 \times W_2 \mid W_1[x] \cong W_2[y]\}$. Potom f nebo f^{-1} je hledaný izomorfismus.

Ukažme, že f je funkce. Mějme $(x, y_1), (x, y_2) \in f$. Potom $W_1[x] \cong W_2[y_1] \cong W_2[y_2]$. Aby tento isomorfismus existoval, musí $y_1 = y_2$.

Dále chceme, aby f byla prostá. To ukážeme analogicky.

Nakonec bychom rádi, aby f byla dostatečně velká. Nechť $S = \operatorname{dom} f$ a $T = \operatorname{ran} f$.

Pokud $S = W_1$ a $T = W_2$, potom $W_1 \cong W_2$. Nebo jestliže $S = W_1$ a $T = W_2[a]$, potom $W_1 \cong W_2[a]$. Podobně pro $S = W_1[a]$ a $T = W_2$.

Dále ukážeme, že pokud T (nebo S) je $\subsetneq W_2$ (nebo W_1), potom T (nebo S) je počáteční segment.

Předpokládejme, že T není počáteční segment, tedy $y_1 \notin T < y_2 \in T$. Potom $\exists x \in W_1 : (x, y_2) \in f$. Mějme $x_1 \in W_1$ takové, že $f(x_1) = y_1$. Tudíž je f izomorfismus $W_1[x_1]$ a $W_2[y_1]$, čímž i $(x_1, y_1) \in f$ a proto $y_1 \in T$, máme spor. Symetricky pro S.

Nakonec chceme, aby $S \neq W_1 \wedge T \neq W_2$ nemohlo nastat.

Nechť $S = W_1[a_1]$ a $T = W_2[a_2]$. Funkce f je bijekce $S \to T$, takže $(a_1, a_2) \in f$. Potom ale $a_1 \in S = W[a_1] \Rightarrow a_1 < a_1$, máme spor. ♡

Vraťme se nyní k ordinálním číslům.

Třídu (ne množinu) ordinálních čísel budeme značit $\mathcal{O}n$.

Definice. Množina T je tranzitivní, jestliže $x \in y \in T \Rightarrow x \in T$.

Tuto definici můžeme i říct jinak: $y \in T \Rightarrow y \subseteq T$.

Definice. Množina α je ordinální číslo, pokud α je tranzitivní a $(\alpha, \in)$ je dobře uspořádaná.

Definice. Množina je limitní ordinál, pokud je ordinál a není následníkem žádného jiného ordinálu.

Věta. Každé přirozené číslo $n \in \mathbb{N}$ je ordinální.

Důkaz. U přirozených čísel víme, že $x < y \Rightarrow x \in y$ a že $<$ je tranzitivní, proto $x < y < z \Rightarrow x < z$. Tedy $\mathbb{N}$ je tranzitivní.

Každá podmnožina $S \subseteq \alpha \in \mathbb{N}$ je taky $S \subseteq \mathbb{N}$, proto je $S = \emptyset$ nebo S má minimum. ♡

Věta. ω je ordinál.

Důkaz. Víme, že $x \in y \in \omega = \mathbb{N}$ splňuje $x \in \mathbb{N}$ podle tranzitivity $<$, a tedy i $\in$. Dále znova víme, že pokud $S \in \omega$, minimum podle indukce existuje. ♡

Lemma. Pokud α je ordinální číslo, potom $\mathsf{S}(\alpha) = \alpha \cup \{\alpha\}$ je ordinální.

Důkaz. Ukážeme tranzitivitu. $x \in y \in \mathsf{S}(\alpha)$ má dvě možnosti. Pokud $y \in \alpha$, potom $x \in \alpha \subseteq \mathsf{S}(\alpha)$. Nebo $y = \alpha$. Potom podle definice $x \in \alpha \subseteq \mathsf{S}(\alpha)$.

Nechť $S \neq \emptyset \subseteq \alpha \cup \{\alpha\}$. Potom buď $S = \{\alpha\}$, potom $\min S = \alpha$. Nebo $S' = S \cap \alpha \neq \emptyset$, potom existuje $m = \min S' \in \alpha$, které je i $m = minS$. ♡

Věta. Nechť α, β, γ jsou ordinály. Potom:

1) $\alpha < \beta < \gamma \Rightarrow \alpha < \gamma$. (Tranzitivita)
2) Neplatí $\alpha < \beta \wedge \beta < \alpha$. (Antisymetrie)
3) $\alpha < \beta \vee \alpha = \beta \vee \alpha > \beta$ (Linearita)
4) $\forall S \subseteq \mathcal{O}n, S \neq \emptyset$ má nejmenší prvek. (Dobré uspořádání)
5) $\forall X \subseteq \mathcal{O}n\ \exists \alpha \in \mathcal{O}n$ takový, že $\alpha \notin X$.

Než se ale pustíme do samotného důkazu, budeme potřebovat několik lemmat.

Lemma. $\alpha \in \mathcal{O}n, x \in \alpha \Rightarrow x \in \mathcal{O}n$.

Důkaz. Nejdříve dokážeme, že x je tranzitivní, tedy že $u \in v \in x \Rightarrow u \in x$. Víme, že $v \in x \in \alpha \Rightarrow v \in \alpha$, stejně tak $u \in v \in \alpha \Rightarrow u \in \alpha$.

Zjistili jsme, že $u, v, x \in \alpha$, a $\in$ je tedy na nich lineárním uspořádáním. Tedy $u \in v \in x \Rightarrow u \in x$.

Nyní ukážeme, že x je dobře uspořádané podle $\in$. Podle $y \in x \in \alpha$ máme $y \in \alpha$. Chceme, aby $x \subseteq \alpha$. Potřebujeme:

a) $\in$ je lineární uspořádaní: $\forall u, v, w \in x : u \in v \in w \Rightarrow u \in w$.
b) $\emptyset \neq S \subseteq X$, potom S má minimum. Ale znova, $S \subseteq x \subseteq \alpha \Rightarrow S \subseteq \alpha \Rightarrow S$ má minimum. ♡

Lemma. $\forall \alpha, \beta \in \mathcal{O}n : \alpha \subset \beta \Rightarrow \alpha \in \beta$

Důkaz. Víme, že $\alpha \subset \beta$. Dříve jsme dokázali, že α potom musí být počáteční segment β.

Zpozorujme, že $y \in \mathcal{O}n \Rightarrow y = \{\xi \mid \xi \in y, \xi \in \mathcal{O}n\}$.

Zadefinujme $\gamma = \min(\beta \setminus \alpha) \neq \emptyset$. Takový prvek jistě existuje, máme dobré uspořádání. Potřebujeme, aby $\gamma = \alpha$.

1) $\gamma \subseteq \alpha$: Pokud ne, potom $\delta \in \gamma \setminus \alpha$, tedy $\delta \in \beta \setminus \alpha$.
   Jelikož $\delta \in \gamma$, rovněž $\delta < \gamma$, máme spor.
2) $\gamma \supseteq \alpha$: Mějme δ, chceme aby $\delta \in \gamma$. Musí platit $\gamma \in \beta$. Pokud $\delta \notin \gamma$, potom $\delta = \gamma \vee \delta \ni \gamma$.
   Potom ale $\gamma \in \delta \in \alpha \vee \gamma = \delta \in \alpha \Rightarrow \gamma \in \alpha$. Podle předpokladu je $\gamma \in \beta \setminus \alpha$, máme spor. ♡

A teď ke skutečnému důkazu věty.

Důkaz.

1) γ je tranzitivní množina, tedy $\alpha \in \beta \in \gamma \Rightarrow \alpha \in \gamma$.
2) $\alpha < \beta < \alpha \Rightarrow \alpha < \alpha$ podle 1), potom $\alpha \in \alpha$, což je spor s dobrou uspořádaností β.
3) $\alpha \cap \beta$ je ordinál. Můžou dále nastat dvě možnosti:
   a) $\alpha \cap \beta \subseteq \alpha$.
      Potom buď $\alpha \cap \beta = \alpha \Rightarrow \alpha \subseteq \beta \Rightarrow \alpha = \beta \vee \alpha \in \beta$. Nebo $\alpha \cap \beta \subset \alpha \Rightarrow \alpha \cap \beta \in \alpha \Rightarrow \alpha \cap \beta \in \alpha \cap \beta$, ale to není ordinál.
   b) $\alpha \cap \beta \subseteq \beta$, v tom případě jsme hotovi nebo $\alpha \cap \beta = \beta$.
4) Mějme $a \in S$. Volme $S' = S \cap \alpha$. Můžou nastat možnosti, že $S' = \emptyset$, potom $\min S = \alpha$. Nebo S' má nejmenší prvek $m < \alpha$, potom $m = \min S$.
5) Nechť $Y = \cup X$. Víme, že $X \neq \emptyset$, tedy X je množina tranzitivních množin. Tedy Y je tranzitivní.
   Y je lineárně uspořádaná podle $\in$ díky vlastnosti 3). Dále je rovněž dobře uspořádaná díky 4).
   Dále Y je ordinál. Buď $\alpha = Y$ nebo $Y \in X$. V tom případě $\alpha = \mathsf{S}(Y)$.
   Jestliže $\alpha \in X$, potom $Y \cup \{Y\} = \alpha \subseteq Y$. Dostáváme $Y \in Y$, což je spor. ♡

Věta. Přirozená čísla jsou právě konečné ordinály.

Než se pustíme do další věty, teorie množin nám prozradí doposud neznámý axiom. Nejprve si pro něj však zavedeme novou notaci:

$a_0 = \emptyset, \alpha_{n+1} = \{\alpha_n\}; a = \{a_n \mid n \in \mathbb{N}\}$. Je však a množina? Rovněž a_n vypadá jako rekurze, ale jedná se skutečně o ni?

Axiom nahrazení

Nechť $P(x, y)$ je vlastnost taková, že $(\forall x)(\exists! y) : P(x, y)$. Potom:

$$(\forall A)(\exists B)(\forall x)(\exists y)(x \in A \wedge y \in B \wedge P(x, y)).$$

Jelikož vždy existuje právě jedno y pro dané x, vlastnost P se chová jako nějaké zobrazení $y = f(x)$. Problém s tímto náhledem je, že dom f jsou všechny množiny, tedy f nemůže být množina.

Použijeme tedy starý dobrý trik a nazvěme f jako třídové zobrazení, které budeme značit F.

Tedy axiom nahrazení říká, že pro dané třídové zobrazení F a pro každou množinu A je $B = F(A)$ množina. Axiom samotný nám sice nezaručuje, že v B nebudou nějaké prvky „navíc", ale ty můžeme jednoduše odstranit pomocí axiomu vydělení.

Nyní se vraťme ke slíbené větě.

Věta. Každá dobře uspořádaná množina je izomorfní s jednoznačně určeným ordinálem (uspořádáným $\in$).

Důkaz. Mějme $(W, <)$ dobře uspořádanou. Nechť $A = \{a \in W \mid W[a] \cong \alpha_a \in \mathcal{O}n\}$ je množina prvků $a \in W$ takových, že $W[a]$ je izomorfní s nějakým ordinálem.

Nazvěme $S = \{\alpha_a \mid a \in A\}$, to je množina ordinálů, která je navíc dobře uspořádaná a tranzitivní. Tedy S vypadá jako ordinál α.

Zdá se, že $\alpha \cong A$. Mějme $f : a \to \alpha_a, A \to S$. Tato funkce je definované pro každé $a \in A$. Je rovněž prostá a na, podle definice S. Tedy f je izomorfismus mezi $A \subseteq W$ a α.

Jestliže $A = W$, je vše hotovo. V případě, že $A = W[b]$, máme spor: $\forall a \in A : a < b \wedge b \in A \Rightarrow b < b$.

Nakonec je možnost, že A není počáteční segment. Pokud $c < a \in A$ a $c \notin A$, potom $\exists f : W[a] \to \alpha_a$ a $f|W[c]$ je izomorfismus $W[c]$ s nějakým počátečním úsekem α_a. Tudíž $c \in A$, spor.

Využijeme nyní axiomu nahrazení, kde $P(x, y) = x \in A \wedge y = \alpha_k$. Tedy S je množina. ♡

Věta (*Transfinitní indukce***).** Nechť $P(x)$ je vlastnost taková, že $\forall \alpha \in \mathcal{O}n : (\forall \beta < \alpha : P(b)) \Rightarrow P(\alpha)$. Potom $\forall \alpha \in \mathcal{O}n : P(\alpha)$.

Důkaz. Pro spor předpokládejme $\alpha \in \mathcal{O}n, \neg P(\alpha)$. Mějme $S = \mathsf{S}(\alpha) = \alpha + 1$, jde o množinu ordinálů. Dále nechť $S' = \{\beta \in S \mid \neg P(\beta)\} \ni \alpha$.

Potom existuje nejmenší $y \in S'$ taková, že $y \in \mathcal{O}n$, $\forall \beta < \gamma : P(\beta)$ a $\neg P(\gamma)$. Máme spor. ♡

Věta (*Transfinitní indukce 2***).** Nechť $P(x)$ je vlastnost taková, že:

1) $P(0)$
2) $\forall \alpha = \beta + 1 : P(\beta) \Rightarrow P(\beta + 1) = P(\alpha)$
3) $\forall \lim \alpha : (\forall \beta < \alpha : P(\beta)) \Rightarrow P(\alpha)$

Potom $\forall \alpha \in \mathcal{O}n : P(\alpha)$.

Věta (*Transfinitní rekurze***).** Nechť G je operace. Potom existuje operace (definovaná na $\mathcal{O}n$) taková, že $\forall \alpha \in \mathcal{O}n : F(\alpha) = G(F|\alpha)$.

13 Aritmetika ordinálů

Sčítání. Máme pevně danou $\beta \in \mathcal{O}n$. Potom:

- $\beta + 0 := \beta$
- $\beta + (\alpha + 1) := (\beta + \alpha) + 1$
- $\beta + \alpha := \sup\{\beta + \gamma \mid \gamma \in \alpha\}$, pokud α je limitní ordinál.

Tato pravidla stačí, ukážeme pomocí rekurze:

Chceme, aby $F(\alpha) = \beta + \alpha \forall \alpha \in \mathcal{O}n$. nechť $G(x) = y$ pokud (x je funkce a dom(x) je nějaký ordinál α a $(\alpha = 0 \wedge y = \beta$ nebo $\alpha = \gamma + 1 \wedge y = x(\gamma) + 1$ nebo α je limitní ord. $\wedge\, y = \sup\{x(\gamma) \mid \gamma \in \alpha\}))$, nebo $x = y$ (v tom případě nám to je jedno).

Příklad. $\beta + 2 = \beta + (1 + 1) = (\beta + 1) + 1) = \mathsf{SS}(\beta)$

$\omega + \omega = \sup\{\omega + n \mid n \in \omega\}$

$2 + \omega = \{2 + n \mid n \in \omega\} = \omega$

Vidíme tedy, že sčítání ordinálů není komutativní.

Věta (*Alternativní definice sčítání***).** Mějme W_1, W_2 disjunktní dobře uspořádané množiny izomorfní s α_1, α_2. Dále nechť $W = W_1 \cup W_2$ a uspořádání $<$ na W bude na W_1 a W_2 definované stejně, a pro $x \in W_1, y \in W_2$: $x < y$.

Potom W je izomorfní s $\alpha_1 + \alpha_2$.

Tato věta může sloužit jako definice $\alpha_1 + \alpha_2$.

Důkaz. Použitím transfinitní indukce na α_2 s pevně daným α_1. Vlastnost bude $P(\alpha_2) : \forall W_2$ typu $\alpha_2 : W$ je typu $\alpha_1 + \alpha_2$.

a) $P(0) : W_2 = \emptyset \dots W = W_1$ typu $\alpha_1 + 0 = \alpha_1$ podle definice $+$.

b) $P(\gamma) \Rightarrow P(\alpha_2) : \alpha_2 = \gamma + 1, W_2 \cong \alpha_2$. Potom W_2 vypadá jako $W_2' \cong \gamma$ spojená s f.

Tedy $W = W_1 \sim W_2' \sim f$. W' je typu $\alpha_1 + \gamma$. Potom $W = (\alpha_1 + \gamma) + 1$. Chceme rozšířit $\varphi' : W' \to \alpha_1 + \gamma$ na $\varphi : W \to (\alpha_1 + \gamma) + 1$ a to přes $\varphi(f) := \alpha_+ + \gamma$

c) Chceme $P(\alpha_2)$ pro α_2 limitní ordinály. Můžeme předpokládat $P(\gamma)$ pro $\gamma < \alpha_2$.

Víme, že $W = W_1 \sim W_2 \overset{\varphi}{\leftarrow} \alpha_1 + \alpha_2$. Podle definice $\alpha_1 + \alpha_2 = \sup\{\alpha_1 + \gamma \mid \gamma \in \alpha_2\} = \{\beta \mid \beta \in \alpha_1\} \cup \{\alpha_1 + \gamma \mid \gamma \in \alpha_2\}$.

Potom $\varphi(\beta) \in W_1$. Využijeme, že $\alpha_1 \cong W_1$. Dále podle předpokladu $\alpha_1 + \gamma \cong W_1 \cup W_2'$ pokud $\gamma \cong W_2'$. Nechť $\varphi_1 : \alpha_1 to W_1$ a $\varphi_2 : \alpha_2 \to W_2$. Potom $\varphi(\alpha_1 + \gamma) = \varphi_2(\gamma)$.

♡

Věta. Nechť $\alpha_1, \alpha_2, \beta \in \mathcal{O}n$. Potom:

1) $\alpha_1 < \alpha_2 \Leftrightarrow \beta + \alpha_1 < \beta + \alpha_2$
2) $\alpha_1 = \alpha_2 \Leftrightarrow \beta + \alpha_1 = \beta + \alpha_2$
3) Platí asociativita

Pozor na nekomutativitu sčítání. Důkaz nebude.

Věta. Mějme ordinály $\alpha \leq \beta$. Potom existuje právě jeden ordinál ξ, že $\beta = \alpha + \xi$.

Důkaz. Podíváme se na $\beta \setminus \alpha$. To je podmnožinou β. Zachovalo se tedy dobré uspořádání, proto existuje právě jedna $\xi \in \mathcal{O}n$, kde $\beta \setminus \alpha \cong \xi$.

Tedy $W_1 = \alpha, W_2 = \beta \setminus \alpha \cong \xi \in \mathcal{O}n$. Tudíž $W = \beta$ typu $\alpha + \xi$ a přitom typu β. Proto $\beta = \alpha + \xi$. ♡

Násobení.

- $\beta \cdot 0 = 0$
- $\beta \cdot (\gamma + 1) = \beta\gamma + \beta$
- $\beta \cdot \alpha = \sup\{\beta\gamma \mid \gamma \in \alpha\}$ pro limitní ordinál α

Příklad. $\beta \cdot 1 = \beta \cdot (0 + 1) = \beta 0 + \beta = 0 + \beta = \beta$.

$\beta \cdot 2 = \beta \cdot (1 + 1) = \beta \cdot 1 + \beta = \beta + \beta$.

$\beta \cdot \omega = \sup\{\beta \cdot 1, \beta \cdot 2, \dots\}$.

$\omega \cdot \omega =$ hodně.

Věta. Mějme $\alpha, \beta \in \mathcal{O}n$. Na $\alpha \times \beta$ definujeme anti-lexikografické pořadí $\prec$ podle $(a_1, b_1) \prec (a_2, b_2) \Leftrightarrow b_1 < b_2 \vee (b_1 = b_2 \wedge a_1 < a_2)$.

Potom toto je dobré uspořádáná množina typu $\alpha \cdot \beta$.

Důkaz. Ukážeme, že jde o dobré uspořádání. Dále definujeme izomorfismus $f : \alpha \times \beta \to \alpha\beta$ a to tak, že $f(a, b) = \alpha \cdot b + a$. Nakonec použijeme indukci. ♡

Mocnění.

- $\beta^0 = 1$.
- $\beta^{\gamma+1} = \beta^\gamma \cdot \beta$.
- $\beta^\alpha = \sup\{\beta^\gamma \mid \gamma \in \alpha\}$ pro α limitní ordinály.

Příklad. $2^\omega = \sup\{2^\gamma \mid \gamma < \omega\} = \omega$. Toto není potenční množina, která se někdy značí 2^ω (kardinální mocnění).

$\omega^2 = \omega^1 \cdot \omega$

$\omega^1 = \omega^{0+1} = \omega^0 \cdot \omega^1 = 1 \cdot \omega = \omega$

$\omega^\omega = \sup\{\omega, \omega^2, \dots\} =$ stále spočetná množina.

$\omega^{\omega^{\omega^\cdots}}$ je stále spočetná množina.

14 Axiom výběru

Dvě přednášky chybí, soustředění KSP + nemoc.

15 Ramseyova teorie

$R(k)$ je nejmenší n takové, že pro každé 2-obarvení grafu $E(K_n)$ v grafu existuje jednobarevný K_k.

$R(\aleph_0) = \aleph_0$

$R(\aleph_1) > 2^{\aleph_0}$

Důkaz. Sporem. Předpokládejme $R(\aleph_1) \leq 2^{\aleph_0}$. Pro každé 2-obarvení $E(G)$, kde $G \cong K_{2^{\aleph_0}}$ a $V = \mathbb{R}$.

Podle axiomu výběru najdeme dobré uspořádání $\mathbb{R}$, budeme je značit $\prec$. Dále si zvolíme normální uspořádání $<$. Dále $c(\{x, y\})$ bude červené, pokud $x < y \wedge x \prec y$ nebo modré, když $x < y \wedge x \succ y$.

Podle předpokladu existuje kopie $K_\aleph = S \subseteq \mathbb{R}$ v G taková, že $|S| = \aleph$ a je celá červená nebo modrá. Jelikož je modrá analogická k červené, stačí uvažovat červenou.

Z definice červených hran získáváme $(S, <) \cong (S, \prec)$, rovněž dobře uspořádanou množinu.

Definujme zobrazení $f : \mu \to V(K_\aleph)$. Z toho dostaneme izomorfismus $(\mu, \in) \to (V(K_\aleph), \prec)$, což je dobře uspořádaná množina.

Z toho vyplývá, že $\mu \geq \aleph_1 \Leftrightarrow \mu$ není spočetná ($|\mu| = \aleph_1$).

Definujeme nespočetnou posloupnost otevřenách intervalů v $\mathbb{R}$: $I_\alpha = (f(\alpha), f(\alpha + 1))$.

- $f(\alpha) < f(\alpha + 1)$ díky tomu, že $f(\alpha) \prec f(\alpha + 1) \wedge \{f(\alpha), f(\alpha + 1)\}$ je červená.
- $\alpha < \beta \Rightarrow I_\alpha \cap I_\beta = \emptyset$, jelikož $\alpha < \beta \Rightarrow \alpha + 1 \leq \beta \Rightarrow f(\alpha + 1) \leq f(\beta)$, ale $I_\alpha \cap I_{\alpha+1} = \emptyset$.

Tímto dostáváme poměrně slušný systém intervalů $I_0, I_1, \ldots$, který je izomorfní s

Zvolme $q_\alpha \in \mathbb{Q} \cap I_\alpha$. Tímto získáváme spor, máme $\{q_\alpha : \alpha \in \mu\}$, z potenční množiny racionálních čísel. ♡

16 Stromy

Dívejme se na nekonečné stromy, ve kterých se může vyskytovat nekonečná cesta. V takovém případě už nemůžeme uvažovat o hranách, místo toho si představme částečné uspořádání.

Definice. Strom je částečné uspořádání $(T, <)$ takové, že

- T má nejmenší prvek (kořen)
- $\forall x \in T : \{y \in T \mid y < x\}$ je dobře uspořádaná podle $<$. (právě jedna cesta z kořenu do x)

Prvky T jsou vrcholy, $x < y \Rightarrow x$ je předek y a y je následník x.

Výška $h(x)$ je typ množiny $\{y \in T : y < x\}$.

Příklad. $\mathcal{T}_\alpha = \alpha = \omega + 4$ s normálním uspořádáním $<$. Potom $\forall \gamma < \alpha : h(\gamma) = \gamma$.

Přímý následník x v $(T, <)$ je takové $y \in T$, kde $x < y \wedge \neg \exists z \in T : x < z < y$.

Pozorování: Pokud x není maximální, potom má přímého následníka.

Důkaz. Zvolme $y > x$. Nechť $S = \{z \in T : z < y\}$, což je dobře uspořádaná množina, která obsahuje x.

Buď neexistuje $z : x < z < y$, nebo $\emptyset \neq S' = \{z : x < z < y\} \subseteq S$. Ta má minimální prvek $s \in S'$. Dále $x < s$ a pokud $x < t < s$, potom $t \in S'$, což by porušilo minimalitu s. ♡

Pokud $(T, <)$ je strom, potom T_α bude $\{x \in T : h(x) = \alpha\}$. Dále $h(T) = \min\{\alpha : T_\alpha = \emptyset\}$.

Větev stromu b je maximální řetězec v T, $l(b)$ je typ b. Kofinální větev je taková větev b, že $l(b) = h(T)$.

Příklad. $V(T) = \{(a, b) \in \omega \times \omega \mid a \leq b \wedge a \geq 1\} \cup \{(0, 0)\}$, $(a, b) < (c, d)$ pokud $(a, b) = (0, 0)$ nebo $b = d \wedge a < c$.

$\forall k \in \omega \exists b : l(b) = k$

$h(T) = \omega \quad \forall k \in \omega : T_k \neq \emptyset$

Neexistuje kofinální větev.

Věta (*Königovo lemma*). Pokud $h(T)$ je spočetná a $\forall k : T_k$ je konečná, potom T má nekonečnou (kofinální) větev.

Důkaz. c_0 je kořen stromu. Množina $\{x \in T \mid x > c_0\}$ je nekonečná. Pokud $c_0, \ldots, c_{n-1}$ je dobře definovaná, nechť S jsou přímí následníci c_{n-1}. S je konečná, z té vybereme $c_n \in S$ takovou, že $\{x \in T \mid x > c_n\}$ je nekonečná.

Jelikož průnik podstromů vrcholů z množiny S je nekonečný, musí být alespoň jedná větev nekonečná. Používáme zde axiom výběru.

Výsledný řetězec $\{c_n \mid n \in \omega\}$ je nekonečná větev. ♡

Věta. Nechť G je graf, kde $V(G) = \omega$. Dále pro $k \in \omega$ platí: $\xi(G) \leq k \Leftrightarrow \forall n : \xi(G[\{0, \ldots, n-1\}]) \leq k$.

Důkaz. Nechť $T = \{c \mid \exists n \in \omega : c \text{ je } k\text{-obarvení } G[\{0, \ldots, n-1\}]\}$ uspořádaný podle inkluze. T je strom, $|T_n| \leq k^n$, tedy strom je konečně větvící se. Dále $\forall n \in \omega : T_n \neq \emptyset$. Tedy $h(T) = \omega$.

Tudíž existuje nekonečná větev $c = \{c_0, c_1, \ldots\}$, potom $\bigcup C$ označuje správné k-obarvení, jelikož přímý následník c označuje rozšíření obarvení c. ♡

Tato věta je konkrétní použití věty o kompaktnosti.