Teorie množin

slidy k přednášce Logika a teorie množin – ZS 2016/17

Petr Glivický

petrglivicky@gmail.com

Ke stažení na www.glivicky.cz

Doporučená literatura

Elektronická:

- **tyto slidy** a **text k přednášce** dostupné na mém webu – primární a požadavkům na zkoušku plně dostačující zdroj
- **slidy Petra Pajase**
  http://ufal.mff.cuni.cz/ pajas/vyuka/logika_temno.pdf

Tištěná: (značně přesahuje rámec přednášky)

- Bohuslav Balcar, Petr Štěpánek, *Teorie množin*.

Historie a motivace

viz slidy Základy moderní matematiky

naivní teorie množin vs. axiomatická teorie množin

Gödel-Bernaysova (GB), Zermelo-Fraenkelova (ZF), Kelley-Morseova (KM), Russelova teorie typů, ...

ZFC $=$ ZF $+$ axiom výběru

Vše je množina.
Všechny vztahy jsou množinové ($\in$).

svět matematiky

Axiomatika ZF

Jazyk $L = \langle \in \rangle$.

existence:	$(\exists x) x = x$
extenzionalita:	$(\forall x)(\forall y)((\forall u)(u \in x \leftrightarrow u \in y) \rightarrow x = y)$
schéma vydělení:	$(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow (u \in x \,\&\, \varphi(u)))$ pro φ formuli
dvojice:	$(\forall x)(\forall y)(\exists z)(\forall u)(u \in z \leftrightarrow u = x \vee u = y)$
sjednocení:	$(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow (\exists y)(y \in x \,\&\, u \in y)$
potence:	$(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow (\forall v)(v \in u \rightarrow v \in x))$
schéma nahrazení:	„definovatelný obraz množiny je množina“
nekonečno:	„existuje nekonečná množina“
fundovanost:	„neexistuje nekonečný klesající $\in$-řetězec“

Třídy, notace

Třída: $X = \{x; \varphi(x)\}$
prvky tříd jsou jen množiny

každá množina je třída

vlastní třída

$\mathbf{V} = \{x; x = x\}$
univerzální třída
je vlastní (Russelův paradox)

používání tříd jako zkratek
$(x \in X \Leftrightarrow \varphi(x))$

Zavedení elementárních pojmů

$$x \subseteq y \leftrightarrow (\forall u)(u \in x \rightarrow u \in y)$$

$$\emptyset = \{u \in x; u \neq u\}$$

$$\bigcup X = \{u; (\exists x)(x \in X \,\&\, u \in x)\}$$

$$\bigcap X = \{u; (\forall x)(x \in X \rightarrow u \in x)\}$$

$$\{x, y\},\ \{x\},\ \{x_1, \ldots, x_n\},\ \{u \in x; \varphi(u)\}$$

$$x \cup y,\ x \cap y,\ x - y$$

$$\mathcal{P}(x)$$

Uspořádaná dvojice a n-tice

uspořádaná dvojice

$$(x, y) = \{\{x\}, \{x, y\}\}$$

uspořádaná n-tice s $n > 2$

$$(x_1, \dots, x_{n+1}) = ((x_1, \dots, x_n), x_{n+1})$$

uspořádaná 1-tice

$$(x) = x$$

uspořádaná 0-tice

$$() = \emptyset$$

Kartézský součin a mocnina

kartézský součin

$$X \times Y = \{(u, v); u \in X \,\&\, v \in Y\}$$

pro množiny x, y lze vydělit z $\mathcal{P}(\mathcal{P}(x \cup y))$

kartézská mocnina

$$X^n = \{(u_1, \ldots, u_n); u_1 \in X \,\&\, \ldots \,\&\, u_n \in X\}$$

($n \geq 0$ je zde „metapřirozené číslo“)

Příklad: $X^1 = X$ $\qquad X^0 = \{\emptyset\}$

Relace

relace (na třídě X)

$R \subseteq X^2$, tj. třída dvojic

domain a range

$$\mathrm{dom}(R) = \{u; (\exists v)((u, v) \in R)\}$$

$$\mathrm{rng}(R) = \{v; (\exists u)((u, v) \in R)\}$$

pro množinovou R lze vydělit z $\bigcup\bigcup R$

inverz

$$R^{-1} = \{(u, v); (v, u) \in R\}$$

obraz a vzor

$$R[Y] = \{v; (\exists u \in Y)((u, v) \in R)\}$$

$R^{-1}[Y]$, tj. obraz v inverzní relaci

restrikce

$$R \restriction Y = \{(u, v) \in R; u \in Y\}$$

skládání

$$R \circ S = \{(u, w); (\exists v)((u, v) \in R \,\&\, (v, w) \in S)\}$$

zobrazení (funkce)
relace F splňující $(u, v), (u, w) \in F \rightarrow v = w$

Je-li $(u, v) \in F$, značíme $F(u) = v$.

Pokud $X = \mathrm{dom}(F)$, $Y \supseteq \mathrm{rng}(F)$, píšeme $F : X \rightarrow Y$

F prostá:	$F(u) = F(u') \rightarrow u = u'$
F na Y:	$Y = \mathrm{rng}(F)$
F bijekce X a Y:	$F : X \rightarrow Y$ prostá a na Y

množinová mocnina

$${}^{y}X = \{f; f : y \to X\}$$

Pro x množinu lze ${}^{y}x$ vydělit z $\mathcal{P}(y \times x)$.

Příklad: ${}^{\emptyset}X = \{\emptyset\}$, $\quad y \neq \emptyset \to {}^{y}\emptyset = \emptyset$

Příklad: ${}^{2}X \approx X^2$

Indexový soubor

indexový soubor

x funkce, $\mathrm{dom}(x) = I$

místo x píšeme též $\langle x_i; i \in I \rangle$ či $\langle x_i \rangle_{i \in I}$,

kde x_i je $x(i)$.

sjednocení a průnik souboru

$$\bigcup_{i \in I} x_i = \bigcup \mathrm{rng}(x)$$

$$\bigcap_{i \in I} x_i = \bigcap \mathrm{rng}(x)$$

kartézský součin (produkt) souboru

$$\prod_{i \in I} x_i = \{f; \text{„}f \text{ je funkce“ } \& \,\mathrm{dom}(f) = I \,\&\, (\forall i \in I) f(i) \in x_i\}$$

Relace ekvivalence

ekvivalence

(binární) relace E, která je reflexivní, symetrická a tranzitivní

reflexivní: $(x,x) \in E$

symetrická: $(x,y) \in E \rightarrow (y,x) \in E$

tranzitivní: $(x,y) \in E \,\&\, (y,z) \in E \rightarrow (x,z) \in E$

třída ekvivalence

$$[x]_E = E[\{x\}] = \{y; (x,y) \in E\}$$

faktorizace

E ekvivalence na A (tj. $E \subseteq A^2$)

$$A/E = \{[x]_E; x \in A\}$$

rozklad na A

$C \subseteq \mathcal{P}(A)$ s $\bigcup C = A$ a $c \cap c' = \emptyset$ for $c \neq c'$ z C

E ekvivalence na $A \Rightarrow \{[x]_E; x \in A\}$ je rozklad na A

C rozklad na $A \Rightarrow E = \{(x,y)(\exists c \in C)x, y \in c;\}$ je ekvivalence na A

Relace uspořádání

(binární) relace R na A

antireflexivní:	$(x,x) \notin R$
antisymetrická:	$(x,y) \in R \rightarrow (y,x) \notin R$
slabě antisymetrická:	$(x,y) \in R \,\&\, (y,x) \in R \rightarrow x = y$
trichotomická:	$(x,y) \in R \vee (y,x) \in R \vee x = y$

(neostré částečné) uspořádání

(binární) relace R, která je reflexivní, slabě antisymetrická a tranzitivní

ostré (částečné) uspořádání

(binární) relace R, která je (antireflexivní), antisymetrická a tranzitivní

lineární uspořádání na A

je-li navíc trichotomická na A

$(x,y) \in R$ značíme xRy

Uspořádání

$\leq$ neostré uspořádání na A

dolní a horní třída

dolní: $X \subseteq A$ taková, že $y \leq x \in X \rightarrow y \in X$

horní: $X \subseteq A$ taková, že $y \geq x \in X \rightarrow y \in X$

$\leq$ neostré uspořádání na A
$X \subseteq A$, $a \in A$

a je pro X vzhledem k $\leq$ na A

minoranta:	$(\forall x \in X) a \leq x$
nejmenší:	$a \in X$ & minoranta
minimální:	$a \in X \,\&\, (\forall x \in X)(x \neq a \rightarrow x \not\leq a)$
infimum:	největší minoranta

majoranta:	$(\forall x \in X) a \geq x$
největší:	$a \in X$ & majoranta
maximální:	$a \in X \,\&\, (\forall x \in X)(x \neq a \rightarrow x \not\geq a)$
supremum:	nejmenší majoranta

Uspořádání

$\langle A, \leq \rangle$ dobré uspořádání

neprázdná podmnožina má nejmenší prvek

Příklad: $\langle \mathbb{N}, \leq \rangle$

dobré $\Rightarrow$ lineární

konečné a lineární $\Rightarrow$ dobré

$\langle A, \leq \rangle$ úplný svaz

neprázdná podmnožina má infimum i supremum

Příklad: $\langle [0,1], \leq \rangle$, $\langle \mathcal{P}(x), \subseteq \rangle$

Věta o pevném bodě

neklesající a nerostoucí funkce

$f : A \to A$ neklesající, pokud $x \leq y \to f(x) \leq f(y)$

$f : A \to A$ nerostoucí, pokud $x \leq y \to f(x) \geq f(y)$

pevný bod funkce

$f : A \to A$, $u \in A$ je pevý bod f, pokud $f(u) = u$

Věta (o pevném bodě)

Neklesající funkce na úplném svazu má pevný bod.

Přirozená čísla v teorii množin

Všechno je množina.
Každé přirozené číslo je množina.

$$0 = \emptyset$$
$$1 = \{0\} = \{\emptyset\}$$
$$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$$
$$3 = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$
$$\vdots$$
$$n + 1 = \{0, 1, \dots, n\} = n \cup \{n\}$$
$$\vdots$$

n je „n-prvková množina“

$$n = \{0, 1, \dots, n - 1\}$$

Každé n je definováno zvlášť.
Není jasné, jak definovat $\{0, 1, 2, \dots\}$
(ani jako třídu).

Množina přirozených čísel

induktivní množina

$$0 \in z \,\&\, (\forall u)(u \in z \rightarrow u \cup \{u\} \in z)$$

Dle axiomu nekonečna existuje nějaká induktivní množina.

množina přirozených čísel

nejmenší induktivní množina = průnik všech induktivních

značíme ω či $\mathbb{N}$

Je $0 \in \omega$, $1 \in \omega$, $2 \in \omega$, ...

Ale obecně: $\omega \neq \{0, 1, 2, \ldots\}$

Může existovat $x \in \omega$ různé od všech čísel $0, 1, 2, \ldots$.

(x je přirozené číslo v teorii množin, které neodpovídá žádnému meta-přirozenému číslu; nestandardní přirozené číslo)

Princip matematické indukce

Tvrzení (princip matematické indukce)

Nechť φ je formule jazyka teorie množin.
$\varphi(0)$ *a* $(\forall u)(\varphi(u) \rightarrow \varphi(u \cup \{u\})) \Rightarrow (\forall u \in \omega)\varphi(u)$

(Alternativně: $0 \in z$ *a* $(\forall u)(u \in z \rightarrow u \cup \{u\} \in z) \Rightarrow \omega \subseteq z$*)*

Důkaz.

Z minimality ω jako induktivní množiny. $\square$

Konstrukce rekurzí

Častá metoda konstrukce funkcí $f : \mathbb{N} \to \mathbf{V}$ ($\mathbf{V}$ univerzální třída) je konstrukce rekurzí.

$(n! = n \cdot (n-1)!)$

Tvrzení (konstrukce rekurzí)

Buď G třídové zobrazení s $\operatorname{dom}(G) = \mathbf{V}$ (konstruující zobrazení). Pak existuje jediná funkce $f : \omega \to \mathbf{V}$ splňující $f(n) = G(f \restriction n)$ pro každé $n \in \omega$.

Důkaz.

f se sestrojí jako $\bigcup_{n\in\omega} f_n$, kde $\emptyset = f_0 \subseteq f_1 \subseteq \dots$ je posloupnost funkcí s $\operatorname{dom}(f_n) = n$ a $f_n(n) = G(f_{n-1})$. Existence f_n pro každé $n \in \omega$ plyne matematickou indukcí.

Jednoznačnost plyne matematickou indukcí dle n. $\square$

Příklad: Pro konstrukci funkce $f(n) = n!$ je třeba zvolit G tak, aby: $G(\emptyset) = 1$ a $G(h) = n \cdot h(n-1)$, pro funkci h s $\operatorname{dom}(h) = n$.

Další číselné obory

celá čísla

$$\mathbb{Z} = (\{0\} \times \mathbb{N}) \cup (\{1\} \times (\mathbb{N} - \{0\}))$$

racionální čísla

$$\mathbb{Q} = \{(m, n); m \in \mathbb{Z},\ 0 \neq n \in \mathbb{N}\}/\sim,$$

kde $(m, n) \sim (m', n') \Leftrightarrow mn' = nm'$.

reálná čísla

$$\mathbb{R} = \{r; \emptyset \neq r \subseteq \mathbb{Q} \text{ je dolní množina}\}$$

(Dedekindovy řezy)

komplexní čísla

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}$$

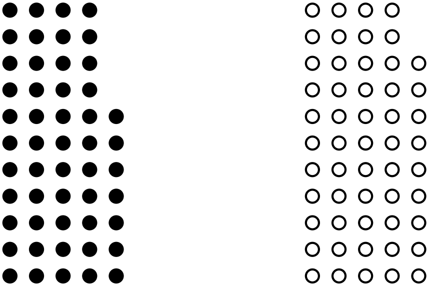
Není tedy např. $\mathbb{N} \subseteq \mathbb{Z}$, ale máme prosté $f : \mathbb{N} \to \mathbb{Z}$, $f(n) = (0, n)$.
Podobně pro ostatní inkluze.

Srovnávání velikostí množin

konečné velikosti

umíme srovnávat i počítat

když neumíme počítat – případ pasáčka ovcí



Subvalence a ekvipotence

$$x \preccurlyeq y$$

$\exists f : x \to y$ prosté

je reflexivní, tranzitivní (ale ne slabě antisymetrická)

$$x \approx y$$

$\exists f : x \to y$ bijekce

je to relace ekvivalence

$$x \prec y$$

$x \preccurlyeq y$ a $x \not\approx y$

Příklad: $\{u, v\} \approx \{a, b\} \prec \{a, c, d\}$

Příklad: $\mathbb{Z} \approx \{z \in \mathbb{Z}; z \text{ sudé}\}$

Příklad: Hilbertův hotel

Tvrzení

$\mathbb{N} \approx \mathbb{Z} \approx \mathbb{Q} \prec \mathbb{R} \approx \mathbb{C}$

Cantor-Bernsteinova věta

Věta (Cantor-Bernsteinova)

$x \preccurlyeq y$ a $y \preccurlyeq x \Rightarrow x \approx y$

Důkaz.

Netriviální!!!

Pomocí věty o pevném bodě. $\square$

Cantorova věta o neomezených velikostech množin

Neexistuje maximální velikost množiny.

Věta (Cantorova)

$x \prec \mathcal{P}(x)$

Důkaz.

Sporem: diagonální metoda. Obdobné Russelovu paradoxu. □

Konečné množiny

x je konečná množina
každá $y \subseteq \mathcal{P}(x)$ má maximální prvek vzhledem k $\subseteq$
značíme $Fin(x)$ a třídu všech konečných množin Fin

Příklad: ω není konečná, $\omega \subseteq \mathcal{P}(\omega)$ nemá maximální prvek

Tvrzení (princip indukce pro konečné množiny)

Buď Z třída.
$0 \in Z$ *a* $(\forall u, v)(u \in Z \rightarrow u \cup \{v\} \in Z) \Rightarrow Fin \subseteq Z$

Tvrzení

x je konečná $\Leftrightarrow$ *$x \approx n$ pro nějaké $n \in \omega$*

Důkaz.

Indukcí. $\square$

Množinová aritmetika

Aritmetické operace na velikostech konečných i nekonečných množin zavedeme pomocí množinových operací.

množinový součet

$$x \uplus y = (\{0\} \times x) \cup (\{1\} \times y)$$

(disjunktní sjednocení)

množinový součin

$$x \times y$$

(kartézský součin)

množinová mocnina

$${}^{y}x$$

Tvrzení

Jsou-li x, y konečné, pak $x \uplus y$, $x \times y$ a ${}^{y}x$ jsou konečné.

Zavedení operací a uspořádání na $\mathbb{N}$

aritmetické operace na $\mathbb{N}$

$$m + n = k \Leftrightarrow k \approx m \uplus n$$

$$m \cdot n = k \Leftrightarrow k \approx m \times n$$

$$m^n = k \Leftrightarrow k \approx {}^n m$$

uspořádání na $\mathbb{N}$

$$m < n \Leftrightarrow m \in n$$

$$m \leq n \Leftrightarrow m \subseteq n \; (\Leftrightarrow m \in n \vee m = n)$$

Tvrzení

1) Operace $+$, $\cdot$, m^n na $\mathbb{N}$ splňují obvyklé zákony (asociativita, komutativita, distributivita, $m^{n+k} = m^n \cdot m^k$, $m^{n \cdot k} = (m^n)^k$, $\ldots$).
2) $\leq$ je dobré uspořádání na $\mathbb{N}$ s nejmenším prvkem 0 a bez největšího prvku, $<$ je jeho ostrá verze.

Spočetné a nespočetné množiny

ω má nejmenší nekonečnou velikost,
tj. x nekonečná $\Rightarrow x \succcurlyeq \omega$.

x je spočetná množina
$x \approx \omega$

x je nespočetná množina
x je nekonečná a $x \not\approx \omega$

Velikosti číselných oborů

Tvrzení

$\mathbb{N}$, $\mathbb{Z}$ a $\mathbb{Q}$ jsou spočetné množiny.

Tvrzení

$\mathbb{R}$ a $\mathbb{C}$ jsou nespočetné množiny. Je $\mathbb{C} \approx \mathbb{R} \approx \mathcal{P}(\omega) \approx {}^{\omega}2$.

mohutnost kontinua

Pokud $x \approx \mathbb{R}$, má x mohutnost kontinua.

Existuje množina x s $\mathbb{N} \prec x \prec \mathbb{R}$?

Záporná odpověď se nazývá hypotéza kontinua (CH).

Nelze ji v ZFC ani dokázat ani vyvrátit.

Příklad: Existence transcendentních čísel

algebraické číslo

$x \in \mathbb{R}$, které je kořenem nějakého nenulového polynomu

$$a_n x^n + \ldots + a_1 x + a_0 \text{ s } a_i \in \mathbb{Z}$$

transcendentní číslo

není algebraické

Příklad: Čísla $1/2$, $\sqrt{2}$, $\sqrt[5]{3\sqrt[3]{7/2}+7}$ jsou algebraická.
Ale ne každé algebraické číslo je možné zapsat pomocí odmocnin (Niels Henrik Abel, neřešitelnost polynomiálních rovnic pátého řádu v radikálech).

Příklad: Čísla e, π jsou transcendentní.

Tvrzení

Množina algebraických čísel je spočetná.

Důsledek

Existuje transcendentní číslo; množina transcendentních čísel je nespočetná, mohutnosti kontinua.

Příklad: Podivné funkce

Tvrzení

Množina všech spojitých funkcí $f : \mathbb{R} \to \mathbb{R}$ *má mohutnost kontinua.*

Důkaz.

Spojitá funkce je jednoznašně určena svými hodnotami na $\mathbb{Q}$. $\square$

Důsledek

Existuje funkce $f : \mathbb{R} \to \mathbb{R}$, *jejíž graf protíná graf každé spojité reálné funkce.*

Ordinální čísla

Připomenutí: dobré uspořádání $\Leftrightarrow$ každá neprázdná množina má nejmenší prvek

tranzitivní množina

x taková, že $u \in x \to u \subseteq x$

Množiny $0, 1, \ldots, \omega$ jsou tranzitivní a dobře uspořádané relací $\in$.

ordinální číslo, ordinál

α tranzitivní a dobře ostře uspořádaná relací $\in$

třída ordinálních čísel: **On**

α ordinál $\Rightarrow$ $\alpha \cup \{\alpha\}$ ordinál

Příklad: Následující množiny jsou ordinály: $\omega+1 = \omega \cup \{\omega\}$, $\omega+2 = (\omega+1) \cup \{\omega+1\}$, $\omega+3, \ldots, \omega+\omega = \omega \cdot 2 = \bigcup\{\omega+n; n \in \omega\}, \omega \cdot 2 + 1, \ldots, \omega \cdot 3, \ldots, \omega \cdot \omega = \omega^2 = \bigcup\{\omega \cdot n; n \in \omega\}, \ldots, \omega^3, \ldots, \omega^{(\omega)} = \bigcup\{\omega^n; n \in \omega\}, \ldots, \omega^{(\omega^{(\omega)})}, \ldots, \omega^{(\omega^{(\omega^{(\omega)})})}, \ldots$.
Každá z uvedených množin je spočetná.

Třída **On**

Tvrzení

On *je tranzitivní a dobře ostře uspořádaná relací* $\in$.

Důkaz.

Cvičení. □

On je vlastní třída
(jinak **On** $\in$ **On** – spor)

uspořádání na **On**
Pro $\alpha, \beta \in$ **On** píšeme $\alpha < \beta \Leftrightarrow \alpha \in \beta$.

Typy dobrých uspořádání

izomorfizmus uspořádání $\langle A, <\rangle$ a $\langle B, \ll\rangle$
$f : A \to B$ bijekce a $x < y \leftrightarrow f(x) \ll f(y)$
píšeme pak $\langle A, <\rangle \cong \langle B, \ll\rangle$

Ordinální čísla jsou právě „izomorfní typy“ dobrých uspořádání.

Tvrzení

Pro každé dobré ostré uspořádání $\langle A, <\rangle$ existuje ordinál α, takový že $\langle A, <\rangle \cong \langle \alpha, \in\rangle$.

Důkaz.

Buď P třída všech „počátkových zobrazení“ z A do **On**. Pak $f = \bigcup P$ je zobrazení s $\mathrm{dom}(f) = A$ a $\mathrm{rng}(f) = \alpha \in$ **On**; f je hledaný izomorfizmus. □

α z tvrzení značíme $\mathrm{otp}(\langle A, <\rangle)$ a nazýváme ordinální (izomorfní) typ $\langle A, <\rangle$.

Ordinální aritmetika – součet a součin

lexikografické uspořádání na **On** $\times$ **On**

$$(\alpha, \beta) <_{lex} (\alpha', \beta') \Leftrightarrow \alpha < \alpha' \vee (\alpha = \alpha' \,\&\, \beta < \beta')$$

$<_{lex}$ je dobré uspořádání

ordinální součet a součin

$$\alpha + \beta = \gamma \Leftrightarrow \langle \gamma, \in \rangle \cong \langle \alpha \uplus \beta, <_{lex} \rangle,$$
$$\alpha \cdot \beta = \gamma \Leftrightarrow \langle \gamma, \in \rangle \cong \langle \beta \times \alpha, <_{lex} \rangle.$$

tj.

$$\alpha + \beta = \mathrm{otp}(\langle \alpha \uplus \beta, <_{lex} \rangle),$$
$$\alpha \cdot \beta = \mathrm{otp}(\langle \beta \times \alpha, <_{lex} \rangle),$$

kde $\mathrm{otp}(\langle A, < \rangle)$ je ordinální typ dobrého uspořádání $\langle A, < \rangle$.

Příklad: $1 + \omega = \omega \neq \omega + 1$

Příklad: $2 \cdot \omega = \omega \neq \omega \cdot 2$

Princip dobrého uspořádání (WO)

Princip dobrého uspořádání (WO)
Každou množinu lze dobře uspořádat.

Přesněji: Pro každou množinu x existuje relace R na x, taková že $\langle x, R \rangle$ je dobré uspořádání.

(WO) je nezávislé tvrzení v teorii množin ZF
(tj. není dokazatelné ani vyvratitelné)
lze ho přijmout jako nový axiom

Transfinitní indukce

Věta (transfinitní indukce)

Nechť X je třída splňující $\alpha \subseteq X \rightarrow \alpha \in X$ pro každé $\alpha \in \mathbf{On}$. Pak $\mathbf{On} \subseteq X$.

Poznámka: $\alpha \subseteq X$ je ekvivalentní s $\beta \in X$ pro každý ordinál $\beta < \alpha$.

Důkaz.

V opačném případě je $\mathbf{On} - X$ neprázdná podtřída $\mathbf{On}$, má tedy nejmenší prvek α. Pro něj platí $\alpha \subseteq X$, ale $\alpha \notin X$. □

Izolované a limitní ordinály

izolované ordinální číslo

α tvaru $\beta \cup \{\beta\}$ pro nějaké $\beta \in \mathbf{On}$

limitní ordinální číslo

α, které není izolované

Příklad: 5, $\omega + 1$, $\omega^\omega + \omega + 3$ jsou izolované ordinály.

Příklad: 0, ω, ω^7, $\omega^\omega + \omega$ jsou limitní ordinály.

Tvrzení (transfinitní indukce – alternativní formulace)

Nechť $X \subseteq \mathbf{On}$ je třída splňující pro každý ordinál α:

(nultý krok)	$0 \in X$,
(izolovaný krok)	$\alpha \in X \to \alpha \cup \{\alpha\} \in X$,
(limitní krok)	$(\forall \beta < \alpha)\beta \in X \to \alpha \in X$, *pro* $0 < \alpha$ *limitní.*

Pak $X = \mathbf{On}$.

Transfinitní rekurze

Věta (transfinitní rekurze)

Buď G třídové zobrazení s $\operatorname{dom}(G) = \mathbf{V}$ (konstruující zobrazení). Pak existuje právě jedno třídové zobrazení F s $\operatorname{dom}(F) = \mathbf{On}$ takové, že platí $F(\alpha) = G(F \restriction \alpha)$ pro každý ordinál α.

Poznámka: Zobrazení G určuje hodnotu $F(\alpha)$ na základě dříve sestrojených hodnot.

Důkaz.

Analogicky jako tvrzení o konstrukci (obyčejnou) rekurzí.
F se sestrojí jako $\bigcup_{\alpha \in \mathbf{On}} F_\alpha$, kde $\emptyset = F_0 \subseteq F_1 \subseteq \dots$ je (transfinitní) posloupnost funkcí s $\operatorname{dom}(F_\alpha) = \alpha$ a $F_\alpha(\alpha) = G(\bigcup_{\beta<\alpha} F_\beta)$.
Existence F_α pro každé $\alpha \in \mathbf{On}$ plyne transfinitní indukcí.
Jednoznačnost plyne transfinitní indukcí dle α. □

Ordinální limita

Připomenutí: Každá neprázdná třída $X \subseteq \mathbf{On}$ má nejmenší prvek $\alpha = \bigcap X$.

supremum

pro množinu $X \subseteq \mathbf{On}$ je $\alpha = \bigcup X$ supremum X
značíme $\sup(X)$

Je-li $X = \{x_\alpha; \alpha < \beta\}$ indexovaná jako rostoucí posloupnost, říkáme supremu X též limita $\langle x_\alpha \rangle_{\alpha < \beta}$.

Ordinální aritmetika – mocnina

ordinální mocnina $\alpha^{(\beta)}$

definována transfinitní rekurzí dle β:

$$\alpha^{(0)} = 1$$
$$\alpha^{(\beta\cup\{\beta\})} = \alpha^{(\beta)} \cdot \alpha$$
$$\alpha^{(\delta)} = \bigcup_{\beta<\delta} \alpha^{(\beta)} \text{ pro } 0 < \delta \text{ limitní}$$

Pozor: $2^{(\omega)} = \bigcup_{n\in\omega} 2^{(n)} = \omega$, tj. $2^{(\omega)} \neq 2^{\omega}$. Dokonce i $\omega^{(\omega)}$ je spočetný ordinál.

Je zvykem značit ordinální mocninu $\alpha^{(\beta)}$ stejně jako mocninu kardinální, tj. α^{β}. Pro správnou interpretaci je pak důležitá znalost kontextu.

Normální funkce

normální funkce $f : \mathbf{On} \to \mathbf{On}$

f je rostoucí a spojitá (tj. $f(\sup(X)) = \sup(f[X])$)

Tvrzení (o pevných bodech normální funkce)

Normální funkce f má pro každé $\beta \in \mathbf{On}$ pevný bod α (tj. takový, že $f(\alpha) = \alpha$) s $\alpha > \beta$.

Důkaz.

Pevný bod α se získá jako limita posloupnosti $\langle \alpha_n \rangle_{n<\omega}$, kde $\alpha_0 = \beta$ a $\alpha_{n+1} = f(\alpha_n)$. $\square$

ordinál ε_0

nejmenší pevný bod α funkce $\omega^{(\alpha)}$

$$\varepsilon_0 = \omega^{(\omega^{(\omega^{(\cdot^{\cdot^{\cdot}})})})}$$

Řada spočetných ordinálů

Třída všech pevných bodů funkce $\omega^{(\alpha)}$ je dobře uspořádaná, tedy očíslovaná ordinály.

ordinál ε_β pro $\beta \in \mathbf{On}$
β-tý pevný bod funkce $\omega^{(\alpha)}$

Řada ordinálů

$$0,1,2,\ldots,\omega,\omega+1,\ldots,\omega\cdot 2,\omega\cdot 2+1,\ldots,\omega\cdot 3,\ldots,\omega\cdot\omega = \omega^{(2)},\omega^{(3)},\ldots,\omega^{(\omega)},\omega^{(\omega^{(\omega)})},\ldots,\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_\omega,\ldots,\varepsilon_{\varepsilon_0},\varepsilon_{\varepsilon_{\varepsilon_0}},\ldots$$

všechny uvedené ordinály jsou stále spočetné

Axiom výběru (AC)

selektor na x

zobrazení f s $\mathrm{dom}(f) = x$ a $f(y) \in y$ pro $\emptyset \neq y \in x$

axiom výběru (AC)

Na každé množině existuje selektor.

(AC) je nezávislé tvrzení v teorii množin ZF
(tj. není dokazatelné ani vyvratitelné)
lze ho přijmout jako nový axiom
výsledná teorie se nazývá ZFC
(Zermelo-Fraenkelova teorie množin s axiomem výběru)

Zornovo lemma

Řetěz v uspořádání $\langle A, \leq \rangle$
$C \subseteq A$ taková, že $\langle C, \leq \rangle$ je lineární

Zornovo lemma (též princip maximality) (PM)
Je-li $\langle A, \leq \rangle$ uspořádání, kde každý řetěz má majorantu, pak $\langle A, \leq \rangle$ má pro každé $a \in A$ maximální prvek $m \geq a$.

(PM) je nezávislé tvrzení v teorii množin ZF
(tj. není dokazatelné ani vyvratitelné)
lze ho přijmout jako nový axiom

Ekvivalence (AC), (WO) a (PM)

Věta

Tvrzení (AC), (WO) a (PM) jsou v teorii ZF vzájemně ekvivalentní.

Důkaz.

Užitečné cvičení. □

Význam axiomu výběru

Axiom výběru je dnes obecně přijímán.
V minulosti (i dnes např. v konstruktivní matematice) byl odmítán pro svůj nekonstruktivní charakter.

V nějaké podobě je nutný pro důkaz řady klasických vět, např.:

- Heineho věta: $f : \mathbb{R} \to \mathbb{R}$ je spojitá $\Leftrightarrow$ kdykoli $\langle a_i \rangle_{i \in \mathbb{N}} \to a$, pak $\langle f(a_i) \rangle_{i \in \mathbb{N}} \to f(a)$.
- Každý vektorový prostor má bázi.
- Existuje lebesgueovsky neměřitelná podmnožina $\mathbb{R}$.
- Lebesgueova míra na $\mathbb{R}$ je σ-aditivní.
- Každé těleso má algebraické zúplnění.
- Sjednocení spočetně mnoha spočetných množin je spočetná množina.
- Relace subvalence $\preccurlyeq$ je trichotomická na $\mathbf{V}$ (je ekvivalentní s (AC)).

Podivuhodné důsledky (AC)

Axiom výběru má řadu na první pohled podivných důsledků:

- Existuje funkce $f : \mathbb{R} \to \mathbb{R}$ taková, že pro každý interval $I \subseteq \mathbb{R}$ je $f[I] = \mathbb{R}$, tj. f nabývá na I všech reálných hodnot.
- Existuje množina $X \subseteq \mathbb{R}^2$ bodů v rovině taková, že každou přímku v rovině protíná právě ve dvou bodech.
- **Banach-Tarského paradox:** Plnou kouli v $\mathbb{R}^3$ o poloměru 1 lze rozdělit na 5 částí tak, že z těchto částí lze jen posouváním a otáčením složit dvě plné koule o poloměru 1.

Podivuhodné důsledky (AC) - příklad

Tvrzení

Existuje funkce $f : \mathbb{R} \to \mathbb{R}$ taková, že pro každý interval $I \subseteq \mathbb{R}$ je $f[I] = \mathbb{R}$, tj. f nabývá na I všech reálných hodnot.

Důkaz.

Množina P všech dvojic (I, y), kde $I \subseteq \mathbb{R}$ je neprázdný otevřený interval s racionálními konci a $y \in \mathbb{R}$, má mohutnost kontinua a je (tedy) dobře uspořádatelná dle ordinálu $\lambda = 2^\omega$.
Nechť pro $\alpha < \lambda$ je (I_α, y_α) α-tý člen P. Zvolme transfinitní rekurzí $x_\alpha \in I_\alpha$ (zde užíváme (AC)) různé od všech x_β s $\beta < \alpha$ (to lze neboť všech takových x_β je vždy méně než kontinuum). Funkci $x_\alpha \mapsto y_\alpha$ lze rozšířit do $f : \mathbb{R} \to \mathbb{R}$, ta je zřejmě hledaná. $\square$

Kardinální čísla

dále předpokládáme (AC)

ordinální čísla . . . „typy dobrých uspořádání“
kardinální čísla . . . „typy velikostí množin“

kardinální číslo (též kardinál)
$\kappa \in \mathbf{On}$ takové, že pro žádný ordinál $\alpha < \kappa$ není $\alpha \approx \kappa$,
tj. nejmenší ordinál ve své faktortřídě dle mohutnosti
třídu všech kardinálů značíme **Cn**.

$$\mathbf{Cn} \subseteq \mathbf{On}$$

Příklad: Každé přirozené číslo je kardinální.
Příklad: ω je nejmenší nekonečné kardinální číslo.
Příklad: Ordinály $\omega + 1$, $\omega \cdot 2$, $\omega^{(\omega)}$ nejsou kardinální čísla.

Mohutnost množiny

Kardinální čísla jsou typy velikostí všech množin
(předpokládáme (AC))

Dle (WO) je každá $x \approx \alpha$ pro nějaký $\alpha \in \mathbf{On}$; nejmenší takové α je kardinál.

mohutnost množiny x
$|x| = \kappa \Leftrightarrow x \approx \kappa \in \mathbf{Cn}$

Třída **Cn**

uspořádání kardinálů

převzato z **On**, tj. $\kappa < \lambda \Leftrightarrow \kappa \in \lambda$

$\langle \mathbf{Cn}, < \rangle$ je dobré uspořádání

Pro $X \subseteq \mathbf{Cn}$ je $\kappa = \bigcap X \in \mathbf{Cn}$ nejmenší prvek X.

Tvrzení

Pro $X \subseteq \mathbf{Cn}$ *je* $\sup(X) = \bigcup X \in \mathbf{Cn}$ *supremum* X.

Důkaz.

Cvičení. $\square$

Neexistuje největší kardinál.
(dle Cantorovy věty $\kappa < |\mathcal{P}(\kappa)|$)

Cn je vlastní třída a neomezená v **On**
(jinak $\bigcup \mathbf{Cn} = \kappa \in \mathbf{Cn}$ je největší kardinál)

Funkce $\aleph$ (alef)

Nekonečná kardinální čísla lze popořadě očíslovat ordinálními, tj. existuje izomorfismus $\langle \mathbf{Cn} - \omega, \leq \rangle$ a $\langle \mathbf{On}, \leq \rangle$.

Funkce $\aleph$ (alef; hebrejská abeceda)

$$\aleph : \mathbf{On} \to \mathbf{Cn} - \omega$$

$$\alpha \mapsto \aleph_\alpha$$

definována transfinitní rekurzí

$$\aleph_\alpha = \min\{\kappa \in \mathbf{Cn}; \kappa > \aleph_\beta \text{ pro každé } \beta < \alpha\}$$

$\aleph_\alpha$ je α-té nejmenší nekonečné kardinální číslo.

Příklad: $\aleph_0 = \omega$
Příklad: $\aleph_1$ je nejmenší nespočetný ordinál.
Příklad: $\aleph_{\alpha+1}$ je nejmenší kardinál větší než $\aleph_\alpha$.

Užíváme-li $\aleph_\alpha$ jako ordinál a nikoli kardinál, píšeme též ω_α.

Normalita a pevné body funkce $\aleph$

Připomeňme: Normální funkce je $f : \mathbf{On} \to \mathbf{On}$ rostoucí a spojitá.

f normální $\Rightarrow$ f má pevný bod

Tvrzení

Funkce $\aleph$ je normální.

Důkaz.

Vynecháváme, je však snadný. (Cvičení) $\square$

κ pevný bod $\aleph$ $\Rightarrow$ pod κ je κ nekonečných kardinálů

Izolované a limitní kardinály

kardinální následník

$\kappa^+ =$ nejmenší $\lambda \in \mathbf{Cn}$ s $\kappa < \lambda$,

tj. ${\aleph_\alpha}^+ = \aleph_{\alpha+1}$.

izolovaný kardinál

λ tvaru κ^+ pro nějaké $\kappa \in \mathbf{Cn}$

limitní kardinál

λ, který není izolovaný

Pozor: Pojmy izolovaný kardinál a izolovaný ordinál nesplývají.
Dokonce: Každý nekonečný kardinál je limitní ordinál
(neboť $\alpha \approx \alpha + 1$).

$\omega \leq \lambda$ je izolovaný kardinál $\Leftrightarrow \lambda = \aleph_\alpha$, kde α je izolovaný ordinál,
$\omega \leq \lambda$ je limitní kardinál $\Leftrightarrow \lambda = \aleph_\alpha$, kde α je limitní ordinál.

Příklad: $\omega = \aleph_0$, $\aleph_\omega$ či $\aleph_{\omega_1}$ jsou limitní kardinály.
Příklad: $\aleph_1$ či $\aleph_{\omega+3}$ jsou izolované kardinály (ale limitní ordinály).

Kardinální aritmetika

Kardinální aritmetika zobecňuje aritmetiku přirozených čísel:

kardinální součet
$$\kappa + \lambda = |\kappa \uplus \lambda|$$

kardinální součin
$$\kappa \cdot \lambda = |\kappa \times \lambda|$$

kardinální mocnina
$$\kappa^\lambda = |{}^\lambda\kappa|$$

Pozor: Kardinální operace se liší od ordinálních.

Kardinální součet a součin jsou komutativní.

Je-li $\alpha = \kappa + \lambda$ ordinálně, je $|\alpha| = \kappa + \lambda$ kardinálně.
Je-li $\alpha = \kappa \cdot \lambda$ ordinálně, je $|\alpha| = \kappa \cdot \lambda$ kardinálně.
Avšak obecně $|\kappa^{(\lambda)}| \neq \kappa^\lambda$.

Příklad: $2^{(\omega)} = \omega \prec 2^\omega$.

Kardinální aritmetika

Tvrzení

Pro kardinál $\kappa \geq \omega$ je $\kappa \times \kappa \approx \kappa$.

Důkaz.

Transfinitní indukcí dle α dokážeme $\aleph_\alpha \times \aleph_\alpha \approx \aleph_\alpha$. Klíčem pro indukční krok je dokázat $\aleph_\alpha = \mathrm{otp}\langle \aleph_\alpha \times \aleph_\alpha, \leq_{max} \rangle$, kde $\leq_{max}$ je maximo-lexikografické uspořádání. $\square$

Důsledek

- $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$, *je-li alespoň jedno z nich* $\geq \omega$,
- $\kappa^n = \kappa$, *pro* $\kappa \geq \omega$ *a* $0 < n < \omega$,
- $\kappa^\lambda = 2^\lambda$, *pro* $2 \leq \kappa \leq \lambda \geq \omega$,
- $2^\lambda > \lambda$ *(Cantorova věta).*

Kardinální aritmetika

součet souboru kardinálních čísel

$$\sum_{i\in I}\kappa_i = |\biguplus_{i\in I}\kappa_i| = |\bigcup_{i\in I}(\{i\}\times\kappa_i)|$$

Tvrzení

Je $\sum_{i\in I}\kappa_i = \max(|I|,\sup\{\kappa_i; i\in I\})$.

součin souboru kardinálních čísel

$$\prod_{i\in I}\kappa_i = |\prod_{i\in I}\kappa_i| = |\{f; f: I\to\bigcup_{i\in I}\kappa_i \text{ a } f(i)\in\kappa_i \text{ pro } i\in I\}|$$

Následující tvrzení je zobecněním Cantorovy věty:

Tvrzení (Königova nerovnost)

Je-li $I\neq\emptyset$ *a* $\kappa_i<\lambda_i$ *pro každé* $i\in I$, *pak* $\sum_{i\in I}\kappa_i<\prod_{i\in I}\lambda_i$.

Důkaz.

$\sum_{i\in I}\kappa_i\leq\prod_{i\in I}\lambda_i$ je evidentní.
Nemožnost rovnosti se dokáže diagonální metodou. □

Průběh kardinální mocniny

Připomenutí: Mohutnost kontinua je $|\mathbb{R}| = |\mathcal{P}(\omega)| = 2^\omega$.
Kardinál 2^ω značíme též $\mathfrak{c}$ a nazýváme kontinuum.

Hypotéza kontinua (CH) - formulace pomocí funkce $\aleph$

$$(\mathfrak{c} =) 2^{\aleph_0} = \aleph_1$$

Zobecněná hypotéza kontinua (GCH)

$$2^{\aleph_\alpha} = \aleph_{\alpha+1} \text{ pro všechna } \alpha \in \mathbf{On}$$

(GCH) je stejně jako (CH) nezávislé tvrzení v ZFC,
tj. nelze ho dokázat ani vyvrátit.

Průběh funkce $2^{\aleph_\alpha}$ není axiomy ZFC téměř vůbec specifikován.
Příklad: $2^{\aleph_0} = \aleph_2$, $2^{\aleph_0} = \aleph_{100}$, $2^{\aleph_0} = \aleph_{\omega+3}$, $2^{\aleph_0} = \aleph_{\omega_1+1}$ jsou všechno nezávislá tvrzení v ZFC (Eastonova věta).

Pro důkazy nezávislosti obdobných tvrzení v ZFC slouží metoda zvaná forcing (Paul Cohen (1963) + Petr Vopěnka, Dana Scott a Robert M. Solovay).

Velké kardinály

κ je regulární kardinál
κ není supremem méně než κ menších ordinálů

κ je singulární kardinál
není regulární

Příklad: $\aleph_\omega = \sup\{\aleph_n; n \in \omega\}$ je singulární.
Příklad: Každý izolovaný kardinál je regulární.

slabě nedosažitelný kardinál
nespočetný, regulární a limitní

Existenci slabě nedosažitelného kardinálu nelze v ZFC dokázat.
(„silnější verze axiomu nekonečna“ – ω je regulární a limitní)

Velké kardinály

silně limitní kardinál

κ takový, že pro $\lambda < \kappa$ je $2^\lambda < \kappa$

nedosažitelný kardinál

nespočetný, regulární a silně limitní

Některé další velké kardinály (dle velikosti):

slabě nedosažitelný

nedosažitelný

Mahlův

kompaktní

Ramseyův

měřitelný

superkompaktní

obří

Není známo, zda je existence slabě nedosažitelného (či většího) kardinálu relativně bezesporná v ZFC.

Lze dokázat, že tuto relativní bezespornost nelze v ZFC dokázat.