1 Úvod

Poznámka (Aplikace)
Transfinitní indukce, axiom výběru (= princip maximality = Zornovo lemma)

Poznámka (Cíl)
Vybudování matematiky na pevných základech. Porozumění nekonečen. Důkaz existence nealgebraických (= transcendentních) reálných čísel. Princip kompaktnosti. Banach-Tarského paradox.

Poznámka (Literatura)
Balcar, Štěpánek – Teorie množin
Seriál PraSete
Hrbáček, Jech – Introduction to set theory
Olšák – Esence teorie množin (videa)

Poznámka (Historie)
Bernard Bolzano (český matematik, 1781-1848, pojem množina), George Cantor (německý matematik, 1845 - 1918, zavedení aktuálního nekonečna, diagonální metoda, kardinální čísla, uzavřená množina), Bertrand Russell (1902, Russellův paradox = paradox holiče = holí holič holící všechny lidi, kteří se neholí sami, sebe?) + Berriho paradox (nechť m je nejmenší přirozené číslo, které nejde definovat méně než 100 znaky), Zermelo-Fraenkel (zavedli axiomatickou teorii množin).

Definice 1.1 (Symboly)

Proměnné pro množiny – $x, y, z, x_1, x_2, \ldots$.

Binární predikátorový symbol = a bin. relační symbol $\in$.

Logické spojky $\neg, \vee, \wedge, \implies, \Leftrightarrow$.

Kvantifikátory $\forall, \exists$.

Závorky () {} []

Definice 1.2 (Formule)

Atomické ($x = y$, $x \in y$). Jsou-li φ a ψ formule, pak $\neg\varphi$, $\varphi \vee \psi$, $\varphi \wedge \psi$, $\varphi \implies \psi$, $\varphi \Leftrightarrow \psi$ jsou formule. Je-li φ formule, x proměnná, pak $(\forall x)\varphi$, $(\exists x)\varphi$ jsou formule. (Vázané vs. volné proměnné – proměnné formule, které do ní lze dosadit jsou volné, proměnné formule, které do ní nelze dosadit jsou vázané). Každou formuli lze dostat konečnou posloupností aplikací výše zmíněného.

Definice 1.3 (Rozšíření jazyka)

$x \neq y$ značí $\neg(x = y)$, $x \notin y$ znamená $\neg(x \in y)$, $x \subseteq y$ znamená $(\forall u)(u \in x \implies u \in y)$, $x \subset y$ značí $x \subseteq y \wedge x \neq y$. Dále uvidíme $\cup$, $\cap$, $\setminus$, $\{x_1, \ldots, x_n\}$, $\emptyset$, $\{x \in a | \varphi(x)\}$.

Definice 1.4 (Axiomy logiky)

Vysvětlují, jak se chovají implikace, kvantifikátory, rovnost, …

Definice 1.5 (Axiomy TEMNA)

Říkají, jak se chová $\in$ a jaké množiny existují. Budeme používat Zermelo-Fraenkelovu teorii (ZF), tedy 9 axiomů (7 + 2 schémata). (Není minimální, tj. lze některé odvodit z jiných) + axiom výběru (AC) s ním se pak ZF značí ZFC.

Definice 1.6 (Axiomy ZFC)

1. Axiom existence množiny: $(\exists x)(x = x)$.
2. Axiom extenzionality: $(\forall z)(z \in x \Leftrightarrow z \in y) \implies x = y$.
3. Schéma axiomů vydělení: je-li $\varphi(x)$ formule, která neobsahuje volnou proměnnou z, potom $(\forall a)(\exists z)(\forall x)(x \in z \Leftrightarrow (x \in a \wedge \varphi(x)))$ je axiom.
4. Axiom dvojice: $(\forall a)(\forall b)(\exists z)(\forall x)(x \in z \Leftrightarrow (x = a \vee x = b))$.
5. Axiom sumy: $(\forall a)(\exists z)(\forall x)(x \in z \Leftrightarrow (\exists y)(x \in y \wedge y \in a))$.
6. Axiom potence: $(\forall a)(\exists z)(\forall x)(x \in z \Leftrightarrow x \subseteq a)$.
7. Schéma axiomů nahrazení[a] Je-li $\psi(u, v)$ formule s volnými proměnnými u, v, jež nemá volné proměnné w, z, pak

$$(\forall u)(\forall v)(\forall w)((\psi(u,v) \wedge \psi(u,w)) \implies v = w) \implies$$

$$\implies (\forall a)(\exists z)(\forall v)(v \in z \Leftrightarrow (\exists u)(u \in a \wedge \psi(u,v)))$$

   je axiom.
8. Axiom fundovanosti (regularity): $(\forall a)(a \neq \emptyset \implies (\exists x)(x \in a \wedge x \cap a = \emptyset))$.

Později ještě:

- Axiom nekonečna

- Axiom výběru

[a] Slogan: Obraz množiny funkcí je množina.

Definice 1.7 (Značení)

$\{x|x \in a \wedge \varphi(x)\}$, zkráceně $\{x \in a|\varphi(x)\}$ je množina z axiomů vydělení.

Definice 1.8 (Průnik, množinový rozdíl, prázdná množina)

$a \cap b = \{x|x \in a \wedge x \in b\}$.

$a \backslash b = a - b = \{x|x \in a \wedge x \notin b\}$.

$\emptyset = \{x|x \in a \wedge x \neq x\}$. ($\emptyset$ je díky prvním třem axiomům dobře definována.)

Definice 1.9 (Neuspořádaná a uspořádaná dvojice)

$\{a, b\}$ je neuspořádaná dvojice, $\{a\}$ znamená $\{a, a\}$.

$(a, b) =< a, b >= \{\{a\}, \{a, b\}\}$ je uspořádaná dvojice.

Lemma 1.1

$(x, y) = (u, v) \Leftrightarrow (x = u \wedge y = v)$.

Důkaz

$\Leftarrow$ $x = u$, pak $\{x\} = \{u\}$ z axiomu extenzionality, stejně tak $\{x, y\} = \{u, v\}$, a tedy $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$.

$\implies$ $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$ pak $\{x\} = \{u\}$ nebo $\{x\} = \{u, v\}$, každopádně $x = u$. Nyní $\{u, v\} = \{x\}$ nebo $\{u, v\} = \{x, y\}$ tedy $v = x$ nebo $v = y$. Pokud $v = y$, tak jsme skončili, pokud $v = x$ pak $v = u = x = y$. □

Definice 1.10 (Potenční množina)

$\mathcal{P}(a) = \{x|x \subseteq a\}$ je potenční množina (potence) a (z axiomu potence).

Definice 1.11 (Uspořádaná n-tice)

Jsou-li $a_1, \ldots, a_n$ množiny, definujeme uspořádanou n-tici $(a_1, \ldots, a_n) =< \ldots >$ následovně: $(a_1) = a_1$, je-li definovaná $(a_1, \ldots, a_k)$, pak $(a_1, \ldots, a_k, a_{k+1}) = ((a_1, a_2, \ldots, a_k), a_{k+1})$.

Lemma 1.2

$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \Leftrightarrow (a_1 = b_1 \wedge a_2 = b_2 \wedge \ldots \wedge a_n = b_n)$.

Důkaz
Domácí cvičení. □

Definice 1.12 (Značení)

$$\bigcup a = \{x | (\exists y)(x \in y \land y \in a\}.$$

Definice 1.13

Pro $a = \{b, c\}$ definujeme $b \cup c = \bigcup a$.

Definice 1.14 (Neuspořádaná n-tice)

Neuspořádanou n-tici $\{a_1, \ldots, a_n\}$ (n-prvkovou množinu) definujeme rekurzivně: je-li definováno $\{a_1, \ldots, a_k\}$, pak $\{a_1, \ldots, a_k, a_{k+1}\} = \{a_1, \ldots, a_k\} \cup \{a_{k+1}\}$.

Poznámka
Axiom nahrazení se využívá v: transfinitní rekurzi, definici $\omega + \omega$, větě o typu dobrého uspořádání, Zornově lemmatu (tj. axiom výběru).

Příklad
Ukažte, že axiom fundovanosti zakazuje existenci konečných cyklů relace $\in$ (tj. takových množin y, pro které $y \in . \in \ldots \in . \in y$).

Důsledek
Všechny množiny lze vygenerovat z $\emptyset$ pomocí operací $\bigcup$ a $\mathcal{P}$ (zhruba).

1.1 Třídy

Definice 1.15

Nechť $\varphi(x)$ je formule, pak $\{x, \varphi(x)\}$ (čteme třída všech x, pro které platí $\varphi(x)$), tzv. třídový term, se nazývá třída (určená formulí x).

Důsledek
Pokud $\varphi(x)$ je tvaru $x \in a \land \varphi(x)$, pak je $\{x, \varphi(A)\}$ množina z axiomu vydělení. Obdobně pro axiom dvojice, sumy, ...

Poznámka
Je-li y množina, pak y má stejné prvky jako třída $\{x, x \in y \wedge x = x\}$.

Poznámka (Vlastní třídy)
Existují i třídy (tzv. vlastní), které nejsou množiny (např. třída všech množin).

Definice 1.16 (Rozšíření jazyka)

Ve formulích na místech volných proměnných připustíme i Třídové termy a proměnné pro třídy (psané velkými písmeny). (Avšak je nebude možné kvantifikovat!)

Definice 1.17 (Eliminace (nahrazování) třídových termů)

Buďte x, y, z, X, Y proměnné (3 množinové + 3 třídové (z zastupuje jak množinu, tak třídu)), $\varphi(x)$, $\psi(y)$ formule základního jazyka, X zastupuje $\{x, \varphi(x)\}$ a Y $\{y, \varphi(y)\}$.

$$z \in X \text{ (schéma formulí pro obecné } X\text{) zastupuje } z \in \{x, \varphi\} \text{ nahradíme } \varphi(z).$$

$$z = \{X\} \text{ zastupuje } z = \{x, \varphi(x)\} \text{ nahradíme } (\forall u)(u \in z \Leftrightarrow \varphi(u)).$$

$$X \in Y \text{ zastupuje } \{x, \varphi(x)\} \in \{y, \varphi(y)\} \text{ nahradíme } (\exists u)(u = \{x, \varphi(x)\}) \wedge u \in \{y, \psi(y)\}.$$

$$X \in y \text{ analogicky předchozí.}$$

$$X = Y \ldots\ldots\ldots\ldots (\forall u)(\varphi(u) \Leftrightarrow \psi(u)).$$

Poznámka
Třídy s rozšířenou formulí nepřináší díky eliminaci nic nového.

Definice 1.18 (Třídové operace)

$A \cap B$ je $\{x, x \in A \wedge x \in B\}$, $A \cup B$ je $\{x, x \in A \vee B\}$, $A \backslash B = A - B = \{x, x \in A \wedge x \notin B\}$.

Definice 1.19 (Univerzální třída, doplněk)

$\{x, x = x\}$ je tzv. univerzální třída a značí se V.

Buď A třída, pak (absolutní) doplněk A je $V - A$, který se značí $-A$.

Definice 1.20 (Inkluze)

$A \subseteq B$ ($A \subset B$) značí „A je (vlastní) částí (= podtřídou) B“.

Definice 1.21 (Suma a průnik)

$\bigcup A$ značící sumu třídy A je třída $\{x, (\exists a)(a \in A \wedge x \in a)\}$. $\bigcap A$ značící průnik třídy A je třída $\{x, (\forall a)(a \in A \rightarrow x \in a)\}$.

Lemma 1.3

V není množina.

Důkaz
Cvičení. □

Lemma 1.4

Je-li A třída, a množina, pak $a \cap A$ je množina.

Důkaz
V podstatě axiom vydělení. □

Definice 1.22 (Kartézský součin tříd)

Kartézský součin tříd A, B, značený $A \times B$, je třída $\{(a, b), a \in A, b \in B\}$ (zkrácený zápis pro $\{x, (\exists a)(\exists b)(x = (a, b) \wedge a \in A \wedge b \in B)\}$).

Lemma 1.5

Jsou-li x, y množiny, pak $x \times y$ je množina.

Důkaz („Vnoření a vydělení")
Stačí dokázat, že $x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y))$ (vpravo je množina z axiomu potence, součin pak vydělíme): Pokud $u \in x$ a $v \in y$, pak $\{u\}, \{u, v\} \subseteq x \cup y$, tedy $\{u\}, \{u, v\} \in \mathcal{P}(x \cup y)$. Tedy $\{\{u\}, \{u, v\}\} \subseteq \mathcal{P}(x \cup y)$, tj. $\in \mathcal{P}(\mathcal{P}(x \cup y))$. □

Definice 1.23 (Mocnina)

X třída, pak $X^1 = X$ a $X^{n+1} = X^n \times X$. (Tj. X^n je třída všech uspořádaných n-tic s prvky v X.)

Pozorování
$V = V^1 \supset V^2 \supset \ldots$.

Příklad
Obecně neplatí $X \times X^2 = X^3$.

1.2 Relace

Definice 1.24 (Relace)

Třída R je (binární) relace pokud, $R \subseteq V \times V$. (n-ární relace, pokud $R \subseteq V^n$.)

xRy je zkratka za $(x, y) \in R$.

Definice 1.25 (Definiční obor, obor hodnot, zúžení)

Je-li X relace (libovolná třída), pak $\mathrm{Dom}(X) := \{u, (\exists v)((u, v) \in X)\}$ je definiční obor třídy X.

Je-li X relace (libovolná třída), pak $\mathrm{Rang}(X) := \{v, (\exists u)((u, v) \in X)\}$ je obor hodnot třídy X.

Je-li navíc Y třída, pak $X''Y$ (nebo také $X[Y]$) $:= \{z, (\exists y)(y \in Y \wedge (y, z) \in X)\}$ je obraz třídy Y třídou X.

Je-li navíc Y třída, pak $X \restriction Y := \{(y, z), y \in Y \wedge (y, z) \in X)\}$ je zúžení třídy X na třídu Y (nebo také parcializace).

Lemma 1.6

Je-li x množina, Y třída, pak $\mathrm{Dom}(x)$, $\mathrm{Rang}(x)$, $x \restriction Y$, $x''Y$ *jsou množiny.*

Důkaz (Vnoření a vydělení)
$\mathrm{Dom}(x) \subseteq \bigcup(\bigcup x))$. Když $u \in \mathrm{Dom}(x)$, $\exists v$, že $(u, v) \in x$, $u \in \{u\} \in (u, v) \in x$, tedy $\{u\} \in \bigcup x$, tj. $u \in \bigcup(\bigcup x))$.

$\mathrm{Rang}(x) \subseteq \bigcup(\bigcup x))$. (Analogicky.) $x \restriction Y \subseteq x$, $x''Y \subseteq \mathrm{Rang}(x)$. □

Definice 1.26 (Inverzní relace, složení relací)

R, S relace, pak $R^{-1} := \{(u, v), (v, u) \in R\}$ je relace inverzní k R. Relace $R \circ S := \{(u, w), (\exists v)(uRv \wedge vSw)\}$ je složení relací R, S.

Definice 1.27 (Zobrazení, na, do, prosté)

Relace F je zobrazení (funkce), pokud $(\forall u)(\forall v)(\forall w)(((u, v) \in F \wedge (u, w) \in F) \implies v = w)$.

Zkracujeme $(u, v) \in F$ na $F(u) = v$.

F je zobrazení třídy X do (na) třídy Y, $F : X \to Y$, pokud $\mathrm{Dom}(F) = X$ a $\mathrm{Rang}(F) \subseteq Y$ ($\mathrm{Rang}(F) = Y$).

Zobrazení F je prosté, pokud inverzní relace F^{-1} je zobrazení. (Zřejmě je pak i F^{-1} prosté).

Definice 1.28 (Zkratka)

A třída, φ formule, pak $(\exists x \in A)\varphi$ je zkratka za $(\exists x)(x \in A \wedge \varphi)$ a $(\forall x \in A)\varphi$ je zkratka za $(\forall x)(x \in A \implies \varphi)$.

Obraz (vzor) třídy X zobrazením F je $F[X]$ místo $F''X$ ($F^{-1}[X]$ místo $F^{-1''}X$).

Definice 1.29

A třída, a množina, pak ${}^aA := \{f, f : a \to A\}$ je třída všech zobrazení a do A.

Důkaz

Axiom nahrazení říká, že $\operatorname{Rang} f$ je množina, $f \subseteq a \times \operatorname{Rang}(f)$, libovolné f je tedy množina a tato třída je dobře definována. □

Důsledek

${}^{\varnothing}y = \{\varnothing\}$, ${}^{x}\varnothing = \varnothing$ $(x \neq \varnothing)$.

Lemma 1.7

Pro libovolné množiny x, y je ${}^xy$ množina. Je-li $x \neq \varnothing$, Y je vlastní třída, pak ${}^xY$ je vlastní třída.

Důkaz

$f \in^x y \dots f : x \to y \dots f \subseteq x \times y \dots f \in \mathcal{P}(X \times y) \implies {}^xy \subseteq \mathcal{P}(x \times y)$.

Pro každé $y \in Y$ definujeme konstantní zobrazení $k_y : x \to Y$ tak, že $(\forall u \in x)(k_y(u) = y)$. Nechť $K = \{k_y, y \in Y\} \subseteq^x Y$. Sporem: pokud ${}^xY$ je množina, pak K je množina. Použijeme axiom nahrazení $F : K \to Y$, $F(k_y) = y$, tj. (protože F zobrazuje na Y) Y je množina. ↯. □

2 Uspořádání

Definice 2.1 (Reflexivní, antireflexivní, symetrická, slabě antisymetrická, antisymetrická, trichotomická, tranzitivní)

Řekneme, že relace $R(\subseteq V \times V)$ je na třídě A reflexivní (antireflexivní, symetrická, slabě antisymetrická, antisymetrická, trichotomická, tranzitivní), pokud … (…, …, $(\forall x \in A)(\forall y \in A)((xRy \wedge yRx) \implies x = y)$, $(\forall x \in A)(\forall y \in A)\neg(xRy \wedge yRx)$, $(\forall x \in A)(\forall y \in A)(xRy \vee yRx \vee x = y)$, …).

Pozorování
Tyto vlastnosti jsou dědičné (tzn. platí i na každé podtřídě $B \subseteq A$).

Definice 2.2 (Uspořádání, porovnatelné)

Řekneme, že relace R je uspořádání na třídě A, je-li R na A reflexivní, slabě symetrická, tranzitivní.

$x, y \in A$ jsou porovnatelné relací R, pokud $xRy \vee yRx$.

Definice 2.3 (Značení)

$x \leqslant_R y$ znamená xRy, x je menší nebo rovno y vzhledem k R.

Definice 2.4 (Lineární uspořádání)

Uspořádání R je lineární, je-li R trichotomická relace.

Definice 2.5 (Ostré uspořádání)

Relace R' je ostré uspořádání, je-li $R' = R - \mathrm{id}$ a R je uspořádání.

Píšeme $x <_R y$, když $xR'y$.

Definice 2.6

Nechť R je uspořádání na třídě A, $X \subseteq A$. Říkáme, že $a \in A$ je (vzhledem k R, A): majoranta (horní mez, horní závora) třídy X, pokud $(\forall x \in X)(x \leqslant_R a)$, maximální prvek třídy X pokud $a \in X \wedge (\forall x \in X)(\neg a <_R x)$, největší prvek třídy X pokud $a \in X \wedge (\forall x \in X)(x \leqslant_R a)$, supremum třídy X, pokud a je nejmenší majoranta.

Obdobně (dolní mez, dolní závora), minimální, nejmenší, infimum.

Pozorování
Největší $\implies$ maximální. V lineárním uspořádání i naopak.

Definice 2.7 (Shora, zdola omezená množina, dolní, horní množina)

X je shora omezená v A, pokud existuje majorita X v A. X je dolní množina v A, pokud $(\forall x \in X)(\forall y \in A)(y \leqslant_R x \implies y \in X)$. $x \in A$, pak $(\leftarrow, x]$ je $\{y, y \in A \wedge y \leqslant_R x\}$ hlavním ideálem určeným x.

Obdobně zdola uzavřená a horní množina. Lze definovat i pro třídy, ale to se nedělá.

Pozorování
R je uspořádání na A, pak pro libovolné $x, y \in A$ platí $x \leqslant_R y \Leftrightarrow (\leftarrow, x] \subseteq (\leftarrow, y]$.

Definice 2.8 (Dobré uspořádání)

Uspořádání R na třídě A je dobré, pokud každá neprázdná podmnožina $u \subseteq A$ má nejmenší prvek.

3 Srovnávání množin

Definice 3.1

Množiny x, y mají stejnou mohutnost (jsou ekvivalentní), $x \approx y$, pokud existuje prosté zobrazení x na y.

Definice 3.2

Množina x má mohutnost menší nebo rovnou mohutnosti y, $x \preceq y$, pokud existuje prosté zobrazení x do y. (Také říkáme x je subvalentní y). x má mohutnost menší než y, $x \prec y$, pokud $x \preceq y \wedge \neg(x \approx y)$.

Pozorování
$x \subseteq y \implies x \preceq y$. $x \subset y \implies x \preceq y$, ale ne nutně $x \prec y$ (viz přirozená čísla).

Lemma 3.1

Jsou-li x, y, z množiny, pak

$$1) x \approx x. \qquad (\text{id})$$

$$2) x \approx y \implies y \approx x. \qquad ({}^{-}1)$$

$$3) (x \approx y \wedge y \approx z) \implies x \approx z. \qquad (\circ)$$

$$4) x \preceq x. \qquad (\text{id})$$

$$5) (x \preceq y \wedge y \preceq z) \implies x \preceq z. \qquad (\circ)$$

Pozorování
$(x \approx y) \implies (x \preceq y \wedge y \preceq x)$.

Definice 3.3

Zobrazení $H : \mathcal{P}(x) \to \mathcal{P}(x)$ je monotónní vzhledem k inkluzi, pokud pro každé podmnožiny $u, v \subseteq x$ platí $u \subseteq v \implies H(u) \subseteq H(v)$.

Lemma 3.2

Je-li $H : \mathcal{P}(x) \to \mathcal{P}(x)$ zobrazení monotónní vzhledem k inkluzi, pak existuje podmnožina $c \subseteq c$, že $H(c) = c$.

Poznámka
Speciální případ Knaster-Tarski, kteří předpokládají jen úplný svaz.

Pozorování
$A \subseteq \mathcal{P}(x) \implies \sup_{\subseteq} A = \bigcup A$.

Důkaz
Nechť $A = \{u, u \subseteq x \wedge u \subseteq H(u)\}$. $c = \bigcup A$. $c \subseteq x$ zřejmě, $u \in A \implies u \subseteq c \wedge u \subseteq H(u) \subseteq H(c)$. Tedy $H(c)$ je majoranta A, tedy $c \subseteq H(c)$. Z monotonie H je $H(c) \subseteq H(H(c))$, tedy $H(c) \in A$, tedy $H(c) \subseteq c$. □

Věta 3.3 (Cantor-Bernstein)

$(x \preceq y \wedge y \preceq x) \implies x \approx y$.

Důkaz
Nechť $f : x \to y, g : y \to x$ jsou prostá zobrazení. Uvažujeme 'indukovaná' zobrazení $\vec{f} : \mathcal{P}(x) \to \mathcal{P}(y)$, $u \mapsto f[u]$. Definujeme $H : \mathcal{P}(x) \to \mathcal{P}(x)$ tak, že pro $u \subseteq x$ $H(u) = X - g[Y - f[u]]$. H je monotónní vzhledem k inkluzi: $u_1 \subseteq u_2 \implies f[u_1] \subseteq f[u_2] \implies Y - f[u_1] \supseteq Y - f[u_2] \implies \dots \implies H(u_1) \subseteq H(u_2)$. Podle lemmatu o pevném bodě existuje $c : H(c) = c$.

Tedy $c = x - g[y - f(c)]$, tj. $x - c = g[y - f[c]]$. Tedy $g^{-1}|_{(x-c)}$ je prosté zobrazení $x - c$ na $y - f[c]$. Tedy definujeme $h : x \to y$, $h(a) = f(a)$ pro $a \in c$, $H(a) = g^{-1}(a)$ jinak. □

Lemma 3.4

x, y, z, x_1, y_1 množiny, pak

$$1)\ x \times y \approx y \times x, \qquad 2)\ x \times (y \times z) \approx (x \times y) \times z,$$

$$3)\ (x \approx x_1 \wedge y \approx y_1) \implies (x \times y) \approx (x_1 \times y_1),$$

$$4)\ x \approx y \implies \mathcal{P}(x) \approx \mathcal{P}(y), \qquad 5)\ \mathcal{P}(x) \approx {}^x 2 = {}^x \{\emptyset, \{\emptyset\}\}.$$

Důkaz
1-4) Triviální. Pro 5) definujeme charakteristickou funkci a je to triviální. □

Definice 3.4 (Konečná množina (Tarski))

Množina x je konečná (značíme $\mathrm{Fin}(x)$), pokud každá neprázdná podmnožina její potenční podmnožiny má vzhledem k inkluzi maximální prvek.

Pozorování
$Fin(x)$ právě tehdy, když každá neprázdná podmnožina $\mathcal{P}(x)$ má minimální prvek vzhledem k $\subseteq$.

Důkaz
$d : \mathcal{P}(x) \to \mathcal{P}(x), y \mapsto x \backslash y$ vše obrátí. □

Definice 3.5 (Dedekindovsky konečná množina)

Množina a je dedekindovsky konečná, pokud má větší mohutnost než každá její vlastní podmnožina. (Tj. neexistuje prosté zobrazení a do $b \subset a$.)

Lemma 3.5

Je-li a konečná, potom je i dedekindovsky konečná.

Důkaz
Víme $b \subset a \implies b \preceq a$. Chceme tedy $a \neq b$. Sporem: Předpokládejme, že $b \subset a \wedge b \approx a$, $Y := \{b, b \subset a \wedge b \approx a\}$. Víme, že Y je neprázdná, $Y \subseteq \mathcal{P}(a)$. Nechť c je minimální prvek Y vzhledem k inkluzi. Existuje tedy bijekce $f : a \to c$. Nechť $d = f[c]$. Zřejmě $f|_c : c \to d$ je bijekce, tedy $c \approx d$ a z tranzitivity $d \approx a$. Tedy $d \in Y$. Ale $d \subset c$, jelikož $\exists s \in c, f^{-1}(s) \in a \backslash c$, tj. $s \notin d$. To je ale spor s volbou c. □

Poznámka
V ZF je opravdu konečnost silnější než dedekindovská konečnost.

Poznámka (Další definice konečnosti)
Existuje lineární uspořádání, které je dobré a jeho inverze je také dobré uspořádání.

Existuje lineární uspořádání a každá dvě lineární uspořádání jsou izomorfní.

Potenční množina od potenční množiny je dedekindovsky konečná.

Věta 3.6

1) Je-li a konečná množina uspořádaná relací (částečným uspořádáním) $\leqslant$, pak každá neprázdná podmnožina $b \subset a$ má maximální i minimální prvek (vzhledem k $\leqslant$).

2) Každé lineární uspořádání na konečné množině je dobré (každá podmnožina má nejmenší prvek).

Důkaz
1) $\implies$ 2): každá podmnožina má minimální prvek, ale ten je při lineárním uspořádání konečný.

1): Pro každé $x \in a$ uvažujeme $(\leftarrow, x] := \{y \in a | y \leqslant x\}$. To jsou zřejmě podmnožiny a. Nechť $u = \{(\leftarrow, x], x \in b\}$. $b \in u \subseteq \mathcal{P}(a)$, tedy z definice konečnosti má maximální prvek $(\leftarrow, m]$. $m \in b$ je maximální prvek v b. Minimum otočením $\leqslant$. $\square$

Definice 3.6 (Izomorfismus)

F je zobrazení A_1 do A_2, R_1, R_2 jsou relace. F je izomorfismus tříd A_1 a A_2 vzhledem k R_1 a R_2, pokud F je bijekce (prosté zobrazení na) a $\forall x, y \in A_1 : xR_1y \Leftrightarrow F(x)R_2F(y)$.

Definice 3.7 (Počátkové vnoření)

A množina uspořádaná relací R, B relací S, potom zobrazení $F : A \to B$ je počátkové vnoření A do B, pokud $A_1 = \mathrm{Dom}(F)$ je dolní množina A, $B_1 = \mathrm{Rang}(F)$ je dolní podmnožina B a F je izomorfismus A_1 a B_1 vzhledem k R, S.

Lemma 3.7

Nechť F, G jsou počátková vnoření dvou dobře uspořádaných množin A, B. Pak $F \subseteq G \vee G \subseteq F$.

Důkaz
Nechť R resp. S je dané uspořádání A resp. B. Víme, že $\mathrm{Dom}(F), \mathrm{Dom}(G)$ jsou dolní podmnožiny. R je lineární (jelikož je dobré), tedy $\mathrm{Dom}(F) \subseteq \mathrm{Dom}(G)$ nebo $\mathrm{Dom}(G) \subseteq \mathrm{Dom}(F)$. BÚNO první možnost. Sporem dokážeme, že $(\forall x \in \mathrm{Dom}(F))(F(x) = G(x))$.

Nechť x je vzhledem k R nejmenší prvek množiny $\{z, z \in A \wedge F(z) \neq G(z)\}$. Tedy pro každé $y <_R x$ je $F(y) = G(y)$. Z linearity S $F(x) <_S G(x)$ nebo $F(x) >_S G(x)$. BÚNO druhá možnost. Nechť $b = F(x)$. $z \in \mathrm{Dom}(G)$, 1) $z <_R x \implies G(z) = F(z) <_S b$, 2) $z \geqslant_R x \implies G(z) \geqslant_s G(x) >_S b$. Tedy $b \notin \mathrm{Rang}\, G$ a $\mathrm{Rang}\, G$ není dolní množina. $\lightning$. $\square$

Věta 3.8 (O porovnávání dobrých uspořádání)

A je množina dobře uspořádaná R, B je množina dobře uspořádaná S, pak existuje právě jedno zobrazení F, které je izomorfismus A a dolní množiny B nebo izomorfismus dolní množiny A a B.

Důkaz
P množina všech počátkových vnoření z A do B. $F := \bigcup P$ je zobrazení: když (x, y_1) a (x, y_2) existují počátková vnoření F_1, F_2 taková, že $(x, y_1) \in F_1$ a $(x, y_2) \in F_2$. Podle lemma: $F_1 \subseteq F_2 \vee F_2 \subseteq F_1$, tedy $y_1 = y_2$.

F je počátkové vnoření: když $x_1 <_R x_2 \in \mathrm{Dom}(F)$, pak existuje počátkové vnoření $F' \in P$ takové, že $x_2 \in \mathrm{Dom}(F')$, tedy $x_1 \in \mathrm{Dom}(F') \subseteq \mathrm{Dom}\, F$, tedy $\mathrm{Dom}(F)$ je dolní množina. Symetricky pro $\mathrm{Rang}(F)$.

TODO.

$\mathrm{Dom}(F) = A \vee \mathrm{Rang}(F) = B$: Sporem: $A - \mathrm{Dom}(F)$, $B - \mathrm{Dom}(F)$ jsou neprázdné. Mají tedy nejmenší prvky a, b. Definujeme $F' := F \cup \{(a, b)\}$. F' je počátkové vnoření, přitom $F' \supsetneq F$, $\lightning$. □

Věta 3.9

a je konečná množina, pak každé dvě lineární uspořádání na a jsou izomorfní.

Důkaz
r, s dvě lineární uspořádání a. Podle věty výše jsou r, s dobrá, tedy (a, r) je izomorfní dolní množině b v (a, s) nebo naopak. Tzn. $a \approx b$, tedy z definice konečnosti $b = a$. □

Lemma 3.10 (Zachovávání konečnosti)

$$1)(\mathrm{Fin}(x) \wedge y \subseteq x) \implies \mathrm{Fin}(y).$$
$$2)(\mathrm{Fin}(x) \wedge y \approx x) \implies \mathrm{Fin}(y).$$
$$3)(\mathrm{Fin}(x) \wedge y \preceq x) \implies \mathrm{Fin}(y).$$

Důkaz
1) z definice. 2) $\mathcal{P}(x) \approx \mathcal{P}(y)$, dokonce jsou izomorfní vzhledem k $\subseteq$. 3) z 1) a 2). □

Lemma 3.11 (Sjednocení konečných množin)

$$1)(\mathrm{Fin}(x) \wedge \mathrm{Fin}(y)) \implies \mathrm{Fin}(x \cup y).$$
$$2)\,\mathrm{Fin}(x) \implies (\forall y)(\mathrm{Fin}(x \cup \{y\})).$$

Důkaz
1) $w \subseteq \mathcal{P}(x \cup y)$ neprázdná. $\mathcal{P}(x) \supseteq w_1 = \{u, (\exists t \in w)(u = t \cap x)\} \neq \emptyset$. Tedy w_1 má maximální prvek (v_1). Nechť $\emptyset \neq w_2 := \{u, (\exists t \in w)(t \cap x = v_1 \wedge t \cap y = u)\} \subseteq \mathcal{P}(y)$. Tedy w_2 má maximální prvek v_2. $v_1 \cup v_2$ je maximální prvek w.

2): důsledek 1). □

Definice 3.8 (Třída konečných množin)

Třída všech konečných množin je $\mathrm{Fin} := \{x, \mathrm{Fin}(x)\}$.

Věta 3.12 (Princip indukce pro konečné množiny)

Je-li X třída, pro kterou platí

$$1)\emptyset \in X, \qquad 2)x \in X \implies (\forall y)(x \cup \{y\} \in X),$$

potom $\mathrm{Fin} \subseteq X$.

Důkaz (Sporem)
Pokud $x \in \mathrm{Fin} \setminus X$, pak označme $w = \{v, v \subseteq x \wedge v \in X\} = \mathcal{P}(x) \cap X$. Potom z definice konečnosti má w (která obsahuje minimálně $\emptyset$) maximální prvek v_1. $v_0 \subseteq X, v_0 \neq x$, tedy $\exists y \in x \setminus v_0$ a $v_0 \subseteq v_0 \cup \{y\} \in X$, tím pádem jsme našli větší prvek než v_0, který je v w, $\lightning$. □

Lemma 3.13

$$\mathrm{Fin}(x) \implies \mathrm{Fin}(\mathcal{P}(x)).$$

Důkaz
Indukcí přes konečné množiny. Nechť $X = \{x, \mathrm{Fin}(\mathcal{P}(x))\}$. 1) $\emptyset \in X$, protože $\mathcal{P}(\emptyset) = \{\emptyset\}$ je konečná. 2) Nechť $x \in X$, y množina. Chceme, aby $x \cup \{y\} \in X$. BÚNO $y \notin x$. Rozdělíme $\mathcal{P}(x \cup \{y\})$ na části $\mathcal{P}(x)$ a $z := \mathcal{P}(x \cup \{y\}) \setminus \mathcal{P}(x)$. Platí $\mathcal{P}(x) \approx z$: pro $u \in \mathcal{P}(x)$ definujeme $f(u) = u \cup \{y\}$. Podle IP $\mathrm{Fin}(\mathcal{P}(x))$, podle lemma $\mathrm{Fin}(z)$ a $\mathrm{Fin}(z \cup \mathcal{P}(x))$. □

Důsledek
$\mathrm{Fin}(x) \wedge \mathrm{Fin}(y) \implies \mathrm{Fin}(x \times y)$.

Lemma 3.14 (Sjednocení konečně mnoha konečných množin)

$(\mathrm{Fin}(a) \wedge (\forall b \in a)(\mathrm{Fin}(b))) \implies \mathrm{Fin}(\bigcup a)$.

Důkaz (Indukcí)
Nechť $X = \{x, x \subseteq \text{Fin} \implies \text{Fin}(\bigcup x)\}$. 1) $\emptyset \in X$, protože $\bigcup \emptyset = \emptyset$ je konečná. 2) Nechť $x \in X$, y množina. Nechť $x \cup \{y\} \subseteq \text{Fin}$, speciálně $x \subseteq \text{Fin}$. $\bigcup(x \cup \{y\}) = (\bigcup x) \cup y$, což je podle IP a lemmatu o sjednocení konečné. □

Důsledek (Dirichletův princip pro nekonečné množiny)
Je-li nekonečná množina sjednocením konečně mnoha množin, pak alespoň jedna z nich je nekonečná.

TODO

4 Přirozená čísla

Definice 4.1 (Přirozené číslo (von Neumann))

Přirozené číslo je množina všech menších přirozených čísel.

Definice 4.2

w je induktivní množina, pokud $0 \in w \wedge (\forall v \in w)(v \cup \{v\} \in w)$

Definice 4.3 (Axiom nekonečna)

$\exists w$. Neboli
$$(\exists z)(\emptyset \in z \wedge (\forall x)(x \in z \implies x \cup \{x\} \in z)).$$

Definice 4.4 (Množina všech přirozených čísel)

Množina všech přirozených čísel (značíme ω), je $\bigcap\{w | w \text{ je induktivní množina}\}$.

Důkaz (ω je induktivní)
$\emptyset \in \omega$, protože $\emptyset$ je prvkem každé induktivní množiny. Stejně tak, pokud $x \in \omega$, pak $(\forall w \text{ induktivní})(w | x \in w)$, tedy i $x \cup \{x\}$ patří do každé induktivní množiny. □

Definice 4.5 (Následník)

Funkce následník je $S : \omega \to \omega$. Pro $v \in \omega : S(v) = v \cup \{v\}$.

Věta 4.1 (Princip indukce pro přirozená čísla)

Je-li $X \subseteq \omega$ taková, že $\emptyset \in X$ a $x \in X \implies S(x) \in X$. Pak $X = \omega$.

Důkaz
Z podmínek na X víme, že X je induktivní množina, tedy $\omega \subseteq X$. Tedy $\omega = X$. $\square$

Lemma 4.2 ($\in$ je ostré uspořádání na ω)

$$1) n \in \omega \implies n \subseteq \omega.$$
$$2) m \in n \implies m \subseteq n.$$
$$3) n \notin n.$$

Důkaz (Indukcí)
1) 1. krok $\emptyset \subseteq \omega$. 2. krok: Nechť $n \in \omega \wedge n \subseteq \omega$. Pak $\{n\} \subseteq \omega$. Tedy i $n \cup \{n\} \subseteq \omega$.

2) 1. krok $\nexists m \in \emptyset$. 2, krok. Nechť $m \in S(m) = m \cup \{m\}$, potom $m = n$, tj. $m \subseteq n$, nebo $m \in n$ pak z IP $m \subseteq n$.

3) 1. krok $\emptyset \notin \emptyset$ platí. 2. krok předpokládejme, že $n \in \omega$ a $n \notin n$. Sporem: Nechť $S(n) \in S(n) = n \cup \{n\}$. Tedy $S(n) = n$, tj $n \in S(n) \in n$, nebo $S(n) \in n$. Tedy podle 2 $n \in n$. ↯. $\square$

Lemma 4.3 (Přirozená čísla jsou konečná)

$$(\forall n \in \omega)(\mathrm{Fin}(n)).$$

Důkaz
$\mathrm{Fin}(\emptyset)$ a podle lemma sjednocení dvou konečných je konečná, tj. $\mathrm{Fin}(x) \implies \mathrm{Fin}(S(x))$. $\square$

Věta 4.4

Množina x je konečná $\Leftrightarrow (\exists n \in \omega)(x \approx n)$.

Důkaz
$\Leftarrow$ plyne z předchozího lemmatu a zachovávání konečnosti při $\approx$.

$\implies$ indukcí podle konečných množin: $\emptyset \approx 0$. Nechť to pro x platí a y je množina. Máme $x \approx n$ pro nějaké $n \in \mathbb{N}$. Buď $y \in x$, pak $x \cup \{y\} = x \approx n$. Jinak $x \cup \{y\} \approx S(n)$ (bijekci rozšíříme o (y, n)). $\square$

Lemma 4.5

Množina ω i každá induktivní množina je nekonečná.

Důkaz
Podle lemmatu výše 1) $n \in \omega \implies n \subseteq \omega$, tedy $n \in \mathcal{P}_\omega$. Tudíž $\omega \subseteq \mathcal{P}(\omega)$. ω je neprázdná, ale nemá maximální prvek vzhledem k $\subseteq$, jelikož $n \in \omega \implies n \notin n$, tj. $n \subset n \cup \{n\}$, tedy n není maximální.

Je-li W induktivní, potom $\omega \subseteq W$ a podle dřívějšího lemma (konečnost se zachovává na podmnožinu) je W nekonečná. □

Příklad (Cvičení)
Dokažte, že ω je dedekindovsky nekonečná.

Lemma 4.6 (Linearita $\in$ na ω)

1) $m \in n \Leftrightarrow m \subset n$.
2) $m \in n \vee m = n \vee n \in m$.

Důkaz
1) Víme $m \in n \implies m \subseteq n$. $\implies$: Kdyby ale $m = n$, pak $n \in n$, $\lightning$. $\Leftarrow$: Indukcí podle n. $n = 0$ nelze splnit $m \subset n$. Nechť platí pro nějaké n a všechna m. Nechť $m \subset S(n)$, pak platí $m \subseteq n$. Kdyby $n \in m$, pak $n \subseteq m$ TODO?

2) Pro $n \in \omega$ nechť $A(n) = \{m \in \omega; m \in n \vee m = n \vee n \in m\}$. Dokážeme, že $A(n)$ je induktivní indukcí podle m. $n = 0 : 0 \in A(0)$, protože $0 = 0$. Pokud $m \in A(0)$, pak $0 \in m \vee m = 0 \ldots 0 \in \{m\}$, tj. $0 \in m \cup \{m\} = S(m)$. Tedy $A(0) = \omega$.

Tedy také $(\forall n \in \omega) 0 \in A(n)$. nechť $n, m \in \omega$, $m \in A(n)$. Ukážeme, že $S(m) \in A(n)$. a) $m \in n$: Podle 1) $m \subset n$, $\{m\} \subseteq n$, tedy $S(m) \subseteq n$: $S(m) = n \vee S(m) \subset n$ a podle 1) $S(m) \in n \subseteq S(n)$. b) $m = n \vee n \in m \implies n \in m \cup \{m\} = S(m)$. Ve všech případech tedy $S(m) \in A(n)$. □

Věta 4.7

Množina ω je dobře ostře uspořádaná relací $\in$.

Důkaz
Nechť $a \subseteq \omega, a \neq \emptyset$. Zvolme $n \in a$. Kdyby n bylo minimální, jsme hotovi, není-li n minimální, definujeme $b = a \cap n$. Z konečnosti plyne, že b má minimum, které je zároveň hledaným minimem. □

Příklad (Cvičení)
Dokažte princip silné indukce na ω.

$f : \omega \to X$, f je zobrazení na, pak $X \preceq \omega$.

Věta 4.8 (Charakterizace uspořádání $\in$ na ω)

Nechť A je nekonečná množina, lineárně ostře uspořádaná relací $<$ tak, že pro každé $a \in A$ je dolní množina $(\leftarrow, a]$ konečná. Potom $<$ je dobré ostré uspořádání na A a množiny A, ω jsou izomorfní vzhledem k $<, \in$.

Důkaz

$<$ je dobré: $\emptyset \neq C \subseteq A$, nechť $a \in c$. Pokud a není minimální, nechť $b = c \cap (\leftarrow, a]$ podle předchozího je b konečná, neprázdná a má minimální prvek m. m je i minimální v c (kdyby $x \in c, x < m$, pak $x \in b$).

Izomorfismus: Podle věty o porovnávání dobrých uspořádání 1) A je izomorfní *dolní* množině $B \subseteq \omega$, pak B není shora omezená (jinak $B \subseteq S(n)$, tedy B by byla konečná). Tedy každé $n \in \omega$ je menší než nějaký prvek B. Tedy $n \in B$. Tedy $B = \omega$.

2) ω je izomorfní s dolní množinou $C \in A$, pak C není shora omezená (obdobně jako v předchozím odstavci), tedy $C = A$. $\square$

5 Spočetné množiny

Definice 5.1

Množina x je spočetná, pokud $x \approx \omega$. x je nejvýše spočetná, je-li konečná nebo spočetná. Jinak je nespočetná.

Poznámka

V ZF nelze dokázat, že každá nekonečná množina obsahuje spočetnou podmnožinu. Platí totiž x je dedekindovsky nekonečná $\Leftrightarrow \omega \preceq x$.

Věta 5.1

1) Každá shora omezená podmnožina ω je konečná, každá shora neomezená podmnožina ω je spočetná.

2) Každá podmnožina spočetné množiny je nejvýše spočetná.

Důkaz

1) A je shora omezená $(\exists n \in \omega)(\forall a \in A)(a \in n \vee a = n)$, tedy $A \subseteq S(n)$, tedy $\mathrm{Fin}(A)$. (Naopak konečná $\implies$ shora omezená.)

A shora neomezená, pak A je nekonečná, dobře ostře uspořádaná $\in$, pro každé $a \in A$ tedy platí, že $(\leftarrow, a]$ je konečná. Tedy podle ? věty $A \approx \omega$, tedy A je spočetná.

2) A spočetná, f prosté zobrazení A na ω. $B \subseteq A$, $B \approx f[B] \subseteq \omega$, podle 1) je konečná nebo spočetná. $\square$

Definice 5.2 (Lexikografické uspořádání)

Lexikografické uspořádání na $\omega \times \omega$ je relace $(n_1, m_1) <_L (n_2, m_2) \Leftrightarrow (n_1 \in m_1 \vee (n_1 = n_2 \wedge m_1 \in m_2))$.

Důsledek
$<_L$ je dobré na $\omega \times \omega$. $<_L$ na $\omega \times 2$ (ne opačně!) je izomorfní s ω uspořádanou $\in$.

Definice 5.3 (Maximum)

Maximum n, m je $\max(m, n) = m$, pokud $n \in m$, a n jinak.

Definice 5.4 (Maximo-lexikografické uspořádání)

Maximo-lexikografické uspořádání na $\omega \times \omega$ je relace $(n_1, m_1) <_{ML} (n_2, m_2) \Leftrightarrow$

$$(\max n_1, m_1 < \max(n_2, m_2) \vee (\max(n_1, m_1) = \max(n_2, m_2) \wedge (n_1, m_1) <_L (n_2, m_2))).$$

Pozorování
$<_{ML}$ je izomorfní s $\in$. Tudíž $\omega \times \omega \approx \omega$.

Věta 5.2 (O zachování spočetnosti)

Jsou-li A, B spočetné množiny, pak $A \cup B$ a $A \times B$ jsou spočetné.

Důkaz
$f : A \to \omega$, $g : B \to \omega$ bijekce. Definujeme zobrazení $h : A \cup B \to \omega \times 2$, že $h(x) = (f(x), 0)$, pokud $x \in A$, $h(x) = (g(x), 1)$ jinak ($x \in B \backslash A$). h je prosté. Podle Cantor-Bernstein $A \cup B \approx \omega$.

$k : A \times B \to \omega \times \omega \approx \omega$ jako $k((a, b)) = (f(a), g(b))$, tedy k je bijekce. □

Důsledek
$\mathbb{Z}$, $\mathbb{Q}$ jsou spočetné.

Důsledek (Pouze s axiomem výběru)
Spočetné sjednocení spočetných množin je spočetné.

Věta 5.3 (Cantorova věta)

Pro každou množinu x platí, že $x \prec \mathcal{P}(x)$. (Dokonce neexistuje zobrazení x na $\mathcal{P}(x)$.)

Důkaz
$x \preceq \mathcal{P}(x)$. Díky zobrazení $f(y) = \{y\}$.

Nechť nyní $f : x \to \mathcal{P}(x)$. Ukážeme, že $\mathrm{Rang}(f) \neq \mathcal{P}(x)$. $y = \{t, t \in x \wedge t \notin f(t)\}$. $y \in \mathcal{P}(x)$, ale nemá vzor při f (jinak by tento vzor nemohl a musel být ve svém obrazu). □

Důsledek
$\mathcal{P}(\omega)$ je nespočetná a V je vlastní.

Věta 5.4

$\mathcal{P}(\omega) \approx \mathbb{R} \approx [0, 1]$.

Důkaz
Víme, že $\mathcal{P}(\omega) =^{\omega} 2$, tj. množina posloupností $(a_0, a_1, \ldots)$, kde $a_i \in \{0, 1\}$. Každé $a \in [0, 1]$ lze zapsat binárně jako $a = 0$ nebo $a = 0, a_0 a_1 a_2 \ldots$. Pokud jsou možné 2 zápisy, tak si vybereme ten, kde je nekonečně mnoho pozic rovných 1. Tím získáváme prosté zobrazení $[0, 1]$ do ${}^{\omega}2$.

Prosté zobrazení ${}^{\omega}2$ do $[0, 1]$ použijeme trojkovou soustavu: $(a_0, a_1, \ldots) \mapsto \sum_{i=0}^{\infty} \frac{a_i}{3^{i+1}}$. Následně použijeme Cantor-Bernstein na ${}^{\omega}2 \approx [0, 1]$.

Pro $[0, 1] \approx \mathbb{R}$ stačí uvažovat něco jako $\frac{\pi/2 + \mathrm{arctg}(x)}{\pi}$ a $[0, 1] \subseteq \mathbb{R}$. □

Poznámka (Algebraická čísla)
Pro definici viz Algebru. Je jich spočetně mnoho.

6 Hypotéza kontinua

Poznámka (Historie)
Cantor 1878, zkracuje se CH. První z 23 Hilbertových problémů (1900). Bezespornost s ZFC dokázána 1940 Gödelem. 1963-4 Cohen ukázal, že i negace je bezesporná s ZFC.

Definice 6.1 (CH)

Každá nekonečná podmnožina $\mathbb{R}$ je buď spočetná nebo ekvivalentní s $\mathbb{R}$. ($\Leftrightarrow$ Neexistuje množina $x \subseteq \mathbb{R}$ pro kterou $\omega \prec x \prec \mathcal{P}(\omega)$.)

7 Axiom výběru

Definice 7.1 (Princip výběru (starší verze))

Pro každý rozklad r množiny X existuje výběrová množina (tj. množina $v \subseteq X$, pro kterou platí $(\forall u \in r)(\exists! x)(v \cap u = \{x\})$) (někdy také transverzála, viz Algebra).

Definice 7.2 (Selektor)

Je-li X množina, pak funkce f definovaná na X a splňující $(y \in X \wedge y \neq \emptyset) \implies f(y) \in y$ se nazývá selektor na množině X.

Definice 7.3 (Axiom výběru (AC))

Na každé množině existuje selektor.

Například (Ekvivalentní tvrzení)
Každou množinu lze dobře uspořádat.

Relace subvalence ($\preceq$) je trichotomická.

Zornovo lemma.

Důsledek
Každý vektorový prostor má bázi.

Součin kompaktních prostorů je kompaktní.

Hall?-Banachova věta (o oddělování nadrovinou).

Princip kompaktnosti.

Definice 7.4 (Indexovaný soubor množin)

$\langle F_j, j \subseteq J \rangle$, kde F je zobrazení s definičním oborem J, pro $j \in J$ je $F_j = F(j)$, je indexová třída (množina), prvky J se nazývají indexy.

$$\bigcup_{j \in J} F_j = \{x, (\exists j \in J) x \in F_j\} = \bigcup_{j \in J} F_j = \bigcup \operatorname{Rang} F.$$

$$\bigcap_{j \in J} F_j = \{x, (\forall j \in J) x \in F_j\} = \bigcap_{j \in J} F_j = \bigcap \operatorname{Rang} F.$$

Definice 7.5 (Kartézský součin souboru množin)

$$\bigtimes_{j \in J} F_j := \{f, f : J \to \bigcup_{j \in J} F_j \wedge (\forall j \in J) f(j) \in F_j\}$$

Lemma 7.1

Je-li J množina, pak $\bigtimes_{j\in J} F_j$ je množina.

Je-li $(\forall j \in J)F_j = y$, pak $\bigtimes_{j\in J} =^J y$.

Důkaz

J množina, tedy z axiomu $\operatorname{Rang} F$ je množina, tedy $\bigcup \operatorname{Rang}(F)$ je množina, ${}^J \bigcup \operatorname{Rang} F$ je množina, $\bigtimes_{j\in J} F_j \subseteq^J \bigcup \operatorname{Rang} F \subseteq J \times (\bigcup \operatorname{Rang} F)$. □

Lemma 7.2 (AC)

Následující je ekvivalentní:

1. *Axiom výběru.*
2. *Princip výběru.*
3. *Pro každou množinovou relaci S existuje funkce $F \subseteq S$ tak, že* $\operatorname{Dom}(F) = \operatorname{Dom}(S)$.
4. *Kartézský součin $\bigtimes_{i\in x} a_i$ neprázdného souboru neprázdných množin je neprázdný.*

Důkaz

$1 \implies 2$: r rozklad X. Podle 1) existuje selektor f na r, potom $\operatorname{Rang}(f)$ je výběrová množina na r.

$2 \implies 3$: BÚNO $S \neq \emptyset$: utvoříme rozklad S. $r = \{\{i\} \times S''\{i\}, i \in \operatorname{Dom}(S)\} = \{\{(i,x)|(i,x) \in S\}, i \in \operatorname{Dom}(S)\}$. Výběrová množina r je přesně funkce $f \subseteq S$. $\operatorname{Dom}(f) = \operatorname{Dom}(S)$.

$3 \implies 4$: $\langle a_i, i \in x\rangle$. Vytvoříme relaci $S = \{(i,y), i \in x \wedge y \in a_i\}$. Funkce f z 3) je prvkem $\bigtimes_{i\in x} a_i$.

$4 \implies 1$: X množina, BÚNO $X \neq \emptyset$ a $\emptyset \notin X$. □

Lemma 7.3

Sjednocení (nejvýše) spočetného souboru (nejvýše) spočetných množin je spočetné.

Důkaz

$\langle B_j, j \in J\rangle$, BÚNO $J = \omega$. Najdeme prosté zobrazení z $\bigcup_{j\in J} B_j$ do $\omega \times \omega$. Uvažujme soubor $\langle E_j, j \in \omega\rangle$, kde E_j je množina všech prostých zobrazení B_j do ω. Z předpokladu $E_j \neq \emptyset$. Podle Lemma o AC bod 4) je $\times_{j\in\omega} E_j$ je neprázdný. Existuje tedy soubor prostých zobrazení $\langle f_j, j \in \omega\rangle$, kde $f_j \subseteq E_j$.

Definujeme $h = \bigcup_j B_j \to \omega \times \omega$ jako $h(x) = (j, f_j(x))$, kde j je $\min\{i|x \in B_i\}$. Toto zobrazení už je zřejmě prosté, tedy $\bigcup_i B_i \preceq \omega \times \omega \approx \omega$. □

Definice 7.6 (Řetězec)

A je množina uspořádaná $\leqslant$. Pak $B \subseteq A$ je řetězec, pokud B je lineárně uspořádaná $\leqslant$.

Definice 7.7 (Zornovo lemma (princip maximality) (PM))

Je-li A množina uspořádaná relací $\leqslant$ tak, že každý řetězec má horní mez, pak $\forall a \in A$ $\exists$ maximální prvek $b \in A$ takový, že $a \leqslant b$.

Poznámka

Ekvivalentní s AC.

Definice 7.8 (Princip maximality II (PMS))

Je-li A množina uspořádaná relací $\leqslant$ tak, že každý řetězec má supremum, pak $\forall a \in A$ $\exists$ maximální prvek $b \in A$ takový, že $a \leqslant b$.

Poznámka

Taktéž ekvivalentní s AC.

Definice 7.9 (Princip trichotomie relace subvalence (PT))

Pro libovolné množiny x, y platí $x \preceq y$ nebo $y \preceq x$. (Každé dvě množiny dokážeme porovnat podle velikosti.)

Lemma 7.4

(PM) $\implies$ *(PT).*

Důkaz

Definujeme $D = \{f|f \text{ prosté zobrazení } \wedge \mathrm{Dom}(f) \leqslant x \wedge \mathrm{Rang}(f) \subseteq y\}$. $(D, \subseteq)$ splňuje předpoklady (PM). Nechť g je maximální prvek $(D, \subseteq)$: Sporem: Kdyby $x \setminus \mathrm{Dom}(g)$ a $y \setminus \mathrm{Rang}(g)$ byly neprázdné, lze g rozšířit o další dvojici – spor. Pokud $\mathrm{Dom}(g) = x$, je $x \preceq y$. Pokud $\mathrm{Rang}(g) = y$, pak $g^{-1}i : y \to x$ je prosté, tedy $y \preceq x$. □

Důsledek
Pro každou nekonečnou množinu x platí $\omega \preceq x$.

Definice 7.10 (Princip dobrého uspořádání (WO))

Každou množinu lze dobře uspořádat.

Poznámka
Také ekvivalentní s AC

Lemma 7.5

(WO) $\implies$ (AC).

Důkaz
$X \neq \emptyset$, $\emptyset \notin X$. Použijeme (WO) na $\bigcup X$ a získáme $\leqslant$. Definujeme si selektor $f : X \to \bigcup x$ jako $f(y) = \min_{\leqslant}(y)$. □

8 Ordinální čísla

Poznámka (Historie)
Historicky se ordinální čísla definovala jako typy dobře uspořádaných množin.

Kardinální čísla $\subseteq$ ordinální čísla. Jsou to mohutnosti dobře uspořádaných množin (s AC libovolných množin).

Ordinální čísla jsou dobře uspořádaná $\in$ a platí pro ně transfinitní indukce.

Definice 8.1 (Tranzitivní třída)

Třída X je tranzitivní, pokud $x \in X \implies x \subseteq X$.

Lemma 8.1

Jsou-li X, Y tranzitivní, pak $X \cap Y$ a $X \cup Y$ jsou tranzitivní.

Je-li X třída a každý prvek $x \in X$ je tranzitivní množina, pak $\bigcap X$, $\bigcup X$ jsou tranzitivní.

Je-li X tranzitivní, pak $\in$ je tranzitivní na $X \Leftrightarrow$ každé $x \in \mathbb{X}$ je tranzitivní množina.

Důkaz
Cvičení. □

Definice 8.2 (Ordinál)

Množina x je ordinální číslo (ordinál), pokud x je tranzitivní množina a $\in$ je dobré ostré uspořádání x.

Třídu všech ordinálních čísel značíme O_n.

Lemma 8.2

O_n je tranzitivní třída (prvky ordinálů jsou ordinály).

Důkaz

Nechť $y \in x \in O_n$. x je ordinální číslo, takže je tranzitivní: $y \subseteq x$, $\in$ je dobré uspořádání na x, tedy je to dobré uspořádání i na y. Také z toho vyplývá, že $\in$ je tranzitivní na x $\implies$ y je tranzitivní podle předchozího lemma. □

Důsledek

$\in$ je tranzitivní na O_n.

Lemma 8.3

$x, y \in O_n$, pak 1) $x \notin x$, 2) $x \cap y \in O_n$, 3) $x \in y \Leftrightarrow x \subset y$.

Důkaz

1) sporem z antireflexivity $\in$ na x, 2) přímo z definice, 3) cvičení. □

Věta 8.4

$\in$ je dobré ostré uspořádání třídy O_n.

Důkaz

$\in$ je ostré uspořádání (víme z dřívějška). Trichotomie: $x, y \in O_n \implies x \cap y \in O_n$. Pro spor předpokládejme, že $x \cap y \subsetneq x, y$. Podle předchozího lemmatu (3. část) $x \cap y \in x, y$, tj. $x \cap y \in x \cap y$, ↯. Tedy buď $x \cap y = x = y$, pak jsme hotovi, nebo BÚNO $x \cap y = x \neq y$, pak $x \subset y$ a tedy $x \in y$.

„Dobrota“: $A \subseteq O_n$, $A \neq \emptyset$. Zvolíme si $\alpha \in A$. Když je minimální, pak máme hotovo, tedy předpokládejme, že není minimální. $b := \alpha \cap A$, $b \subseteq \alpha$, $b \neq \emptyset$. b má nejmenší prvek (podmnožina ordinálu), označme ho β. β je minimální v A: Sporem $\exists \gamma \in \beta$, $\gamma \in A$, $\beta \in b \subseteq \alpha$, α je tranzitivní, tedy $\gamma \in \alpha$, tedy i $\gamma \in b$. ↯. □

Důsledek

O_n není množina. (Jinak O_n je ordinální číslo, tedy $O_n \in O_n$, ↯.)

Důsledek
Je-li X vlastní tranzitivní třída, kde $\in$ je dobré ostré uspořádání na X, pak $X = O_n$.

Poznámka (Značení)
Ordinály se značí malými řeckými písmeny.

Místo $\alpha \in \beta$ se píše $\alpha < \beta$. Obdobně $\alpha \leqslant \beta$.

Lemma 8.5

1) Množina $x \subseteq O_n$ je ordinální číslo $\Leftrightarrow$ x je tranzitivní.

2) $A \subseteq O_n$, $A \neq \emptyset$ třída, pak $\bigcap A$ je nejmenší prvek A.

3) $a \subseteq O_n$ množina, pak $\bigcup a \in O_n$ a $\bigcup a = \sup a$.

Důsledek
ω je supremum množiny všech přirozených čísel v O_n. ($\omega = \sup \omega$.)

Konečné ordinály jsou právě přirozená čísla.

Lemma 8.6

$\alpha \in O_n$, pak $\alpha \cup \{\alpha\}$ je nejmenší ordinál větší než α.

Důkaz
Z tranzitivity O_n máme $\alpha \subseteq O_n$, tedy $\alpha \cup \{\alpha\} \subseteq O_n$. Je-li $\beta \in \alpha \cup \{\alpha\}$, pak buď $\beta \in \alpha$ nebo $\beta = \alpha$. □

Definice 8.3 (Následník, předchůdce)

$\alpha \cup \{\alpha\}$ se nazývá následník α; α je předchůdce $\alpha \cup \{\alpha\}$.

Definice 8.4 (Izolovaný, limitní ordinál)

α je izolovaný, pokud $\alpha = 0$ nebo α má předchůdce. Jinak se nazývá limitní.

Věta 8.7

Je-li a množina dobře uspořádaná relací r, pak existuje právě jedno ordinální číslo α a právě jeden izomorfismus (a, r) na $(\alpha, <)$.

Definice 8.5 (Typ)

α se nazývá typ uspořádání r.

Poznámka
Takto definoval ordinální čísla Cantor 1895. (Naše definice je Von Neumann 1923.)

Důkaz
V dalším semestru (předmět o nekonečných množinách). □

Poznámka
Na $O_n^2 = O_n \times O_n$ lze definovat lexikografické uspořádání, maximo-lexikografické uspořádání, která jsou dobrá a maximo-lexikografické je úzké ($(\leftarrow, x]$ je množina $\forall x$).

Věta 8.8 (Princip transfinitní indukce)

Je-li $A \subseteq O_n$ třída splňující $(\forall \in O_n)(\alpha \subseteq A \implies \alpha \in A)$, pak $A = O_n$.

Důkaz
Sporem: předpokládejme, že $O_n \setminus A \neq \emptyset$, pak díky dobrému uspořádání O_n existuje nejmenší prvek $\alpha \in O_n \setminus A$, tedy každé $\beta \in \alpha$ už je prvek A, tedy $\alpha \subseteq A$ a podle předpokladu $\alpha \in A$. ↯. □

Věta 8.9 (PTI 2. verze:)

Je-li $A \subseteq O_n$ třída splňující $0 \in A$ a pro každé $\alpha \in O_n : \alpha \in A \implies \alpha \cup \{\alpha\} \in A$ nebo $\alpha \subseteq A \implies \alpha \in A$, pokud α je limitní, pak $A = O_n$.

Věta 8.10 (O konstrukci transfinitní rekurzí)

Je-li $G : V \to V$ třídové zobrazení, pak existuje právě jedno (třídové) zobrazení $F : O_n \to V$ splňující $\forall \alpha \in O_n : F(\alpha) = G(F|_\alpha)$. (Další varianty jsou $F(\alpha = G(F[\alpha]))$, $F(\alpha) = G(\alpha, F|_\alpha)$, jiné varianty pro limitní a pro izolované).

Důkaz
Transfinitní indukcí a Axiomem nahrazení -> v navazujícím předmětu. □

Důkaz (AC $\implies$ WO, náznak)
A množina, g selektor na $\mathcal{P}(A)$. $f(0) = g(A)$, $f(\beta) = g(A \setminus f[\beta])$. □

Příklad (Pro zajímavost)
$\mathbb{R}^3$ je disjunktní sjednocení jednotkových kružnic.

Důkaz
Očíslují se všechny body v $\mathbb{R}^3$ pomocí ordinálů. Potom sestrojíme soubor $\langle C_\alpha, \alpha < 2^\omega \rangle$ disjunktních jednotkových kružnic (a $\emptyset$) tak, že $x_\alpha \in C_\alpha$ nebo $x_\alpha \in \bigcup_{\beta \subseteq \alpha} C_\beta$.

C_α definujeme rekurzivně. Protože $\alpha < |\mathbb{R}|$, tak vždy najdeme rovinu bez kružnice a na ní kružnici, která neprotíná žádnou jinou (každá kružnice protínající tuto rovinu nám zakáže maximálně 2 kružnice). $\square$