Poznámky - teorie množin

Petr Chmel, LS 2019/20

Poznámka (Jazyk)**.** Jazyk teorie množin obsahuje

- proměnné (malá, případně oindexovaná písemena)
- binární predikátový symbol $=$
- binární predikátový symbol $\in$
- logické spojky $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$
- kvantifikátory $\forall, \exists$
- závorky $(,), [,]$

Pojem formule stejný z logiky, volný vs vázaný výskyt.

Zkratka	význam	slovně	potřebné axiomy
$x \neq y$	$\neg(x = y)$	-	-
$x \notin y$	$\neg(x \in y)$		-
$x \subseteq y$	$(\forall u)(u \in x \rightarrow u \in y)$	„x je podmnožinou y“	-
$x \subset y$	$x \subseteq y \wedge (x \neq y)$		-
$\{x : x \in a \wedge \varphi(x)\}$	z z axiomu 3		3
$a \cap b$	$\{x : x \in a \wedge x \in b\}$	průnik	3
$a \setminus b$	$\{x : x \in a \wedge x \notin b\}$	množinový rozdíl	3
$\emptyset$	$\{x : x \in a \wedge x \neq x\}$	prázdná množina	3
$\{a, b\}$	z z axiomu 4	neuspořádaná dvojice	4
$\{a\}$	$\{a, a\}$	jednoprvková množina	4
(a, b)	$\{\{a\}, \{a, b\}\}$	uspořádaná dvojice	4
$\bigcup a$	$\{x : (\exists y)(x \in y \wedge y \in a)\}$	suma	5
$a \cup b$	$\bigcup\{a, b\}$	sjednocení	5
$\mathcal{P}(a)$	z z axiomu 6	potenční množina množiny a	6

Poznámka (Zkratky v jazyce)**.**

Axiom 1 (Axiom existence množiny)**.** $(\exists x)(x = x)$ – „Budiž množina“

Axiom 2 (Axiom extenzionality)**.** $((\forall z)(z \in x \leftrightarrow z \in y)) \rightarrow x = y$ – „Množina je určena svými prvky“

Poznámka (O axiomu extenzionality)**.** Píšeme jen jednu implikaci, neboť druhou dostáváme z logiky a axiomů o rovnosti.

Axiom 3 (Schéma axiomů vydělení)**.** Je-li $\varphi(x)$ formule, která nemá volnou proměnnou z, pak $(\forall a)(\exists z)(\forall x)(x \in z \leftrightarrow (x \in a \wedge \varphi(x)))$ je axiom. – „Z množiny a vybereme prvky s vlastností $\varphi(x)$, ty utvoří novou množinu z.“

Poznámka (O schématu axiomů vydělení)**.** Z axiomu extenzionality máme jednoznačnost z.

Axiom 4 (Axiom dvojice)**.** $(\forall a)(\forall b)(\exists z)(\forall x)(x \in z \leftrightarrow (x = a \vee x = b))$ – „Ke každým dvěma množinám a, b existuje množina z tak, že její prvky jsou právě a a b.“

Poznámka (O axiomu dvojice)**.** Jednoznačnost plyne z axiomu extenzionality.

Lemma 1 (Uspořádané dvojice fungují tak, jak bychom čekali)**.** $(x, y) = (u, v) \leftrightarrow (x = u \wedge y = v)$

Důkaz. TODO $\boxplus$

Definice 1 (Uspořádaná k-tice (složitější zkratka))**.** Jsou-li $a_1, \dots, a_n$ množiny, definujeme uspořádanou n-tici následovně:

- (a_1) znamená a_1
- Máme-li definované $(a_1, \dots, a_k)$, pak $(a_1, \dots, a_{k+1})$ je $((a_1, \dots, a_k), a_{k+1})$.

Lemma 2 (Uspořádané k-tice fungují tak, jak bychom čekali)**.** $(a_1, a_2, \dots, a_k) = (b_1, b_2, \dots, b_k) \leftrightarrow (a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_n = b_n)$

Důkaz. Bez důkazu, analogicky jako u dvojic. ⊞

Axiom 5 (Axiom sumy)**.** $(\forall a)(\exists z)(\forall x)(x \in z \leftrightarrow (\exists y)(x \in y \wedge y \in a))$ – „z je tvořena prvky prvků a“

Poznámka (O axiomu sumy)**.** Jednoznačnost plyne z extenzionality.

Definice 2 (n-prvková množina)**.** Je-li $\{a_1, \dots, a_k\}$ k-prvková množina, pak $\{a_1, \dots, a_{k+1}\}$ definujeme jako $\{a_1, \dots, a_k\} \cup \{a_{k+1}\}$

Axiom 6 (Axiom potence)**.** $(\forall a)(\exists z)(\forall x)(x \in z \leftrightarrow x \subseteq a)$ – „Existuje množina z, jejíž prvky jsou právě všechny podmnožiny množiny a.“

Poznámka (O axiomu potence)**.** Jednoznačnost máme z extenzionality, axiom je hlavně potřeba pro konstrukci „velkých“ nekonečen. Korespondence: $x \subseteq a \to x \in \mathcal{P}(a)$, $x \in a \to x \subseteq \bigcup a$.

Axiom 7 (Schéma axiomu nahrazení)**.** Je-li $\psi(u,v)$ formule, která neobsahuje volné proměnné w, z, pak $(\forall u)(\forall v)(\forall w)((\psi(u,v) \wedge \psi(u,w)) \to v = w) \to (\forall a)(\exists z)(\forall x)(v \in z \leftrightarrow (\exists u)(u \in a \wedge \psi(u,v)))$ – „Je-li ψ částečná funkce určená formulí, pak obraz a tou funkcí je množina z“

Poznámka (O substituci ve schématu axiomu nahrazení)**.** Jako $\psi(u,w)$ myslíme $\psi(u, v/w)$ - substituci.

Toto schéma implikuje schéma axiomu vydělení - $\psi(u,v) = \varphi(u) \wedge u = v$.

Využití schématu: transfinitní indukce, sčítání nekonečen, věta o typu dobrého uspořádání, Zornovo lemma.

Axiom 8 (Axiom fundovanosti)**.** $(\forall a)(a \neq \emptyset \to (\exists x)(x \in a \wedge a \cap x = \emptyset))$ – „každá neprázdná množina má prvek, který je s ní disjunktní“

Třídy

Definice 3 (Třída, třídový term, vlastní třída)**.** Buď $\varphi(x)$ formule. Pak $\{x : \varphi(x)\}$ označuje „soubor“ množin pro které platí $\varphi(x)$. Pokud $\varphi(x)$ je tvaru $x \in a \wedge \psi(x)$, jedná se o množinu.

$\{x : \varphi(x)\}$ je třídový term a soubor množin, který označuje, nazveme třídou určenou formulí $\varphi(x)$.

Řekneme, že třída je vlastní, pokud se nejedná o množinu.

Definice 4 (Třídové operace)**.** $A \cap B$ je $\{x : x \in A \wedge x \in B\}$
$A \cup B$ je $\{x : x \in A \vee x \in B\}$
$A \setminus B$ je $\{x : x \in A \wedge x \notin B\}$
$V = \{x : x = x\}$ je třída všech množin (*univerzální třída*).
Pro třídu A je (absolutní) doplněk A $V \setminus A$, značeno $-A$.
$\bigcup A$ je $\{x : (\exists a)(a \in A \wedge x \in a)\}$
$\bigcap A$ je $\{x : (\forall a)(a \in A \to x \in a)\}$

Lemma 3 (V není množina)**.** V není množina.

Důkaz. Pokud by V byla množina, pak $V \in V$, což je spor s axiomem fundovanosti. ⊞

Lemma 4 (O průniku třídy a množiny)**.** Je-li A třída a a množina, pak $a \cap A$ je množina.

Důkaz. $a \cap A$ je $\{x : x \in a \wedge x \in A\}$, což je množina ze schématu axiomu vydělení. ⊞

Definice 5 (Kartézský součin tříd)**.** Kartézský součin tříd A, B je třída $A \times B$, což je $\{(a,b) : a \in \wedge b \in B\}$.

Lemma 5 (Kartézský součin množin je množina)**.** Jsou-li x, y množiny, pak i $x \times y$ je množina.

Důkaz. Platí: $x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y))$. Pro $u \in x, v \in y : \{u\} \in \mathcal{P}(x \cup y), \{u, v\} \in \mathcal{P}(x \cup y)$, a tedy $\{\{u\}, \{u, v\}\} \subseteq \mathcal{P}(x \cup y)$, a tedy $\{\{u\}, \{u, v\}\} \in \mathcal{P}(\mathcal{P}(x \cup y))$. ⊞

Definice 6 (Násobný kartézský součin)**.** Buď X třída. Pak X^1 je X, X^{n+1} je $X^n \times X$.

Definice 7 (Relace)**.** Řekneme, že třída Rje relace, je-li $R \subseteq V \times V$.

Je-li $R \subseteq V^n$ pro nějaké $n \geq 2$, říkáme, že R je n-ární relace.

Poznámka (Důležité relace, definiční obor a obor hodnot)**.** $E = \{\langle x, y \rangle : x \in y\}$,$Id = \{\langle x, y \rangle : x = y\}$.

$Dom(X) = \{u : (\exists v)((u, v) \in X)\}$, $Rng(X) = \{v : (\exists u)((u, v) \in X)\}$, dále obor X je $Dom(X) \cup Rng(X)$.

Definice 8 (Obraz a zúžení třídy)**.** Říkáme, že třída $X'Y = \{z : (\exists y)(y \in Y \wedge (y, z) \in X)\}$ je obraz třídy Y daný třídou X.

Říkáme, že třída $X|Y = \{(y, z) : y \in Y \wedge (y, z) \in X\}$ je zúžení třídy X na třídu Y.

Lemma 6 (Dom, Rng, zúžení a obraz množiny jsou množiny)**.** Je-li x množina, pak $Dom(x), Rng(x), x|Y, x'Y$ pro Y libovolnou třídu jsou také množiny.

Důkaz. $Dom(x) \subseteq \bigcup(\bigcup x)$, pak pro $u \in Dom(x)$ máme v tak, že $(u, v) \in x$. Pak $\{u\} \in (u, v)$, a tedy $\{u\} \in \bigcup x$, a tedy $u \in \bigcup(\bigcup x)$.

$Rng(x) \subseteq \bigcup(\bigcup x)$, pak pro $u \in Rng(x)$ máme nějaké v tak, že $(v, u) \in x$, tedy $\{u, v\} \in (v, u)$, tedy $\{u, v\} \in \bigcup x$, tedy $u \in \bigcup(\bigcup x)$.

Z axiomu sumy je $\bigcup(\bigcup x)$ množina, a tedy můžeme vydělit schématem vydělení oba obory. Dále $x'Y \subseteq Rng(x), x|Y \subseteq x$. ⊞

Definice 9 (Inverzní relace a složení relací)**.**

1. $R^{-1} = \{(u, v) : (v, u) \in R\}$,
2. $R \circ S = \{(u, v) : (\exists w)((u, w) \in R \wedge (w, v) \in S)\}$.

Lemma 7 (Inverz a asociativita skládání relací)**.** Pro libovolné relace R, S, T platí:

1. $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$
2. $R \circ (S \circ T) = (R \circ s) \circ T$

Důkaz. 1: $(u, v) \in (R \circ S)^{-1}$, tedy $(v, u) \in R \circ S$, a tedy existuje w tak, že $(v, w) \in R, (w, u) \in S$.

„$\subseteq$“: $(u, w) \in S^{-1}, (w, v) \in R^{-1}$, tedy $(u, v) \in S^{-1} \circ R^{-1}$.

„$\supseteq$“: $(u, v) \in S^{-1} \circ R^{-1}$, tedy pro nějaké $w : (u, w) \in S^{-1}, (w, v) \in R^{-1}$, tedy $(w, u) \in S, (v, w) \in R, (v, u) \in R \circ S$, a tedy $(u, v) \in (R \circ S)^{-1}$.

2: $(u, v) \in R \circ (S \circ T)$, tedy existuje $r : (u, r) \in R, (r, v) \in S \circ T$, tedy existuje s tak, že $(r, s) \in S, (s, v) \in T$, a tedy $(u, s) \in R \circ S$, a tedy $(u, v) \in (R \circ S) \circ T$. ⊞

Definice 10 (Funkce, prostá, na)**.** Říkáme, že relace je zobrazení (funkce), jestliže pro libovolná u, v, w platí $((u, v) \in F \wedge (u, w) \in F) \rightarrow v = w$.

Říkáme, že F je zobrazením třídy X do třídy Y, jestliže $Dom(F) = X, Rng(X) \subseteq Y$.

Říkáme, že F je zobrazením třídy X na třídu Y, jestliže $Dom(F) = X, Rng(X) = Y$.

Říkáme, že F je prosté, jestliže F^{-1} je zobrazení.

Lemma 8 (O prostých funkcích, inversech a restrikcích)**.** Pro $F : X \rightarrow Y, G \colon Y \rightarrow Z$ prosté zobrazení, pak

1. GF je prosté z X do Z a $(GF)^{-1} = F^{-1}G^{-1}$
2. je-li navíc $Rng(F) = Y$, pak $F^{-1}F = Id|X, FF^1 = Id|Y$

Důkaz.

1. Plyne z předchozího lemmatu, $(GF)^{-1}$ je funkce z předpokladu
2. F^{-1} prosté Y na X, tedy $F^{-1}(F(x)) = x$ pro libovolné $x \in X$, stejně tak $F(F^{-1}(y)) = y$ pro libovolné $y \in Y$.

⊞

Definice 11 (Třída zobrazení)**.** Nechť A je třída, a je množina. Pak ${}^aA = \{f : f : a \to A\}$.

Lemma 9 (Třídovost/množinovost zobrazení)**.** 1. Pro x, y množiny: ${}^xy$ je také množina.

2. Je-li $x \neq \emptyset$ a Y je vlastní třída, pak ${}^xY$ je vlastní třída.

Důkaz. 1. Každé zobrazení $f : x \to y$ je podmnožinou $x \times y$, a tedy ${}^xy \in \mathcal{P}(x \times y)$.

2. $x \neq \emptyset$, tedy pro každé $y \in Y$ definujeme $k_y : k_y(u) = y$ pro všechny $u \in x$. Kdyby ${}^xY$ byla množina, pak Y je také množina dle schématu axiomu nahrazení, tedy ${}^xY$ je vlastní třída.

$\boxplus$

Definice 12 (Vlastnosti relace)**.** Řekneme, že relace R na třídě A je

1. *reflexivní*, jestliže pro libovolný prvek $x \in A : (x, x) \in R$,
2. *antireflexivní*, jestliže pro žádné $x \in A$ neplatí $(x, x) \in R$,
3. *symetrická*, jestliže pro libovolné $x, y \in A$ platí $(x, y) \in R \to (y, x) \in R$,
4. *slabě antisymetrická*, jestliže pro libovolné $x, y \in A$ platí $((x, y) \in R \wedge (y, x) \in R) \to x = y$,
5. *antisymetrická*, jestliže pro libovolná $x, y \in A$ platí $(x, y) \in R \to (y, x) \notin R$,
6. *trichotomická*, jestliže pro libovolné $x, y \in A$ platí $(x, y) \in R \vee x = y \vee (y, x \in R)$,
7. *tranzitivní*, jestliže pro libovolná $x, y, z \in A$ platí $((x, y) \in R \wedge (y, z) \in R) \to (x, z) \in R$.

Dále řekneme, že vlastnost je dědičná, pokud se zachovává i na podmnožině.

Všechny tyto vlastnosti jsou elementární (vlastnosti prvního řádu). Ne všechny takové jsou dědičné, ale jde ukázat, že ty, jež lze zapsat otevřenými formulemi, jsou dědičné.

Definice 13 (Uspořádání, srovnatelnost, linearita uspořádání)**.** Řekneme, že relace R je uspořádání na třídě A, je-li R reflexivní, slabě antisymetrická a tranzitivní na A.

Prvky $x, y \in A$ jsou srovnatelné vzhledem k R, pokud $(x, y) \in R \vee (y, x) \in R$.

Uspořádání R na A je lineární, je-li navíc R na A trichotomická.

Definice 14 (Prvky uspořádání)**.** Nechť $\leq$ je uspořádání na $A, X \subseteq A$. Říkáme, že $a \in A$ je

1. *majoranta* nebo *horní mez* třídy X, jestliže pro každý prvek $x \in X$ je $x \leq a$,
2. *maximální prvek* třídy X, jestliže $a \in X$ a pro žádně $x \in X$ není $a < x$,
3. *největší prvek* třídy X, jestliže a je majoranta X a $a \in X$,
4. *minoranta* nebo *dolní mez* třídy X, jestliže pro každý prvek $x \in X$ je $x \geq a$,
5. *minimální prvek* třídy X, jestliže $a \in X$ a pro žádné $x \in X$ není $a > x$,
6. *nejmenší prvek* třídy X, jestliže a je minoranta X a $a \in X$,
7. *supremum* třídy X, jestliže a je nejmenší prvek třídy všech majorant třídy X,
8. *infimum* třídy X, jestliže a je největší prvek třídy všech minorant třídy X.

Definice 15 (Omezení, usměrnění, horní, dolní, ideál, filtr, (úplný) svaz)**.** Nechť množina A je uspořádána relací $\leq, X \subseteq A$. Říkáme, že X je:

1. *shora omezená*, jestliže existuje majoranta $a \in A$ množiny X,
2. *zdola omezená*, jestliže existuje minoranta $a \in A$ množiny X,
3. *horní množina* v A, jestliže pro libovolné $x, y \in A : y \leq x \in R \to y \in X$

4. *dolní množina* v A, jestliže pro libovolné $x, y \in A : y \geq x \in R \rightarrow y \in X$
5. *dolů usměrněná*, jestliže pro libovolné $x, y \in X$ existuje $z \in X$ takové, že $z \leq x \wedge z \leq y$
6. *nahoru usměrněná*, jestliže pro libovolné $x, y \in X$ existuje $z \in X$ takové, že $z \geq x \wedge z \geq y$
7. *ideál* v A, jestliže X je nahoru usměrněná dolní množina
8. *filtr* v A, jestliže X je dolů usměrněná horní množina.

Dále řekneme, že A je svaz, jestliže $A \neq \emptyset$ a $\forall x, y \in A$ existuje $\sup_{\leq}\{x, y\}, \inf_{\leq}\{x, y\}$.
Navíc svaz A je úplný, jestliže existují suprema a infima pro každou podmnožinu $a \subset A$.

Definice 16 (Hlavní ideál a filtr)**.** Nechť R je uspořádání na množině A. Pro libovolné $x \in A$ je množina $\{y : y \in A \wedge y \leq_R x\}$ dolní vzhledem k R a je nahoru usměrněná, protože má největší prvek. Označíme ji $(\leftarrow, x]$ a říkáme, že se jedná o hlavní ideál určený prvkem x.
Dále říkáme, že ideál $X \subseteq A$ je hlavní, jestliže pro nějaké $x \in A$ platí $X = (\leftarrow, x]$.
Hlavní filtr daný $x \in A$ je $[x, \rightarrow) = \{y : y \in A \wedge y \geq_R x\}$.
Řekneme, že filtr $X \subset A$ je hlavní, jestliže pro nějaké $x \in A$ platí $X = [x, \rightarrow)$.

Lemma 10 (Uspořádání a ideály)**.** Nechť R je uspořádání na množině A. Pro libovolné $x, y \in A$ platí $x \leq y \leftrightarrow (\leftarrow, x] \subseteq (\leftarrow, y]$.

Poznámka (Dedekindovy řezy)**.** Možnost, jak definovat reálná čísla pomocí racionálních:
$X \subseteq \mathbb{Q}$ je Dedekindův řez, pokud je X dolní množina a navíc, existuje-li $\sup X$, pak $\sup X \in X$.
Např: $\mathbb{Q} \cap (-\infty, 1)$ není Dedekindův řez, ale $\mathbb{Q} \cap (-\infty, 1], \mathbb{Q} \cap (-\infty, \sqrt{2}]$.

Definice 17 (Dobré uspořádání)**.** Řekneme, že uspořádání R na třídě A je dobré, jestliže každá neprázdná podmnožina $a \subseteq A$ má nejmenší prvek vzhledem k R.
Dále říkáme, že A je dobře uspořádané, je-li uspořádána nějakou relací dobrého uspořádání.

Poznámka (Ekvivalence)**.** Relace R na třídě A je ekvivalence, je-li symetrická, reflexivní a tranzitivní.
Třída ekvivalence je $R'a = [a]_R$.
Lemma: pro ekvivalenci $R \subseteq A \times A$ platí právě 1 z $[a]_R = [b]_R, [a]_R \cap [b]_R = \emptyset$ pro libovolná $a, b \in A$.
Rozklad A je P taková, že $\bigcup P = A, \emptyset \notin P \wedge u, v \in P$ jsou disjunktní. Pro ekvivalenci R máme $A/R = \{[a]_R : a \in A\}$ faktorizaci A podle R, $F : A \rightarrow A/R : a \mapsto [a]_R$ je kanonická projekce.
Věta: Buď $R \subseteq A \times A$ ekvivalence na množině A, pak A/R je rozkladem množiny A.

Definice 18 (Subvalence)**.**

1. Řekneme, že množiny x, y mají stejnou mohutnost a píšeme $x \approx y$, jestliže existuje bijekce x a y.
2. Říkáme, že množina x má mohutnost menší nebo rovnou mohutnosti množiny y, pokud existuje prosté zobrazení x do y, psáno $x \preceq y$.
3. Je-li $x \preceq y$ a neexistuje-li bijekce x a y, říkáme, že x má mohutnost menší než y a píšeme $x \prec y$

Lemma 11 (O mohutnosti)**.**

1. $x \approx x$,
2. $x \approx y \rightarrow y \approx x$,
3. $(x \approx y \wedge y \approx z) \rightarrow x \approx z$,
4. $x \preceq x$,
5. $(x \preceq y \wedge y \preceq z) \rightarrow x \preceq z$.

Důkaz.

1. Okamžitě z $f = Id|x$.
2. Pokud f je bijekce, pak i f^{-1} je bijekce.
3. $f : x \rightarrow y, g : y \rightarrow z$ bijekce, pak i $gf = x \rightarrow z$ bijekce.

4. Okamžitě z $f = Id|x$.

5. $f : x \to y, g : y \to z$ prostá, pak i $gf = x \to z$ je prosté.

$\boxplus$

Věta 1 (Cantorova–Bernsteinova)**.** $(x \preceq y \wedge y \preceq x) \to x \approx y$

Důkaz. Buď f prosté zobrazení x do y a g prosté zobrazení y do x. Pak máme takto dvě zobrazení $\mathcal{P}(x)$ do $\mathcal{P}(y)$ a naopak, která jsou monotónní vzhledem k inkluzi. Zadefinujeme $H : \mathcal{P}(x) \to \mathcal{P}(x)$ takové, že $H(u) = x \setminus (g(y \setminus f(u)))$ pro všechna $u \in \mathcal{P}(x)$-

H je také monotónní vzhledem k inkluzi: mějme $u \subseteq v \subseteq x$. Pak $H(u) = x \setminus g(y \setminus f(u)), H(v) = x \setminus g(y \setminus f(v))$. $y \setminus f(u) \supseteq y \setminus f(v)$, a tedy $x \setminus g(y \setminus f(u)) \subseteq x \setminus g(y \setminus f(v))$.

Z lemmatu o pevném bodě toto zobrazení má pevný bod, tedy existuje $x \subseteq x : H(c) = c$. Pak $c = H(c) = x \setminus g(y \setminus f(c))$, tedy $x \setminus c = g(y \setminus f(c))$. Neboť g je prosté y do x a $x \setminus x$ je obrazem $y \setminus f(c)$. Tedy $g^{-1}|x \setminus c$ je prosté zobrazení $x \setminus c$ na $y \setminus f(c)$. Pak definujeme $h(a) = f(a)$ pro $a \in c$ a $g^{-1}(a)$ pro $a \in x \setminus c$, což je naše hledaná bijekce. $\boxplus$

Lemma 12 (O pevném bodě)**.** Je-li H zobrazení $\mathcal{P}(x)$ do $\mathcal{P}(x)$, které je monotónní vzhledem k inkluzi, pak existuje množina $x \subseteq x$ taková, že $H(c) = c$.

Důkaz. Uvažme $C = \{u \subseteq x : u \subseteq H(u)\}$, položme $c = \bigcup C$. Jistě $c \subseteq c$ a pro každé $u \in C$ platí $u \subseteq c$. Z monotonie H máme $u \subseteq H(u) \subseteq H(c)$ pro každé $u \in C$. Tedy $x = \bigcup C \subseteq H(c)$. Opět z monotonie H máme $H(c) \subseteq H(H(c))$, tedy $H(c) \in C$, a z definice $H(c) \subseteq c$. Tedy $H(c) = c$ a c je hledaným pevným bodem. $\boxplus$

Lemma 13 (O mohutnosti kartézského součinu a potence)**.** 1. $x \times y \approx y \times x, x \times (y \times z) = (x \times y) \times z$

2. $(x \approx x_1 \wedge y \approx y_1) \to (x \times y) \approx (x_1 \times y_1)$

3. $x \approx y \to \mathcal{P}(x) \approx \mathcal{P}(y)$

4. $\mathcal{P}(x) \approx^x 2$, kde $2 = \{\emptyset, \{\emptyset\}\}$

Důkaz. 1: $f((x, y)) = (y, x), f((x, (y, z))) = ((x, y), z)$
2: $f : x \to x_1, g : y \to y_1 : h((x, y)) = (f(x), g(y))$
3: plyne z předchozích lemmat
4: $y \in \mathcal{P}(x) : i_y(z) = 1$ pro $z \in y$ a 0 jinak. $\boxplus$

Definice 19 (Tarského definice konečnosti)**.** Množina x je konečná, psáno $\mathrm{Fin}(x)$, pokud každá neprázdná podmnožina $y \subseteq \mathcal{P}(x)$ má maximální prvek vzhledem k inkluzi.

Definice 20 (Dedekindova definice konečnosti)**.** Množina x je dedekindovsky konečná, pokud má větší mohutnost než každá její vlastní podmnožina.

Lemma 14 (Konečnost implikuje dedekindovskou konečnost)**.** Je-li a konečná množina, pak a má větší mohutnost než libovolná vlastní podmnožina $b \subset a$.

Důkaz. Zjevně $b \preceq a$. Sporem, nechť $b \subset a \wedge a \approx b$. Pak nechť $y \subseteq \mathcal{P}(a)$ je množina, sestávající se ze všech takových b. Víme $y \neq \emptyset$, z konečnosti má minimální prvek vzhledem k inkluzi.

Ať $c \in y$ je minimální prvek y. Z definice y máme $c \subset a \wedge c \approx a$. Je-li f prosté zobrazení a na c a $d = f[c]$, potom a, c, d mají stejnou mohutnost a navíc $d \subset c$, protože f je prsoté a d neobsahuje obrazy z $a \setminus c \neq \emptyset$. To je spor s předpokladem, že c je minimální v inkluzi. $\boxplus$

Definice 21 (Počátkové vnoření)**.** Nechť A je množina uspořádaná relací R a B je množina uspořádaná relací S.

Řekneme, že zobrazení F je počátkové vnoření A do B, jestliže $A_1 = Dom(F)$ je dolní podmnožina množiny A a B_1 je dolní podmnožina b V a F je izomorfismus A_1, B_1 vzhledem k R, S.

Lemma 15 (O počátkových vnořeních)**.** Nechť F, G jsou počátková vnoření dobře uspořádané množiny A do dobře uspořádané množiny B. Pak $F \subseteq G \vee G \subseteq F$.

Důkaz. Nechť R je dobré uspořádání A a S je dobré uspořádání B. Z linearity Rplyne, že libovolné dvě dolní podmnožiny A jsou srovnatelné vzhledem k inlkuzi, a tedy $Dom(F) \subseteq Dom(G)$ nebo $Dom(G) \subseteq Dom(F)$. Bez újmy na obecnosti, nechť platí první inlkuze. Sporem ukážeme, že pro každé $x \in Dom(F) : F(x) = G(x)$.

Nechť x je vzhledem k R nejmenší prvek takový, že $F(x) \neq G(x)$. Tedy pro každé $y : y <_R x$ platí $F(y) = G(y)$ Z linearity S plyne, že $F(x), G(x)$ jsou srovnatelné. Nechť například $F(x) <_S G(x)$, označme $b = F(x)$. Protože G respektuje uspořádání, $\forall z \in Dom(G) : z \geq_R x$, a tedy $G(z) >_S b$. Tedy $b \notin Rng(G)$ a $Rng(G)$ není dolní množibna v B, což je náš hledaný spor. ⊞

Věta 2 (O izomorfismech dobrých uspořádání)**.** Nechť množiny A, B jsou dobře uspořadány relací R, S. Pak existuje právě jedno zobrazení Ftakové, že F je izomorfismus A a nějaké dolní množiny b V nebo F je izomorfismus B a nějaké dolní množiny v A.

Důkaz. Nechť P je množina všech poátkových vnoření A do B a buď $F = \bigcup P$. Jistě F je zobrazení: je-li $(x, y_1) \in F, (x, y_2) \in F$, pak existují počátková vnoření F_1, F_2 tak, že $(x, y_1) \in F_1, (x, y_2) \in F_2$. Z předchozího lemmatu máme $F_1 \subseteq F_2 \vee F_2 \subseteq F_1$, tedy $y_1 = y_2$.

Dále F je také počátkové vnoření: $x_1 <_R x_2 \in Dom(F)$, pak eixstuje $F' \in P$ tak, že $x_1, x_2 \in Dom(F')$, a protože F je počátkové vnoření, máme $F(x_1) = F'(x_1) <_S F'(x_2) = F(x_2)$. Navíc $Dom(F)$ je sjednocení dalních množin $Dom(F'), F' \in P$ a je dle předchozího lemmatu dolní množinou v A. Podobě $Rng(F)$ je dolní v B.

Ukážeme, že $Dom(F) = A$ nebo $Rng(F) = B$. První příad: F je hledaný izomorfismus A a nějaké dolní podmnožiny množiny B, jinak to je F^{-1}. Pokud $A \setminus Dom(F)$ i $B \setminus Rng(F)$ byly neprázdné, pak vezememe jejich nejmenší prvky a, b. Rozšíříme-li F na F' tak, že $F'(a) = b$, je F' také počátkové vnoření, a tedy $F' \in P$, což je spor s definicí P. ⊞

Věta 3 (O uspořádáních)**.**
1. Je-li a konečná uspořádaná množina, pak každá neprázdná podmnožina $b \subset a$ má alespoň jeden maximální prvek a alespoň jeden minimální prvek.
2. Každé lineární uspořádání na konečné množině je dobré a libovolná dvě lineární uspořádání na téže konečné množině jsou izomorfní.

Důkaz.
1. Buď a uspořádána relací $<$, $b \subset a$, $b \neq \emptyset$. Ukážeme existenci meximálního prvku b. $\forall x \in a$: splu s relací $\leq$ určuje $(\leftarrow, x] = \{y : y \in a \wedge y \leq x\}$. Nechť u je množina, jejíž prvky jsou všechny dolní množiny $(\leftarrow, x]$ pro $x \in b$. Pak $u \neq \emptyset, u \subseteq \mathcal{P}(a)$. Jelikož a je konečná, existuje prvek $m \in b$ tak, že $(\leftarrow, b]$ je maximální prvek u vzhledem k inkluzi. Z předchozího lemmatu je m maximálnáí prkvek b vzhledem k $<$.

   Analogicky pro horní množiny a minimální prvek.
2. V lineárně uspořádané množině je minimální prvek nejmenší. Jsou-li r, s dvě lineární uspořádání na konečné a, jsou dobrá. Z předchozí věty máme (a, r) izomorfní s $b \subset a : (b, s)$ nebo opačně. V obou případech mají a, b stejnou mohutnost, tedy $a = b$ z předchozího lemmatu o dedekindovské konečnosti.

⊞

Lemma 16 (O konečnosti)**.**
1. $(Fin(x) \wedge y \subseteq x) \to Fin(y)$
2. $(Fin(x) \wedge x \approx y) \to Fin(y)$
3. $(Fin(x) \wedge y \preceq x) \to Fin(y)$

Důkaz.
1. x konečná, $y \subseteq x \Rightarrow \mathcal{P}(y) \subseteq \mathcal{P}(x)$ a máme vše z definice.
2. je-li $f : x \to y$ bijekce, podle předch. tvrzení jsou $\mathcal{P}(x)$ a $\mathcal{P}(y)$ izomorfní k $\subseteq$, tedy y je také konečná.
3. Plyne z předchozích dvou.

⊞

Lemma 17 (O konečnosti sjednocení a přidání prvku)**.**
1. $(Fin(x) \wedge Fin(y)) \to Fin(x \cup y)$
2. $Fin(x) \to \forall Fin(x \cup \{y\})$

Důkaz. 1. Nechť $w \neq \emptyset, w \subseteq \mathcal{P}(x \times y)$. Nalezneme maximální prvek $v \in w$. Položíme $w_1 = \{w : (\exists t \in w)(u = t \cap x)\}$, což je neprázdná podmnožina $\mathcal{P}(x)$. Nechť v_1 je maximální prvek w_1 vzhledem k $\leq$. Dále položme $w_2 = \{u : (\exists t \in w)(t \cap x = v_1 \wedge t \cap y = u)\}$, pak w_2 je neprázdná podmnožina $\mathcal{P}(y)$. Pro $v_2 \in w_2$ maximální k $\subseteq$ je $v = v_1 \cup v_2$ hledaný maximální prvek množiny w.

2. Plyne z 1, neboť $Fin(\{y\})$ platí pro libovolné y.

$\boxplus$

Definice 22 (Třída všech konečných množin)**.** $Fin = \{x : Fin(x)\}$

Věta 4 (Princip indukce pro konečné množiny)**.** Je-li X třída splňující:

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

pak $Fin \subseteq X$.

Důkaz. Sporem: nechť X splňuje 1,2 a $Fin \not\subseteq X$, tedy $Fin \setminus X \neq \emptyset$ a mějme $v \in Fin \setminus X$. Definujeme $s = \{v : v \subseteq c \wedge v \in X\}$. Podle 1: $\emptyset \in w$, tedy $w \neq \emptyset, w \subseteq \mathcal{P}(X)$. Nechť v_0 je maximální prvek w vzhledem k inkluzi. Pak $v_0 \subset x$, ale $v_0 \neq x$, protože $v_0 \subseteq X$. Pak existuje $y \in x \setminus v_0$. Položíme $v_1 = v_0 \cup \{y\}$, pak $v_1 \in w$, v_0 není maximální vzhledem k inkluzi, což je spor.

$\boxplus$

Lemma 18 (Je-li x konečná, pak i potence je konečná)**.** $Fin(x) \to Fin(\mathcal{P}(x))$

Důkaz. Indukce na třídu $X = \{x : Fin(\mathcal{P}(x))\}$. Zjevně $\mathcal{P}(\emptyset) = \{\emptyset\}$, což splňuje 1. Dále pro 2: mšjme $x \in X, y$ libovolná. chceme $x \cup \{y\} \in X$. Pokud $y \in x$, je to triviální. Mějme $y \notin x$. Pak $\mathcal{P}(x \cup \{y\}) = \mathcal{P}(x) \sqcup z$, kde $z = \mathcal{P}(x \cup \{y\}) \setminus \mathcal{P}(x)$. Tedy z se sestává z podmnožin $v \subseteq x \cup \{y\}$ takových, že $y \in v$. Snadno $\mathcal{P}(x) \approx z$ funkcí $f(u) = \{y\} \cup u$ je bijekce. Pak $Fin(z)$, a tedy $Fin(\mathcal{P}(x \cup \{y\}))$. $\boxplus$

Důsledek 1 (Konečnost kartézského součinu)**.** $(Fin(x) \wedge Fin(y)) \to Fin(x \times y)$

Důkaz. Položme $z = x \cup y$, ta je konečná. Dále $z \times z \subseteq \mathcal{P}(\mathcal{P}(z))$, ta je konečná a konečnost se zachovává při podmnožině. $\boxplus$

Lemma 19 (Konečné sjednocení konečných množin je konečné)**.** Je-li a konečná množina a každý její prvek je také konečná množina, pak $\bigcup a$ je konečná množina.

Důkaz. Použijeme princip indukce pro $X = \{x : x \subseteq Fin \to Fin(\bigcup x)\}$. Zjevně $\emptyset \in X$. Pro $x \in X$, y libovolnou: chceme $x \cup \{y\} \in X$ Je-li $x \bigcup \{y\} \subseteq Fin$, pak $x \subseteq Fin$ a y je konená. Proože $x \in X$, je $\bigcup x$ konečná. Dále $\bigcup(x \cup \{y\}) = (\bigcup x) \cup y$, což je konečná množina z předchozích lemmat. $\boxplus$

Lemma 20 (Konečné množiny jsou vždy porovnatelné)**.** $Fin(x) \to (\forall y)(x \preceq y \vee y \preceq x)$.

Důkaz. Indukcí pro konečné množiny pro $X = \{x : (\forall y)(x \preceq y \vee y \preceq x)\}$. Zjevně $\emptyset \in X$. Dále nechť $x \in X$, u libovolná množina, $z := x \cup \{u\}$. Chceme $c \in X$. Mějme $u \notin x$, jinak to je triviální. Mjěme y libovolnou. Z předpokladu máme $x \preceq y \vee y \preceq x$. Pokud $y \preceq x$, pak i $y \preceq z$ týmž zobrazením.

Zbývá $x \prec y$. Je-li g prosté: $g : x \to y$, existuje $v \in y \setminus Rng(g)$, protože $x \not\approx y$. Tedy $h = g \cup \{(u, v)\}$ máme prosté zobrazení z do y, a tedy $z \preceq y$, tedy $z \in X$ a $Fin \subseteq X$ z principu indukce. $\boxplus$

Definice 23 (Přirozená čísla)**.** $0 = \emptyset, n + 1 = n \cup \{n\}$

Definice 24 (Induktivní množina)**.** Řekneme, že w je induktivní množina, jestliže platí $\emptyset \in w \wedge (\forall v \in w)(v \cup \{v\} \in w)$

Axiom 9 (Axiom nekonečna)**.** $(\exists z)(\emptyset \in z \wedge (\forall x)(x \in z \to x \cup \{x\} \in z))$

Definice 25 (Množina přirozených čísel)**.** Množinu všech přirozených čísel značíme ω a definujeme ji $\omega = \bigcap\{w : w \text{ je induktivní}\}$.

Lemma 21 (Množina přirozených čísel je nejmenší induktivní). ω je nejmenší induktivní množina.

Důkaz. Zjevně induktivní. Kdyby byla nějaká ostře menší množina m, pak z definice $\omega \subseteq m$, což je spor. ⊞

Poznámka (Funkce následníka). Na ω definujeme zobrazení $s : s(n) = n \cup \{n\}$, nazýváme jej funkce následníka.

Věta 5 (Princip indukce pro přirozená čísla). Je-li X množina přirozených čísel, pro niž platí

1. $\emptyset \in X$
2. $x \in X \to s(x) \in X$,

potom $X = \omega$.

Důkaz. Splňuje-li nějaká množina X obě podmínky, je pak X induktivní a $\omega \subseteq X$ plyne z předchozího lemmatu. ⊞

Lemma 22 (O inkluzi a podmnožinovosti na přirozených číslech). Pro libovolná dvě přirozená čísla m, n platí:

1. $n \in \omega \to n \subseteq \omega$ (prvky přirozených čísel jsou opět přirozená čísla)
2. $m \in n \to m \subseteq n$ ($\in$ je na ω tranzitivní)
3. $n \notin n$. ($\in$ je na ω antireflexivní)

Důkaz. 1. Pro 0 zjevně, máme $n \subseteq \omega$. Pak i $n \cup \{n\} \subseteq \omega$.

2. Indukcí podle n, nechť $C = \{n : n \in \omega \wedge (\forall m)(m \in n \to m \subseteq n)\}$. Jistě $0 \in X$. Mějme $n \in X$, ukážeme $s(n) \in X$. mějme m libovolný prvek z $s(n)$, tedy $m \in n \vee m = n$. V obou případech $m \subseteq n$, dále $n \subseteq s(n) \to s(n) \in X$.

3. $\emptyset \notin \emptyset$, mějme dálně n přirozené číslo, $n \notin n$. Kdyby $s(n) \in s(n)$, pak $s(n) \in n \vee s(n) = n$. V obou případech máme $s(n) = n \cup \{n\} \subset n$, z čehož máme $n \in n$.

⊞

Věta 6 (Konečnost a přirozená čísla). 1. Každé přirozené číslo je konečná množina

2. Množina x je konečná, právě když má stejnou mohutnost jako nějaké přirozené číslo
3. Množina ω a každá induktivní množina je nekonečná

Důkaz. 1. indukcí: $Fin(0)$ jistě, mějme $Fin(n)$, pak máme $Fin(s(n)) = Fin(n \cup \{n\})$, což jistě platí.

2. $x \approx n$ pro $n \in \omega$ - $Fin(x)$, neboť $Fin(n)$ z 1 a díky $x \approx b$ máme $Fin(x)$. Druhou implikaci ukážeme indukcí pro $X = \{x : (\exists n \in \omega : x \approx n)\}$ Jistě $\emptyset \in X$. Mějme $x \in X$, y libovolnou, $y \notin x$ (jinak triviální). Pak $x \cup \{y\} \approx n \cup \{n\}$.

3. Z předchozího lemmatu máme $\omega \subset \mathcal{P}(\omega)$, ale žádný $n \in \omega$ není maximální, jelikož $n \subset s(n)$. Dále ω je podmnožinou každé induktivní podmnožiny, a tedy musí být nekonečná.

⊞

Lemma 23 (O relaci $\in$ na ω). Pro libovolná přirozená čísla m, n platí

1. $m \in n \leftrightarrow m \subset n$
2. $m \in n \vee m = n \vee m \ni n$

Důkaz. 1. „$\to$“: plyne z předchozího lemmatu a $m \notin m$.

„$\leftarrow$“: indukcí podle n. Mějme 1 pro nějaké n a každé m (zjevně pro $n = 0$) Nechť $m \subseteq s(n)$, pak $m \subset n$. Kdyby $n \in m$, pak z předchozího lemmatu $n \subseteq m$, tedy i $s(n) \subseteq m$, což je spor s $m \subset s(n)$. Tedy $n \notin m \wedge m \subseteq n$. Je-li $m \subset n$, pak $m \in n$ máme z IP, a tedy i $m \in s(n)$. Je-li $m = n$, pak $m \in s(n)$ z definice.

2. Pro každé přirozené číslo n nechť $A(n)$ oznauje množinu všech přirozených čísel m, pro něž platí $m \in n \vee m = n \vee m \ni n$. Ukážeme, že každé $A(n)$ je induktivní. Pro $A(O) : 0 \in A(O) : 0 = 0$, pro $m \in A(0)$ nutně $0 \in m \vee 0 = m$. V obou případech $0 \in s(n)$, tedy $A(0)$ je induktivní.

   Dále zjevně $0 \in A(n)$ pro každé $n \in \omega$. Mějme $n \in \omega, m \in A(n)$. Ukážeme, že $s(m) \in A(n)$. Z IP $m \in n \vee m = n \vee m \ni n$. Pro $m \in n$ nutně $s(m) \subset n$,m tedy $s(m) \in n \vee s(m) = n$. Pro $m = n \vee m \ni n$ pak $s(m) \ni n$, tím jsme ukázali induktivnost.

$\boxplus$

Věta 7 (ω je dobře uspořádaná)**.** Množina všech přirozených čísel je dobře uspořádaná relací $\in$.

Důkaz. Už víme, že $\in$ je antireflexivní a tranzitivní na ω: pro $l, m, n \in \omega : l \in m, m \in n$ máme $l \subset m \subset n$, a tedy $l \subset n$, načež $l \in n$. Dále $\in$ je na ω trichotomická, tedy $\in$ je lineární uspořádání na ω.

Ukážeme, že je i dobré: ať $\neq \emptyset$ je množina přirozených čísel a zvolme libovolně $n \in a$. Pokud n není nejmenší prvek a, pak $b = a \cap n$ je konečná podmnožina množiny a. Navíc je neprázdná z toho, že n není nejmenší. Tedy existuje nejmenší prvek množiny b, který je také nejmenší prvek množiny a. $\boxplus$

Věta 8 (Charakterizace dobrých uspořádání izomorfních přirozeným číslům s relací náležení)**.** Je-li A nekonečná množina lineárně uspořádaná relací $<$ tak, že pro každé $a \in A$ je dolní množina $(\leftarrow, a]$ konečná, potom je $<$ dobré uspořádání množiny A a množina A je izomorfní s ω vzhledem k $<$ a $\in$.

Důkaz. Prvně $<$ je dobré: buď $a \subseteq A : a \neq \emptyset$. Zvolme $n \in a$. Pokud n není nejmenší prvek a, pak $b = a \cap (\leftarrow, n]$ je neprázdná podmnožina a. Z předpokladu je konečná, a tedy existuje nejmenší prvek m množiny b, který je také nejmenší prvek množiny a. Nyní A, ω jsou obě nekonečné a dobře uspořádané relacemi $<$, resp $\in$. Z věty o dobrých uspořádáních je buď A izomorfní s nějakou dolní množinou $B \subset \omega$, nebo ω je izomorfní s nějakou dolní podmnožinou $C \subset A$. První příad: B není shora omezená žádným n neboť pak by A byla konečná. Tedy $\forall n \in \omega$ platí, že nějaký prvek B je větší než n, a navíc $n \in B$, neboť B je dolní množina, tedy $B = \omega$.

Druhý případ: analogicky ukážeme $C = A$. $\boxplus$

Definice 26 (Spočetná, nejvýš spočetná, nespočetná množina)**.** Množina x je spočetná, pokud má stejnou mohutnost jako ω.

Množina x je nejvýše spočetná, je-li konečná nebo spočetná. V opačném případě je nespočetná.

Věta 9 (O podmnožinách ω)**.**

1. Každá shora omezená podmnožina $A \subseteq \omega$ je konená a každá shora neomezená podmnožina ω je spočetná.
2. Každá podmnožina spočetné podmnožiny je nejvýše spočetná.

Důkaz.

1. Je-li A shora omezená n. pak $A \subseteq s(n)$ a A je konečná. Nechť A je neomezená. Pak nemůže být konečná, neboť by pak měla největší prvek, tedy je nekonečná dobře uspořádaná a pod každým $a \in A$ je jen konečně mnoho prvků. Z předchozí věty je tedy A spočetné.
2. Buď A spočetná množina a f prosté zobrazení A na ω. Z 1 je $B \subseteq A$ spočetná nebo konečná podle toho, zda $f[B]$ je shora omezená nebo neomezená podmnožina množiny ω.

$\boxplus$

Definice 27 (Lexikografické a maximo-lexikografické uspořádání)**.** Na $\omega \times \omega : (a, b) <_L (c, d) \leftrightarrow (a \in c \vee (a = c \wedge b \in d))$ nazveme lexikografickým uspořádáním.

Dále uspořádání $(a, b) \lhd (c, d) \leftrightarrow (\max(a, b) \in \max(c, d) \vee (\max(a, b) = \max(c, d) \wedge ((a, b) <_L (c, d)))$ nazveme maximo-lexikografickým uspořádáním.

Věta 10 (Spočetnost se přenáší na sjednocení a kartézský součin)**.** Jsou-li A, B spočetné množiny, pak $A \cup B$ i $A \times B$ jsou spočetné množiny.

Důkaz. Nechť f je prosté zobrazení A na ω, g je prosté zobrazení B na ω. Pooožíme-li $h(x) = (f(x), 0)$ pro $x \in A$, $(g(x), 1)$ pro $x \in B \setminus \{a\}$, máme prosté zobrazení $h : A \cup B \to \omega \times 2$, $\omega \times 2$ je spočetná, tedy $A \cup B$ je spočetná.

Dále pro $a \in A, b \in B : k((a, b)) = (f(a), g(b))$ je prosté zobrazení do $\omega \times \omega$, která je také spočetná. $\boxplus$

Důsledek 2 (Konečné sjednocení/kartézský součin spočetných množin je spočetný)**.** Je-li I neprázdná konečná množina a je-li A_i pro každé $i \in I$ spočetná, pak $\bigcup_{i \in I} A_i, \bigtimes_{i \in I} A_i$ jsou spočetné množiny.

Věta 11 (Spočetnost $\mathbb{Z}, \mathbb{Q}$.)**.** $\mathbb{Z}$ i $\mathbb{Q}$ jsou spočetné.

Důkaz. $\mathbb{Z}^-$ se zobrazí na $\mathbb{N}$ absolutní hodnotou, tedy $\omega \cup \mathbb{Z}^- = \mathbb{Z}$ je spočetná.
Pak $f[\mathbb{Q}] \subseteq \mathbb{Z} \times \mathbb{N}$ pro $f(p/q) = (p, q)$, tedy i $\mathbb{Q}$ je spočetná. ⊞

Věta 12 (Cantorova)**.** $x \prec \mathcal{P}(x)$

Důkaz. Jistě $f : x \to \mathcal{P}(x) : x \mapsto \{x\}$ je prosté, tedy $x \preceq \mathcal{P}(x)$.
Ukážeme, že neplatí $x \approx \mathcal{P}(x)$. Nechť $f : x \to \mathcal{P}(x)$ je pro spor bijekce. Pak definujeme $y \subseteq x : y = \{t : t \in x \wedge t \notin f(t)\}$. Ukážeme, že y nemá vzor. Kdyby $f(v) = y$ pro nějaké $v \in x$, pak buď $v \in y$, nebo $v \notin y$, ovšem oba případy končí sporem.
Tedy f nezobrazuje x na $\mathcal{P}(x)$ a věta je dokázána. ⊞

Důsledek 3 (Nespočetnost $\mathcal{P}(\omega)$)**.** $\mathcal{P}(\omega)$ je nespočetná.

Věta 13 (O nespočetných množinách)**.** Nechť $\mathbb{R}$ je množina všech reálných čísel a $I = [0, 1]$. Pak $\mathcal{P}(\omega) \approx I \approx \mathbb{R}$.

Důkaz. Víme, že $\mathcal{P}(\omega)$ je ekvivalentní s ${}^{\omega}2$ všech nekonečných posloupností nul a jedniček. Přitom každé $i \in I$ lze zapsat ve dvojkové soustavě jako $0.a_0a_1\ldots$, kde $a_i \subset \{0, 1\}$. Tím máme prosté zobrazení $I \to^2 \omega$. Pro $s = \sum_{n=0}^{\infty} 2a_n \frac{1}{3^{n+1}}$ je přiřazení ${}^{\omega}2$ na I.
Pro $\mathbb{R} : I \subset \mathbb{R}$, tedy $I \preceq \mathbb{R}$. $\mathbb{R} \preceq I$ z $f(x) = arctg(x) + \pi/2$ a z Canotorovy–Bernsteinovy věty máme rovnost mohutností. ⊞

Poznámka (Hypotéza kontinua)**.** Neexistuje množina $x : \omega \prec x \prec \mathcal{P}(\omega)$.
CH je nezávislá na ZFC.

Axiom 10 (Princip výběru)**.** Pro každý rozklad r množiny X existuje výběrová množina $v \subseteq X$ splňující: $(\forall u \in r)(\exists x)(V \cup u = \{x\})$.

Definice 28 (Selektor na množině)**.** Funnkce f definovaná na množině X, pro niž platí $(y \in X \wedge y \neq 0) \to f(y) \in y$ se nazývá selektor na množině X.

Axiom 11 (Axiom výběru)**.** Na každé množině existuje selektor.

Definice 29 (Indexovaný soubor množin, jeho sjednocení, průnik a kartézský součin)**.**

1. Indexovaný soubor $\langle F_j : j \in J\rangle$ je $F : J \to$ někam.
2. Říkáme, že $\langle F_j : j \in J\rangle$ je soubor množin, J je indexová třída a prvky jsou indexy.
3. Sjednocení souboru $\langle F_j : j \in J\rangle$ definujeme $\bigcup_{j \in j} F_j = \{x : (\exists j \in J)(x \in F_j)\}$
4. Průnik souboru $\langle F_j : j \in J\rangle$ definujeme $\bigcap_{j \in j} F_j = \{x : (\forall j \in J)(x \in F_j)\}$
5. Kartézský součin souboru $\langle F_j : j \in J\rangle$ definujeme $\bigtimes_{j \in J} F_j = \{f : f : J \to \bigcup F_j \wedge (\forall j \in J)(f(j) \in F_j)\}$.

Lemma 24 (Množinovost kartézského součinu souboru)**.** Je-li J množina, pak $\bigtimes_{j \in J} F_j$ je také množine. Jestliže pro každé $j \in J$ platí $F_j = Y$, pak $\bigtimes_{j \in J} F_j =^J Y$.

Důkaz. J je množina, tedy $\bigcup_{j \in J}$ je také množina a $\bigtimes_{j \in J} F_j \subseteq^J F$. ⊞

Lemma 25 (Ekvivalence AC, PC a dalších)**.** Následující jsou ekvivalentní:

1. axiom výběru
2. princip výběru
3. pro každou množinovou relaci s existuje funkce f takocvá, že $f \subseteq \wedge Dom(f) = Dom(s)$,

4. kartézský součin neprázdného souboru neprázdných množin je neprázdný

Důkaz. $1 \to 2$: Buď r rozklad nějaké množiny a f selektor na r. Pak $v = Rng(f)$ je výběrová množina pro r.

$2 \to 3$: $s \neq \emptyset$: tedy $r = \{\{(i,x) : (i,x \in s)\} : i \in Dom(s)\}$, pak r je rozklad množiny s a výběrová množina je hledaná funkce.

$3 \to 4$: Neprázdný soubor neprázdných množin $\langle a_i : i \in x\rangle$ určuje relaci $s = \{(i,y) : i \in c \wedge y \in a_i\}$. Z 3 existuje funkce $f \subseteq s$ splňující $Dom(f) = Dom(s) = x$, atedy $f \in \bigtimes\langle a_i, i \in x\rangle$.

$4 \to 1$: Je-li x nějaká množina, musíme ukázat existenci selektoru f na x. BÚNO $x \neq \emptyset, \emptyset \notin x$. Pak $Id|x$ určuje neprázdný soubor neprázdných množin $\langle y : y \in x\rangle$. Dle 4 je $\bigtimes\langle y : y \in c\rangle$ neprázdný a každý prvek je selektorem na x. ⊞

Lemma 26 (Spočetné sjednocení nejvýše spočetných množin je nejvýše spočetné (AC))**.** Spočetné sjednocení spočetných množin je nejvýše spočetná množina (za předpokladu AC).

Důkaz. Nechť $\langle B_j : j \in I\rangle$ je uvažovaný soubor, bez újmy na obecnosti nechť $I = \omega$. Víme, že $\omega \times \omega$ je spočetná, stačí ukázat $\bigcup\langle B_j : j \in I\rangle \preceq \omega \times \omega$. Nechť je pro každé j E_j množina všech prostých zobrazení B_j do ω. Soubor $\langle E_j : j \in \omega\rangle$ sestává z neprázdných množin, neboť B_j jsou nejvýše spočetné. Z předchozího lemmatu existuje výběrová posloupnost $\langle f_j : j \in \omega\rangle$, kde $f_j = E_j$. Definujeme $h : S \to \omega \times \omega$ předpisem $h(x) = (j, f_j(x))$ kde j je nejmenší index z ω takový, že $x \in B_j$. Zjevně h je prosté. ⊞

Definice 30 (Řetězec)**.** Nechť A je množina uspořádaná relací $\leq$. Podmnožinu $B \subseteq A$ nazveme řetězcem, pokud je lineárně uspořádaná relací $\leq$.

Axiom 12 (Princip maximality (PM), Zornovo lemma)**.** Nechť A je množina uspořádaná relací $\leq$ tak, že každý řetězec je shora omezený. Pak ke každému $a \in A$ existuje maximální prvek $b \in A$ takový, že $a \leq b$.

Axiom 13 (Princip trichotomie (PT))**.** Pro libovolné množiny A, B je buď $A \preceq B$ nebo $B \preceq A$.

Lemma 27 (PM implikuje PT)**.** PM implikuje PT

Důkaz. Množina $D = \{f : f \text{ je prosté}, Dom(f) \subseteq A, Rng(f) \subseteq B\}$ uspořádaná inkluzí splňuje ředpoklady PM. Nechť f ne nějaký maximální prvek v D. Kdyby $A \setminus Dom(g), B \setminus Rng(g)$ byly neprázdné, mohli bycho g rozšířit, což by byl spor s minimalitou. Tedy $Dom(g) = A$, nebo $Rng(g) = B$. V prvním případě $A \preceq B$ z g, jinak $B \preceq A$ z g^{-1}. ⊞

Axiom 14 (Princip maximality přes suprema (PMS))**.** Nechť $(A, \leq)$ je uspořádaná množina taková, že pro každý řetězec existuje supremum. Pak ke každému $a \in A$ existuje maximální prvek b množiny A takový, že $a \leq b$.

Axiom 15 (Princip dobrého uspořádání (WO))**.** Pro každou množinu A existuje relace R, která je dobrým uspořádáním na A.

Věta 14 (WO implikuje AC)**.** WO implikuje AC.

Důkaz. Nechť $A \neq \emptyset, \emptyset \notin A$. Zadefinujeme $X := \bigcup A$. Z WO máme $\leq$ dobré uspořádání na X. Umíme tdy pro každou $a \in A$ najít minimální prvek, který je jednoznačný. Tedy $f = \{(a,x) : a \in A, x \in a \wedge \{x\} = \{y \in a : y \leq x\}\}$, což je selektor na a. ⊞

Definice 31 (Tranzitivní třída/množina)**.** Řekneme, že X je tranzitivní, jestliže platí $x \in X \to x \subseteq X$.

Pozorování (O tranzitivitě)**.** X je tranzitivní, právě když pro libovolná x, y platí $y \in x \in X \to y \in X$.

Lemma 28 (O tranzitivitě)**.**

1. Pro X, Y tranzitivní třídy jsou i $X \cap Y, X \cup Y$ tranzitivní.
2. Je-li každý prvek třídy X tranzitivní množina, pak $\bigcap X, \bigcup X$ jsou tranzitivní.
3. Je-li X tranzitivní třída, pak $\in$ je na X tranzitivní, právě když každé $x \in X$ je tranzitivní množina.

Důkaz.

1. Plyne z definice.

2. $\bigcap X$ je tranzitivní, tedy mějme $y, z : y \in z \in \bigcap X$, tedy $\forall x \in X : z \in x \wedge y \in x \rightarrow y \in \bigcap X$ a máme tranzitivitu, $\bigcup X$ analogicky.

3. x, y, z libovolné množiny takové, že $z \in y \in x \in X$, pak z tranzitivity X máme $y, z \in X$. Je-li $\forall x \in X$ trazitivní, pak $z \in x$, a tedy $\in$ je tranzitivní na X. Je-li $\in$ tranzitivní na X, pak je každý prvek množiny X tranzitivní.

$\boxplus$

Definice 32 (Ordinální čísla)**.** Řekneme, že množina x je ordinální číslo, jestliže je tranzitivní a $\in$ je dobré (ostré) uspořádání množiny x. Třídu všech ordinálních čísel značíme On.

Lemma 29 (On je tranzitivní třída)**.** On je tranzitivní třída.

Důkaz. Ukážeme, že každý prvek y ordinálu x je ordinál. Relace náležení je tranzitivní na ordinálu, z třetí části předchozího lemmatu máme $y \in x$ také tranzitivní. Z tranzitivity x plyne $y \subseteq x$, a tedy y je dobře uspořádaná $\in$. $\boxplus$

Lemma 30 (O ordinálech)**.** Pro ordinály x, y platí:

1. $x \notin x$

2. $x \cap y$ je ordinál

3. $x \in y \leftrightarrow x \subseteq y$.

Důkaz.

1. sporem: $x \in x$, pak $\in$ není antireflexivní, tedy $\in$ není ostré uspořádání na x.

2. $x \cap y$ je tranzitivní z průniku tranzitivních množin, dobrost $\in$ máme z $x \cap y \subseteq x$.

3. $x \in y \rightarrow x \subseteq y$, víme $x \neq y$. Naopak, pro $x \subset y : y \setminus x \neq \emptyset$. Buď z nejmenší prvek $y \setminus x$ vzhledem k $\in$. Ukážeme $x = z$: $x \subseteq z$: $u \in x$, tedy i $u \in y$ a z linearity $\in$ máme $u \in z \vee u = z \vee z \in u$. Vzhledem k volbě z může nastat jen $u \in z$, pokud $u = z$, pak $u \notin x, z \in u \rightarrow z \in x$.

   Naopak pro $u \in z$, kdyby $u \notin x$, máme spor s minimalitou z v množině $y \setminus x$, tedy také $z \subseteq x$.

$\boxplus$

Věta 15 ($\in$ je dobré ostrá na On)**.** Relace náležení je dobré ostré uspořádání On.

Důkaz. Máme antireflexivitu $\in$ na On, tranzitivitu On a každý prvek On je ordinál, tedy tranzitivní množina. Z předchozího lemmatu máme $\in$ tranzitivní na On, tedy $\in$ je ostré uspořádání na On. Relace $\in$ je trichotomická na $On : x, y \in On$, tedy $x \cap y \in On$. Víme $x \cap y \subseteq x, x \cap y \subseteq y$. Máme tři možnosti: $=, =$, pak $x = y$, $\subset, =$, pak $y \in x$, nebo $=, \subset$, pak $x \in y$.

Tedy každá neprázdná množina ordinálních čísel má nejmenší prvek: $a \neq \emptyset, a \subseteq On$, pak $\alpha \in a$. Pokud α není minimální prvek, pak $b := a \cap \alpha, b \neq \emptyset, b \subseteq \alpha$. $\beta := \min_\in b$. Ukážeme $\beta = \min_\in a$. Pokud $\exists \gamma \in a : \gamma \in \beta \rightarrow \gamma \in a$, a tedy $\gamma \in a \cap \alpha = b$, tedy $\beta \neq \min_\in b$, což vede ke sporu. $\boxplus$

Důsledek 4 (On není množina)**.** On není množina

Důkaz. Kdyby On byla množina, pak je ordinál, a tedy $On \in On$, což je spor. $\boxplus$

Důsledek 5 (O tranzitivitě a $\in$)**.** Je-li X tranzitivní vlastní třída uspořádaná relací $\in$, pak $X = On$.

Důkaz. Zjevně $\forall x \in X : x \in On$, tedy $X \subseteq On$. Pokud $X \subset On$, pak $\exists x : x \in On \wedge x \notin X$, tedy $X \subseteq X$, což je spor s vlastní třídovostí, tedy $X = On$. $\boxplus$

Lemma 31 (O množinách ordinálů)**.**

1. Množina $x \subseteq On$ je ordinálem, právě když x je tranzitivní množina.

2. Je-li A neprázdná třída ordinálních čísel, potom $\bigcap A$ je nejmenší prvek A vzhledem k $\in = <$.

3. Je-li a množina ordinálních čísel, potom $\bigcup a$ je také ordinální číslo a je to supremum množiny a vzhledem k $<$.

Důkaz. 1. Každá množina ordinálů je dobře uspořádaná, je tedy ordinálem, právě když je tranzitivní.

2. Je-li X neprázdná podtřda On, má nejmenší prvek $\alpha \in A$. Tedy z tranzitivnosti ordinálů pro $\beta \in A$ máme $\alpha \in \beta$, načež $\alpha = \bigcap A$.

3. Nechť $a \subseteq On$. Z předchozí věty je $\bigcap a$ tranzitivní množina a z 1 je ordinál. Je-li $\alpha \in a$, potom $\alpha \subseteq \bigcup a = \beta$, tedy $\alpha \leq \beta$ podle předchozího lemmatu. Je-li $\gamma < \beta$, tj., je-li $\gamma = \bigcup a$, pak existuje $\alpha \in a$ takové, že $\gamma \in \alpha$, tedy $\gamma < \alpha$. Tím jsme ukázali, že $\bigcup a$ je nejmenší majoranta množiny a.

$\boxplus$

Důsledek 6 (ω je supremem ω v On)**.** Ordinál ω je supremem množiny všech přirozených čísel ve třídě On. Tedy ω je nejmenší nekonečné ordinální číslo a konečné ordinály jsou právě přirozená čísla.

Lemma 32 (O nejmenším větším ordinálu)**.** Je-li α ordinál, pak $\alpha \cup \{\alpha\}$ je nejmenší ordinál větší než α. (Říkáme, že $\alpha \bigcup \{\alpha\}$ je následníkem množiny α a předchůdce je naopak.)

Důkaz. Pro každý ordinál α je $\alpha \bigcup \{\alpha\}$ tranzitivní množina ordinálů, a tedy je ordinál z předchozího lemmatu. Je-li $\beta < \alpha \bigcup \{\alpha\}$, pak $\beta \in \alpha \bigcup \{\alpha\}$, a tedy $\beta \in \alpha \vee \beta = \alpha$. $\boxplus$

Definice 33 (Izolované a limitní ordinály)**.** 1. Řekneme, že ordinál α je izolovaný, jestliže $\alpha = 0$ nebo α má předchůdce.

2. Řekneme, že ordinál α je limitní, je-li nenulový a nemá předchůdce.

Věta 16 (Ordinály jsou typy dobře uspořádaných množin)**.** Je-li R dobré uspořádání množiny A, pak existuje právě jeden ordinál α a jednozačně určený izomorfismus $A(R)$ a $\alpha(<)$.

Důkaz. Z věty o izomorfismu dobrých uspořádání máme pro každý ordinál α izomorfismus zobrazující A na dolní podmnožinu α nebo α na dolní podmnožinu A. Je-li $\alpha < \beta$ a i je izomorfismus, který zobrazuje ordinál β na dolní podmnožinu A, potom $i|\alpha$ je izomorfní zobrazení α na dolní podmnožinu A a podle téže věty žádný jiný takový izomorfismus neexistuje.

Dále On je vlastní třída, a tedy není možné, aby každý ordinál β byl izomorfní s nějakou dolní podmnožinou A. Nechť β je ordinál takový, že $A \simeq a$, kde $a \subset \beta$ je dolní podmnožina. Dolní je totéž, co tranzitivní, což je tedy náš hledaný ordinál, a tedy je jediný. $\boxplus$

Důsledek 7 (O neizomorfismu ordinálů)**.** Dva různé ordinály nejsou izomorfní.

Věta 17 (První princip transfinitní indukce)**.** Nechť A je třída ordinálních čísel taková, že pro každý ordinál α platí $\alpha \leq A \to \alpha \in A$. Potom $A = On$.

Důkaz. $\alpha \subseteq A$ je totéž, jako $\forall \beta : \beta < \alpha \to \beta \in A$. Nechť $On \setminus A \neq \emptyset$. Pak pro nejmenší ordinál z $On \setminus A$ platí $\alpha \leq A$, ale $\alpha \notin A$, což je spor. $\boxplus$

Věta 18 (Druhý princip transfinitní indukce)**.** Nechť A je třída ordinálních čísel taková, že

1. $\emptyset \in A$

   A pro každý ordinál α platí:

2. $\alpha \subseteq A \to \alpha \bigcup \{\alpha\} \in A$

3. $\alpha \subseteq A \to \alpha \in A$, je-li α limitní.

Pak $A = On$.

Věta 19 (O transfinitní rekurzi ($!\delta$))**.** Nechť G je (třídové) zobrazení, které každé množině x přiřazuje množinu $G(x)$. Potom existuje právě jedno zobrazení F, které každému ordinálu α přiřazuje množinu $F(\alpha) = G(F|\alpha)$.

Věta 20 (O transfinitní rekurzi II ($!\delta$))**.** Nechť G_1 je zobrazení definované na univerzální třídě. Pak existuje právě jedno zobrazení $F : On \to V$ takové, že $F(\alpha) = G_1(F[\alpha])$ pro každý ordinál α.

Věta 21 (O transfinitní rekurzi III (!δ))**.** Je-li dána množina a a zobrazení G_1, G_2 definovaná pro každou množinu, pak eixstuje právě jedno zobrazení $F : On \to V$ takové, že platí:

- $F(0) = a$
- $F(\alpha) = G_1(F(\beta))$, je-li α následníkem ordinálu β
- $F(\alpha) = G_2(F[\alpha])$, je-li α limitní ordinál.

Věta 22 (AC implikuje WO)**.** AC implikuje WO

Důkaz. Nechť A je libovolná množina. Bez újmy na obecnosti je neprázdná, jinak není co dokazovat.

Stačí sestrojit prosté zobrazení f nějakého ordinálu α na A, které přenese dobré uspořádání $<$ ordinálu. Nechť g je selektor na $\mathcal{P}0(A)$, který vybírá z každé neprázdné podmnožina $a \subseteq A$ prvek $g(a) \in a$.

Pak $f(0) = g(A)$ Jsou-li sestrojeny $f(\gamma)$ pro všechna $\gamma < \beta$ a $A \setminus f[\beta] \neq \emptyset$, položíme $f(\beta) = g(A \setminus f[\beta])$. Existenci zobrazení zajišťuje věta o transfinitní rekurzi. Operaci G definujeme vztahem $G(x) = g(A \setminus x)$ pro každé x. Dle věty o transfinitní rekurzi existuje právě jedno zobrazení F takové, že pro každý ordinál α je $F(\alpha) = G(F[\alpha])$. Je-li α nejmenší ordinál takový, že $A \setminus F[\alpha] = \emptyset$ a $f = F|\alpha$, z definuce F a vlastností F se snadno ukáže, že f je prosté zobrazení α na A. ⊞

Seznam témat