ZÁKLADY TEORIE MNOŽIN

Dříve byl rozhodčím pravdy v matematice prostor. Záleželo jen na umění jednotlivých matematiků, jak pravdu z prostoru získat. Když se ukázalo, že prostor není schopen rozhodnout platnost postulátu o rovnoběžkách, pozice tohoto rozhodčího se otřásla a matematici začali hledat nové základy. G. Cantor vypracoval teorii množin a navrhl ji jako základ pro matematiku pro její formální jednoduchost a širokou použitelnost. Později se ukázalo, že v teorii množin lze modelovat prakticky všechnu současnou matematiku.

Teorie množin používá pouze symbol $\in$ pro označení být prvkem, $=$ pro označení rovnosti množin a dále již používá běžné logické symboly - logické spojky a kvantifikátory. Pro zlepšení vyjadřovacích schopností další matematické objekty definuje. (Na př. $\emptyset$ pro prázdnou množinu, $\langle 0, 1\rangle$ pro uspořádanou dvojici a mnoho dalších.)

Množina je systém dobře určených objektů, který takto tvoří opět objekt. Rozhodující je obsah (extenze) množiny, dvě množiny jsou stejné, mají-li stejný obsah (stejné prvky). Ukázalo se, že takto intuitivně pojatá teorie je nedostatečná, zvláště vzhledem k nejasnosti, co jsou dobře určené objekty. To vede až k Russellově paradoxu nazvanému podle objevitele následující úvahy B. Russella. Za předpokladu, že množiny jsou dobře určené objekty označme R množinu všech množin, které nejsou svými prvky. Pak $R \in R \to R \notin R$ a $R \notin R \to R \in R$. Obě možnosti vedou ke sporu.

Protože teorie množin již v době objevení paradoxů přinesla mnoho zajímavých výsledků, poukazujících k tomu, že by mohla dobře sloužit jako základní matematická teorie, nebyla odmítnuta, ale matematici se ji snažili vylepšit.

Popišme intuitivní strukturu univerza množin tak, jak s ní většina současných matematiků pracuje. Vychází se od prázdné množiny a stálým prováděním operace tvorby potenční množiny (t.j. množiny všech podmnožin) všeho, co bylo až dosud získáno, se stále obor množin zbohacuje. Tímto postupem se jednak vyloučí, aby množina byla svým prvkem, jednak se vyloučí existence množiny všech množin (neboť množiny vznikají postupně). Takto se teorie množin vyhnula nejen Russellově, ale i všem ostatním známým paradoxům. Nejasné zůstává, které soubory prvků mají být uznány za množiny (při tvorbě potenční množiny) a podle jaké struktury se má postupná tvorba stále větších množin provádět. Obvykle se požaduje, aby tato struktura obsahovala na počátku přirozená čísla a dále se jim velmi podobala v tom, že je lineárně uspořádaná, každý prvek má následovníka a každá její neprázdná podmnožina má nejmenší prvek. Tato struktura se nazývá ordinální čísla.

Neurčenost ordinálních čísel a operace potenční množiny vede k různým možnostem, jak univerzum množin vypadá. (Např. může, ale nemusí platit hypotéza kontinua, mohou, ale nemusí existovat tzv. velké kardinály, je mnoho dalších tvrzení, které mohou platit ve vhodných univerzech a v jiných univerzech mohou platit tvrzení opačná.)

Teorie množin popisuje univerza množin jak zmíněného, tak i jiného typu. Jejím úkolem je být "světem matematiky", v ní se má matematika odehrávat, třebaže mnozí specialisté

v jiných oborech matematiky o tom ani nemusí vědět. Teorie množin má obzvláště být obecnou teorií aktuálního nekonečna.

Základní vlastností, kterou při tvorbě potenční množiny vyžadujeme, je, aby existovala množina všech prvků již stanovené množiny, které mají vlastnost popsanou formulí teorie množin. Není tedy předem zajištěno, že existuje množina všech přirozených čísel, vyjadřujících počty lidí, kteří se mohou vejít do tramvaje. Uvedená vlastnost totiž není popsaná formulí teorie množin, není však předem vyloučeno, že nějaká množinová vlastnost popíše stejná přirozená čísla, nebo, že uvedená množina existovat bude, třebaže existenci množinové formule ji popisující předem nezaručíme.

Situace je jiná, pokud vydělíme množinovou vlastností část univerza množin. Takto vydělená část nemusí být množina, přesto se s takto vydělenými částmi v teorii množin často setkáváme, proto pro ně zavádíme označení třída. Podobně jako pro množiny, není pro třídy podstatné jakou vlastností byly definovány, ale je podstatné, které prvky obsahují. (Množina sestávající se z dvojnásobků přirozených čísel je rovna množině všech přirozených čísel vzniklých z těch, které nejsou dvojnásobky, odečtením jedničky.)

Základní operace s třídami a množinami.

Při zkoumání množin a tříd se často setkáváme se vztahem být částí, dále s operacemi vytvářející třídu (množinu) obsahující právě všechny prvky dvou tříd, třídu obsahující právě všechny prvky alespoň jedné ze dvou tříd, třídu obsahjící prvky jedné třídy, které nejsou prvky druhé třídy. Často pracujeme též s třídou mající za prvky všechny množiny (nazýváme ji univerzální třída) a s prázdnou třídou, která nemá žádný prvek. Přesné definice a značení zavádíme v následujícím odstavci.

Definice: 1) $x \in V \equiv x = x$ (univerzální třída). Pro přehlednější zápis užíváme pro definici tříd vymezením prvků následujícího značení $V = \{x;\ x = x\}$ a podobně dále.

2) $\emptyset = \{x;\ x \neq x\}$ (prázdná množina)

3) $X \subseteq Y \equiv (\forall x)(x \in X \to x \in Y)$ (X je částí Y)

4) $X \cap Y = \{x;\ x \in X\ \&\ x \in Y\}$ (průnik X a Y)

5) $X \cup Y = \{x;\ x \in X \vee x \in Y\}$ (sjednocení X a Y)

6) $X - Y = \{x;\ x \in X\ \&\ x \notin Y\}$ (rozdíl X a Y)

7) $-X = V - X = \{x;\ x \notin X\}$ (doplněk X)

8) $\triangle(X, Y) = (X - Y) \cup (Y - X)$ (symetrická diference X a Y).

Symetrická diference je míra odlišnosti X a Y a doporučujeme čtenáři, aby si promyslel její vztah k operaci XOR (neekvivalence, vylučovací nebo) používané ve výpočetní technice.

Pro tyto zavedené operace a vztah platí "algebraické" zákony obdobné zákonům známým pro běžné počítání s čísly.

Věta: Zákony typu uspořádání

1) $X \subseteq X$ (reflexivita)

2) $(X \subseteq Y\ \&\ Y \subseteq X) \to X = Y$ (slabá antisymetrie)

3) $(X \subseteq Y\ \&\ Y \subseteq Z) \to X \subseteq Z$ (tranzitivita)

Pozor obecně neplatí linearita uspořádání $X \subseteq Y \vee Y \subseteq X$. Množiny $\{0\}$ a $\{1\}$ jsou navzájem nesrovnatelné (pokud $0 \neq 1$).

Vlastnost 2) se často používá k důkazům rovnosti tříd a tedy i množin.

Další vlastnosti typu uspořádání:
$(\forall X)(\emptyset \subseteq X)$ (prázdná třída je nejmenší)
$(\forall X)(X \subseteq V)$ (universální třída je největší)
$X \cap Y \subseteq X$ & $X \cap Y \subseteq Y$ & $(\forall Z)((Z \subseteq X \ \& \ Z \subseteq Y) \to Z \subseteq X \cap Y)$ (průnik je infimem X a Y)
$X \subseteq X \cup Y$ & $Y \subseteq X \cup Y$ & $(\forall Z)((X \subseteq Z \ \& \ Y \subseteq Z) \to X \cup Y \subseteq Z)$ (sjednocení je suprémem X a Y).

Všechny uvedené vlastnosti se dokáží bezprostředně z definic.

Algebraické vlastnosti $\cap$, $\cup$, $-$:

1) $X \cap Y = Y \cap X$	$X \cup Y = Y \cup X$	(komutativita)
2) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$	$(X \cup Y) \cup Z = X \cup (Y \cup Z)$	(asociativita)
3) $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$	$(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$	(distributivita)
4) $-(-X)) = X$	(dvojí doplněk).	

Distributivní zákony zde platí oba; můžeme se dívat při algebraické práci na $\cap$ jako na $\cdot$ a na $\cup$ jako na $+$, ale i obráceně.

Rozdílná od běžného počítání s čísly jsou následující pravidla.

$X \cap X = X$	$X \cup X = X$	(idempotence)
$-(X \cap Y) = (-X) \cup (-Y)$	$-(X \cup Y) = (-X) \cap (-Y)$	(De Morganova
$X \cap \emptyset = \emptyset$	$X \cup \emptyset = X$	pravidla)
$X \cap V = X$	$X \cup V = V$	
$X \cap -X = \emptyset$	$X \cup -X = V$	

Všechny uvedené vlastnosti se ověří přímo z definic.

Operace $\cap$, $\cup$ a $-$ se nazývají booleovské operace a kalkulace s nimi se nazývají booleovské kalkulace.

Při důkazu rovností různých třídových výrazů postupujeme často tak, že obě strany dokazované rovnosti rozvineme na sjednocení jednotlivých členů, které jsou průniky tříd a jejich doplňků. Tyto členy pak porovnáme. Je to "algebraická" obdoba kreslení Venových diagramů. Tuto metodiku použijeme v následující části týkající se symetrické diference. Samozřejmě, že je možno využít i jiných cest k důkazu rovnosti, které mohou být i kratší.

Vlastnosti symetrické diference:
1) $\triangle(X, Y) = (X \cup Y) - (X \cap Y)$
2) $\triangle$ je komutativní a asociativní operace, dále platí distributivní zákon k $\cap$ (ne vzhledem k $\cup$), t.j. $A \cap \triangle(X, Y) = \triangle(A \cap X, A \cap Y)$
3) $\triangle(X \cap Y, A) \subseteq \triangle(X, A) \cup \triangle(Y, A)$
$\triangle(X \cup Y, A) \subseteq \triangle(X, A) \cup \triangle(Y, A)$
4) Když $X \subseteq A$ a $Y \subseteq A$, pak $\triangle(A - X, A - Y) = \triangle(X, Y)$.
Důkaz: 1) Levá strana $(X - Y) \cup (Y - X) = (X \cap -Y) \cup (Y \cap -X)$,
pravá strana $(X \cup Y) - (X \cap Y) = (X \cup Y) \cap (-(X \cap Y)) = (X \cup Y) \cap (-X \cup -Y) =$
$(X \cap -X) \cup (X \cap -Y) \cup (Y \cap -Y) \cup (Y \cap -X) = (X \cap -Y) \cup (Y \cap -X)$
2) Komutativita je jasná ze symetrie definice. Pro důkaz asociativity vyjádřeme levou stranu $\triangle(\triangle(X, Y), Z) = (((X \cap -Y) \cup (Y \cap -X)) \cap -Z) \cup (Z \cap (-((X \cap -Y) \cup (Y \cap -X)))) =$

$(X \cap -Y \cap -Z) \cup (Y \cap -X \cap -Z) \cup (Z \cap ((-X \cup Y) \cap (-Y \cup X))) = (X \cap -Y \cap -Z) \cup (Y \cap -X \cap -Z) \cup (Z \cap -X \cap -Y) \cup (Z \cap -X \cap X) \cup (Z \cap Y \cap -Y) \cup (Z \cap Y \cap X) = (X \cap -Y \cap -Z) \cup (Y \cap -X \cap -Z) \cup (Z \cap -X \cap -Y) \cup (Z \cap Y \cap X)$. Pro pravou stranu dostáváme $\triangle(X, \triangle(Y, Z)) = \triangle(\triangle(Z, Y), X)$ vzhledem ke komutativitě. Záměnou písmen Z a X získáme výraz z levé strany, zaměníme-li Z a X po úpravě, dostaneme opět stejný výraz. K důkazu distributivního zákona máme prověřit rovnost $X \cap \triangle(Y, Z) = \triangle(X \cap Y, X \cap Z)$. Levá strana se upraví na $X \cap ((Y \cap -Z) \cup (Z \cap -Y)) = (X \cap Y \cap -Z) \cup (X \cap Z \cap -Y)$. Pravá strana se upraví na $((X \cap Y) - (X \cap Z)) \cup ((X \cap Z) - (X \cap Y)) = (X \cap Y \cap (-X \cup -Z)) \cup (X \cap Z \cap (-X \cup -Y)) = (X \cap Y \cap -Z) \cup (X \cap Z \cap -Y) \cup ((X \cap -X) \cap Y) \cup ((X \cap -X) \cap Z)$. Třetí a čtvrtý člen sjednocení jsou však prázdné, proto platí rovnost levé a pravé strany.

3) Levá strana $(X \cap Y \cap -A) \cup (A \cap -(X \cap Y)) = (X \cap Y \cap -A) \cup (A \cap -X) \cup (A \cap -Y)$. Pravá strana $(X \cap -A) \cup (A \cap -X) \cup (Y \cap -A) \cup (A \cap -Y)$. $X \cap Y \cap -A \subseteq X \cap -A$ i $X \cap Y \cap -A \subseteq Y \cap -A$. V druhém případě vychází levá strana $((X \cup Y) \cap -A) \cup (A \cap -(X \cup Y)) = (X \cap -A) \cup (Y \cap -A) \cup (A \cap -X \cap -Y)$ a postupujeme analogicky.

4) $((A - X) \cap -(A - Y)) \cup ((A - Y) \cap -(A - X)) = (A \cap -X \cap (-A \cup Y)) \cup (A \cap -Y \cap (-A \cup X)) = ((A \cap Y) \cap -X) \cup ((A \cap X) \cap -Y) = (Y \cap -X) \cup (X \cap -Y)$.

Speciálně, budeme-li zkoumat strukturu s nosnou množinou $\mathcal{P}(a)$ (množina všech podmnožin a) pro $a \neq \emptyset$ a operacemi: $\triangle(x, y)$ chápeme jako $+$, $x \cap y$ chápeme jako $\cdot$, x chápeme jako $-x$, $\emptyset$ chápeme jako 0 a a chápeme jako 1, dostaneme poněkud zvláštní komutativní okruh.

Dvojice, n-tice, relace a funkce.

Jedním ze základních úkolů teorie množin je vytvářet modely pro objekty běžné matematiky. Tyto modely se pak stávají matematickými objekty, které původně pouze reprezentovaly, kanonisují se. Jako první uveďme modelování uspořádané dvojice.

Definice: $\langle x_1, x_2 \rangle = \{\{x_1\}, \{x_1, x_2\}\}$. Uspořádaná dvojice množin x_1, x_2 (v daném pořadí) je množina skládající se z množiny obou složek a množiny obsahující právě první složku. Následující věta ukazuje, že je to dobrý model.

Věta: $(x_1 = y_1 \ \& \ x_2 = y_2) \equiv \langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle$.

Důkaz: $\rightarrow$) Vyplývá z našeho obecného pohledu na rovnost. Když v matematických výrazech nahradíme sobě rovné objekty, získáme sobě rovné výrazy.

$\leftarrow$) a) Nechť $x_1 \neq x_2$, pak $\{\{x_1\}, \{x_1, x_2\}\}$ obsahuje jednu dvouprvkovou a jednu jednoprvkovou množinu, $\{\{y_1\}, \{y_1, y_2\}\}$ musí tedy rovněž obsahovat jednu jednoprvkovou a jednu dvouprvkovou množinu, jednoprvkové se musí rovnat, tedy $\{x_1\} = \{y_1\}$, tedy $x_1 = y_1$. Aby $\{y_1, y_2\}$ byla dvouprvková, musí být $y_1 \neq y_2$ a z rovností $x_1 = y_1$ a $\{x_1, x_2\} = \{y_1, y_2\}$ plyne $x_2 = y_2$.

b) Když $x_1 = x_2$, pak $\{x_1, x_2\} = \{x_1\}$, tedy $\{\{x_1\}, \{x_1, x_2\}\} = \{\{x_1\}, \{x_1\}\} = \{\{x_1\}\}$. Aby tato množina byla rovna $\{\{y_1\}, \{y_1, y_2\}\}$, musí platit $y_1 = y_2$ (pouze jednoprvkové množiny jsou přípustné jako prvky) a odtud již snadno plyne $y_1 = x_1$ a $y_2 = x_2 = x_1$. V tomto případě je tedy kanonickým modelem uspořádané dvojice jednoprvková množina.

Uspořádané n-tice definujeme rekurzí.

Definice: 1) $\langle x_1 \rangle = x_1$

2) $\langle x_1, \ldots, x_{n+1}\rangle = \langle\langle x_1, \ldots, x_n\rangle, x_{n+1}\rangle$.

Zadá-li nám někdo n prvků a jejich pořadí, umíme postupně podle uvedeného předpisu vytvořit množinový model n-tice. To, že lze popsat uvedený model jedinou formulí s parametrem n a tudíž, že existují uspořádané n-tice i pro libovolné prvky n z kanonické struktury, která přirozená čísla v teorii množin modeluje, je již ne zcela triviální tvrzení teorie množin (věta o konstrukci rekurzí - zformulujeme a dokážeme ji později) o této kanonické struktuře.

Neuspořádané n-tice modelujeme v teorii množin jako n-prvkové množiny.

Model pro uspořádanou dvojici nám umožňuje definovat další užitečné objekty.

Definice: $X \times Y = \{\langle x, y\rangle;\ x \in X\ \&\ y \in Y\}$ (kartézký součin)
$dom(X) = \{x;\ (\exists y)(\langle x, y\rangle \in X)\}$ (definiční obor třídy X)
$rng(X) = \{x;\ (\exists y)(\langle y, x\rangle \in X)\}$ (obor hodnot třídy X)
$X^{-1} = \{\langle x, y\rangle;\ \langle y, x\rangle \in X)\}$ (inverzní třída)
$X"Y = \{x;\ (\exists y \in Y)(\langle y, x\rangle \in X)\}$ (obraz třídy Y přes třídu X)
$X \restriction Y = \{\langle x, y\rangle\ ; \langle x, y\rangle \in X\ \&\ x \in Y\}$ (parcializace X na Y).

Relací (vztahem) byla původně v matematice míněna nějaká, obvykle definovaná, vlastnost, která byla daným počtem objektů splněna, nebo ne. Příkladem je $=$, uspořádání, ležet na přímce (pro trojice bodů). Jestliže vytvoříme třídu všech n-tic prvků majících danou vlastnost, pak tato třída přesně vlastnost zachycuje. Naopak každá třída n-tic X určuje vlastnost n prvků popsanou vztahem $\langle x_1, \ldots, x_n\rangle \in X$. Třídy, nebo množiny uspořádaných n-tic jsou proto dobrým kanonickým modelem pro relace. Protože každá uspořádaná n-tice je dvojicí (díky kanonickému modelu) můžeme modelovat relace v teorii množin jako třídy, které jsou částí kartézké druhé mocniny V.

Definice: 1) $Rel(X) \equiv X \subseteq V \times V$
2) $Fce(F) \equiv Rel(F)\ \&\ (\forall x, y, z)((\langle x, y\rangle \in F\ \&\ \langle x, z\rangle \in F) \to y = z)$.
Funkce jsou takové relace, ve kterých je prvku z definičního oboru přiřazen jediný prvek.

3) Pokud pro funkci F platí $Fce(F^{-1})$, nazývá se F *prostá* funkce.

4) Pokud F je prostá funkce a $dom(F) = X$ a $rng(F) = Y$, říkáme, že F zobrazuje X a Y *vzájemně jednoznačně.*

Věta: Kartézký součin je distributivní vzhledem k $\cap$ i $\cup$. Platí tedy
$(X_1 \cap X_2) \times (Y_1 \cap Y_2) = (X_1 \times Y_1) \cap (X_1 \times Y_2) \cap (X_2 \times Y_1) \cap (X_2 \times Y_2)$
$(X_1 \cup X_2) \times (Y_1 \cup Y_2) = (X_1 \times Y_1) \cup (X_1 \times Y_2) \cup (X_2 \times Y_1) \cup (X_2 \times Y_2)$
Pro $-$ (doplněk do V) distributivita obecně neplatí.
Kartézký součin je monotonní vůči inkluzi t.j.
$(X_1 \subseteq Y_1)\ \&\ (X_2 \subseteq Y_2) \to X_1 \times X_2 \subseteq Y_1 \times Y_2$
Důkaz: Všechny důkazy jsou jednoduché a přenecháváme je čtenáři.

Dále uvádíme některá tvrzení pro obraz.

Věta: $X"Y = rng(X \restriction Y) = rng(X \cap (Y \times V))$
$(X_1 \subseteq X_2\ \&\ Y_1 \subseteq Y_2) \to X_1"Y_1 \subseteq X_2"Y_2$ (monotonie)
$(T \cup U)"(X \cup Y) = T"X \cup T"Y \cup U"X \cup U"Y$
$X"(Y \cap Z) \subseteq X"Y \cap X"Z$, obecně ne obráceně
$X"Y - X"Z \subseteq X"(Y - Z)$, obecně ne obráceně.

Důkaz: Dokažme poslední tvrzení. Nechť t je prvkem levé strany, t.j. $(\exists u)(u \in Y \,\&\, \langle u,t\rangle \in X) \,\&\, \neg(\exists u)(u \in Z \,\&\, \langle u,t\rangle \in X)$. Druhou složku konjunkce přepišme ekvivalentně na $(\forall u)(\langle u,t\rangle \in X \to u \notin Z)$. První část konjunkce tvrdí, že existuje $u \in Y$ takové, že $\langle u,t\rangle \in X$. Vezměme jedno takové u. Druhá část konjunkce použitá na toto u tvrdí, že $u \notin Z$, což znamená, že t je prvek pravé strany.

Pokud je třída X v posledních dvou tvrzeních inverzní relací k funkci, pak dokonce platí rovnost.

Věta: Je-li F funkce, pak platí $(F^{-1})"(Y \cap Z) = (F^{-1})"Y \cap (F^{-1})"Z$ a $(F^{-1})"Y - (F^{-1})"Z = (F^{-1})"(Y - Z)$.

Dále definujeme skládání relací.

Definice: Jsou-li R a S relace, pokládáme $R \circ S = \{\langle x,y\rangle; (\exists z)(\langle x,z\rangle \in R \,\&\, \langle z,y\rangle \in S)\}$.

Věta: Jsou-li R, S a T relace, pak $(R^{-1})^{-1} = R$, $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$, $R \circ (S \circ T) = (R \circ S) \circ T$.

Operace potence a sumy.

Definice: 1) $\mathcal{P}(X) = \{u;\ u \subseteq X\}$ (potenční třída X)
2) $\bigcup(X) = \{x;\ (\exists y \in X)(x \in y)\}$ (sjednocení třídy X)

Intuitivně zdůvodněme, že, je-li x množina, je $\mathcal{P}(x)$ také množina. Je-li x prvkem některého kroku vytváření univerzální třídy stálým prováděním operace potenční množiny, označme tento krok V_α, pak x je též částí V_α. Odtud plyne $\mathcal{P}(x) \subseteq \mathcal{P}(V_\alpha)$, přitom $\mathcal{P}(V_\alpha)$ je opět množina a $\mathcal{P}(x)$ je z $\mathcal{P}(V_\alpha)$ vyčleněno množinovou formulí $\mathcal{P}(x) = \{t \in \mathcal{P}(V_\alpha); t \subseteq x\}$. Dále intuitivně zdůvodněme, že, je-li x množina, je též $\bigcup x$ množina. Je-li $x \in V_\alpha$, tedy též $x \subseteq V_\alpha$ a také $\bigcup x \subseteq V_\alpha$ a $\bigcup x$ je opět vyčleněno z V_α množinovou formulí $\bigcup x = \{t;\ (\exists u \in x)(t \in u)\}$.

Důležitým, ne však již tak přesvědčivě zdůvodněným požadavkem na množinové univerzum je požadavek, aby obrazem množiny byla množina. Tento požadavek je dalším požadavkem na bohatost struktury (ordinálních čísel), podle které se postupné provádění operace potenční množiny provádí. Máme-li zobrazení F (definované množinovou formulí) z již získané množiny u, přiřaďme každému prvku $F(t)$ $(t \in u)$ hladinu α, na které byl prvek $F(t)$ získán. Dostáváme tak zobrazení z u do ordinálních čísel. Je přirozené požadovat, aby ordinální čísla pokračovala ještě někam výš z důvodů analogických našemu požadavku, že proces tvorby stále bohatších potenčních množin neukončíme u přirozených čísel, neboť takové omezení by bylo příliš restriktivní.

Vlastnosti operací $\mathcal{P}(X)$ a $\bigcup X$.
$X \times Y \subseteq \mathcal{P}(\mathcal{P}(X \cup Y))$

Zobrazení f z X do Y indukuje zobrazení F z $\mathcal{P}(X)$ do $\mathcal{P}(Y)$, které je definováno předpisem $F(x) = f"x$. Pochopitelně né každé zobrazení z $\mathcal{P}(X)$ do $\mathcal{P}(Y)$ je indukováno zobrazením z X do Y.

$dom(X) \subseteq \bigcup\bigcup X$, $rng(X) \subseteq \bigcup\bigcup X$
$\bigcup\mathcal{P}(X) = X$, $X \subseteq \mathcal{P}(\bigcup X)$, $x \cup y = \bigcup\{x,y\}$.

Definice: $\bigcap X = \{t;\ (\forall y \in X)(t \in y)\}$ (průnik třídy X).

Platí $(\forall t \in X)(\bigcap X \subseteq t)$; je-li tedy X neprázdná, je $\bigcap X$ množina. $\bigcap \emptyset = V$ v souladu s definicí. Analogicky jako u sjednocení, platí $x \cap y = \bigcap\{x, y\}$.

Axiomatika ZFC.

Nyní, když jsme se již seznámili se základními pojmy teorie množin, je vhodná doba pro to, abychom uvedli nejběžnější axiomatický popis teorie množin, sice Zermelovu a Fraenkelovu teorii množin s axiomem výběru, která se označuje ZFC.

Axiom existence množin
$(\exists x)(x = x)$ (existuje alespoň jedna množina)

Axiom etenzionality
$(\forall u)(u \in x \equiv u \in y) \to x = y$ (množiny, které mají tytéž prvky se rovnají)

Schéma axiomů vydělení
Je-li $\psi(x)$ formule, která neobsahuje volně proměnnou z, potom formule
$(\forall a)(\exists z)(\forall x)(x \in z \equiv (x \in a \ \& \ \psi(x)))$
je axiom vydělení (z každé množiny lze vydělit množinu všech prvků, ktré splňují danou formuli).

Axiom dvojice
$(\forall a)(\forall b)(\exists z)(x \in z \to (x = a \vee x = b))$
(libovolné dvě množiny určují množinu obsahující přesně tyto prvky).

Axiom sumy
$(\forall a)(\exists z)(\forall x)(x \in z \equiv (\exists y)(x \in y \ \& \ y \in a))$.
(ke každé množině a je dána množina všech prvků, které náležejí do některého prvku množiny a).

Axiom potence
$(\forall a)(\exists z)(\forall x)(x \in z \equiv x \subseteq a)$
(ke každé množině existuje množina všech podmnožin).

Schéma axiomů nahrazení
Je-li $\psi(u, v)$ formule, která neobsahuje volně proměnné w, z, potom formule
$(\forall u)(\forall v)(\forall w)((\psi(u, v) \& \psi(u, w)) \to v = w) \to$
$(\forall a)(\exists z)(\forall v)(v \in z \equiv (\exists u)(u \in a \ \& \ \psi(u, v)))$
je axiom nahrazení (definovatelné zobrazení zobrazuje množinu na množinu).

Axiom nekonečna
$(\exists z)(\emptyset \in z \ \& \ (\forall x)(x \in z \to x \cup \{x\} \in z))$
(existuje nekonečná množina).

Axiom fundovanosti
$(\forall a)(a \neq \emptyset \to (\exists x)(x \in a \ \& \ x \cap a = \emptyset))$
(srovnej s principem nejmenšího prvku na přirozených číslech).

Axiom výběru
$(\forall a)((\forall x)(x \in a \to x \neq \emptyset) \to (\exists S)(Fce(S) \ \& \ (\forall x)(x \in a \to S(x) \in x))$
(každá množina neprázdných množin má selektor).

Kromě uvedené axiomatiky používající množiny jako základní objekty, jsou též axiomatiky (Gödelova a Bernaysova, nebo Kellyho a Morseova), používající třídy jako základní objekty. V rámci Zermelovy a Fraenkelovy axiomatiky se též upouští od axiomu regularity a připouštějí se např. i nekonečné klesající řetězce v relaci $\in$, nebo se místo axiomu výběru zkoumá axiom determinovanosti, zaručující, že i nekonečné hry mají vyhrávající strategii (v rozporu s axiomem výběru). Při tom jak existenci selektoru, tak i existenci vyhrávající strategie lze pro konečné množiny dokázat.

Uspořádání.

Důležitými relacemi vyšetřovanými v matematice (a nejen v ní) jsou relace uspořádání.

Definice: Říkáme, že relace R je na třídě A
1) *reflexivní* jestliže $(\forall x \in A)(\langle x, x\rangle \in R)$
2) *antireflexivní* jestliže $(\forall x \in A)(\langle x, x\rangle \notin R)$
3) *symetrická* jestliže $(\forall x, y \in A)(\langle x, y\rangle \in R \to \langle y, x\rangle \in R)$
4) *slabě antisymetrická* jestliže $(\forall x, y \in A)((\langle x, y\rangle \in R \ \& \ \langle y, x\rangle \in R) \to x = y)$
5) *antisymetrická* jestliže $(\forall x, y \in A)(\langle x, y\rangle \in R \to \langle y, x\rangle \notin R)$
6) *trichotomická* jestliže $(\forall x, y \in A)(\langle x, y\rangle \in R \vee x = y \vee \langle y, x\rangle \in R)$
7) *tranzitivní* jestliže $(\forall x, y, z \in A)((\langle x, y\rangle \in R \ \& \ \langle y, z\rangle \in R) \to \langle x, z\rangle \in R)$.

Definice: Relace R je *neostré uspořádání na* A, je-li na A reflexivní, slabě antisymetrická a tranzitivní. Neostré uspořádání na A se nazývá *lineární* na A, platí-li navíc $(\forall x, y \in A)(\langle x, y\rangle \in R \vee \langle y, x\rangle \in R)$.

Zajímavé jsou i relace reflexivní a tranzitivní (od požadavku slabé antisymetrie se upouští), takovéto relace se nazývají kvaziuspořádání a lze k nim přirozeně přiřadit vhodné uspořádání.

Kromě neostré verze uspořádání se používá i ostré uspořádání.

Definice: Řekneme, že relace R je *ostré uspořádání na* A, jestliže je antireflexivní a tranzitivní na A. Je-li navíc relace trichotomická, nazývá se *ostré lineární uspořádání na* A.

Poznamenejme, že ostré uspořádání je antisymetrická relace.

Příklady: 1) Relace inkluze na $\mathcal{P}(x)$ je neostré uspořádání, které není lineární, pokud je x alespoň dvouprvková.

2) Běžné uspořádání přirozených čísel je uspořádání, které je lineární.

3) $\emptyset$ je ostré uspořádání, které není lineární na žádné alespoň dvouprvkové třídě.

Mezi ostrou a neostrou verzí uspořádání je snadný přechod, který vystihuje následující věta.

Věta: Je-li R neostré uspořádání na A, pak $R - \{\langle t, t\rangle;\ t \in A\}$ je ostré uspořádání na A a je-li R ostré uspořádání na A, pak $R \cup \{\langle t, t\rangle;\ t \in A\}$ je neostré uspořádání na A.

Je-li třída, na které je relace R uspořádání jasná ze souvislosti, neuvádí se. Pro zvýraznění, že se jedná o uspořádání se používá symbolika $t < x$, $t \leq x$, $t \prec x$, $t \preceq x$ a pod. (místo $\langle t, x\rangle \in <$, $\langle t, x\rangle \in \leq$ a pod.).

Definice: Buď $\leq$ uspořádání na A.

1) Prvek $a \in A$ je *nejmenší* (resp. *největší*) prvek třídy $X \subseteq A$, platí-li $a \in X$ &

$(\forall x \in X)(a \leq x)$ (resp. $a \in X$ & $(\forall x \in X)(x \leq a)$).

2) Prvek $a \in A$ je *minoranta* (resp. *majoranta*) třídy $\emptyset \neq X \subseteq A$, platí-li $(\forall x \in X)(a \leq x)$ (resp. $(\forall x \in X)(x \leq a)$).

3) Prvek $a \in A$ je *minimální* (resp. *maximální*) prvek třídy $\emptyset \neq X \subseteq A$, platí-li $a \in X$ & $(\forall x \in X)\neg(x < a)$ (resp. $a \in X$ & $(\forall x \in X)\neg(a < x)$). Používáme značení $a = min(X)$ (resp. $a = max(X)$).

4) Prvek $a \in A$ je *infimum* (resp. *suprémum*) třídy $X \subseteq A$, jestliže a je největší minoranta (resp. nejmenší majoranta) třídy X. Používáme značení $a = inf(X)$ (resp. $a = sup(X)$).

Pokud v bodech 3) a 4) není jasné uspořádání ze souvislosti, vyznačíme je v indexu.

Tvrzení : Nejmenší prvek a infimum jsou určeny jednoznačně (pokud existují). Minimální prvek nemusí být určen jednoznačně. V lineárním uspořádání pojem minimálního a nejmenšího prvku splývá. Obdobná tvrzení platí pro suprémum, maximální a největší prvek.

V literatuře se místo minoranta, majoranta též používá dolní, horní odhad, nebo dolní, horní závora.

Definice: Nechť $<$ je uspořádání na X a $\prec$ je uspořádání na Y.

1) Zobrazení F t.ž. $dom(F) = X$ & $rng(F) \subseteq Y$ se nazývá *vnoření* $\langle X, < \rangle$ do $\langle Y \prec \rangle$, platí-li, že F je prosté a $(\forall x, y \in X)(x < y \equiv F(x) \prec F(y))$.

2) Zobrazení F se nazývá *izomorfizmus* X s $<$ a Y s $\prec$, platí-li, že F je vnoření X s $<$ do Y s $\prec$ a navíc $rng(F) = Y$.

3) Zobrazení F se nazývá *automorfizmus* X s $<$, je-li izomorfizmem X s $<$ a X s $<$.

Jsou-li dvě uspořádání izomorfní, znamená to, že je nelze z pohledu uspořádání rozlišit, že jsou "téměř stejná". Rovněž všechny dříve definované pojmy se izomorfizmem přenášejí. Tedy např. izomorfním obrazem supréma třídy je suprémum obrazu třídy. Pro pouhé vnoření toto tvrzení obecně neplatí.

Definice: Nechť $\leq$ je uspořádání na třídě A.

1) $X \subseteq A$ se nazývá *dolní* (resp. *horní*) třída, platí-li $(\forall t \in A)((\exists x \in X)(t \leq x) \rightarrow t \in X)$ (resp. $(\forall t \in A)((\exists x \in X)(x \leq t) \rightarrow t \in X)$).

2) Pro $a \in A$ definujeme $seg(a) = \{t \in A; t \leq a\}$ a tuto třídu nazýváme *(dolním) segmentem* určeným a, nebo též *hlavním ideálem* určeným a.

Segment je příkladem dolní množiny, ne každá dolní množina však je segmentem. Následující věta ukazuje univerzální roli $\subseteq$ mezi uspořádáními.

Věta: Nechť $\leq$ je uspořádání na a, pak lze nadefinovat funkci f, která je vnoření a s $\leq$ do $\mathcal{P}(a)$ s $\subseteq$.

Důkaz: Pro $t \in a$ definuj $f(t) = seg(t)$. Ověřit, že takto definovaná funkce je vnoření, je již snadné.

Dalším důležitým pojmem, který se váže k uspořádání je pojem hustoty. (Původní zdroj tohoto pojmu je však topologie.)

Definice: Nechť $<$ je ostré uspořádání na A.

1) Řekneme, že $X \subseteq A$ je hustá v A, jestliže platí $(\forall x, y \in A)(x < y \rightarrow (\exists z \in X)$ $(x < z < y))$.

2) Řekneme, že $<$ je husté na A, jestliže A je hustá v A.

Typickým příkladem husté podmnožiny je množina racionálních čísel, která je v přirozeném uspořádání hustá v množině reálných čísel. Racionální i reálná čísla jsou přirozeným uspořádáním uspořádána hustě.

Ekvivalence.

Dalším důležitým typem relací zkoumaných v matematice jsou relace ekvivalence.

Definice: 1) Relace E se nazývá *ekvivalence* na A, jestliže je reflexivní, symetrická a tranzitivní na A.

2) Relace E se nazývá *ekvivalence*, jestliže je ekvivalencí na svém definičním oboru.

Typickým příkladem ekvivalence je $=$. To, že je relace E ekvivalence, znamená, že je "téměř" rovnost. Tento fakt se zvýrazňuje značením. Místo $\langle x, y\rangle \in E$ se používá $x \sim y$, $x \approx y$, $x \equiv y$, $x \doteq y$ a pod.

Dalším příkladem ekvivalence je relace dvě jednotky zboží mají stejnou cenu. Jiným příkladem je relace na dvojicích celých čísel jejichž druhé složky jsou nenulové popsaná vztahem $\langle c_1, c_2\rangle \approx \langle d_1, d_2\rangle$, když $c_1 \cdot d_2 = d_1 \cdot c_2$. Tento vztah jsme si zvykli vyznačovat $c_1/c_2 = d_1/d_2$. Jako poslední příklad uveďme příklad z teorie množin. Položme $x \approx y$, když existuje vzájemně jednoznačné zobrazení x a y (t.j. $(\exists f)(f : x \longleftrightarrow y)$.

Můžeme si povšimnout, že druhý a třetí příklad můžeme sdružit pod jednu společnou charakterizaci: Pro vhodnou funkci f platí $x \approx y$ právě tehdy, když $f(x) = f(y)$. Rovněž první a čtvrtý příklad lze takto popsat. V prvním případu je touto funkcí identita a ve čtvrtém případu je příslušnou funkcí funkce přiřazující množině její tzv. kardinální číslo.

Definice: Je-li E ekvivalence a $x \in dom(E)$, pak $E"\{x\}$ se nazývá třída ekvivalence prvku x. Pro třídu ekvivalence $E"\{x\}$ se též používá značení $[x]_E$.

Zřejmě platí následující věta.

Věta: Je-li E ekvivalence, $x, y \in dom(E)$, pak $E"\{x\} = E"\{y\} \equiv \langle x, y\rangle \in E$ a $E"\{x\} \cap E"\{y\} = \emptyset \equiv \langle x, y\rangle \notin E$.

Ekvivalence nám určuje rozklad svého definičního oboru na navzájem disjunktní neprázdné třídy. Naopak každý rozklad třídy na neprázdné disjunktní třídy určuje ekvivalenci - dva prvky jsou ekvivalentní, jestliže padnou do téže třídy rozkladu.

S ekvivalencí souvisí ještě jedna důležitá matematická konstrukce.

Definice: Buď E ekvivalence na množině $a \neq \emptyset$. Množina $a/E = \{[x]_E;\ x \in a\}$ se nazývá *faktorizace množiny a podle ekvivalence E.*

Příklad s racionálními čísly dává tušit, že faktorizace množin hrají důležitou úlohu při konstrukci matematických struktur.

Faktormnožina nám také umožňuje prokázat, že každou ekvivalenci na množině lze popsat jako ekvivalenci určenou funkcí. Je-li totiž E ekvivalence na a, definujeme funkci f předpisem $f(x) = [x]_E$.

Srovnání mohutností množin.

Přirozeným srovnáním množin podle velikosti je inkluze. Při tomto pohledu však dvě různé jednoprvkové množiny jsou nesrovnatelné. Proto se zavádí v teorii množin srovnání

podle mohutností (kardinalit).

Definice: 1) Řekneme, že množiny x, y *mají stejnou mohutnost* (značíme $x \approx y$), jestliže $(\exists f)(f : x \longleftrightarrow y)$.

2) Řekneme, že množina x *má mohutnost menší nebo rovnu* y (značíme $x \preceq y$), jestliže $x \approx z$ pro nějakou podmnožinu z množiny y. Řekneme, že množina x *má mohutnost menší než* y (značíme $x \prec y$), jestliže $x \preceq y$ a $\neg x \approx y$.

Čtenář snadno nahlédne, že $\approx$ je ekvivalence. Na třídy této ekvivalence se můžeme dívat jako na jistý číselný obor rozšiřující (do nekonečna) obor přirozených čísel. Čísla určená těmito třídami byla Cantorem nazývána kardinální čísla. V moderní matematice pro kardinální čísla volíme speciální reprezentanty (nejmenší ordinální číslo v dané třídě), podobně jako ve dvojicích celých čísel $\langle n, m\rangle$ reprezentujících racionální čísla (používáme při tom značení n/m) volíme reprezentanta tak, aby n, m byla nesoudělná a m bylo kladné. Při tomto pohledu nám relace $\preceq$ reprezentuje uspořádání, zatím však vidíme pouze reflexivitu a tranzitivitu uvedené relace. Slabá antisymetrie plyne z Cantorovy a Bernsteinovy věty ke které budeme směřovat. Nejdříve si dokažme pomocnou větu.

Věta (o pevném bodu neklasající funkce): Nechť $F : \mathcal{P}(x) \longrightarrow \mathcal{P}(x)$ je neklesající (vzhledem k $\subseteq$) funkce. (Tedy $u \subseteq v \to F(u) \subseteq F(v)$.) Pak existuje $t \subseteq x$ takové, že $F(t) = t$ (t je pevný bod F).

Důkaz: Položme $M = \{u \subseteq x;\ u \subseteq F(u)\}$. Ukážeme, že $t = \bigcup M$ je hledaným pevným bodem. Nejdříve ukážeme, že $t \in M$, tedy $t \subseteq F(t)$. Nechť $z \in t$, tedy $z \in u$, pro nějaké $u \in M$. Pak z $u \subseteq t$ (připomeňme $u \in M$ a $t = \bigcup M$) a monotonie F, plyne $z \in u \subseteq F(u) \subseteq F(t)$, tedy $t \subseteq F(t)$. Odtud z monotonie F plyne $F(t) \subseteq F(F(t))$, tedy $F(t) \in M$. Protože $t = \bigcup M$, platí $F(t) \subseteq t$. Dokázali jsme obě inkluze, a proto platí $t = F(t)$.

Věta (Cantor, Bernstein): Nechť $x \preceq y$ a $y \preceq x$, pak $x \approx y$.

Důkaz: Nechť f a g jsou prosté funkce takové, že $f : x \longrightarrow y$ a $g : y \longrightarrow x$. Pro $u \subseteq x$ položme $F(u) = x - g"(y - f"u)$. Takto definovaná funkce je neklesající funkce z $\mathcal{P}(x)$ do $\mathcal{P}(x)$ a má proto pevný bod t ($F(t) = t$), tedy $t = x - g"(y - f"t)$. Přechodem k doplňkům odtud dostaneme $x - t = g"(y - f"t)$. Definujme nyní funkci h předpisem $h(z) = f(z)$ pro $z \in t$ a $h(z) = g^{-1}(z)$ pro $z \in x - t$. Ukážeme, že $h : x \longleftrightarrow y$.

Nejdříve ukažme prostotu h. Nechť z, v jsou dva různé prvky x. Jsou-li z, $v \in t$ (resp. $\in x - t$), pak jejich obrazy jsou různé, jak plyne z prostoty f (resp. g^{-1}). Je-li $z \in t$ a $v \in x - t$, pak $h(z) = f(z) \in f"t$ a $h(v) = g^{-1}(v) \in y - f"t$, tedy $h(z) \neq h(v)$. Tím je prostota h dokázána.

Nyní ukažme že h je na y. Je-li $v \in f"t$, pak existuje $z \in t$ takové, že $v = f(z) = h(z)$. Je-li $v \in y - f"t$, pak existuje $z \in x - t$ takové, že $v = g^{-1}(z) = h(z)$.

Díváme-li se na $\approx$ jako na rovnost, je $\preceq$ uspořádání. Linearita tohoto uspořádání je ekvivalentní s axiomem výběru (mnohem později dokážeme jednu implikaci). Na naznačené struktuře (vzniklé faktorizací podle $\approx$) rozšiřující strukturu přirozených čísel máme zatím zavedenu rovnost a uspořádání. Zaveďme zde ještě běžné početní operace, rozšiřující operace známé z přirozených čísel (některé vlastnosti těchto operací budou mnohdy neobvyklé). Nejdříve však upřesněme naznačený číselný obor následující definicí.

Definice: Kardinálním číslem x (značíme $|x|$) rozumíme třídu rozkladu podle ekvivalence $\approx$ obsahující x jako svůj prvek. (Později doplníme též množinového reprezentanta této třídy).

Vedeni analogií z přirozených čísel definujeme mocninu množin následujícím způsobem.

Definice: ${}^x y = \{f;\ f : x \longrightarrow y\}$.

Dále definujeme početní operace na kardinálních číslech.

*Definice:*1) $|x| + |y| = |\{0\} \times x \cup \{1\} \times y|$
2) $|x| \cdot |y| = |x \times y|$
3) $|x|^{|y|} = |{}^y x|$

Příslušnou soustavu lemat ukazujících, že ve shora uvedených definicích nezávisí na volbě reprezentantů tříd a asociativní, komutativní a distributivní zákony pro $+$ a $\cdot$ přenecháváme čtenáři.

Zavedené početní operace mají však v nekonečném případě mnohdy odlišné vlastnosti od těch, na které jsme zvyklí v konečném případě. Nechť $\mathbb{N}$ označuje množinu přirozených čísel a $\mathbb{R}$ označuje množinu reálných čísel. Pak platí následující rovnosti.

Věta: 1) $|\mathbb{N}| + |\mathbb{N}| = |\mathbb{N}| \cdot |\mathbb{N}| = |\mathbb{N}|$
2) $|\mathbb{R}| + |\mathbb{R}| = |\mathbb{R}| \cdot |\mathbb{R}| = |\mathbb{R}|$

Důkaz: 1) Dva exempláře $\mathbb{N}$ zobrazíme vzájemně jednoznačně na $\mathbb{N}$ tak, že jeden zobrazíme na lichá a druhý na sudá čísla. $\mathbb{N}$ vnoříme do $\mathbb{N} \times \mathbb{N}$ tak, že $\mathbb{N}$ zobrazíme na $\{0\} \times \mathbb{N}$ a $\mathbb{N} \times \mathbb{N}$ vnoříme do $\mathbb{N}$ tak, že dvojici $\langle n, m\rangle$ přiřadíme číslo $2^n \cdot 3^m$. Cantorova a Bernsteinova věta nám pak zaručuje existenci vzájemně jednoznačného zobrazení $\mathbb{N} \times \mathbb{N}$ a $\mathbb{N}$.

2) Nejdříve si uvědomme, že funkce $tg(\pi \cdot (x - 1/2))$ zobrazuje vzájemně jednoznačně $\mathbb{R}$ a otevřený interval $(0, 1)$. Dva exempláře tohoto intervalu (např. $(0, 1)$ a $(1, 2)$) vnoříme do $\mathbb{R}$ a Cantorova a Bernsteinova věta nám pak zaručuje existenci požadovaného vzájemně jednoznačného zobrazení. Tím je ukázáno, že součet dvou exemplářů kardinálního čísla odpovídajícího $\mathbb{R}$ je roven $|\mathbb{R}|$. Nyní ukažme, že $(0, 1) \times (0, 1) \approx (0, 1)$. Interval $(0, 1)$ vnoříme do jeho kartézké druhé mocniny tak, že každému číslu x přiřadíme dvojici $\langle 1/2, x\rangle$. Kartézkou druhou mocninu vnoříme do intervalu tak, že dvojici $\langle x, y\rangle$ s dvojkovými rozvoji $x = 0, x_1x_2x_3\ldots$, $y = 0, y_1y_2y_3\ldots$ přiřadíme číslo $z = 0, x_1y_1x_2y_2x_3y_3\ldots$. Takto dostaneme hledané vnoření (např. číslo $0, 1010\ldots$ nebude mít vzor). Cantorova a Bernsteinova věta nám pak zaručuje existenci požadovaného vzájemně jednoznačného zobrazení.

Následující slavná Cantorova diagonální úvaha ukazuje, že reálných čísel je v rámci teorie množin ostře více než čísel přirozených.

Věta (Cantor): $\mathbb{N} \prec \mathbb{R}$

Důkaz: $\mathbb{N} \preceq \mathbb{R}$ je jasné, neboť $\mathbb{N}$ je částí $\mathbb{R}$. Dovedeme ke sporu předpoklad $(\exists f)(f : \mathbb{N} \longleftrightarrow \mathbb{R})$. Stačí ukázat, že nelze očíslovat reálná čísla otevřeného intervalu $(0, 1)$ přirozenými čísly. Nechť tedy $a_1, a_2, a_3, \ldots$ je takové očíslování. Nechť

$a_1 = 0, a_1^1 a_1^2 a_1^3 \ldots$
$a_2 = 0, a_2^1 a_2^2 a_2^3 \ldots$
$a_3 = 0, a_3^1 a_3^2 a_3^3 \ldots$
$\ldots$

jsou desetinné zápisy příslušných čísel. Definujme číslo $c = 0, c^1c^2c^3\ldots$ předpisem:

$c^i = 7$, když $a_i^i < 5$ a $c^i = 2$, když $a_i^i > 4$.

Toto číslo c je v intervalu $(0, 1)$, ale nemůže být žádným číslem a_i, neboť $c^i \neq a_i^i$ a zápis c je jednoznačný, protože obsahuje jen cifry 2 a 7.

Uvedená úvaha se ukázala být velice mocným matematickým prostředkem. Ukazuje např., že existuje reálné číslo, které není kořenem algebraické rovnice s celočíselnými koeficienty, aniž by nějaké takové číslo skutečně uvedla (jsou to např. čísla π, e, důkazy těchto faktů jsou však mnohem obtížnější), protože tyto kořeny lze očíslovat přirozenými čísly. Poznamenejme ještě, že kořeny algebraických rovnic s celočíselnými koeficienty se nazývají čísla algebraická a kořeny algebraických rovnic s algebraickými koeficienty jsou opět čísla algebraická.

Heslovitě ukažme ještě jednu úvahu z jiné oblasti matematiky používající diagonální úvahu. Jedná se o **problém zastavení algoritmu**. Asi každý, kdo se učil programovat se setkal se situací, že jeho program se dostal do nekonečného cyklu. Vzniká otázka, zda lze takové programy algoritmicky odhalit. (Zde již implicitně používáme tzv. Churchovu tezi, algoritmy - intuitivní pojem - ztotožňujeme s programy - přesně definovanými objekty např. posloupnostmi instrukcí idealizovaného výpočetního stroje.)

Pro upřesnění problému si uvědomme několik faktů:

1) Každý program je určen zdrojovým textem, což je jisté číslo v 256-kové soustavě. Funkci f vyčíslovanou tímto algoritmem (obecně parciální funkci jejíž hodnota $f(x)$ je hodnota výstupu při kterém algoritmus zastaví při vstupu x a není definována pokud algoritmus nezastaví) můžeme očíslovat číslem představovaným uvedeným zdrojovým textem. (Při tom stejná funkce může být v tomto očíslování uvedena vícekrát, neboť např. poznámky v zdrojovém textu mohou být různě formulovány.)

2) Dříve popsané kódování dvojic $(2^n \cdot 3^m)$ lze zvládnout algoritmem (programem) a existuje algoritmus $T(\langle n, m\rangle)$, který dvojici $\langle n, m\rangle$ přiřadí výstup (číslo, nebo neskončí) stejný, jako získáme programem se zdrojovým textem n a vstupem m. V případě, že n není zdrojový text (je syntakticky chybný) dává výstup 0. (Takovým programem je např. upravený interpret programovacího jazyka, který místo chybových hlášek dává 0).

Kdyby existoval algoritmus $H(\langle n, m\rangle)$, který by dával hodnotu 0, pokud program se zdrojovým textem n neskončí při vstupu m a hodnotu 1, pokud skončí, definovali bychom totální (pro všechna přirozená čísla definovanou funkci) C následujícím (algoritmickým) předpisem.

$C(n) = T(\langle n, n\rangle) + 1$, pokud $H(\langle n, n\rangle) = 1$

$C(n) = 1$, pokud $H(\langle n, n\rangle) = 0$

Funkce C je vyjádřitelná programem se zdrojovým textem c. Úvahou anologickou dříve uvedené Cantorově diagonální úvaze spočítáme, že $C(c) = T(\langle c, c\rangle)$ podle bodu 2). Podle definice C však máme $C(c) = T(\langle c, c\rangle) + 1$. Tím je ukázáno, že funkce H nemůže být popsána algoritmem.

Dále zobecníme Cantorovu větu dokázanou diagonální úvahou, že reálných čísel je více než přirozených (je jich tzv. nespočetně).

Věta (Cantor): $x \prec \mathcal{P}(x)$

Důkaz: $x \preceq \mathcal{P}(x)$ dokážeme tak, že každému $t \in x$ přiřadíme $\{t\} \in \mathcal{P}(x)$.

Důkaz $\neg x \approx \mathcal{P}(x)$ je mírnou reformulací úvahy z Russellova paradoxu. Nechť $f : x \longleftrightarrow \mathcal{P}(x)$. Dovedeme ke sporu existenci takové funkce. Položme $C = \{t;\ t \in x\ \&\ t \notin f(t)\}$. Pak existuje c takové, že $C = f(c)$. Zkoumejme, zda $c \in C$. Pokud $c \in C$, pak podle definice C platí $c \notin C$. Pokud $c \notin C$, pak podle definice C platí $c \in C$ podobně jako v Russellově paradoxu. Bijekce x a $\mathcal{P}(x)$ tedy nemůže existovat.

Právě uvedená věta zobecňuje dříve uvedenou větu (o nespočetnosti $\mathbb{R}$), neboť každý dvojkový zápis čísla x z uzavřeného intervalu $\langle 0, 1\rangle$ můžeme chápat jako zakódování podmnožiny $\mathbb{N}$ těch indexů i, že pro příslušnou cifru platí $x^i = 1$. Při tom čísel s dvojznačným zápisem je jen málo (dvojkově racionální čísla), dají se očíslovat přirozenými čísly (je jich tzv. spočetně).

Vzhledem ke vztahu uvedených dvou vět se někdy též uvahy analogické důkazu druhé věty nazývají diagonální.

Definice: Charakteristickou funkcí χ_u množiny u (podmnožiny množiny x zřejmé obvykle z kontextu) je funkce taková, že $dom(\chi_u) = x$ a $(\forall t \in x)((t \in u \equiv \chi_u(t) = 1)\ \&\ (t \notin u \equiv \chi_u(t) = 0))$.

Mezi charakteristickými funkcemi podmnožin x a podmnožinami x je vzájemně jednoznačný vztah, který prokazuje následující ekvivalenci.

Věta: ${}^x2 \approx \mathcal{P}(x)$

Z uvedené věty a z rovnosti $2^{|x|+|y|} = (2^{|x|}.2^{|y|})$, kterou doporučujeme čtenáři k rozmyšlení, plyne okamžitě rovnost $|\mathbb{R}| \,.\, |\mathbb{R}| = 2^{|\mathbb{N}|+|\mathbb{N}|} = 2^{|\mathbb{N}|} = |\mathbb{R}|$, kterou jsme poněkud klopotněji dokázali dříve.

Uvedené rovnosti lze za pomoci axiomu výběru zobecnit do rovnosti:

Jsou-li x, y neprázdné množiny, z nichž alespoň jedna je nekonečná, pak

$|x| + |y| \ = |x| \,.\, |y| \ = max(|x|, |y|)$.

Toto tvrzení zde dokazovat nebudeme, odkazujeme čtenáře na kteroukoliv odbornou knihu z teorie množin. (Dokáže se transfinitní indukcí za pomoci maximolexikografického uspořádání. Transfinitní indukci zde probereme později, maximolexikografické uspořádání zde probírat nebudeme. Axiom výběru potřebujeme pouze pro fakt, že x i y lze tzv. dobře uspořádat, což budeme rovněž definovat později.)

Analogický ke známým vlastnostem mocniny je též následující fakt.

Věta: ${}^x({}^yz) \approx^{x\times y} z$

Důkaz: Vzájemně jednoznačnou korespondenci prvků levé a pravé strany $\approx$ stanovíme tak, že zobrazení z x do funkcí z y do z, které vyznačíme indexem (f_t pro $t \in x$ je hodnota tohoto zobrazení v bodě t) je prvkem levé strany, přiřadíme funkci $g : x \times y \longrightarrow z$ (prvek pravé strany) definovanou předpisem $g(\langle t, u\rangle) = f_t(u)$ pro $u \in y$ a obráceně.

Za pomoci této věty (a věty Cantorovy a Bernsteinovy) dostaneme následující možná poněkud překvapivou rovnost.

Věta: Je-li $2 \le |x| \le 2^{|y|}$, pak $|x|^{|y|} = 2^{|y|}$.

Důkaz: Platí totiž $2^{|y|} \le \ |x|^{|y|} \le \ (2^{|y|})^{|y|} = 2^{|y|.|y|} = 2^{|y|}$.

Jako speciální důsledek uvedené rovnosti získáme $|\mathbb{R}|^{|\mathbb{N}|} = |\mathbb{R}|$, což využijeme dále.

Není divu, že tato podivuhodná struktura (kardinálních čísel) jejíž další překvapivé vlastnosti jsme neuvedli nachází velké uplatnění při konstrukci různých dalších matematických struktur.

Jako poslední příklad kardinální aritmetiky ukážeme, že spojitých funkcí na reálných číslech je stejně jako čísel reálných, zatímco všech funkcí je stejně jako $\mathcal{P}(\mathbb{R})$.

Věta: 1) $\{f;\ f$ *je spojitá na* $\mathbb{R}\} \approx \mathbb{R}$.
2) $\{f;\ f : \mathbb{R} \longrightarrow \mathbb{R}\} \approx \mathcal{P}(\mathbb{R})$.

Důkaz: 1) Každá konstantní funkce je spojitá, proto je spojitých funkcí neostře více než reálných čísel. Pro důkaz opačné nerovnosti si uvědomme, že ze spojitosti plyne, že funkční hodnota v limitě se rovná limitě funkčních hodnot a tedy spojitá funkce je určena svými hodnotami v racionálních číslech. (Každé reálné číslo je limitou racionálních čísel např. stále delších neúplných desetinných zápisů.) Racionální čísla však umíme očíslovat čísly přirozenými a za pomoci výše uvedené úvahy umíme tedy vnořit množinu všech spojitých funkcí do ${}^{\mathbb{N}}\mathbb{R}$. Již jsme však dokázali rovnost $|\mathbb{R}|^{|\mathbb{N}|} = |\mathbb{R}|$, což ukazuje požadovanou rovnost.

2) Všech podmnožin $\mathbb{R}$ je stejně jako všech jejich charakteristických funkcí, tedy neostře méně než všech funkcí. Na druhé straně víme, že každá funkce je částí $\mathbb{R} \times \mathbb{R}$, tedy všech funkcí je neostře méně než $2^{|\mathbb{R}\times\mathbb{R}|} = 2^{|\mathbb{R}|} = |\mathcal{P}(\mathbb{R})|$.

Přirozená čísla.

Protože teorie množin má být světem matematiky, musí být schopna v sobě vytvořit representanty (modely) všech matematických objektů. Tyto modely se pak mnohdy kanonisují, stávají se "těmi pravými matematickými objekty". Základním objektem, který v teorii množin zmodelujeme bude struktura přirozených čísel.

Velký italský matematik Giuseppe Peano charakterisoval přirozená čísla následujícími požadavky:

P1) 0 je přirozené číslo.
P2) Každé přirozené číslo n má jediného následovníka Sn.
P3) $Sn = Sm \rightarrow\ n = m$.
P4) 0 není následovník.
P5) Indukce (druhého řádu): Každá podmnožina přirozených čísel M, která má vlastnosti $0 \in M$ a $(\forall n)(n \in M \rightarrow Sn \in M)$ již obsahuje všechna přirozená čísla.

Tyto požadavky jsou tzv. kategorické, každé dvě struktury vyhovující těmto požadavkům jsou izomorfní (ukážeme později).

Protože uvedený požadavek indukce v sobě zahrnuje pojem množiny, který není ostatními požadavky dobře specifikován. (Místo množina je možno použít "libovolná matematická vlastnost". Podobné teorie se nazývají teoriemi druhého řádu a není jim přikládána v matematice taková důležitost jako námi vyšetřovaným teoriím prvního řádu.) Můžete se též setkat v literatuře s následující teorií prvního řádu popisující přirozená čísla, která se na počest Peana nazývá Peanova aritmetika. (Zaměňování této teorie s Peanovými požadavky však může vést k nedorozuměním.)

Jazyk Peanovy aritmetiky (PA) obsahuje konstantní symbol 0, unární funkční symbol S (následovník), dva binární funkční symboly $+$ a $\cdot$, binární relační symbol $=$ a někdy se

přidává binární relační symbol $<$. Axiomy této teorie jsou jednak obecné axiomy týkající se rovnosti.

R1) $x = x$

R2) $x = y \to F(\dots, x, \dots) = F(\dots, y, \dots)$ pro každý funkční symbol (tedy speciálně $x = y \to z + x = z + y$)

R3) $x = y \to (P(\dots, x, \dots) \to P(\dots, y, \dots))$ pro každý relační symbol.

Dále jsou to axiomy týkající se již zcela specificky aritmetiky.

N1) $Sx \neq 0$ N2) $Sx = Sy \to x = y$

N3) $x + 0 = x$ N4) $x + Sy = S(x + y)$

N5) $x \cdot 0 = 0$ N6) $x \cdot Sy = (x \cdot y) + x$

N7) $\neg(x < 0)$ N8) $x < Sy \equiv x < y \vee x = y$

(Poslední dva axiomy se uvádějí jen v případě, že $<$ je zahrnuta do základního jazyka PA.)

Schéma axiomů indukce: Pro každou formuli $\psi(n, x_1, \dots, x_k)$ je následující formule axiom $(\psi(0)\&(\forall n)(\psi(n) \to \psi(Sn))) \to (\forall n)\psi(n)$.

Tato teorie již není kategorická. (Žádná teorie prvního řádu, která má nekonečný model není kategorická.) Jí se však týkají známé Gödelovy výsledky o existenci nerozhodnutelné věty.

Nyní přistoupíme ke konstrukci množiny přirozených čísel v teorii množin. Použijeme přitom v mnohém způsobu uvedeného v studijních textech Josefa Mlčka z teorie množin.

Při konstrukci přirozených čísel (a později ordinálních čísel) v teorii množin se používá myšlenka Johna von Neumanna, přirozené (ordinální) číslo je množina všech čísel menších. Tedy 0 je v teorii množin jak prázdná množina, tak i číslo 0. Nadále budeme proto používat 0 i pro označení prázdné množiny. Množina $\{0\}$ je číslo 1, $\{0, \{0\}\}$ je číslo 2, atd. Tato reprezentace má tu výhodu, že přirozené číslo n (jeho model v teorii množin) má přesně n prvků. Takto můžeme postupně sestrojit model pro libovolné "skutečné" přirozené číslo. Přirozená čísla máme takto v možnosti (v potenci), nemáme je však všechna najednou aktualizovaná. Pro existenci nekonečné množiny (jakou je např. $\mathbb{N}$) používá B. Bolzano ve své knize Paradoxy nekonečna myšlenek v Boží mysli. My použijeme množiny zaručené axiomem nekonečna.

Definice: Řekneme, že množina x je *induktivní*, jestliže platí: $0 \in x \ \& \ (\forall t)(t \in x \to t \cup \{t\} \in x)$.

Axiom nekonečna tedy tvrdí, že existuje induktivní množina.

Definice: $\mathbb{N} = \bigcap\{x;\ x \text{ je induktivní}\}$ (množina přirozených čísel).

$\mathbb{N}$ je opravdu množina, neboť podle axiomu nekonečna nějaká induktivní množina existuje a výše uvedený průnik je proto množina.

Věta: $\mathbb{N}$ je induktivní množina. (Nejmenší v $\subseteq$ induktivní množina.)

Důkaz: 0 je v každé induktivní množině a proto je i v $\mathbb{N}$. Nechť $n \in \mathbb{N}$, pak n je v každé induktivní množině, tedy $n \cup \{n\}$ je v každé induktivní množině a proto $n \cup \{n\} \in \mathbb{N}$.

Definice: $n \cup \{n\}$ reprezentuje funkci *následovníka* (Sn) na $\mathbb{N}$ v teorii množin.

Věta (Princip matematické indukce): Nechť $X \subseteq \mathbb{N}$ je taková podmnožina $\mathbb{N}$, pro níž platí $0 \in X$ a $(\forall n)(n \in X \rightarrow\ n \cup \{n\} \in X)$. Pak $X = \mathbb{N}$.

Důkaz: X je induktivní množina, proto je nadmnožinou $\mathbb{N}$, která je průnikem všech induktivních množin. Je však také podmnožinou $\mathbb{N}$ podle předpokladu. Tedy platí $X = \mathbb{N}$.

Věta: Pro každá n, m z $\mathbb{N}$ platí:

1) $m \in n \rightarrow\ m \subseteq n$ 2) $m \in n \equiv\ m \subsetneq n$

3) $n \notin n$ 4) $m \in n \vee\ n = m \vee\ n \in m$

Důkaz: Třetí formule plyne bezprostředně z druhé, ostatní dokážeme postupně indukcí.

Pro $n = 0$ první formule platí. Nechť $m \in n \cup \{n\}$. Je-li $m = n$, pak $m \subseteq n \cup \{n\}$. Je-li $m \in n$, pak podle indukčního předpokladu $m \subseteq n \subseteq n \cup \{n\}$.

Pro $n = 0$ druhá formule platí. Nechť $m \in n \cup \{n\}$. Je-li $m \in n$, pak podle indukčního předpokladu $m \subsetneq n \subseteq n \cup \{n\}$. Je-li $m = n$, pak $m \subseteq n \subseteq n \cup \{n\}$ a protože $n \notin n$ podle 3) (toto tvrzení používáme pro n, což umožňuje indukční předpoklad) je inkluze ostrá. Nechť obráceně $m \subsetneq n \cup \{n\}$. Pokud by platilo $n \in m$, dostali bychom podle 1) $n \subseteq m$ a $n \cup \{n\} \subseteq m \subsetneq n \cup \{n\}$, což není možné. Je tedy $m \subseteq n$. Je-li $m \subsetneq n$ dostáváme z indukčního předpokladu $m \in n \subseteq n \cup \{n\}$. Pokud $n = m$, platí $m \in n \cup \{n\}$.

Čtvrtá formule pro $n = 0$ $(m \in 0\ \vee\ 0 = m\ \vee\ 0 \in m)$ platí, neboť první část disjunkce neplatí nikdy, a pokud $0 \neq m$, pak $0 \subsetneq m$ odkud plyne třetí část disjunkce podle tvrzení 2). Dokážeme indukční krok. Z prvních dvou částí indukčního předpokladu plyne $m \in n \cup \{n\}$. Z $n \in m$ plyne $n \subseteq m$ (podle 1)), tedy $n \cup \{n\} \subseteq m$. Je-li $n \cup \{n\} \subsetneq m$, je $n \cup \{n\} \in m$ (tedy i dokazovaná disjunkce). Je-li $n \cup \{n\} = m$, pak dokazovaná disjunkce opět platí.

Uvedené čtyři vlastnosti ukazují, že základní množinové relace $\in$ a $\subsetneq$ obě reprezentují přirozené ostré uspořádání na $\mathbb{N}$. Neostré uspořádání je pak reprezentováno $\subseteq$.

Nyní jsme schopni ukázat, že kanonický model $\mathbb{N}$ spolu s následovníkem reprezentovaným $n \cup \{n\}$ splňuje Peanovy požadavky. První dva (0 je přirozené číslo a každé přirozené číslo má jediného následovníka) jsou splněny bezprostředně. Ukažme třetí požadavek ($Sn = Sm \rightarrow n = m$). Nechť tedy $n \cup \{n\}\ = m \cup \{m\}\ \&\ n \neq m$. Za využití trichotomie (vlastnost 4) z předešlé věty) dostáváme $m \in n \vee n \in m$. Předpokládejme (bez újmy na obecnosti) $m \in n$, pak (podle 1)) máme $m \subseteq n$, dále $m \cup \{m\} \subseteq n \subsetneq n \cup \{n\}$ ve sporu s předpokladem. Čtvrtý požadavek (0 není následovník) plyne okamžitě z faktu, že následovník v $\mathbb{N}$ je neprázdná množina. Indukce je v obou případech formulována stejně.

Operace sčítání a násobení na $\mathbb{N}$

.

Operace $+$ a $\cdot$ (popřípadě i mocnění) zavedeme na $\mathbb{N}$ stejně jako na kardinálních číslech. Je to mnohem jednodušší (zvláště v důkazech komutativních, asociativních a distributivních zákonů), než alternativní způsob zavedení $+$ a $\cdot$ jako opakovaného následovníka a opakovaného sčítání (což použijeme pro ordinální čísla). Budeme k tomu potřebovat pouze následující tři tvrzení.

Věta: 1) $(\forall m, n)(m \approx n\ \rightarrow\ m = n)$.

2) $(\forall m, n)(\exists k)((\{0\} \times m\ \cup\ \{1\} \times n) \approx k)$.

3) $(\forall m, n)(\exists k)((n \times m) \approx k)$.

Důkaz: Všechna tvrzení dokážeme indukcí. Nejdříve indukcí dokažme $(\forall n)(n \neq 0 \to (\exists m)(n = m \cup \{m\}))$. Položme $X = \{n;\ (n \neq 0 \to (\exists m)(n = m \cup \{m\}))\}$. Platí $0 \in X$, protože předpoklad implikace není splněn. Je-li $n \in X$, pak $n \cup \{n\} \in X$, stačí položit $m = n$ (předpoklad $n \in X$ jsme ani nepotřebovali). Tím je indukcí dokázáno $X = \mathbb{N}$ a tvrzení platí.

Dokažme 1). Pro $n = 0$ tvrzení platí, neboť $m \approx 0 \to m = 0$. Platí-li $n \cup \{n\} \neq 0$, tedy i $m \neq 0$ a rovnou jej pišme ve tvaru $m \cup \{m\}$. Nechť $f : n \cup \{n\} \longleftrightarrow m \cup \{m\}$. Pokud $f(n) = m$, platí $f : n \longleftrightarrow m$ a podle indukčního předpokladu platí $n = m$, tedy $n \cup \{n\} = m \cup \{m\}$. Pokud $f(n) \neq m$, pozměníme definici f v bodech n a $f^{-1}(m)$ tak, že definujeme $g(n) = m$, $g(f^{-1}(m)) = f(n)$ a $g(t) = f(t)$ jinak. Pak postupujeme jako v předešlém případě.

Dokažme 2). Pro $n = 0$ je hledaným k číslo m. Je-li $(\{0\} \times m \ \cup \ \{1\} \times n) \approx k$, pak $(\{0\} \times m \ \cup \ \{1\} \times (n \cup \{n\})) = (\{0\} \times m \ \cup \ \{1\} \times n) \ \cup \ \{1\} \times \{n\} \approx k \cup \{k\}$

Dokažme 3). Pro $n = 0$ tvrzení platí, neboť hledaným k je 0. Je-li $m \times n \approx k$, pak $m \times (n \cup \{n\}) = (m \times n) \ \cup \ (m \times \{n\}) \approx k + m$

Početní zákony pro $+$ a $\cdot$ jsou bezprostředně zřejmé ze zavedení operací a příslušných zákonů pro množinové operace (např. distributivního zákona pro $\times$ a $\cup$).

Konstrukce rekurzí.

Např. funkci $n!$ jste zaváděli předpisem $n! = n \cdot (n-1) \cdot (n-2) \ldots 2 \cdot 1$. Tento předpis vám sice dává porozumění pro definici např. 5!, nedává vám však žádný návod jak funkci $n!$ zavést jako množinový objekt. (Teorie množin, má-li být základní matematickou teorií musí být schopna i takovéto objekty v sobě modelovat.) Konstrukce rekurzí dává možnost zavést podobně definované objekty do teorie množin. Než přistoupíme k formulaci a důkazu příslušné věty, uveďme ještě dvě další formulace principu indukce, které budou pro důkaz věty o konstrukci rekurzí lépe použitelné.

Věta: 1) (Princip ordinální indukce) Nechť pro $X \subseteq \mathbb{N}$ platí $(\forall n)(n \subseteq X \to \ n \in X)$, pak $X = \mathbb{N}$.

2) (Princip nejmenšího prvku) Nechť $X \subseteq \mathbb{N}$ & $X \neq 0$, pak $(\exists n)(n \in X \ \& \ n \cap X = 0)$, t.j. n je nejmenší prvek (v přirozeném uspořádání $\mathbb{N}$, což je $\in$) X.

Důkaz: Nejdříve ukážeme, že 1) a 2) jsou ekvivalentní. Položme $Y = \mathbb{N} - X$. 1) přepišme tak, že obě strany implikace (která je tvrzením) znegujme a implikaci otočme (což je ekvivalentní úprava). Dostaneme $X \neq \mathbb{N} \ \to \ (\exists n)(n \subseteq X \ \& \ n \notin X)$, což je přesně tvrzení 2) pro Y.

Nyní dokažme 1). Položme $Y = \{n;\ n \subseteq X\}$. Z předpokladů 1) dokážeme, že Y splňuje předpoklady indukce. $0 \in Y$, neboť samozřejmě $0 \subseteq X$. Nechť $n \in Y$, tedy $n \subseteq X$ (podle definice Y), tedy $n \in X$ (podle předpokladu tvrzení 1)), tedy $n \cup \{n\} \subseteq X$, tedy $n \cup \{n\} \in Y$. Protože Y splňuje předpoklady indukce, platí $Y = \mathbb{N}$. Z toho ukážeme, že i $X = \mathbb{N}$. Nechť $n \in \mathbb{N}$ je libovolné, pak $n \cup \{n\} \in Y$, tedy $n \cup \{n\} \subseteq X$, tedy $n \in X$.

Poznamenejme, že naopak z 1) nebo z 2) spolu s tvrzením, že každé nenulové přirozené číslo je následovníkem lze základní verzi matematické indukce dokázat.

Nyní přistupme ke konstrukci rekurzí v rámci teorie množin.

Věta (O konstrukci rekurzí): Buď G všude definovaná funkce. Pak existuje jediná funkce f taková, že $dom(f) = \mathbb{N}$ a $(\forall n)(f(n) = G(f \restriction n))$.

Důkaz: Položme $f = \bigcup\{g;\ (dom(g) \in \mathbb{N})\ \&\ ((\forall n \in dom(g))(g(n) = G(g \restriction n))\}$. Ukážeme, že f je hledaná funkce. Označme M množinu (částečných funkcí) jejímž sjednocením je f.

Ukážeme, že parciální funkce z M prodlužují jedna druhou, tedy $\bigcup M$ je funkce. Nechť $g_1, g_2 \in M$ jsou takové funkce, že $dom(g_1) \subseteq dom(g_2)$, pak $g_1 \subseteq g_2$. Pokud by totiž existovalo k takové, že $g_1(k) \neq g_2(k)$, muselo by (podle principu nejmenšího prvku) existovat takové k nejmenší, což by znamenalo $g_1 \restriction k = g_2 \restriction k$, tedy $g_1(k) = G(g_1 \restriction k) = G(g_2 \restriction k) = g_2(k)$, ve sporu s předpokladem. $\bigcup M$ je proto funkce.

Ukážeme, že $dom(\bigcup M) = \mathbb{N}$. K tomu stačí ukázat, že $(\forall n)(\exists g \in M)(dom(g) = n)$. Nechť k je nejmenší takové, že pro něj $g \in M$ neexistuje, pak $\bigcup M$ je funkce splňující rekurentní podmínku $((\forall n \in dom(g))(g(n) = G(g \restriction n)))$ definovaná pro všechny prvky k, tedy na k, tato funkce musí být prvkem M a její definiční obor je k, ve sporu s předpokladem. Proto platí $dom(\bigcup M) = \mathbb{N}$.

Jednoznačnost f se ukáže analogicky jako jsme ukázali, že funkce z M mají stejné hodnoty.

Funkce $f(n) = n!$ se nadefinuje větou o konstrukci rekurzí tak, že definujeme konstruující funkci G následujícím předpisem. $G(0) = 1$, $G(x) = max(rng(x)) \cdot dom(x)$, pokud má pravá strana (v rámci $\mathbb{N}$) smysl, $G(x) = 0$ jinak.

Nyní ukážeme, že libovolné dvě množinové struktury vyhovující Peanovým požadavkům jsou izomorfní. Ukážeme totiž následující větu.

Věta: Nechť $\langle \mathcal{N}, \mathcal{O}, \mathcal{S}\rangle$ je množinová struktura vyhovující Peanovým požadavkům, pak existuje izomorfismus f struktury $\langle \mathbb{N}, 0, n \cup \{n\}\rangle$ a této struktury.

Důkaz: Izomorfizmus f sestrojíme konstrukcí rekurzí. Definujme konstruující funkci G následovně: $G(0) = \mathcal{O}$, $G(x) = \mathcal{S}x(max(dom(x)))$, pokud má pravá strana smysl, $G(x) = 0$ jinak.

Dokažme že f je izomorfizmus $\mathbb{N}$ a $\mathcal{N}$. Nejdříve se indukcí (v $\mathcal{N}$) dokáže $(\forall \mathfrak{n} \in \mathcal{N})(\mathfrak{n} \neq \mathcal{O} \rightarrow (\exists \mathfrak{m} \in \mathcal{N})(\mathfrak{n} = \mathcal{S}\mathfrak{m}))$ analogicky, jako jsme to dokázali pro $\mathbb{N}$.

Dále dokažme, že f je prostá. Nechť m je nejmenší takové, že pro některé větší n platí $f(m) = f(n)$. Nechť nejdříve $f(m) = \mathcal{O}$. Protože $n \neq 0$, existuje l takové, že $n = l \cup \{l\}$. Podle konstrukce f pak máme $\mathcal{O} = f(n) = \mathcal{S}f(l)$ ve sporu s Peanovým požadavkem ($\mathcal{O}$ není následovník). Je-li $f(n) \neq \mathcal{O}$, tedy $m \neq 0$, existuje také k takové, že $m = k \cup \{k\}$. Podle konstrukce f pak platí $f(m) = \mathcal{S}f(k) = \mathcal{S}f(l) = f(n)$. Podle Peanova požadavku $(\mathcal{S}\mathfrak{m} = \mathcal{S}\mathfrak{n} \rightarrow \mathfrak{m} = \mathfrak{n})$, plyne odtud $f(k) = f(l)$, ve sporu s minimalitou m. Tím je prostota f ukázána.

Dokažme nyní, že f zobrazuje $\mathbb{N}$ na $\mathcal{N}$. Nechť $X = rng(f)$. Pak $\mathcal{O} = f(0) \in X$ a pokud $\mathfrak{n} \in X$, tedy $\mathfrak{n} = f(n)$ pro nějaké n, je $\mathcal{S}\mathfrak{n} = f(n \cup \{n\}) \in X$ (podle konstrukce f). X splňuje předpoklady indukce (v $\mathcal{N}$) a proto platí $X = \mathcal{N}$.

Zbývá dokázat, že $f(0) = \mathcal{O}$ a $\mathcal{S}f(n) = f(n \cup \{n\})$, což však bezprostředně plyne z konstrukce f.

Konečné množiny.

Definice: Množina x je *konečná* (značíme $Fin(x)$), jestliže $(\exists n \in \mathbb{N})(x \approx n)$.

V literatuře lze nalézt mnoho ekvivalentních definic konečnosti. Nejznámější z nich jsou definice Tarského a definice Dedekindova. Tarského definice je

$Fin_{Tar}(x) \equiv (\forall y)((y \subseteq \mathcal{P}(x) \ \& \ y \neq 0) \rightarrow (\exists t)(t \in y \ \& \ t$ *je minimální (vzhledem* $k \subseteq$*)* $v\ y)$.

Dedekindova definice je

$Fin_{Ded}(x) \equiv \neg(\exists y)(y \subsetneq x \ \& \ y \approx x)$.

Tarského definice je ekvivalentní námi uvedené definici. Má však tu výhodu, že je zapsána množinovou formulí, která se neodvolává na žádnou zvláštní strukturu (my se v definici odvoláváme na $\mathbb{N}$). Dedekindova definice je formálně jednodušší než Tarského, rovněž se neodvolává na žádnou zvláštní strukturu, je však ekvivalentní Tarského definici jen za předpokladu axiomu výběru. (Je zmodelována teorie množin bez axiomu výběru, ve které je nekonečná množina x taková, že $Fin_{Tar}(x)$).

V dalším ukážeme, že z množin, které jsou konečné a jejichž prvky jsou konečné a prvky těchto prvků jsou konečné atd. (toto se formálně přesně vyjádří tak, že tzv. univerzum x je konečné) nemůžeme množinovými operacemi získat nekonečnou množinu. (Množina všech právě uvedených množin x - tzv. dědičně konečných množin tvoří model teorie množin ve které je nahrazen axiom nekonečna jeho negací.)

Věta: 0 a $\{x\}$ jsou konečné množiny.

Věta: 1) $(Fin(x) \ \& \ y \subseteq x) \rightarrow Fin(y)$.

2) $(Fin(x) \ \& \ Fin(y) \rightarrow Fin(x \cup y)$.

Důkaz: Důkaz (jako všechny důkazy v tomto oddílu) bude probíhat indukcí podle počtu prvků.

1) Pro $x = 0$ tvrzení platí, neboť $y = 0$. Je-li $y \subseteq x \cup \{t\}$, kde $t \notin x$, pak buď $y \subseteq x$ a $Fin(y)$ podle indukčního předpokladu, nebo $y = z \cup \{t\}$ & $z \subseteq x$ a $Fin(z)$ podle indukčního předpokladu. Tedy $z \approx k$ pro vhodné přirozené číslo k a $y \approx k + 1$.

2) Můžeme bez újmy na obecnosti předpokládat, že $x \cap y = 0$ (jinak budeme místo y uvažovat $y - x$, které je podle 1) konečné). Pak $x \approx k$ a $y \approx m$ pro vhodná $k, m \in \mathbb{N}$ a tedy $y \cup x \approx m + k$.

Uvedené dvě vlastnosti říkají, že konečné množiny mají vlastnost ideálu množin. (Pro souvislost s ostatními oblastmi matematiky připomeňme, že část I okruhu O se nazývá ideál, jestliže $x, y \in I \rightarrow x + y \in I$ a $x \in I \ \& \ y \in O \rightarrow x \,.\, y \in I$. Uvažujeme-li $\cup$ jako $+$ a $\cap$ jako $.$ získáme námi uvedený pojem.)

Dále ukážeme, že sjednocení konečné množiny konečných množin je konečná množina.

Věta: $(Fin(x) \ \& \ (\forall t)(t \in x \rightarrow Fin(t))) \rightarrow Fin(\bigcup x)$

Důkaz: Pro $x = 0$ je $\bigcup x = 0$ a tvrzení platí. Pro $Fin(t)$ & $t \notin x$ platí $\bigcup(x \cup \{t\}) = \bigcup x \cup t$. Při tom $\bigcup x$ je konečná množina podle indukčního předpokladu a sjednocení dvou konečných množin je konečná množina.

Dále ukážeme, že obraz konečné množiny je konečný.

Věta: $Fin(x) \ \& \ y = f"x \rightarrow Fin(y)$.

Důkaz: Bez újmy na obecnosti můžeme předpokládat, že $dom(f) = x$ ($Fin(dom(f) \cap x)$ podle 1)). Na x uvažujme rozklad podle ekvivalence $\sim$, definované předpisem $t \sim u \equiv f(t) =$

$f(u)$. Nechť $z \subseteq x$ je množina nejmenších prvků tříd ekvivalence $\sim$, tedy z je konečná a $y \approx z \approx k$, pro vhodné $k \in \mathbb{N}$, neboť $f : z \longleftrightarrow y$.

Věta: $Fin(x) \to Fin(\mathcal{P}(x))$.

Důkaz: Pro $x = 0$ tvrzení platí. Nechť $t \notin x$, pak $\mathcal{P}(x \cup \{t\}) = \mathcal{P}(x) \cup \{u; (\exists v)(v \in \mathcal{P}(x)\ \&\ u = v \cup \{t\})\}$ a množina na pravé straně $\cup$ je bijekcí $\mathcal{P}(x)$. $\mathcal{P}(x)$ je konečná podle indukčního předpokladu, její obraz je konečný podle předešlé věty a sjednocení dvou konečných množin je konečná množina.

Protože dvojice je konečná množina, ukázali jsme, že analogony všech tvrzení axiomů ZFC (existence výběrové funkce pro konečnou množinu se dá také dokázat indukcí) s vyjímkou axiomu nekonečna platí pro dědičně konečné množiny. Nekonečnou množinu jsme nemohli žádnými množinovými operacemi z dědičně konečných získat a axiom nekonečna byl proto pro existenci nekonečné množiny opravdu nutný.

Nyní ještě ukážeme, že konečné množiny jsou též dedekindovsky konečné.

Věta: $(Fin(x)\ \&\ y \subsetneq x) \ \to\ \neg(\exists f)(f : x \longleftrightarrow y)$.

Důkaz: Pro $x = 0$ tvrzení platí, neboť 0 nemá žádné vlastní podmnožiny. Dokažme indukční krok. Nechť pro x tvrzení platí, $t \notin x$ a pro nějaké $y \subsetneq x \cup \{t\}$ existuje funkce f taková, že $f : x \cup \{t\} \longleftrightarrow y$. Nechť nejdříve $f(t) = t$, tedy $t \in y$ a $y - \{t\}$ je vlastní podmnožina x, která je obrazem x při bijekci f ve sporu s indukčním předpokladem. Pokud $f(t) \neq t$, předefinujeme f analogicky jako v definici + na $\mathbb{N}$ ($g(t) = t$ & $g(f^{-1}(t)) = f(t)$ a $g(u) = f(u)$ jinak).

Spočetné množiny.

V tomto oddíle ukážeme, že spočetné množiny jsou (podobně jako konečné) v jistém smyslu "malé".

Definice: 1) Řekneme, že množina x je *spočetná*, pokud $x \approx \mathbb{N}$.

2) Řekneme, že množina x je *nejvýše spočetná*, pokud je konečná, nebo spočetná.

3) Řekneme, že množina x je *nespočetná*, pokud není nejvýše spočetná.

Věta: 1) Je-li x nejvýše spočetná a $y \subseteq x$, pak y je nejvýše spočetná.

2) Jsou-li x a y nejvýše spočetné, je i $x \cup y$ nejvýše spočetná.

Důkaz: 1) Pokud je x konečná je i y konečná. Pokud je x spočetná, stačí tvrzení dokázat pro $x = \mathbb{N}$ (bijekcí se konečnost i spočetnost přenese). Nechť tedy $y \subseteq \mathbb{N}$. Pomocí konstrukce rekurzí zkonstruujeme zobrazení f následovně. Položme $G(u) =$ nejmenší (v $\in$) prvek $y - rng(y)$, pokud takové existuje (příslušná množina je neprázdná) a $G(u) = \{\{0\}\}$ jinak. Nechť f je funkce takto nadefinovaná rekurzí. Pokud f nenabyde hodnoty $\{\{0\}\}$, je f bijekce $\mathbb{N}$ a y, pokud n je nejmenší přirozené číslo takové, že $f(n) = \{\{0\}\}$, pak f je bijekce n a y.

2) Vzhledem k 1) můžeme bez újmy na obecnosti předpokládat, že x a y jsou disjunktní ($x \cup y = x \cup (y - x)$). Jsou-li obě konečné, je konečné i sjednocení. Jinak x a y lze vnořit do dvou exemplářů $\mathbb{N}$ a tedy jejich sjednocení lze vnořit do $\mathbb{N}$ (podle toho, jak jsme počítali s kardinály).

Věta: Obraz nejvýše spočetné množiny x je nejvýše spočetná množina.

Důkaz: Pokud je x konečná množina, je i její obraz konečný. Je-li x spočetná, stačí tvrzení

dokázat pro $x = \mathbb{N}$ (bijekcí se konečnost i spočetnost zachová). Nechť $\sim$ je ekvivalence popsaná předpisem $t \sim u \ \equiv \ f(t) = f(u)$. Položme $z = \{t \in \mathbb{N};\ t$ *je nejmenší* $(v \in)$ *prvek třídy ekvivalence* $\sim\}$. Pak $z \subseteq \mathbb{N}$, tedy je z nejvýše spočetná a f je bijekce z a $f"\mathbb{N}$.

Věta: Je-li x nejvýše spočetná a každý její prvek je nejvýše spočetný, pak $\bigcup x$ je nejvýše spočetná množina.

Důkaz: V důkazu se podstatně využije axiom výběru. Je-li x konečná, dokáže se tvrzení (bez pomoci axiomu výběru) indukcí podle počtu prvků. Dále můžeme bez újmy na obecnosti předpokládat, že prvky x jsou navzájem disjunktní. Je-li totiž $x = \{x_i;\ i \in \mathbb{N}\}$ očíslování prvků x, pak $\bigcup x = \bigcup\{y_i;\ i \in \mathbb{N}\}$, kde $y_i = x_i - \bigcup\{x_k;\ k \in i\}$. Předpokládejme tedy nadále, že x_i jsou navzájem disjunktní. Nechť $\mathcal{F}_i$ označuje množinu všech bijekcí $\mathbb{N}$ (popřípadě přirozeného čísla $\approx x_i$) a x_i. $\{\mathcal{F}_i;\ i \in \mathbb{N}\}$ je množina neprázdných množin a podle axiomu výběru na ní existuje selektor. Nechť f_i označuje bijekci vybranou z $\mathcal{F}_i$. Každý prvek $\bigcup x$ je tvaru $f_i(j)$, kde $j \in dom(f_i) \subseteq \mathbb{N}$. Tomuto prvku přiřaďme dvojici $\langle i, j\rangle$. Takto jsme popsali vnoření $\bigcup x$ do $\mathbb{N} \times \mathbb{N}$ a tím dokázali spočetnost $\bigcup x$.

Použití axiomu výběru v důkazu předešlé věty bylo podstatné, neboť je dokázána bezespornost teorie množin bez axiomu výběru, ve které je množina reálných čísel $\mathbb{R}$ sjednocením spočetné množiny spočetných množin a $\mathbb{R}$ je nespočetná, jak jsme již dokázali.

Na rozdíl od konečných množin se z nejvýše spočetných množin množinovými operacemi dostaneme, neboť jsme již dokázali, že $\mathcal{P}(\mathbb{N})$ je nespočetná.

Ordinální čísla.

Čtenář si už asi povšiml, že indukce a konstrukce rekurzí jsou velmi mocné matematické nástroje, a proto se matematici snažili rozšířit užití těchto nástrojů co nejdále do nekonečna. Právě toto umožňují ordinální čísla. Připomeňme čtyři základní vlastnosti přirozených čísel (1) $m \in n \rightarrow \ m \subseteq n$, 2) $m \in n \equiv \ m \subsetneq n$, 3) $n \notin n$ a 4) $m \in n \vee \ n = m \vee \ n \in m$) a další formulace indukce (princip nejmenšího prvku a ordinální verzi indukce). Odtud vychází následující definice ordinálů. Nejdříve však definujme, co je dobré uspořádání.

Definice: Řekneme, že uspořádání $\langle a, <\rangle$ je *dobré*, jestliže platí, že každá neprázdná podmnožina a má nejmenší prvek. $((\forall b)((b \subseteq a \ \&\ b \neq 0) \rightarrow (\exists t)(t \in b \ \&\ (\forall u)(u \in b \rightarrow t \leq u)))$.

Definice: $Ord(X)$ (třída X je *ordinál*), jestliže

1) $(\forall t)(t \in X \rightarrow t \subseteq X)$ (X je úplná - $Comp(X)$).

2) $\in$ je na X ostré dobré uspořádání $(\forall t, u \in X)(t \in u \vee t = u \vee u \in t)$ & $(\forall B \subseteq X)(\exists t \in B)(t \cap B = 0))$.

Připomeňme, že vlastnost 1) je přesnou reformulací vlastnosti 1) přirozených čísel a vlastnost 2) je reformulací vlastnosti 4) přirozených čísel spolu s principem dobrého uspořádání. Odtud plyne, že každé přirozené číslo je ordinál a že též množina přirozeených čísel je ordinál. Množiny, které jsou ordinály nazýváme ordinální čísla a označujene je malými písmeny řecké abecedy. Třídu ordinálních čísel značíme On.

Definice: $On = \{\alpha; Ord(\alpha)\}$ (třída všech *ordinálních čísel*).

Třída ordinálních čísel rozšiřuje (do nekonečna) množinu přirozených čísel $\mathbb{N}$, neboť $\mathbb{N}$ je ordinální číslo (značí se ω). Zanedlouho ukážeme, že On není množina (je to vlastní třída),

a tedy rozšiřuje $\mathbb{N}$ do těch největších nekonečen.

Věnujme se nyní zkoumání ordinálních čísel. Stejně jako u přirozených čísel je u ordinálních čísel zachována von Neumannova myšlenka, že ordinální číslo je množina všech menších ordinálních čísel.

Věta: 1) $(\forall\alpha)(\alpha \in On \to (\forall\beta)(\beta \in \alpha \to \beta \in On))$ (Každý prvek ordinálního čísla je ordinální číslo - ordinální číslo je množina všech menších ordinálních čísel.)

2) $(\forall\alpha)(\alpha \in On \to \alpha \cup \{\alpha\} \in On)$ (Následovník ordinálního čísla.)

3) $(\forall\alpha,\beta)(\alpha,\beta \in On \to \alpha \cap \beta \in On)$

4) $(\forall\alpha,\beta)(\alpha,\beta \in On \to (\alpha \in \beta \vee \alpha = \beta \vee \beta \in \alpha))$ ($\in$ je lineární uspořádání na On.)

Důkaz: 1) Dokážeme úplnost β. Nechť $\gamma \in \beta$. Máme dokázat, že $(\forall\delta \in \gamma)(\delta \in \beta)$. Z úplnosti α a tranzitivity $\in$ na α plyne $\gamma,\delta \in \alpha$ & $\delta \in \beta$. Protože $\in$ je ostré dobré uspořádání α a β je podmnožina α, je $\in$ ostré dobré uspořádání β.

2) Dokážeme úplnost $\alpha \cup \{\alpha\}$. Je-li $\beta \in \alpha \cup \{\alpha\}$, pak buď $\beta \in \alpha$ a tedy $\beta \subseteq \alpha \subseteq \alpha \cup \{\alpha\}$, nebo $\beta = \alpha \subseteq \alpha \cup \{\alpha\}$. Nyní ukažme, že $\in$ je dobré uspořádání $\alpha \cup \{\alpha\}$. Víme, že $\in$ je dobré uspořádání na α, dále víme, že každý prvek α je v $\in$ pod α, tedy víme, že antireflexivita $\in$ na α platí. Kdyby platilo $\alpha \in \alpha$, bylo by α prvkem sama sebe, ve sporu s antireflexivitou $\in$ na α. (Antireflexivita $\in$ na V je důsledkem axiomu regularity, my ji zde dokazujeme zvlášť, neboť se zkoumají též teorie množin bez tohoto axiomu.) Tranzitivita $\in$ je přímý důsledek úplnosti. Zbývá dokázat podmínku nejmenšího prvku. Nechť $x \subseteq \alpha \cup \{\alpha\}$ & $x \neq 0$. Je-li $x \cap \alpha \neq 0$, pak nejmenší prvek x vzhledem k α je i nejmenším prvkem vzhledem k $\alpha \cup \{\alpha\}$. Je-li $x = \{\alpha\}$, je α nejmenší prvek x.

3) To, že průnik dvou úplných množin je úplná množina plyne přímo z definice úplnosti. To, že $\in$ je ostré dobré uspořádání na průniku, je důsledkem toho, že vlastnost být dobrým uspořádáním se přenáší na části (je to tzv. dědičná vlastnost).

4) Nechť $\alpha \neq \beta$, tedy $\Delta(\alpha,\beta) \neq 0$. Nechť např. $\beta - \alpha = \beta - (\alpha \cap \beta) \neq 0$. Nechť β_1 je nejmenší prvek $\beta - \alpha$. Pak pro každé $\gamma \in \beta$ platí $\gamma \in \beta_1 \equiv \gamma \in \alpha \cap \beta$, tedy $\beta_1 = \alpha \cap \beta$. Kdyby též platilo $\alpha - \beta \neq 0$, zvolili bychom analogicky α_1 nejmenší prvek $\alpha - \beta$ a ukázali $\alpha_1 = \alpha \cap \beta = \beta_1$, tedy $\alpha_1 = \beta_1 \in \alpha \cap \beta$ ve sporu s volbou $\alpha_1,\beta_1 \in \Delta(\alpha,\beta)$. Celkem tedy máme $\alpha - \beta = 0$, tedy $\alpha = \alpha \cap \beta = \beta_1 \in \beta$. Případ $\alpha - \beta \neq 0$ je analogický. Tím je dokázána požadovaná trichotomie.

Věta: $Ord(On)$. (On je ordinál.)

Důkaz: Každé ordinální číslo je množina všech (v $\in$) menších ordinálních čísel, tedy je částí On (úplnost On).

Relace $\in$ je antireflexivní na On (již dokázáno), tranzitivita $\in$ na On plyne z úplnosti každého ordinálního čísla. Zbývá ověřit vlastnost nejmenšího prvku. Nechť $X \subseteq On$ & $X \neq 0$. Nechť $\alpha \in X$, pokud $\alpha \cap X = 0$, je α hledaný nejmenší prvek. Jinak je nejmenším prvkem X nejmenší prvek $\alpha \cap X$ (za využití již dokázané trichotomie), jehož existence plyne z $Ord(\alpha)$.

Věta: On není množina.

Důkaz: Kdyby On byla množina, byla by ordinálním číslem, tedy svým prvkem ve sporu s $\in$ je ostré dobré uspořádání.

K důkazu následující věty použijeme opět princip nejmenšího prvku.

Věta: Je-li f izomorfizmus (vzhledem k $\in$) ordinálních čísel α a β (tedy f je bijekce a $\gamma \in \delta \equiv f(\gamma) \in f(\delta)$), pak $\alpha = \beta$ a f je identita.

Důkaz: Dovedeme ke sporu existenci takového neidentického izomorfizmu f. Nechť γ je nejmenší ordinální číslo takové, že $\delta = f(\gamma) \neq \gamma$. Pak nutně $\gamma \in \delta$, neboť $\delta \in \gamma$ by znamenalo $\delta = f(\delta)$ v rozporu s volbou δ. Nechť $\kappa \in \delta - \gamma$, pak $\lambda = f^{-1}(\kappa) \in \gamma \subseteq \kappa$ (neboť f je izomorfizmus). Ale $\kappa(\in \delta - \gamma) = f(\lambda) \neq \lambda(\in \gamma)$ ve sporu s minimalitou γ.

Uvedená věta ukazuje na specifickou vlastnost ordinálních čísel. Např. na reálných číslech existuje mnoho izomorfizmů (vzhledem k přirozenému uspořádání). Jedním takovým je násobení číslem 2. Je přitom podstatné, že f je izomorfizmus. Nestačí, že f je bijekce, neboť např. $\omega + 1 = \mathbb{N} \cup \{\mathbb{N}\} \approx \omega$, neboť obě množiny jsou spočetné.

Připomeňme, že pro přirozená čísla jsme dokázali, že princip nejmenšího prvku je ekvivalentní principu ordinální indukce. Analogicky se ukáže, že již dokázaný princip nejmenšího prvku na On je ekvivalentní následujícímu principu transfinitní indukce.

Věta (Princip transfinitní indukce): Nechť $X \subseteq On$ má vlastnost $(\forall \alpha \in On)(\alpha \subseteq X \rightarrow \alpha \in X)$ pak $X = On$.

Následující věta je přesnou reformulací věty o konstrukci rekurzí pro On (místo $\mathbb{N}$).

Věta (Princip konstrukce transfinitní rekurzí): Nechť G je všude definovaná třídová funkce (funkce popsaná množinovou formulí). Pak existuje (je popsána množinovou formulí vytvořenou z popisu G) právě jedna funkce F taková, že $dom(F) = On$ & $(\forall \alpha \in On)(F(\alpha) = G(F \restriction \alpha))$.

Důkaz: Analogicky jako v důkazu věty o konstrukci rekurzí položíme $F = \bigcup\{f;\ dom(f) \in On$ & $(\forall \alpha \in dom(f))(f(\alpha) = G(f \restriction \alpha))\}$. Označíme-li $\mathcal{F}$ právě uvedenou třídu (jejímž sjednocením je F), ukážeme pomocí principu nejmenšího prvku, že funkce z $\mathcal{F}$ prodlužují jedna druhou (tedy sjednocení $\mathcal{F}$ je funkce) a pro každé ordinální číslo α existuje $f \in \mathcal{F}$ taková, že $dom(f) = \alpha$ (tedy $dom(F) = On$). Formule popisující F je $\langle \alpha, x\rangle \in F \equiv (\exists f \in \mathcal{F})(\langle \alpha, x\rangle \in f)$, kde v popisu $\mathcal{F}$ se uvede místo G formule popisující G.

Konstrukce transfinitní rekurzí a transfinitní indukce jsou mocné matematické prostředky, které nám umožňují pracovat s velkými nekonečny tak, jako by to byla "téměř" přirozená čísla. Jako první aplikaci ukážeme, že každé množinové dobré uspořádání je izomorfní nějakému ordinálnímu číslu.

Věta: Ke každému množinovému dobrému uspořádání $\langle a, <\rangle$ existuje jediné ordinální číslo α a jediný izomorfizmus f uspořádaných množin $\langle \alpha, \in\rangle$ a $\langle a, <\rangle$.

Důkaz: Dokažme nejdříve existenci f. Nechť $c \notin a$. Definujme konstruující funkci G následujícím předpisem. $G(x) = \textit{nejmenší prvek}\ a - rng(x)$, pokud $a - rng(x) \neq 0$, $G(x) = c$ jinak. Nechť F je funkce vykonstruovaná G větou o konstrukci transfinitní rekurzí. Ukážeme, že pokud $F(\alpha), F(\beta) \in a$, platí $\alpha \in \beta \equiv F(\alpha) < F(\beta)$. Postupujme sporem. Nechť $\alpha \in \beta$ & $F(\beta) = min\{F(\alpha), F(\beta)\}$. Pak $F(\beta) \in a - rng(F \restriction \alpha)$ a $F(\beta) < F(\alpha)$ ve sporu s volbou $F(\alpha) = min(a - rng(F \restriction \alpha))$. Nyní ukážeme, že existuje α takové, že $F(\alpha) = c$. Postupujeme opět sporem. Kdyby pro žádné $\alpha \in On$ rovnost $F(\alpha) = c$ nenastala, byla by F prostá funkce na celém On podle dříve dokázaného. Podle schématu axiomů vydělení by $rng(F) \subseteq a$ byla množina a podle schématu axiomů nahrazení by $On = F^{-1}$"$rng(F)$ byla množina, my jsme však již dokázali, že On množina není. (Postupný proces vybírání

nejmenšího prvku množinu a vyčerpá u nějakého ordinálního čísla.) Nechť α je nejmenší ordinální číslo takové, že $F(\alpha) = c$. Položme $f = F \restriction \alpha$, pak $(\forall \beta, \gamma \in \alpha)(f(\beta), f(\gamma) \in a)$ a podle dříve dokázaného je f vnoření $\langle \alpha, \in \rangle$ do $\langle a, < \rangle$. Protože $F(\alpha) = c$, platí, že $a - rng(f) = 0$, tedy f je izomorfizmus.

Nyní dokažme jednoznačnost f a α. Pokud by existovali dva izomorfizmy f a g, pak $f \circ g^{-1}$ by byl izomorfizmus ordinálních čísel. My jsme však již dokázali, že jediný takový izomorfizmus je identita.

Právě dokázaná věta nám ukazuje, že třída všech dobrých množinových uspořádání se rozkládá na třídy navzájem izomorfních uspořádání, přitom žádné dobré uspořádání není izomorfní se svým ostrým segmentem (pro $t \in a$ je ostrý segment určený t množina $seg(t) = \{u \in a; u < t\}$) a pro dvě neizomorfní dobrá množinová uspořádání platí, že je jedno izomorfní segmentu druhého, nebo naopak. Takto chápal ordinální čísla Cantor. My navíc máme v každé třídě izomorfních množinových dobrých uspořádání jednoho zvláštního reprezentanta, ordinální číslo ve smyslu moderní teorie množin (jak bylo definováno).

Konstrukce transfinitní rekurzí též umožňuje zpřesnit námi na začátku uvedenou vágní představu univerza množin, rozčleněného do jednotlivých hladin postupně vznikajících stálým opakováním operace potenční množiny na vše dříve dosažené. Položíme-li $G(x) = \mathcal{P}(rng(x))$ a je-li F funkce vykonstruovaná z G větou o konstrukci transfinitní rekurzí, pak (za pomoci axiomu regularity) lze dokázat $V = rng(F)$. V případě zkoumání teorie množin bez axiomu regularity takto dostaneme tzv. jádro vyhovující axiomům teorie množin včetně regularity.

Konstrukce transfinitní rekurzí dále umožňuje např. zavést na On početní operace $+$, $\cdot$ a α^β iterací (opakovaným prováděním) nižších operací. Operaci $+$ jako opakované přičítání 1 (t.j. následovníka), násobení jako opakované přičítání a mocnění jako opakované násobení.

Transfinitní rekurzí vyjádříme $\alpha + \beta = F(\beta)$, kde F je zkonstruováno z G definované předpisem $G(0) = \alpha$, $G(x) = \bigcup(\{\gamma \cup \{\gamma\}; \gamma \in rng(x)\})$. $\alpha \cdot \beta = F(\beta)$, kde F je zkonstruováno z G definované předpisem $G(0) = 0$, $G(x) = \bigcup(\{\gamma + \alpha; \gamma \in rng(x)\})$ pokud je pravá strana definována, $G(x) = 0$ jinak. $\alpha^\beta = F(\beta)$, kde F je zkonstruhováno z G definované předpisem $G(0) = 1$, $G(x) = \bigcup(\{\gamma \cdot \alpha; \gamma \in rng(x)\})$ pokud je pravá strana definována, $G(x) = 0$ jinak.

Protože mocnina na přirozených číslech definovaná opakovaným násobením není komutativní, nemusí čtenáře překvapit, že sčítání ani násobení nejsou na ordinálních číslech komutativní. Platí totiž, že $1 + \omega = \omega \neq \omega + 1$ a $2 \cdot \omega = \omega \neq \omega \cdot 2 = \omega + \omega$.

Připomeňme ještě, že početní operace jsme do nekonečna rozšířili již dříve v kardinální aritmetice. Tato dvě rozšíření jsou v nekonečnu podstatně různá. Zatímco v kardinální aritmetice je součet roven součinu je roven maximu, tak v ordinální aritmetice je (pro nekonečná α, β) součet i součin vždy větší než jeden člen. Naopak ω^ω je spočetné sjednocení spočetných množin, tedy spočetná množina, zatímco $|\mathbb{N}|^{|\mathbb{N}|} = |\mathbb{R}|$ je nespočetné.

Již dříve jsme diskutovali problém zastavení algoritmu. Nyní uvedeme jeden speciální algoritmus, pro který se za pomoci ordinální aritmetiky dokáže, že při libovolném vstupu (přirozené číslo) výpočet skončí. Přitom je použití nekonečných objektů pro důkaz nutné (je dokázána bezespornost teorie množin s negací axiomu nekonečna ve které platí, že existuje přirozené číslo, pro které se algoritmus nezastaví). Nekonečná matematika tedy rozhoduje typicky konečný problém.

Čtenář se již jistě setkal s vyjadřováním čísel v pozičních soustavách, zcela jistě má

zkušenosti s desítkovou soustavou, asi ví o dvojkové soustavě a možná se též setkal s šestnáctkovou (hexadecimální) soustavou ve výpočetní technice. Budeme se zajímat o vyjadřování přirozených čísel v pozičních soustavách. Pro vyjádření čísla se používají cifry, což jsou čísla menší než je základ poziční soustavy. (V dvojkové soustavě se používají cifry 0 a 1, v desítkové cifry 0, 1, 2, 3, 4, 5, 6, 7, 8 a 9.) Vyjádřené číslo se pak ze zápisu získá tak, že cifra v 0-té pozici (nejpravější) se vynásobí základem na 0-tou, přičte se cifra v 1-té pozici vynásobená základem na 1-tou atd. Cifry budeme nadále nazývat koeficienty vyjádření zkoumaného čísla.

Zkoumejme následující algoritmus: Vstup n vyjádříme v dvojkové soustavě včetně očíslování pozic, očíslování čísel těchto pozic atd. Jeden krok algoritmu spočívá v tom, že o 1 zvedneme základ poziční soustavy při zachování koeficientů a od takto vzniklého čísla odečteme 1 a vyjádříme jej v aktuální číselné soustavě. Získáme nové koeficienty (mohou se mezi nimi vyskytovat cifry *základ* -1, které se dříve mezi koeficienty nevyskytovaly) a v dalším kroku za použití těchto koeficientů vyjádříme číslo při znovu zvednutém základu, od kterého opět odečteme 1 atd. Pokud tímto procesem dospějeme k číslu 0 algoritmus končí. Ukažme si proces na třech počátečních členech pro číslo 11.

$11 = (1011)_2 = 1 \cdot 2^{1 \cdot 2^1+1} + 1 \cdot 2^1 + 1$

$84 = (10010)_3 = 1 \cdot 3^{1 \cdot 3^1+1} + 1 \cdot 3^1$

$1027 = (100003)_4 = 1 \cdot 4^{1 \cdot 4^1+1} + 3$

Posloupnost takto vznikajících čísel se nazývá Goodsteinova posloupnost s počátkem 11 a Goodsteinova věta tvrdí, že při libovolném vstupu n Goodsteinova posloupnost s počátkem n po konečném počtu kroků dospěje k 0.

Naznačme zhruba důkaz této věty. Členy Goodsteinovy posloupnosti omezme shora ordinálními čísly takovými, že používáme koeficienty jednotlivých kroků, ale bereme "základ" ω (mocniny "základu" přitom násobíme koeficienty zprava). Takto získáme klesající posloupnost ordinálních čísel, která musí po konečném počtu kroků skončit (jak plyne z principu nejmenšího prvku). Detailní znění a důkaz věty lze nalézt v knize Bohuslav Balcar, Petr Štěpánek: Teorie množin, Academia Praha 1986. Zde lze též najít odkaz na důkaz bezespornosti teorie konečných množin s negací Goodsteinovy věty.

Axiom výběru a jeho základní ekvivalenty.

Axiom výběru jsme již uvedli v axiomatice teorie množin. Tento axiom tvrdí, že na každé množině neprázdných množin existuje selektor - funkce přiřazující množinám jejich prvky. Jeho nejběžněji používanými ekvivalenty jsou *Zornův princip maximality* a *Princip dobrého uspořádání*. Zopakujme nyní znění axiomu výběru a uveďme znění uvedených dvou principů.

AC (axiom of choice) $(\forall x)((\forall t)(t \in x \to t \neq 0) \to (\exists S)(Fce(S)\ \&\ dom(S) = x\ \&\ (\forall t)(t \in x \to S(t) \in t)))$

ZPM (Zornův princip maximality) Nechť $\langle a, \leq \rangle$ je (částečné) uspořádání splňující následující Zornovu podmínku: Pro každou podmnožinu $b \subseteq a$, která je $\leq$ uspořádána lineárně (taková podmnožina se nazývá řetězec) existuje neostrý horní odhad u množiny b $((\forall t)(t \in b \to t \leq u))$. Pak (neostře) nad každým prvkem $t \in a$ existuje u maximální v $\langle a, \leq \rangle$.

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

Než přistoupíme k důkazu ekvivalence uvedených tří tvrzení, uveďme typické použití Zornova principu maximality.

Věta: Každou lineárně nezávislou množinu x vektorů vektorového prostoru $\mathbb{V}$ lze rozšířit do báze b.

Důkaz: Připomeňme, že báze vektorového prostoru je taková lineárně nezávislá množina vektorů, že každý vektor lze vyjádřit lineární kombinací prvků báze. Stejně jako v konečnědimenzionálním případu bude bází maximální lineárně nezávislá množina. Je-li totiž u maximální lineární množina a vektor t není lineární kombinací prvků u, je $u \cup \{t\}$ lineárně nezávislá množina ve sporu s maximalitou u. Máme tedy dokázat, že (v $\subseteq$) nad x existuje (v $\subseteq$) maximální lineárně nezávislá množina b. Položme $a = \{y;\ y \subseteq \mathbb{V}\ \&\ y$ *je lineárně nezávislá*$\}$ (a ze znění ZPM) a $\leq$ (ze znění ZPM) nechť je $\subseteq$. Ukažme, že je splněna Zornova podmínka. Nechť c je řetězec v a ukážeme, že $\bigcup c$ je požadovaný horní odhad c. To, že $\bigcup$ je horní odhad v $\subseteq$ čtenář dávno ví. Je potřeba ukázat, že $\bigcup c \in a$, tedy, že $\bigcup c$ je lineárně nezávislá množina. Postupujme sporem. Nechť $a_1t_1 + \cdots + a_kt_k = 0$, kde $a_i \neq 0$ jsou prvky příslušného tělesa (např. reálná čísla) a $t_i \in \bigcup c$, nechť $t_i \in \bigcup y_i$, kde $y_i \in c$ jsou vhodné lineárně nezávislé množiny. Protože $\subseteq$ je na c lineární, je některé y_j největší v $\subseteq$, proto platí $t_i \in y_j$ pro všechna i ve sporu s lineární nezávislostí y_j. Zornova podmínka je splněna a (v $\subseteq$) nad x existuje maximální prvek, což je hledaná báze b.

Nyní přistupme k důkazu ekvivalence tří výše uvedených tvrzení.

Věta: AC, ZPM a WO jsou navzájem ekvivalentní tvrzení.

Důkaz: Ekvivalenci dokážeme formou tzv. "kolečka". Ukážeme AC$\to$ZPM$\to$WO$\to$AC, přitom budeme postupovat odzadu.

WO$\to$AC) Nechť x je množina neprázdných množin. Podle WO existuje na $\bigcup x$ dobré uspořádání ($\leq$). Definujme selektor S na x předpisem $S(t) =$nejmenší (v $\leq$) prvek t.

ZPM$\to$WO) Chceme dokázat existenci dobrého uspořádání $\prec$ na x. Položme $a = \{\langle y, \prec_y\rangle;\ \prec_y$ *je dobré uspořádání* $y\}$ a $\langle y, \prec_y\rangle \leq \langle z, \prec_z\rangle$ položme $y \subseteq z\ \&\ \prec_y \subseteq \prec_z\ \&\ (\forall u)(\forall t)((u \in y\ \&\ t \in z - y) \to u \prec_z t)$, t.j. rozšíření uspořádání (na z) je tzv. koncové, všechny rozšiřující prvky jsou až za původními. Ukážeme, že takto nadefinované uspořádání $\leq$ na a splňuje Zornovu podmínku a maximální prvek bude hledané dobré uspořádání x. Nechť $b \subseteq a$ je řetězec. Ukážeme, že $\langle \bigcup\{y;\ \langle y, \prec_y\rangle \in b\}, \bigcup\{\prec_y;\ \langle y, \prec_y\rangle \in b\}\rangle$ je horní odhad b v $\leq$. To, že sjednocení (po složkách) je v inkluzi (po složkách) nad každým členem je jasné. Je však potřeba ukázat, že sjednocení uspořádání z b je dobrým uspořádáním sjednocení nosných množin z b. Antireflexivita sjednocení plyne z antireflexivity jednotlivých členů, neboť prvek tvaru $\langle t, t\rangle$ se do sjednocení nemůže dostat. Dokažme tranzitivitu. Nechť t, u, v jsou takové prvky sjednocení nosných množin, že $\langle t, u\rangle$ a $\langle u, v\rangle$ jsou prvky sjednocení relací. Nechť $t \in y_1$, $u \in y_2$ a $v \in y_3$. Protože y_1, y_2 a y_3 jsou uspořádány inkluzí lineárně, je některý z nich největší, označme jej y. Pak t, u i v jsou všechno prvky y, $\langle t, u\rangle$ a $\langle u, v\rangle$ jsou prvky $\prec_y$ a z tranzitivity $\prec_y$ plyne $\langle t, v\rangle \in \prec_y$ a tedy $\langle t, v\rangle$ je prvek sjednocení relací, které je tedy uspořádání. Nechť M je neprázdná podmnožina sjednocení nosných množin. Musíme ukázat, že M má nejmenší prvek v sjednocení relací. Nechť $t \in M$ a $t \in y$. Uspořádání $\prec_y$ je dobré uspořádání y a tedy existuje nejmenší prvek $u \in M \cap y$ vzhledem k $\prec_y$. Ukážeme, že u je též nejmenší prvek M vzhledem k sjednocení relací. Kdyby existoval $v \in M$ menší než

u ve sjednocení relací, nemohl by být prvkem y, vzhledem k minimalitě u na $y \cap M$. Nechť tedy $v \in z$ a $y \subset z$ (inkluze je lineární na nosných množinách). Protože jsme jednotlivá uspořádání rozšiřovali koncově a $v \in z - y$, platí $u \prec_z v$ a tedy i u je menší než v v sjednocení relací ve sporu s naším předpokladem. Prvek u je nejmenší prvek M i vzhledem k sjednocení relací a toto sjednocení je dobrým uspořádáním sjednocení nosných množin. Zornova podmínka je dokázána a existuje maximální prvek $\langle y, \prec_y \rangle$ uspořádané množiny $a, \leq$. Stačí již dokázat $y = x$. Pokud by $x - y \neq 0$, tedy by existoval $t \in x - y$, rozšířili bychom $\prec_y$ na $y \cup \{t\}$ tak, že bychom postavili t za všechny prvky y, takto definované uspořádání by bylo dobré koncově rozšiřující $\prec_y$ ve sporu s maximalitou $\prec_y$. Uspořádání $\prec_y$ je proto dobré uspořádání x.

AC→ZPM) Budeme postupovat konstrukcí transfinitní rekurzí. Nechť S je selektor na $\mathcal{P}(a) - \{0\}$. Nechť $c \notin a$. Řekneme že $u \in a$ je *ostrý horní odhad* množiny $b \subseteq a$, jestliže platí $(\forall v)(v \in b \ \rightarrow \ v < u)$. Definujme G následujícím předpisem $G(0) = t$, $G(x) = S(\{u;\ u \textit{ je ostrý horní odhad } rng(x \cap a)\})$, pokud je selektor definován (příslušná množina je neprázdná) a $G(x) = c$ jinak. Nechť F je funkce vykonstruovaná G větou o konstrukci transfinitní rekurzí. Analogicky jako v důkazu věty, že každé množinové dobré uspořádání je izomorfní některému ordinálnímu číslu ukážeme, že dokud F nenabyde hodnotu c je to vnoření ordinálních čísel do $\langle a, < \rangle$, tedy $\alpha \in \beta \ \equiv \ F(\alpha) < F(\beta)$. Pokud by pro žádné α neplatilo $F(\alpha) = c$, bylo by F vnoření celé třídy On do $\langle a, < \rangle$. Obraz $rng(F) \subseteq a$ by byla množina podle schematu vydělení a $On = F^{-1}"(rng(F))$ by byla množina podle schematu nahrazení. Existuje tedy α takové, že $F(\alpha) = c$. Nechť α je nejmenší této vlastnosti, $F"\alpha$ je řetězec v $\langle a, \leq \rangle$, který má podle Zornovy podmínky horní odhad, nemá však ostrý horní odhad (neboť $F(\alpha) = c$), tento horní odhad již nad sebou nemá větší prvek, je to tedy hledaný maximální prvek nad t.

Protože podle principu WO víme, že každou množinu lze dobře uspořádat a dále víme, že každé dobré uspořádání je izomorfní jedinému ordinálnímu číslu, obsahuje každá třída rozkladu podle $\approx$ nějaké ordinální číslo. Nejmenší takové ordinální číslo volíme jako reprezentant této třídy a nazývá se v moderním množinovém pojetí kardinálním číslem. Odtud vychází následující definice.

Definice: 1) Ordinální číslo α se nazývá *kardinální číslo* jestliže není vzájemně jednoznačně zobrazitelné na žádné menší ordinální číslo.

2) $Cn = \{\kappa;\ (\forall \alpha)(\alpha \in \kappa \ \rightarrow \ \neg \alpha \approx \kappa)\}$

Protože $Cn \subseteq On$ je dobře (a tedy též lineárně) uspořádáno $\in$, je $\preceq$ lineární, a mohutnosti jsou proto srovnatelné.

Zhruba naznačíme, jak se dokáže obrácená implikace (ze srovnatelnosti mohutností plyne WO). *Hartogsovo číslo množiny* x (značme $H(x)$) nechť je množina všech ordinálních čísel α takových, že $\alpha \preceq x$. Uvažujeme-li množinu všech tříd ekvivalence navzájem izomorfních dobrých uspořádání podmnožin x (v jedné třídě leží navzájem izomorfní dobrá uspořádání, která jsou částí $x \times x$), je to podmnožina $\mathcal{P}(\mathcal{P}(x \times x))$ (s dobrým uspořádáním "prvek třídy je izomorfní segmentu prvku větší třídy"), která je izomorfní $H(x)$. Proto je $H(x)$ skutečně ordinální číslo. Nemůže platit $H(x) \preceq x$, neboť z toho by plynulo $H(x) \in H(x)$. Pokud jsou $H(x)$ a x srovnatelné, musí nutně být $x \prec H(x)$, tedy x je vzájemně jednoznačně

zobrazitelná na podmnožinu $H(x)$ a tímto zobrazením na x přeneseme dobré uspořádání $H(x)$.

Číselné obory.

Pokud chce teorie množin hrát úlohu základní matematické teorie, musí být schopna v sobě vytvořit modely základních matematických struktur, speciálně číselných oborů. Zatím jsme tak učinili pro obor přirozených čísel.

Celá čísla $\mathbb{Z}$ můžeme v teorii množin zmodelovat jako faktor množinu $\mathbb{N} \times \mathbb{N}$ podle ekvivalence $\langle m_1, n_1\rangle \sim \langle m_2, n_2\rangle$ definované předpisem $m_1 + n_2 = m_2 + n_1$. Přitom jsme zvyklí označovat tyto uspořádané dvojice jako $m - n$. Nebudeme zde (na učené úrovni) dokazovat, že příslušná ekvivalence je kongruence (přenáší strukturu - početní operace), to již čtenář zvládl v základní škole. Radši podotkněme, že uvedená konstrukce byla zobecněna do konstrukce podílové grupy k pologrupě.

Podobně rozšíříme celá čísla do racionálních $\mathbb{Q}$ tak, že budou faktormnožinou $\mathbb{Z} \times \mathbb{Z}$, kde druhé složky budou nenulové a příslušná ekvivalence $\sim$ bude definována předpisem $\langle m_1, n_1\rangle \sim \langle m_2, n_2\rangle$ když $m_1 . n_2 = m_2 . n_1$, přitom jsme zvyklí označovat dvojice jako m/n. Tato konstrukce našla v algebře zobecnění v konstrukci podílového tělesa k oboru integrity.

Reálná čísla lze charakterizovat jako uspořádané těleso, ve kterém platí věta o suprému. Ukážeme, že toto je opět kategorický požadavek - libovolné dvě struktury vyhovující uvedenému požadavku jsou izomorfní. Zopakujme nejdříve axiomatický popis reálných čísel.

Jazyk (použité symboly) je: konstanty 0, 1, unární funkční symboly $-$, $^{-1}$ (opačný prvek a převrácená hodnota), binární funkční symboly $+$, $.$ (sčítání a násobení), binární relační symboly $=$, $\leq$ (rovnost a přirozené uspořádání).

Axiomy jsou: 1) Obecné axiomy rovnosti $x = x$ (reflexivita), $x = y \to y = x$ (symetrie), $(x = y \ \& \ y = z) \to x = z$ (tranzitivita), $x = y \to F(\dots, x, \dots) = F(\dots, y, \dots)$ pro každý funkční symbol, $x = y \to (R(\dots, x, \dots) \to R(\dots, y, \dots))$ pro každý relační symbol (substitutivita $=$).

2) Axiomy komutativní grupy pro sčítaní (s 0 jako neutrálním prvkem a $-$ jako inverzním prvkem) a násobení nenulových prvků (s 1 jako neutrálním prvkem a $^{-1}$ jako inverzním prvkem). (Speciálně požadujeme $0 \neq 1$.)

$(x + y) + z = x + (y + z)$, $(x . y) . z = x . (y . z)$ (asociativní zákony)

$x + y = y + x$, $x . y = y . x$ (komutativní zákony)

$0 + x = x$, $1 . x = x$ (neutrální prvek)

$-x + x = 0$, $x \neq 0 \to x^{-1} . x = 1$ (inverzní prvek)

3) Distributivní zákon: $x . (y + z) = (x . y) + (x . y)$

4) Zákony uspořádání: $\leq$ je lineární uspořádání a $x \leq y \to x + z \leq y + z$, $(0 \leq z \ \& \ x \leq y) \to x . z \leq y . z$

5) Věta o suprému (požadavek druhého řádu). Každá neprázdná shora omezená množina reálných čísel má suprémum.

$(\forall M \subset \mathbb{R})(M \neq 0 \ \& \ (\exists z)(\forall t)(t \in M \to t \leq z)) \to (\exists x)((\forall t)(t \in M \to t \leq x) \ \& \ (\forall y)((\forall t)(t \in M \to t \leq y) \to x \leq y)))$.

Věta: 1) $0 . x = 0$.

2) $(-1)^2 = 1$ (Používáme zde mocninu na přirozený exponent jako opakované násobení.)
3) $(-1) \cdot x = -x$.
4) $0 \leq x^2$, speciálně $0 \leq 1^2 = 1$.
5) $x < y \ \rightarrow \ -y < -x$.
Důkaz: 1) $0 = -x + x = -x + (1 + 0) \cdot x = -x + x + 0 \cdot x = 0 \cdot x$
2) $1 = 1 + 0 = 1 + (-1 + 1)^2 = 1 + (-1)^2 + (-1) + (-1) + 1 = (-1)^2 + 0 + 0 = (-1)^2$.
3) $-x = -x + (1 + (-1)) \cdot x = -x + x + (-1) \cdot x = (-1) \cdot x$.
4) a) Je-li $0 \leq x$, pak $0 = 0 \cdot x \leq x^2$.
b) Je-li $x \leq 0$, pak $0 = x - x \leq -x$ a podle a) $0 \leq (-x)^2 = (-1)^2 \cdot x^2 = x^2$.
5) $x < y \ \rightarrow \ -y = x + (-x + -y) < (-x + -y) + y = -x$.

Uvedených pět tvrzení bylo ukázkou, jak se běžné vlastnosti počítání s reálnými čísly odvodí přímo z axiomů. Další běžné vlastnosti již dokazovat nebudeme spoléhaje na to, že čtenář dostal ve výše uvedených důkazech dostatečnou instruktáž.

Z věty o suprému a z pátého tvrzení snadno dokážeme větu o infimu.

Věta (věta o infimu): Nechť $M \subset \mathbb{R}$ je neprázdná zdola omezená množina, pak M má infimum.

Důkaz: Použij větu o suprému pro $M = \{-x;\ x \in M\}$.

Z věty o suprému odvodíme dále následující Archimedovu podmínku.

Věta: Pro každé $x \in \mathbb{R}$ existuje $n \in \mathbb{N}$ takové, že $x \leq \mathfrak{n}$, kde $\mathfrak{n}$ je n-krát provedený součet 1 se sebou. (Nadále budeme $\mathfrak{n}$ ztotožňovat s n).

Důkaz: Je-li $x \leq 1$, je hledaným číslem 1. Je-li $1 \leq x$, položme $M = \{n;\ n \in \mathbb{N} \ \& \ n \leq x\}$. Množina M je neprázdná shora omezená množina a má proto podle věty o suprému suprémum y. Podle definice supréma $y - 1$ není horní závora, tedy existuje $n \in M$ takové, že $y - 1 \leq n$, proto $y + 1 \leq n + 2$ a $n + 2 \notin M$, proto $x \leq n + 2$ z linearity uspořádání $\leq$.

Příkladem uspořádaného tělesa, které není archimedovsky uspořádané (proto v něm neplatí ani věta o suprému) je těleso racionálních funkcí jedné neurčité nad tělesem reálných (popřípadě racionálních) čísel, ve kterém jsou reálná (popřípadě racionální) čísla uspořádána přirozeně, dále $(\forall a \in \mathbb{R})(a < x)$ a obecné racionální funkce jsou uspořádány v souladu s tím co uvedená podmínka vynucuje (uspořádání musí být v souladu s operacemi $+$ a $\cdot$).

Věta: Množina racionálních čísel je v reálných číslech hustá. (Tj. $(\forall x, y \in \mathbb{R})(x < y \rightarrow (\exists r \in \mathbb{Q})(x < r < y))$.)

Důkaz: Bez újmy na obecnosti můžeme předpokládat, že $0 \leq x < y$ (jinak přejdeme k opačným hodnotám). Nechť $n \in \mathbb{N}$ je nejmenší takové číslo, že $1/(y - x) < n$ (t.j. $y - x > 1/n$). Nechť $m \in \mathbb{N}$ je nejmenší přirozené číslo takové, že $nx < m$ (t.j. $(m - 1)/n \leq x < m/n$). Z $(m - 1)/n \leq x$ a $1/n < y - x$ dostaneme $m/n < y$. K dokončení důkazu stačí položit $r = m/n$.

Nyní můžeme přistoupit k důkazu faktu, že dvě struktury vyhovující požadavkům kladeným na reálná čísla jsou izomorfní.

Věta: Nechť $\mathbb{R}$ a $\mathfrak{R}$ jsou dvě struktury vyhovující výše uvedeným axiomům pro reálná čísla. Pak existuje izomorfizmus F těchto struktur.

Důkaz: Během důkazu budeme značit prvky a konstanty ve strukturách různě, relace a funkce (operace) stejně (s důvěrou, že k nedorozumění nedojde).

Definujeme (jak z definice izomorfizmu plyne) $F(0) = (\mathfrak{o})$ a $F(1) = (\mathfrak{1})$. Tím je již určeno též rozšíření pro vnořená přirozená čísla $\mathbb{N}$ a $\mathfrak{N}$ příslušných struktur $F(n) = \mathfrak{n}$, kde nalevo je n-krát sečtená 1 a napravo n-krát sečtená $\mathfrak{1}$ (přesnou definici je možno udělat pomocí věty o konstrukci rekurzí). Z dokázané vlastnosti $0 < 1$ odvodíme, že přirozené uspořádání $\mathbb{N}$ se po vnoření zachová (po vnoření je uspořádáním relace uspořádání na uspořádaném tělese).

Dále rozšíříme F na vnořená celá čísla $\mathbb{Z}$ a $\mathfrak{Z}$ předpisem $F(n - m) = F(n) - F(m) = \mathfrak{n} - \mathfrak{m}$, kde n, m jsou přirozené násobky 1. Obdobně rozšiřujeme izomorfizmus pro vnořená racionální čísla předpisem $F(n/m) = F(n)/F(m)$, kde n, m jsou vnořená celá čísla.

Vše, co jsme doposud potřebovali k důkazu, že F je prosté zobrazení je fakt, že pro žádné přirozené číslo n není přirozený n-násobek 1 číslo 0 (tělesa vyhovující tomuto požadavku se nazývají tělesa charakteristiky 0). V dosavadní úvaze jsme ukázali, že uspořádaná tělesa jsou charakteristiky 0 a že do těles charakteristiky 0 jsou jednoznačně vnořena racionální čísla. Příkladem tělesa charakteristiky 0, které nemůže být uspořádaným tělesem je těleso komplexních čísel, neboť $i^2 = -1 < 0$ v rozporu s dříve ukázanou vlastností uspořádaných těles ($0 \leq x^2$).

Nakonec rozšiřme izomorfizmus F předpisem $F(x) = sup\{F(t);\ t \in \mathbb{Q}\ \&\ t < x\}$. Toto rozšíření zachovává původní hodnoty pro racionální čísla, neboť pro $r \in \mathbb{Q}$ platí, že $r = sup\{t;\ t \in \mathbb{Q}\ \&\ t < r\}$. Dokažme, že po tomto rozšíření je již F izomorfizmus $\mathbb{R}$ a $\mathfrak{R}$. Dokažme, že F je prosté. Nechť $x \neq y$ a nechť např. $x < y$. Pak podle hustoty $\mathbb{Q}$ existuje $r \in \mathbb{Q}$ takové, že $x < r < y$ a ještě jednou aplikací hustoty získáme $s \in \mathbb{Q}$ takové, že $x < r < s < y$. Kdyby platilo že $F(x) = F(y)$, pak $\mathfrak{r} = F(r)$ by byl horní odhad $\{F(t);\ t \in \mathbb{Q}\ \&\ t < x\}$ jejímž suprémem je $F(x) = F(y)$, proto $F(y) \leq \mathfrak{r}$, proto $\mathfrak{r}$ by též byl horní odhad množiny $\{F(t);\ t \in \mathbb{Q}\ \&\ t < y\}$ jejímž suprémem je $F(y)$ ve sporu s tím, že $\mathfrak{s} = F(s)$ je prvkem této množiny a $\mathfrak{r} < \mathfrak{s}$. Tím je prostota F dokázána. Dokažme, že F je na $\mathfrak{R}$. Nechť $\mathfrak{x} \in \mathfrak{R}$. Bez újmy na obecnosti můžeme předpokládat $\mathfrak{o} < \mathfrak{x}$ (jinak přejdeme k opačnému prvku). Z Archimedovy podmínky víme, že pro vhodné n platí $\mathfrak{x} < \mathfrak{n}$. Množina $\{t; t \in \mathbb{Q}\ \&\ F(t) < \mathfrak{x}\}$ je neprázdná (obsahuje 0), shora omezená (číslem n), proto má suprémum x. Stačí ukázat $F(x) = \mathfrak{x}$. Kdyby např. platilo $F(x) < \mathfrak{x}$, existovali by $\mathfrak{r}, \mathfrak{s} \in \mathfrak{Q}$ takové, že $F(x) < \mathfrak{r} < \mathfrak{s} < \mathfrak{x}$, což bychom dovedli ke sporu obdobně, jako při důkazu prostoty F.

Podobně dovedeme ke sporu $x < y\ \&\ F(y) \leq F(x)$ a tím dokážeme izomorfizmus F vůči $\leq$.

Ukažme, že $F(x+y) = F(x) + F(y)$. Dokažme tvrzení pro x, y iracionální. Postupujeme opět sporem. Nechť např. $F(x) + F(y) < F(x+y)$, pak z Archimedovy podmínky vyplyne existence $\mathfrak{n}$ takového, že $\mathfrak{1}/\mathfrak{n} < F(x+y) - F(x) - F(y)$. Nechť $m_x \in \mathbb{Z}$ je takové, že $m_x/2n < x < (m_x+1)/2n$ a analogicky $m_y \in \mathbb{Z}$ je takové, že $m_y/2n < y < (m_y+1)/2n$. Pak $(m_x/2n) + (m_y/2n) < x + y < (m_x/2n) + (m_x/2n) + (1/n)$. Po zobrazení F dostaneme $F(m_x/2n) + F(m_y/2n) < F(x) + F(y) < F(m_x/2n) + F(m_x/2n) + (\mathfrak{1}/\mathfrak{n}) < F(x+y)$, ve sporu s $x + y < (m_x/2n) + (m_x/2n) + (1/n)$.

Podobně argumentujeme i pro $F(x \cdot y) = F(x) \cdot F(y)$.

Přistupme nyní ke konstrukci modelu $\mathbb{R}$ v teorii množin.

Definice: Dedekindovým řezem x na $\mathbb{Q}$ nazveme dolní množinu, která je neprázdná, různá od $\mathbb{Q}$ a nemá největší prvek. Formálně $x \subset \mathbb{Q}$ & $x \neq 0$ & $(\forall r, s \in \mathbb{Q})((s \in x \ \& \ r < s) \to r \in x)$ & $(\forall r \in x)(\exists s \in x)(r < s)$.

Množina všech Dedekindových řezů s vhodně zavedenou strukturou bude hledaný model pro $\mathbb{R}$.

Definice: $\mathbb{R} = \{x;\ x \text{ je Dedekindův řez na } \mathbb{Q}\}$. Přirozené uspořádání $\leq$ na $\mathbb{R}$ je $\subseteq$. Operace (funkční symboly) a konstanty 0, 1 budeme definovat později.

Ostrý segment racionálního čísla r, $seg_<(r) = \{t \in \mathbb{Q};\ t < r\}$ je příklad Dedekindova řezu. Množina $\{t \in \mathbb{Q};\ t < 0 \ \vee \ t^2 < 2\}$ je příklad Dedekindova řezu, který není ostrým segmentem žádného racionálního čísla (reprezentuje $\sqrt{2}$).

Věta: Pro racionální čísla r, s platí $r \leq s \ \equiv \ seg(r) \subseteq seg(s)$ (kde index $<$ je zřejmý ze souvislosti).

Důkaz: Jednoduchý důkaz přenecháváme čtenáři.

Věta ukazuje, že funkce $F : \mathbb{Q} \longrightarrow \mathbb{R}$ je vnoření (vzhledem k $\leq$). Takto máme zavedeny konstanty 0 a 1 v modelu reálných čísel (jako $seg(0)$ a $seg(1)$).

Ukážeme nyní, že v modelu $\mathbb{R}$ platí věta o suprému.

Věta: Nechť $M \subset \mathbb{R}$ je neprázdná shora omezená (t.j. $(\exists x \in \mathbb{R})(\forall y \in M)(y \subseteq x)$). Pak $\bigcup M$ je dedekindův řez, který je suprémum M.

Důkaz: To, že $\bigcup M$ je suprémum M v inkluzi (která je přirozeným uspořádáním $\mathbb{R}$), čtenář již dávno ví. Je potřeba dokázat, že $\bigcup M$ je Dedekindův řez. Množina $\bigcup M$ je neprázdná, neboť je sjednocením neprázdné množiny neprázdných množin, $\bigcup M \neq \mathbb{Q}$, neboť $\bigcup M \subseteq x \subset \mathbb{Q}$. Množina $\bigcup M$ je dolní množina, neboť je sjednocením dolních množin. Je-li totiž $t < u$ a $u \in \bigcup M$, pak $u \in y \in M$ pro nějaké y, $t \in y \subseteq \bigcup M$. Zbývá ukázat, že $\bigcup M$ nemá největší prvek. Kdyby $t \in \bigcup M$ byl největší prvek, pak $t \in y \in M$ pro vhodné y. Řez y však nemá největší prvek, proto existuje $u \in y \subseteq \bigcup M$ takové, že $t < u$ ve sporu s maximalitou t.

Zbývá rozšířit početní operace $-$, $^{-1}$, $+$ a $\cdot$ z $\mathbb{Q}$ na $\mathbb{R}$ a ukázat, že po tomto rozšíření bude $\mathbb{R}$ uspořádané těleso. Ten kdo si pročetl důkaz, že dvě struktury vyhovující požadavkům kladeným na reálná čísla jsou izomorfní asi již věří, že se to povede. V dalším textu toto rozšíření a příslušné důkazy popíšeme.

Definice: Pro $x, y \in \mathbb{R}$ položíme $x + y = \{t + u;\ t \in x \ \& \ u \in y\}$.

Můžeme již přenechat čtenáři jednoduché prověření toho, že $x + y$ je řez a že $\mathbb{R}$ s takto definovaným $+$ a s 0 jako neutrálním prvkem tvoří komutativní pologrupu s jednotkou, tedy, že jsou splněny výše uvedené grupové axiomy s výjimkou $-x + x = 0$, neboť $-x$ ještě nebyl zaveden. Zavedení $-x$ následuje.

Definice: Pro $x \in \mathbb{R}$ položíme $-x = \{t \in \mathbb{Q};\ (\exists u \in \mathbb{Q} - x)(t < -u)\}$.

Věta: Množina $-x$ je řez a platí $-x + x = 0$.

Důkaz: To, že $-x$ je dolní množina (s každým svým prvkem obsahuje všechny menší racionální čísla) vyplývá přímo z definice. Je-li $u \in \mathbb{Q} - x$ a $u < t$, pak $-t \in -x$ a $-x$ je proto neprázdná množina. Je-li $t \in x$, pak $-t \notin -x$, proto platí $-x \neq \mathbb{Q}$. Je-li $t \in -x$ a

$u \in \mathbb{Q} - x$ takové, že $t < -u$, pak $t < (t-u)/2 < -u$, $(t-u)/2 \in -x$, tedy $-x$ nemá největší prvek a je proto řezem.

Dokažme, že $-x + x = 0$, tedy, že $(\forall t \in -x)(\forall v \in x)(t + v < 0)$ a $(\forall r \in \mathbb{Q})(r < 0 \rightarrow (\exists t \in -x)(\exists v \in x)(r = t + v))$. Nechť $u \in \mathbb{Q} - x$ je takové, že $t < -u$. Víme, že $v < u$, tedy $-u < -v$, tedy $t < -v$, proto $t + v < 0$. Je-li $r < 0$, nechť $n \in \mathbb{N}$ je takové, že $1/n < -r$ a $m \in \mathbb{Z}$ je takové, že $m/n \in x$ a $(m+1)/n \in \mathbb{Q} - x$. Položme $v = m/n$ a $t = r - v < -(1/n) - v = -(m+1)/n$, pak $v \in x$, $t \in -x$ a $r = t + v$.

Před rozšířením . na $\mathbb{R}$ a důkazem zákonů uspořádaného tělesa pro $\mathbb{R}$ uveďme trochu teorie. Ta nám pak navíc umožní např. rozšířit mocninu definovanou pro racionální exponenty na všechny reálné exponenty.

Definice: Řekneme, že funkce $\rho : T \times T \longrightarrow \mathbb{R}$ je *metrika na* T, jestliže
1) $0 \leq \rho(x, y)$
2) $\rho(x, y) = 0 \ \equiv \ x = y$
3) $\rho(x, y) = \rho(y, x)$
4) $\rho(x, z) \leq \rho(x, y) + \rho(y, z)$ (*trojúhelníková nerovnost*).

Množinu T s metrikou ρ nazýváme *metrický prostor*.

Věta: $|x - y| = max(x - y, y - x)$ je metrika na $\mathbb{R}$.

Důkaz přenecháváme čtenáři, jedná se o obvyklou vzdálenost na číselné ose reálných čísel.

Věta: Jsou-li $\rho_1(x_1, y_1)$ a $\rho_2(x_2, y_2)$ metriky na T_1 a T_2, je $\rho(\langle x_1, x_2\rangle, \langle y_1, y_2\rangle) = max(\rho_1(x_1, y_1), \rho_2(x_2, y_2))$ metrika na $T_1 \times T_2$.
Důkaz: Ověří se podmínky z definice metriky.

Definice: Uzávěrem $\overline{M}$ množiny M v metrickém prostoru T nazýváme množinu všech bodů x prostoru T, které mají nulovou vzdálenost od M, t.j $\overline{M} = \{x;\ (\forall n \in \mathbb{N})(\exists y \in M)(\rho(x, y) < 1/n)$.

Věta: $\overline{\mathbb{Q}} = \mathbb{R}$ v metrickém prostoru $\mathbb{R}$.

Jednoduchý důkaz přenecháváme čtenáři. Využije se hustoty $\mathbb{Q}$ v $\mathbb{R}$. Ke každému x a $\varepsilon > 0$ existuje $r \in \mathbb{Q}$, takové, že $x < r < x + \varepsilon$.

Zesilme nyní poněkud pojem spojitosti funkce.

Definice: Řekneme, že funkce $f : M \longrightarrow T_2$ je spojitá stejnoměrně na M (podmnožině metrického prostoru T_1, T_2 je také metrický prostor) jestliže pro každé $\varepsilon > 0$ existuje $\delta > 0$ takové, že pro každé $x, y \in M$ platí, že $\rho_1(x, y) < \delta \ \rightarrow \ \rho_2(f(x), f(y)) < \varepsilon$.

Věta: 1) Funkce $f(x) = -x$ je stejnoměrně spojitá na $\mathbb{R}$.
2) Funkce $f(x, y) = x + y$ je stejnoměrně spojitá na $\mathbb{R}^2$.
Důkaz: 1) Stačí položit $\delta = \varepsilon$ pro ověření požadavku z definice.
2) Stačí položit $\delta = \varepsilon/2$ a ověřit požadavky z definice.

Věta: 1) Pro každé $K \in \mathbb{N}$ & $K > 0$ je funkce $f(x) = 1/x$ stejnoměrně spojitá na $\mathbb{Q} - (-1/K, 1/K)$.
2) Pro každé $K \in \mathbb{N}$ & $K > 0$ je funkce $f(x, y) = x.y$ stejnoměrně spojitá na $([-K, K] \cap \mathbb{Q})^2$.
Důkaz: 1) Platí $1/x - 1/y = (y - x)/x.y$, stačí proto položit $\delta = \varepsilon/K^2$ a ověřit požadavky z definice stejnoměrné spojitosti.

2) Platí $x_1 . y_1 - x_2 . y_2 = y_1(x_1 - x_2) + x_2(y_1 - y_2)$, stačí proto položit $\delta = \varepsilon/2K$ a ověřit požadavky z definice stejnoměrné spojitosti.

Věta (o rozšiřování stejnoměrně spojité funkce): Nechť $f : M \longrightarrow \mathbb{R}$ (kde M je podmnožina metrického prostoru T) je stejnoměrně spojitá funkce na M, pak existuje právě jedna funkce $F : \overline{M} \longrightarrow \mathbb{R}$ stejnoměrně spojitá na $\overline{M}$ taková, že $F \restriction M = f$.

Důkaz: Dokažme nejdříve jednoznačnost F. Nechť tedy F a G jsou dvě takové funkce. Nechť pro nějaké $x \in \overline{M}$ platí $G(x) - F(x) > \varepsilon$. K $\varepsilon/2$ existuje δ z podmínky stejnoměrné spojitosti. K tomuto δ existuje $y \in M$ takové, že $\rho(x, y) < \delta$. Pak ale $G(x) - F(x) = (G(x) - f(y)) + (f(y) - F(x)) < \varepsilon$ ve sporu s dřívější nerovností.

Dokažme existenci. Nechť δ je odpovídající $\varepsilon = 1$ z podmínky stejnoměrné spojitosti. Pro $x \in \overline{M}$ položme $F(x) = inf\{sup(f"\{y \in M;\ \rho(x, y) < \delta/n\});\ n \in \mathbb{N}\ \&\ n > 1\}$. Nechť $z \in M$ je takové, že $\rho(x, z) < \delta/2$, pak pro každé $y \in \{y \in M;\ \rho(x, y) < \delta/n\}$ z výše uvedených množin platí $\rho(z, y) < \delta$ (jak plyne z trojúhelníkové nerovnosti), a proto platí $|f(z) - f(y)| < 1$ (z volby δ). Obrazy jsou proto omezené jak zhora, tak zdola, supréma proto existují a jsou omezená zdola, proto existuje infimum a definice $F(x)$ má smysl.

Dokažme stejnoměrnou spojitost F na $\overline{M}$. Zvolme $\varepsilon_1 > 0$. K $\varepsilon_1/4$ existuje δ_1 z definice stejnoměrné spojitosti pro f na M. Ukážeme, že $\delta_1/4$ vyhovuje podmínce stejnoměrné spojitosti pro F a ε_1. Nechť tedy $x_1, x_2 \in \overline{M}$ jsou takové, že platí $\rho(x_1, x_2) < \delta_1/4$. Nechť $n \in \mathbb{N}$ je takové, že $\delta/n < \delta_1/4$. Nechť $z_1 \in M$ je takové, že $\rho(x_1, z_1) < \delta/n$ a podobně nechť $z_2 \in M$ je takové, že $\rho(x_2, z_2) < \delta/n$. Pak $\rho(z_1, z_2) \leq \rho(z_1, x_1) + \rho(x_1, x_2) + \rho(x_2, z_2) < \delta_1$, proto $|f(z_1) - f(z_2)| < \varepsilon_1/4$. Pro všechna $y \in \{ y \in M;\ \rho(x_1, y) < \delta/n\}$ platí $\rho(z_1, y) \leq \rho(z_1, x_1) + \rho(x_1, y) < \delta_1$, proto $|f(z_1) - f(y)| < \varepsilon_1/4$, proto $|f(z_1) - F(x_1)| \leq \varepsilon_1/4$. Analogicky získáme $|f(z_2 - F(x_2)| \leq \varepsilon_1/4$. Celkem máme, že $|F(x_1) - F(x_2)| \leq |F(x_1) - f(z_1)| + |f(z_1) - f(z_2)| + |f(z_2) - F(x_2)| < \varepsilon_1$.

To, že pro každé $x \in M$ platí $F(x) = f(x)$, dokážeme tak, že pro každé $\varepsilon > 0$ ukážeme $|f(x) - F(x)| < \varepsilon$. Při tom postupujeme podobně jako dříve.

Uvedenou větu jsme dokázali jen pro funkce s reálnými hodnotami. Větu je možno rozšířit i pro funkce s hodnotami v úplných metrických prostorech. Podmínka stejnoměrné spojitosti f byla podstatná, neboť např. funkce $sin(1/x)$ je spojitá na $(0, 1)$, na uzávěr ($[0, 1]$) však spojitě rozšířit nejde.

Na základě právě dokázané věty rozšíříme operace $x . y$ a x^{-1} z racionálních čísel na čísla reálná. Je-li $|x| < K$ a $|y| < K$, stačí připomenout stejnoměrnou spojitost $x . y$ na $([-K, K] \cap Q)^2$ a je-li $1/K < |x|$ připoměňme stejnoměrnou spojitost x^{-1} na $\mathbb{Q} - (-1/K, 1/K)$.

Zbývá dokázat, že $\mathbb{R}$ se zavedenými operacemi a uspořádáním je uspořádané těleso. Nejdříve si poněkud prohlubme znalosti o stejnoměrně spojitých funkcích.

Připomeňme, že skládání funkcí (obecněji jsme zavedli skládání relací) lze přepsat formulí $(f \circ g)(x) = g(f(x))$, dále zaveďme kombinaci funkcí.

Definice: Nechť $f : X \longrightarrow Y$ a $g : X \longrightarrow Z$ jsou funkce. *Kombinace* f a g je funkce $f \times g : X \longrightarrow Y \times Z$ definovaná předpisem $f \times g(x) = \langle f(x), g(x)\rangle$. (Věříme, že díky souvislosti nenastane záměna s kartézským součinem f a g.)

Dále definujme funkci projekce.

Definice: Projekcí $Pr^i_k : V^k \longrightarrow V$ (kde $0 < i \leq k$) nazýváme funkci definovanou před-

pisem $Pr_k^i(\langle x_1, \ldots, x_k \rangle) = x_i$.

Věta: 1)Projekce Pr_k^i je stejnoměrně spojitá na $\mathbb{R}^k$.

2) Nechť $f : T \longrightarrow S$ a $g : S \longrightarrow R$ jsou funkce takové, že f je stejnoměrně spojitá na $M \subseteq T$ a g je stejnoměrně spojitá na $f"M$, pak $f \circ g$ je stejnoměrně spojitá na M.

3) Nechť $f : T \longrightarrow S$ a $g : T \longrightarrow R$ jsou funkce takové, že f i g jsou stejnoměrně spojité na $M \subseteq T$, pak $f \times g$ je stejnoměrně spojitá na M.

Důkaz: 1) Stačí položit $\delta = \varepsilon$ v definici stejnoměrné spojitosti.

2) Mějme stanoveno $\varepsilon > 0$ v podmínce stejnoměrné spojitosti. K tomuto ε existuje δ v podmínce stejnoměrné spojitosti pro g, a k tomuto δ (chápanému jako ε_1) existuje δ_1 v podmínce stejnoměrné spojitosti pro f. Toto δ_1 je hledané pro ε v podmínce stejnoměrné spojitosti pro $f \circ g$.

3) Mějme stanoveno $\varepsilon > 0$ v podmínce stejnoměrné spojitosti. K tomuto ε existuje δ_1 v podmínce stejnoměrné spojitosti pro f a δ_2 v podmínce stejnoměrné spojitosti pro g. Stačí položit $\delta = min(\delta_1, \delta_2)$.

To, že $\mathbb{R}$ spolu s 0, $-$ a $+$ splňuje vlastnosti komutativní grupy jsme již dokázali. Dokažme nyní komutativitu násobení.

Věta: Pro každé $x, y \in \mathbb{R}$ platí $x \centerdot y = y \centerdot x$.

Důkaz: Nechť $|x| < K$ a $|y| < K$. Požadovanou rovnost můžeme též vyjádřit jako $x \centerdot y - y \centerdot x = 0$, kde na levé straně rovnosti je funkce dvou proměnných, kterou můžeme vyjádřit operacemi složení a kombinace provedené na funkce Pr_2^1, Pr_2^2, $-$, $+$, $\centerdot$. Konkrétně jde o výraz $((\centerdot) \times (((Pr_2^2 \times Pr_2^1) \circ (\centerdot)) \circ (-))) \circ (+)$. Uvedená funkce je na $[-K, K]^2$ stejnoměrně spojitá a v racionálních číslech nabývá hodnotu 0, musí proto nabývat hodnotu 0 i na číslech reálných.

Analogicky se dokáží ostatní grupové zákony pro 1, $^{-1}$ a $\centerdot$, a zákon distributivní.

Pro důkaz, že $\mathbb{R}$ je uspořádané těleso, přenecháváme čtenáři, aby ukázal, že $x \leq y \equiv 0 \leq y + (-x)$ a pak již zbývá ukázat $0 \leq x \;\&\; 0 \leq y \;\rightarrow\; 0 \leq x \centerdot y$, což se opět přenese z racionálních čísel na základě stejnoměrné spojitosti funkce $\centerdot$.

Pro ty čtenáře, kterým se více líbil přístup rozšiřování číselných oborů vhodnými faktorizacemi, uveďme, že reálná čísla lze též budovat jako faktorstrukturu na množině všech cauchyovských posloupností racionálních čísel.

Zajímavý způsob vybudování reálných čísel je uveden v knize P. Vopěnky: Úvod do matematiky v alternatívnej teórii mnžín, alfa Bratislava 1989. Zde jsou vybudována reálná čísla jako faktortřídy těch racionálních čísel, jejichž desetinný rozvoj se liší až za horizontem rozpoznatelnosti (liší se jen v nekonečně velkých indexech za desetinnou čárkou).