—1—

Základy logiky a teorie množin část II

Petr Pajas
pajas@matfyz.cz

URL (slajdy): http://pajas.matfyz.cz/vyuka

—2—

Teorie množin

Její význam spočívá v tom, že všechny matematické pojmy (čísla, funkce, relace, prostory, struktury...) lze redukovat na pojem množiny a důkazy tvrzení o těchto pojmech provádět formálně v této teorii. Lze říci, že *„veškerá matematika se odehrává ve světě teorie množin“*; střízlivěji, že matematiku lze v teorii množin formalizovat (a tak je také většina matematických disciplín dnes chápána).

Úspěch teorie množin je založen na tom, že

- stojí na pevném formálním základě (axiomy, predikátová logika)
- umožňuje redukovat veškeré matematické objekty na množiny (*„všechno je množina“*)
- v důsledku redukuje všechny matematické vztahy na relaci *„být prvkem“* ($\in$)

—3—

Za zakladatele teorie množin je považován německý matematik Georg Cantor (1845–1918).

Teorii množin budeme formulovat jako teorii v logice 1. řádu s rovností v jazyce s jediným mimologickým symbolem $\in$. Individuím, o nichž tato teorie vypovídá, říkáme *množiny*.

Teorii s axiomy, jež vzápětí uvedeme, se říká *Zermelo-Fraenkelova* teorie množin. Existují i jiné axiomatiky, tato je však dnes zdaleka nejužívanější. Uvedenou teorii budeme označovat $\mathrm{ZF}\_$.

—4—

(A1) *Axiom existence*. Existuje aspoň jedna množina (tento axiom nemá v naší axiomatizaci valný význam, neboť jde o sentenci dokazatelnou přímo v logice s rovností; uvádí se z tradičních důvodů).

$$(\exists x)x = x$$

(A2) *Axiom extenzionality*. Množiny, jež mají stejné prvky se rovnají.

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

(Opačná implikace vyplývá z axiomů rovnosti v logice).

(A3) *Schéma axiomů vydělení*. Z každé množiny lze vydělit množinu prvků vyhovujících dané formuli:

Je-li $\varphi(u)$ formule, která neobsahuje volně proměnnou z, potom formule $(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow (u \in x \wedge \varphi(u)))$ je axiom vydělení.

—5—

(A4) *Axiom dvojice*. Každé dvě množiny určují dvouprvkovou množinu.

$$(\forall x)(\forall y)(\exists z)(\forall u)(u \in z \leftrightarrow u = x \vee u = y)$$

(A5) *Axiom sjednocení*. Sjednocení všech prvků množiny je množina.

$$(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow (\exists y)(y \in x \wedge u \in y)$$

(A6) *Axiom potence*. Ke každé množině existuje množina všech jejích podmnožin (tzv. *potenční množinu*, označuje se $\mathcal{P}(x)$).

$$(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow (\forall v)(v \in u \rightarrow v \in x))$$

(A7) *Schéma axiomů nahrazení*. Obraz množiny při definovaném zobrazení je množinou: Je-li $\varphi(u, v)$ formule neobsahující volně z, w, je následující formule axiomem nahrazení.

$$(\forall u)(\forall v)(\forall w)(\varphi(u, v) \wedge \varphi(u, w) \rightarrow v = w) \rightarrow$$
$$(\forall x)(\exists z)(\forall v)(v \in z \leftrightarrow (\exists u)(u \in x \wedge \varphi(u, v)))$$

—6—

(A8) *Axiom nekonečna*.

Existuje nekonečná množina (konkrétněji existuje množina, obsahující prázdnou množinu a s každým svým prvkem u také množinu $u \cup \{u\}$).

$$(\exists z)((\exists u)(u \in z \wedge (\forall v)(\neg v \in u)) \wedge$$
$$(\forall u)(u \in z \rightarrow (\forall w)((\forall t)(t \in w \leftrightarrow (t \in u \vee t = u)) \rightarrow w \in z))$$

Zermelo-Fraenkelova teorie množin tradičně zahrnuje ještě axiom zvaný *axiom regularity* (též *fundovanosti*), jenž stanoví, že každá neprázdná množina x musí obsahovat prvek disjunktní s x. Tím se zakáží například všechny množiny, pro něž by platilo $x \in x$, apod. Axiom regularity nemá uplatnění v běžné matematické praxi a z našich dalších úvah jej vypustíme.

V množinové matematice má dnes své pevné místo také tzv. *axiom výběru*. Formulovat jej budeme ale až později.

—7—

Třídy

Schéma axiomů vydělení umožňuje z dané množiny vyčlenit podmnožinu těch prvků splňujících určitou množinovou vlastnost.

Často je ale výhodné hovořit o souboru vůbec **všech** množin splňujících danou vlastnost (bez omezení do nějaké předem dané množiny).

Třídový term je výraz tvaru $\{x \ ; \ \varphi\}$, který čteme *třída všech množin x splňujících formuli φ*. Formule φ přitom kromě x smí obsahovat další množiny jako parametry.

Třídy označujeme zpravidla velkými písmeny (malá písmena označují výhradně množiny).

S třídami lze pracovat velmi podobně jako s množinami. Prvkem třídy $X = \{x \ ; \ \varphi\}$ je každá množina x, splňující formuli φ. Píšeme $x \in X$. Analogicky, $X = Y$ právě když třídy X, Y mají za prvky tytéž množiny.

—8—

Třídy versus množiny

Množina x obsahuje tytéž prvky jako třída $\{y \ ; \ y \in x\}$. Uvedenou třídu můžeme proto s množinou x ztotožnit.

Každá množina se tak současně stává třídou.

Třídám, které neodpovídají žádné množině, říkáme *vlastní třídy*.

—9—

Třídy jsou výhodné zejména terminologicky, umožňují nám pracovat s vlastnostmi množin jako s objekty.

Formálně bychom se bez nich obešli:

Zápis obsahující třídové termy či proměnné můžeme totiž zpátky přeložit do jazyka teorie množin takto:

1. nejprve všechny výrazy tvaru $X = Y$ resp. $x = X$ nahradíme výrazy $(\forall z)(z \in X \leftrightarrow z \in Y)$ resp. $(\forall z)(z \in x \leftrightarrow z \in X)$, kde z je nějaká dosud nepoužitá proměnná.
2. zastupuje-li X třídový term $\{x\ ;\ \varphi\}$, nahradíme výraz tvaru $z \in X$ formulí $\varphi(x/z)$.

—10—

Universální třídou nazýváme třídu $\mathbf{V}$ obsahující vůbec všechny množiny, tj. $\mathbf{V} = \{x\ ;\ x = x\}$.

Tvrzení: $\mathbf{V}$ *je vlastní třída.*

Důkaz. Kdyby totiž $\mathbf{V}$ byla množina, $\mathbf{V} = v$, byla by podle axiomu vydělení též $y = \{x \in v\ ;\ x \notin x\}$ množina, speciálně $y \in v$. Přitom z definice y bezprostředně vyplývá, že $y \in y \leftrightarrow y \notin y$, což není možné. □

Hned také vidíme, proč v axiomu vydělení máme omezení do jisté předem dané množiny. Bez takového omezení by byla teorie množin sporná. Takto získaný spor se nazývá Russelův paradox. Bertrand Russel jej našel v první, tehdy ještě ne zcela formální, Cantorově teorii množin.

—11—

Jazyk teorie množin (nyní rozšířený o třídy) dále postupně rozšíříme definicemi o další výrazové prostředky zavedením nových funkčních a predikátových symbolů. Každou formuli takto obohaceného jazyka lze na základě definující formule nahradit s ní ekvivalentní formulí základního jazyka $\{\in\}$.

$\emptyset$ – konstanta označující *prázdnou množinu*, jejíž existence plyne z axiomu existence a axiomu vydělení pro formuli $x \neq x$ a jednoznačnost z axiomu extenzionality.

$\bigcup X$ – unární symbol označující *sjednocení* třídy X, tedy třídu

$$\bigcup X = \{x\ ;\ (\exists y)(y \in X \wedge x \in y)\}.$$

Z axiomu sjednocení vyplývá, že sjednocením množiny získáme množinu.

$\bigcap X$ – označuje *průnik* třídy X, tedy třídu

$$\bigcap X = \{y\ ;\ y \in \bigcup X \wedge (\forall z \in X)(y \in z)\}$$

Průnik množiny je množina dle axiomů sjednocení a vydělení ($\bigcap \emptyset = \bigcup \emptyset = \emptyset$).

—12—

$X - Y$ značí *rozdíl* tříd X a Y:

$$X - Y = \{z\ ;\ (z \in X) \wedge \neg(z \in Y)\}$$

Je-li x množina a Y třída, je $x - Y$ množina.
(Někdy se místo $X - Y$ píše $X \setminus Y$.)

Symboly $X \cup Y$ a $X \cap Y$ označují *sjednocení* a *průnik* tříd X a Y, tedy třídy

$$X \cup Y = \{z\ ;\ (z \in X) \vee (z \in Y)\} \quad \text{a}$$
$$X \cap Y = \{z\ ;\ (z \in X) \wedge (z \in Y)\}.$$

Pro množiny x,y máme ovšem $x \cup y = \bigcup\{x, y\}$, $x \cap y = \bigcap\{x, y\}$, kde $\{x, y\}$ označuje (neuspořádanou) množinovou *dvojici*, jejíž existenci zaručuje axiom dvojice. Pro $x = y$ je $\{x, y\} = \{x\}$, tzv. *singleton* z x.

Třídy X, Y jsou *disjunktní*, jestliže $X \cap Y = \emptyset$.

—13—

Predikáty $\neq, \notin, \subset, \subseteq, \supset, \supseteq$ zavádíme následujícími definicemi:

$$x \neq y \overset{\text{df}}{\leftrightarrow} \neg(x = y)$$
$$x \notin y \overset{\text{df}}{\leftrightarrow} \neg(x \in y)$$
$$x \subseteq y \overset{\text{df}}{\leftrightarrow} (\forall z)(z \in x \to z \in y)$$
$$x \subset y \overset{\text{df}}{\leftrightarrow} (x \subseteq y \wedge x \neq y)$$
$$x \supseteq y \overset{\text{df}}{\leftrightarrow} y \subseteq x$$
$$x \supset y \overset{\text{df}}{\leftrightarrow} y \subset x$$

—14—

Uspořádané dvojice

Uspořádaná dvojice množin x a y je definována jako

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}.$$

Speciálně je $\langle x, x\rangle = \{\{x\}\}$.

Úkol: dokažte, že uvedená definice zaručuje požadovanou vlastnost uspořádané dvojice, tj. že

$$\langle x_1, y_1\rangle = \langle x_2, y_2\rangle \leftrightarrow (x_1 = x_2 \wedge y_1 = y_2)$$

—15—

Uspořádané n-tice

Uspořádané n-tice lze definovat pomocí dvojic induktivně takto:

$$\langle x\rangle_1 = x, \quad \langle x_1, \ldots, x_{n+1}\rangle_{n+1} = \langle\langle x_1, \ldots, x_n\rangle_n, x_{n+1}\rangle$$

Později, až zavedeme přirozené čísla v teorii množin, budeme místo takto definovaných n-tic dávat spíše přednost konečným posloupnostem délky n, tj. zobrazením s definičním oborem $\{0, \ldots, n-1\}$.

—16—

Další důležité operace na množinách a třídách

$-X = \{x\ ;\ x \notin X\}$ — *doplněk*; doplněk množiny je vždy vlastní třída.

$X \times Y = \{\langle x, y\rangle\ ;\ x \in X \wedge y \in Y\}$ — *kartézský součin*

$X^n = \{\langle x_1, \ldots, x_n\rangle_n\ ;\ x_1 \in X \wedge \ldots \wedge x_n \in X\}$ — *kartézská mocnina*

$\mathrm{dom}(X) = \{x\ ;\ (\exists y)(\langle x, y\rangle \in X)\}$ — *definiční obor*

$\mathrm{rng}(X) = \{y\ ;\ (\exists x)(\langle x, y\rangle \in X)\}$ — *obor hodnot*

$X^{-1} = \{\langle y, x\rangle\ ;\ \langle x, y\rangle \in X\}$ — *inverze*

$X''Y = \{z\ ;\ (\exists y)(\langle y, z\rangle \in X\}$ — *obraz*; místo $X''Y$ se někdy píše též $X[Y]$.

$X{\restriction}Y = \{\langle x, y\rangle\ ;\ \langle x, y\rangle \in X \wedge x \in Y\}$ — *parcializace*

$\mathcal{P}(X) = \{u\ ;\ u \subseteq X\}$ — *potence*

—17—

Tvrzení: *Jsou-li x a y množiny, jsou i $x \times y$, x^n, $\mathrm{dom}(x)$, $\mathrm{rng}(x)$, x^{-1}, $x''y$, $x{\restriction}y$ a $\mathcal{P}(x)$ množiny.*

Pro $\mathcal{P}(x)$ to vyplývá z axiomu potence, dále se užije toho, že usp. dvojice $\langle u, v\rangle = \{\{u\}, \{u, v\}\}$ je prvkem $\mathcal{P}(\mathcal{P}(\{u, v\}))$, tudíž

$x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y))$
$\mathrm{dom}(x) \subseteq \bigcup\bigcup x$,
$\mathrm{rng}(x) \subseteq \bigcup\bigcup x$,
$x^{-1} \subseteq (\mathrm{rng}(x) \times \mathrm{dom}(x))$,
$x''y \subseteq \bigcup\bigcup x$,
$x{\restriction}y \subseteq x$,
$x^n = x^{n-1} \times x$.

Tvrzení je tedy důsledkem axiomu vydělení.

—18—

Omezené kvantifikátory, značení

Zápis $(\forall x \in X)\varphi$ užíváme jako zkratku za $(\forall x)(x \in X \to \varphi)$.

Analogicky, $(\exists x \in X)\varphi$ je zkratka za $(\exists x)(x \in X \wedge \varphi)$.

Úkol: *ověřte, že* $(\forall x \in X)\varphi \leftrightarrow \neg(\exists x \in X)\neg\varphi$.

Dále píšeme $(\forall x_1, \ldots, x_n)$ jako zkratku za blok kvantifikátorů $(\forall x_1) \ldots (\forall x_n)$.
Analogicky pro $(\forall x_1, \ldots, x_n \in X)$, $(\exists x)$ a $(\exists x_1, \ldots, x_n \in X)$.

Podobně $\{x \in X\ ;\ \varphi\}$ je zkratka za třídový term $\{x\ ;\ x \in X \wedge \varphi\}$.

—19—

Relace

n-ární relace na třídě X je třída $R \subseteq X^n$.

Místo 2-ární říkáme *binární relace* nebo jen *relace*.
Zřejmě pak $R \subseteq \mathrm{dom}(R) \times \mathrm{rng}(R)$.

Nechť R je relace na X.
Je-li $\langle x, y\rangle \in R$, říkáme, že x a y jsou *v relaci* R. Třída $R''\{x\}$ je tzv. *obraz* neboli *extenze* prvku x v relaci R. Je to třída všech y, jež jsou s x v relaci R.

Složením relací R, S nazveme relaci

$$R \circ S = \{\langle x, y\rangle\ ;\ (\exists z)(\langle x, z\rangle \in R \wedge \langle z, y\rangle \in S\}.$$

—20—

Zobrazení

Zobrazení, neboli *funkce*, každá relace F (na univerzální třídě $\mathbf{V}$) splňující následující podmínku jednoznačnosti:

$$(\forall x, y, z)((\langle x, y\rangle \in F \wedge \langle x, z\rangle \in F) \to y = z)$$

Je-li F zobrazení a $\langle x, y\rangle \in F$, značíme y symbolem $F(x)$.

$\mathrm{dom}(F)$ je tzv. *definiční obor* zobrazení F;
$\mathrm{rng}(F)$ je tzv. *obor hodnot* zobrazení F.

Je-li F zobrazení takové, že $X = \mathrm{dom}(F)$, $Y \supseteq \mathrm{rng}(F)$, píšeme $F : X \to Y$, čteme: F je *zobrazení X do Y*.

Jsou-li F,G zobrazení, platí $(\forall x \in \mathrm{dom}(F))((F \circ G)(x) = G(F(x))$.

—21—

Zobrazení F je *prosté*, jestliže

$$(\forall a, b \in \mathrm{dom}(F))(a \neq b \to F(a) \neq F(b))$$

Je-li $F : X \to Y$ a $\mathrm{rng}(F) = Y$, říkáme, že F je zobrazení X *na* Y. Je-li zřejmé, že se jedná o třídu Y, říkáme krátce, že F je *na*.

Zobrazení $F : X \to Y$ je *vzájemně jednoznačné* neboli *bijekce*, je-li současně prosté a na.

Příkladem je např. *identické zobrazení* $\mathbf{Id} = \{\langle x, x\rangle \ ; \ x \in V\}$ (též *identická relace* či *diagonála*). Pro třídu X dále klademe $\mathbf{Id}_X = \mathbf{Id} \restriction X$.

—22—

Kartézská mocnina

Je-li a množina a X libovolná třída, definujeme dále ${}^aX$ jako třídu všech zobrazení množiny a do X:

$${}^aX = \{f \ ; \ f : a \to X\} \quad \text{tzv. } \textit{množinová} \text{ (též } \textit{kartézská}\text{) } \textit{mocnina}$$

Jsou-li a, x množiny, je ${}^ax$ množina (je totiž ${}^ax \in \mathcal{P}(\mathcal{P}(a \times x))$).

Pro $a = \emptyset$ máme ${}^\emptyset X = \{\emptyset\}$, neboť $\emptyset$ je zobrazení, $\mathrm{dom}(\emptyset) = \emptyset$.

—23—

Indexovaný soubor množin

Zobrazení x s $\mathrm{dom}(x) = I$ lze chápat též jako *soubor množin* $x(i)$ *indexovaný prvky množiny* I. Místo $x(i)$ pro $i \in I$ pak píšeme jen x_i a místo x píšeme

$$\langle x_i \ ; \ i \in I\rangle \text{ či krátce } \langle x_i\rangle_{i\in I}, \text{ případně jen } \langle x_i\rangle_I \qquad (1)$$

O množinách x_i pak mluvíme jako o prvcích souboru $\langle x_i\rangle_I$.

Sjednocení souboru množin (1) je množina $\bigcup_{i\in I} x_i = \bigcup \mathrm{rng}(x)$.
Průnik souboru množin (1) je množina $\bigcap_{i\in I} x_i = \bigcap \mathrm{rng}(x)$.
Kartézský součin souboru množin (1) je množina

$$\bigtimes_{i\in I} x_i = \{f \ ; \ f \text{ je zobrazení, } \mathrm{dom}(f) = I \text{ a } (\forall i \in I) f(i) \in x_i\}.$$

Je to množina, neboť $\bigtimes_{i\in I} x_i \subseteq {}^I(\bigcup_{i\in I} x_i)$.

Místo $\bigtimes_{i\in I} x_i, \bigcup_{i\in I} x_i, \bigcap_{i\in I} x_i$ píšeme běžně jen $\bigtimes_I x_i, \bigcup_I x_i, \bigcap_I x_i$.

—24—

Booleovské vlastnosti operací $\cap$, $\cup$, $-$

$X \cap Y = Y \cap X, \quad X \cup Y = Y \cup X$	*komutativita*
$(X \cap Y) \cap Z = X \cap (Y \cap Z)$	*asociativita*
$(X \cup Y) \cup Z = X \cup (Y \cup Z)$	
$X \cap X = X, \quad X \cup X = X$	*idempotence*
$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	*distributivita*
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	
$X \cup (X \cap Y) = X, \quad X \cap (X \cup Y) = X$	*zákony absorpce*
$-(X \cap Y) = (-X) \cup (-Y)$	*De Morganova pravidla*
$-(X \cup Y) = (-X) \cap (-Y)$	
$-(-X) = X$	*pravidlo dvojího komplementu*
$X \cap \emptyset = \emptyset, \quad X \cup \emptyset = X$	*zákony o* $\emptyset$ *a univerzální třídě* $\mathbf{V}$
$X \cap \mathbf{V} = X, \quad X \cup \mathbf{V} = \mathbf{V}$	
$X \cap -X = \emptyset, \quad X \cup -X = \mathbf{V}, \quad \emptyset \neq \mathbf{V}$	

—25—

Uvedené rovnosti pro operace $\cap, \cup, -$, jsou vlastně axiomy Booleových algeber.

Omezíme-li se na množinu všech podmnožin nějaké množiny x, tj. na $\mathcal{P}(x)$, přičemž všude třídu $\mathbf{V}$ nahradíme množinou x (takže např. $-y$ bude značit množinu $x - y = \{z \in x \ ; \ z \notin y\}$), pak $\mathcal{P}(x)$ tvoří s operacemi $\cap, \cup, -$ Booleovu algebru.

—26—

Další vlastnosti operací

Pravidla o rozdílu tříd

$$X - Y = X \cap (-Y) \qquad X - \emptyset = X, \quad \emptyset - X = \emptyset$$
$$X - X = \emptyset \qquad X - \mathbf{V} = \emptyset$$
$$(X - Y) - Z = X - (Y \cup Z)$$
$$X - (Y - Z) = (X - Y) \cup (X \cap Z)$$
$$(X - Y) - Z \subseteq X - (Y - Z)$$

Vlastnosti inkluze

$$X \subseteq Y \wedge Y \subseteq X \leftrightarrow X = Y \qquad X \subseteq \mathbf{V}, \quad \emptyset \subseteq X$$
$$X \subseteq Y \leftrightarrow X \cap Y = X \qquad X \subseteq Y \leftrightarrow X \cup Y = Y$$

Vlastnosti potence a sjednocení:

$$\bigcup \mathcal{P}(X) = X, \quad X \subseteq \mathcal{P}(\bigcup X)$$

—27—

Distributivní zákony pro $\times$: Buď $\square$ operace $\cup$ nebo $\cap$. Pak:

$$X \times (Y \square Z) = (X \times Y) \square (X \times Z), \quad (X \square Y) \times Z = (X \times Z) \square (Y \times Z)$$

Vlastnosti obrazu:

$$X''(Y \cup Z) = X''Y \cup X''Z \qquad X''(Y \cap Z) \subseteq X''Y \cap X''Z$$
$$X''Y - X''Z \subseteq X''(Y - Z)$$

Je-li F funkce, platí

$$F^{-1}[Y \cap Z] = F^{-1}[Y] \cap F^{-1}[Z],$$
$$F^{-1}[Y - Z] = F^{-1}[Y] - F^{-1}[Z].$$

Pro relace R, S, T platí:

$$(R^{-1})^{-1} = R, \quad (R \circ S)^{-1} = S^{-1} \circ R^{-1}, \quad R \circ (S \circ T) = (R \circ S) \circ T$$

—28—

Relace ekvivalence

Relace R na třídě A je:

- *reflexivní* na A, jestliže $(\forall x \in A)\langle x, x\rangle \in R$, tj. $\mathbf{Id}_A \subseteq R$
- *symetrická*, když $\langle x, y\rangle \in R \to \langle y, x\rangle \in R$,
- *tranzitivní*, když $(\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R) \to \langle x, z\rangle \in R$.

Relace E je *ekvivalence na třídě* A, je-li reflexivní na A, symetrická a tranzitivní.

Říkáme, že E je *ekvivalence*, je-li ekvivalencí na svém definičním oboru.

Extenzi prvku x v relaci E, $E''\{x\}$, nazýváme též *třídou ekvivalence prvku* x a značíme ji symbolem $[x]_E$. Říkáme, že x je *reprezentant* třídy $[x]_E$.

—29—

Faktorizace, pokrytí, rozklady

Je-li E ekvivalence na množině A, nazýváme množinu

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

faktorizací či faktorem množiny A podle ekvivalence E.

Řekneme, že třída C je *pokrytí* třídy X, neboli že *pokrývá* třídu X, jestliže $C \subseteq \mathcal{P}(X) - \{\emptyset\}$ a $\bigcup C = X$.

C je *rozklad* neboli *disjunktní pokrytí* třídy X, je-li pokrytím třídy X sestávajícím ze vzájemně disjunktních množin, tj. $(\forall x, y \in C)(x \neq y \to x \cap y = \emptyset)$.

Je-li E ekvivalence na množině A, je A/E rozklad množiny A.

Naopak, je-li C rozklad množiny A, je relace

$$E = \{\langle a, b\rangle \in A \times A \,;\, (\exists u \in C)(\{a, b\} \subseteq u)\}$$

ekvivalencí na A a $A/E = D$.

—30—

Kongruence

Buď A třída, $F : A^n \to A$ funkce a E ekvivalence na A.

Řekneme, že E je *kongruence vůči F na A*, jestliže platí

$$(\forall x_1, \ldots, x_n)(\forall x'_1, \ldots, x'_n)(\langle x_1, x'_1\rangle \in E \wedge \ldots \wedge \langle x_n, x'_n\rangle \in E \to \langle F(x_1, \ldots, x_n), F(x'_1, \ldots, x'_n)\rangle \in E)$$

Je-li E kongruence vůči F na A, můžeme funkci F přenést z A na A/E jakožto funkci $F' : (A/E)^n \to A/E$ definovanou předpisem:

$$F'([x_1]_E, \ldots, [x_n]_E) = [F(x_1, \ldots, x_n)]_E.$$

(tj. tzv. pomocí reprezentantů; kongruence zaručuje, že definice je korektní).
Faktorizace je důležitý a hojně užívaný matematický obrat. Často konstruujeme určitou strukturu tak, že nejprve vytvoříme nějakou o dost větší množinu a poté některé její prvky tzv. ztotožníme. Je-li toto ztotožnění kongruence, zachovají se i operace definované na původní větší množině.

—31—

Příklad: Strukturu $\mathbb{Q}$ racionálních čísel s operacemi sčítání, odčítání, násobení a inverzního prvku, lze získat faktorizací struktury $\langle \mathbb{Z} \times (\mathbb{N} - \{0\}), \oplus, \ominus, \odot, {}^{-1}\rangle$,

- $\langle a, b\rangle \oplus \langle c, d\rangle = \langle ad + bc, bd\rangle$,
- $\langle a, b\rangle \ominus \langle c, d\rangle = \langle ad - bc, bd\rangle$,
- $\langle a, b\rangle \otimes \langle c, d\rangle = \langle ac, bd\rangle$,
- $\langle a, b\rangle^{-1} = \langle b, a\rangle$, pro $a \geq 0$
- $\langle a, b\rangle^{-1} = \langle -b, |a|\rangle$, pro $a < 0$

podle kongruence $\sim$ definované vztahem: $\langle a, b\rangle \sim \langle c, d\rangle \leftrightarrow ad = bc$.

(Obvyklé uspořádání lze na $\mathbb{Q}$ zavést vztahem $[\langle a, b\rangle]_\sim <^{\mathbb{Q}} [\langle c, d\rangle]_\sim \leftrightarrow ad < bc$, kde na pravé straně $<$ značí uspořádání celých čísel.)

—32—

Příklad: Nechť $\equiv_p$ („rovnost modulo p“) je relace definovaná na $\mathbb{Z}$ vztahem

$$a \equiv_p b \leftrightarrow p \,|\, a - b,$$

kde $p \,|\, x$ značí *„p dělí x“*.

Úkol: *Ověřte: je-li p prvočíslo, je $\equiv_p$ kongruence vůči sčítání a násobení na $\mathbb{Z}$.*

Faktorizací okruhu $\langle \mathbb{Z}, 0, 1, +, \cdot\rangle$ podle kongruence $\equiv_p$, kde $p > 1$ je prvočíslo, získáme konečné, algebraicky uzavřené těleso charakteru p, označované $\mathbb{Z}_p$.

—33—

Uspořádání

Relace R na třídě A je:

- *slabě antisymetrická*, jestliže $\langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \to x = y$
- *antisymetrická*, tj. platí-li $\langle x,y\rangle \in R \to \langle y,x\rangle \notin R$
- *trichotomická* na A, platí-li $(\forall x,y \in A)(\langle x,y\rangle \in R \vee x = y \vee \langle y,x\rangle \in R)$.

R je *uspořádání* na A, je-li reflexivní na A, slabě antisymetrická a tranzitivní.

R je *ostré uspořádání*, je-li antisymetrická a a tranzitivní.

Z uvedených vlastností ihned plyne, že ostré uspořádání je též *antireflexivní*, tj. že platí $(\forall x \in A)(\langle x,x\rangle \notin R)$.

Je-li relace R uspořádání (resp. ostré uspořádání) a R je trichotomická na A, nazývá se R *lineární uspořádání* (resp. *ostré lineární uspořádání*) na A.

—34—

Řekneme-li, že (A,R) je (ostré) uspořádání, znamená to, že R je (ostré) uspořádání na A a $A \neq \emptyset$. Místo $\langle x,y\rangle \in R$ v takovém případě obvykle píšeme $x\,R\,y$.

Neostrému uspořádání (A,R) odpovídá ostré uspořádání $(A, R - \mathbf{Id}_A)$.

Relaci uspořádání na nějaké třídě značíme nejčastěji symboly $\leq, \preceq, \sqsubseteq, \trianglelefteq$ apod. Odpovídající ostré uspořádání pak symboly $<, \prec, \sqsubset, \triangleleft$.

Třída $X \subseteq A$ je tzv. *dolní třída* v uspořádání $(A,\leq)$, jestliže

$$(\forall x \in X)(\forall y \in A)(y \leq x \to y \in X).$$

Platí-li naopak

$$(\forall x \in X)(\forall y \in A)(x \leq y \to y \in X)$$

je to tzv. *horní třída*.

—35—

Nechť $\emptyset \neq X \subseteq A$. Prvek $y \in A$ je v uspořádání $(A,\leq)$

- *minoranta třídy* X, jestliže $(\forall x \in X)(y \leq x)$,
- *majoranta třídy* X, jestliže $(\forall x \in X)(x \leq y)$.
- *nejmenší prvek třídy* X, je-li minorantou a prvkem X
- *největší prvek třídy* X , je-li majorantou a prvkem X
- *minimální prvek třídy* X, platí-li $y \in X$ a $(\forall x \in X)\neg x < a$
- *maximální prvek třídy* X, platí-li $y \in X$ a $(\forall x \in X)\neg y < x$
- *infimum třídy* X (píšeme $y = \inf_{(A,\leq)}(X)$), jestliže je největším prvkem třídy všech minorant třídy X
- *supremum třídy* X (píšeme $y = \sup_{(A,\leq)}(X)$), jestliže je nejmenším prvkem třídy všech majorant třídy X

Pokud existují, jsou nejmenší prvek, největší prvek, infimum a supremum určeny jednoznačně. V lineárním uspořádání pojmy minimálního a nejmenšího prvku splývají. Obdobně je tomu s maximálním a největším prvkem.

—36—

$(A,\leq)$ je tzv. *dobré uspořádání*, má-li každá neprázdná podmnožina $u \subseteq A$ v uspořádání $(A,\leq)$ nejmenší prvek.

Každé dobré uspořádání je lineární, neboť jsou-li $x,y \in A$, musí mít množina $\{x,y\} \subseteq A$ nejmenší prvek, tudíž buď $x \leq y$ nebo $y \leq x$.

Množinové uspořádání $(a,\leq)$ je *úplný svaz*, má-li každá neprázdná podmnožina množiny a v $(a,\leq)$ infimum i supremum.

Příklad: Nechť $(\mathcal{P}(a),\subseteq)$ značí uspořádání $(\mathcal{P}(a),R)$, kde

$$R = \{\langle x,y\rangle \,;\, x \subseteq y \subseteq a\}.$$

Je-li $\emptyset \neq u \subseteq \mathcal{P}(a)$, pak $\sup_{(\mathcal{P}(a),\subseteq)}(u) = \bigcup u$ a $\inf_{(\mathcal{P}(a),\subseteq)}(u) = \bigcap u$, $(\mathcal{P}(a),\subseteq)$ je tedy úplný svaz.

Je-li $x \in a$, je $\{x\}$ minimální prvek třídy $\mathcal{P}(a) - \{\emptyset\}$ v uspořádání $(\mathcal{P}(a),\subseteq)$.

Jiným příkladem úplného svazu je třeba uzavřený interval $[0,1]$ reálných čísel s obvyklým uspořádáním reálných čísel.

—37—

Věta (*o pevném bodu*): *Buď* $(a, \leq)$ *úplný svaz a* f neklesající funkce *na* $(a, \leq)$, *tj.*

$$f : a \to a \quad \text{a} \quad (\forall x, y \in a)(x \leq y \to f(x) \leq f(y)).$$

Pak existuje $u \in a$ *tak, že* $f(u) = u$. *(Říkáme, že* u *je pevný bod funkce* f*.)*

Důkaz. Uvažujme množinu $t = \{v \in a\ ;\ v \leq f(v)\} \subseteq a$. Platí $t \neq \emptyset$, neboť zjevně $\inf_{(a,\leq)}(a) \in t$. Označme u supremum množiny t. Ukážeme, že u je pevný bod f. Pro každé $v \in t$ tedy platí $v \leq u$ a díky definici t a monotónnosti zobrazení f tedy $v \leq f(v) \leq f(u)$ a tudíž i $u = \sup_{(a,\leq)}(t) \leq f(u)$ z definice suprema. Z monotónnosti proto plyne $f(u) \leq f(f(u))$. Pak ovšem $f(u) \in t$ (dle definice t), tudíž $f(u) \leq u$ (neb u je majoranta t); jelikož víme i $u \leq f(u)$, dostáváme celkem $u = f(u)$ díky slabé antisymetrii uspořádání. □

—38—

Mohutnost množiny

Pojem mohutnost množiny, jenž odpovídá intuitivně pojmu *„počet prvků“*, zavádíme formálně poněkud oklikou, totiž prostřednictvím srovnání. Otázce zda a případně kdy je možné se ptát *„**kolik** je mohutnost množiny“*, se budeme věnovat později.

Pro porovnávání *„velikostí“* množin zavádíme dvě důležité relace:

Množina x je *subvalentní* množině y, neboli, x má *mohutnost menší nebo rovnu mohutnosti* y (píšeme $x \preccurlyeq y$), jestliže existuje prosté zobrazení množiny x do y.

Množiny x a y jsou *ekvipotentní*, neboli *mají stejnou mohutnost* (píšeme $x \approx y$), existuje-li prosté zobrazení x na y (bijekce).

Platí-li $x \preccurlyeq y$, nikoli však $x \approx y$, říkáme, že x je *ostře subvalentní* y, neboli že množina x má (ostře) *menší mohutnost než množina* y, a píšeme $x \prec y$.

—39—

Evidentně platí následující vztahy

$x \approx x$	(identická bijekce $\mathbf{Id}_x : x \to x$)
$x \approx y \to y \approx x$	(inverze f^{-1} bijekce f je bijekcí)
$(x \approx y \wedge y \approx z) \to x \approx z$	(složení bijekcí je bijekce)
$x \subseteq y \to x \preccurlyeq y$	$\mathbf{Id}_x : x \to y$ je prosté
$x \preccurlyeq x$	
$(x \preccurlyeq y \wedge y \preccurlyeq z) \to x \preccurlyeq z$	(složení prostých zobrazení je prosté)

Z uvedených vlastností vidíme, že

- relace $\approx$ je ekvivalence na třídě $\mathbf{V}$. Je-li $x \neq \emptyset$, je ovšem $[x]_\approx$ vlastní třída (stačí například uvážit, že $\{\{y\} \times x\ ;\ y \in \mathbf{V}\}$ je vlastní třída a část $[x]_\approx$),
- relace $\preccurlyeq$ je reflexivní a tranzitivní.

—40—

Věta (*Cantor, Bernstein*):

$$(x \preccurlyeq y \wedge y \preccurlyeq x) \to x \approx y$$

Důkaz. Podle předpokladu existují prosté funkce $f : x \to y$ a $g : y \to x$. Stačí dokázat, že existuje $u \subseteq x$ takové, že platí

$$x - u = g[y - f[u]], \quad \text{neboli} \quad u = x - g[y - f[u]],$$

neboť pak můžeme definovat prosté zobrazení h množiny x na množinu y předpisem

$$h(z) = \begin{cases} f(z) & \text{pro } z \in u \\ g^{-1}(z) & \text{pro } z \in x - u \end{cases}$$

u nalezneme jako pevný bod funkce $H : \mathcal{P}(x) \to \mathcal{P}(x)$, $H(u) = x - g[y - f[u]]$. Jelikož $(\mathcal{P}(x), \subseteq)$ je úplný svaz, stačí podle věty o pevném bodu, ukážeme-li, že H je $\subseteq$-neklesající. Nechť $u \subseteq v \subseteq x$. Pak zřejmě $f[u] \subseteq f[v]$, $y - f[u] \supseteq y - f[v]$, tedy $g[y - f[u]] \supseteq g[y - f[v]]$ a konečně $H(u) = x - g[y - f[u]] \subseteq x - g[y - f[v]] = H(v)$. □

—41—

Škála mohutností množin není shora omezená; ke každé množině totiž existuje množina větší mohutnosti, jak ukazuje následující věta:

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

Důkaz. Zřejmě $x \preccurlyeq \mathcal{P}(x)$ (stačí např., položíme-li $f(z) = \{z\}$ pro $z \in x$). Zbývá dokázat $\neg(x \approx \mathcal{P}(x))$.

Sporem: nechť f je prostá funkce zobrazující x **na** $\mathcal{P}(x)$. Položme $u = \{z \in x \,;\, z \notin f(z)\}$. Je $u \in \mathcal{P}(x)$, tudíž musí existovat $a \in x$ tak, že $f(a) = u$. Platí buď $a \in f(a)$, nebo $a \notin f(a)$. Každá z těchto formulí je však v bezprostředním s sporu s definicí množiny u. □

—42—

➠ Domluvme se, že prázdnou množinu $\emptyset$ budeme též označovat symbolem 0, singleton $\{0\}$ symbolem 1 a dvouprvkovou množinu $\{0,1\}$ symbolem 2 (posléze analogicky zavedeme všechna přirozená čísla).

Disjunktní sjednocení tříd X, Y je třída $X \uplus Y$ definovaná vztahem

$$X \uplus Y = (\{0\} \times X) \cup (\{1\} \times Y) = \{\langle 0, a\rangle \,;\, a \in X\} \cup \{\langle 1, b\rangle \,;\, b \in Y\}.$$

Pak: $X = (X \uplus Y)''\{0\}$ a $Y = (X \uplus Y)''\{1\}$.

Pro množiny x, y platí zřejmě $x \cup y \preccurlyeq x \uplus y$. Je-li x alespoň dvouprvková, je $x \uplus x \preccurlyeq x \times x$. Pro $x \approx x'$, $y \approx y'$ a z dále platí:

$$x \uplus y \approx x' \uplus y' \qquad x \times y \approx x' \times y'$$
$$x \uplus y \approx y \uplus x \qquad x \times y \approx y \times x$$
$$x \uplus (y \uplus z) \approx (x \uplus y) \uplus z \qquad x \times (y \times z) \approx (x \times y) \times z$$
$$x \times (y \uplus z) \approx (x \times y) \uplus (x \times z)$$
$${}^{y}x \approx {}^{y'}x' \qquad \mathcal{P}(x) \approx \mathcal{P}(x')$$

—43—

Příklad: Ověříme např. $x \times (y \uplus z) \approx (x \times y) \uplus (x \times z)$:

Náznak důkazu. Prvky množiny vlevo jsou tvaru $d = \langle a, \langle i, b\rangle\rangle$, kde $a \in x, b \in y \cup z$, a $i \in \{0,1\}$, přičemž

$$(i = 0 \to b \in y) \wedge (i = 1 \to b \in z)$$

Nechť f je zobrazení přiřazující libovolnému takovému prvku $d = \langle a, \langle i, b\rangle\rangle$ množinu $f(d) = \langle i, \langle a, b\rangle\rangle$.

Snadno se ověří, že:

1. $f(d) \in (x \times y) \uplus (x \times z)$,
2. $\mathrm{rng}(f) = (x \times y) \uplus (x \times z)$, neboli f je na,
3. f je prosté

□

—44—

Množinové operace $x \uplus y$, $x \times y$ a ${}^{y}x$ splňují podobné zákony vůči relacím $\approx$ a $\preccurlyeq$, jako platí pro sčítání, násobení a mocnění přirozených čísel vůči $\leq$ a $=$. Platí totiž:

- ${}^{\emptyset}x = \{\emptyset\}$ a ${}^{y}\emptyset = \emptyset$ pro $y \neq \emptyset$.
- Pro množiny x, y, u, v dále platí:

$$\emptyset \neq x \preccurlyeq y \to {}^{x}u \preccurlyeq {}^{y}u \qquad \boxed{{}^{y}({}^{x}u) \approx {}^{(y\times x)}u}$$
$$u \preccurlyeq v \to {}^{x}u \preccurlyeq {}^{x}v \qquad {}^{(x\uplus y)}u \approx {}^{x}u \times {}^{y}u$$

Dokažme například formuli v rámečku:

Pro každé zobrazení $f : y \to {}^{x}u$ definujme funkci $h_f : y \times x \to u$ vztahem

$$h_f(\langle a, b\rangle) = f(a)(b).$$

Přiřazení $h : f \mapsto h_f$ určuje funkci $h : {}^{y}({}^{x}u) \to {}^{(y\times x)}u$.

Snadno se ověří,že h je prostá a na. □

—45—

Tvrzení: *1.* $\mathcal{P}(a) \approx {}^a2$.

2. Je-li $a \times a \approx a$ *a* $a \not\approx 1$, *pak* ${}^a2 \approx {}^aa$ *a* $\mathcal{P}(a) \times \mathcal{P}(a) \approx \mathcal{P}(a)$.

Důkaz. 1. Zobrazení $h : \mathcal{P}(a) \to {}^a2$ buď definováno předpisem

$$h(x)(z) = \begin{cases} 1 & \text{pro } z \in x \\ \emptyset & \text{pro } z \in a - x \end{cases}$$

Snadno se nahlédne, že h je prosté zobrazení $\mathcal{P}(a)$ na ${}^a2$.

2. Pro $a = \emptyset$ platí tato část tvrzení evidentně. Buď tedy $a \succcurlyeq 2$.

Pak zřejmě ${}^aa \succcurlyeq {}^a2$. Dále ${}^aa \subseteq \mathcal{P}(a \times a)$, tedy ${}^aa \preccurlyeq \mathcal{P}(a \times a)$ a tudíž, je-li $a \times a \approx a$, je ${}^aa \preccurlyeq \mathcal{P}(a) \approx {}^a2$.

Dále: $a \preccurlyeq 2 \times a \preccurlyeq a \times a \approx a$ a tedy

$$\mathcal{P}(a) \times \mathcal{P}(a) \approx {}^a2 \times {}^a2 \approx {}^{a \uplus a}2 = {}^{2 \times a}2 \approx {}^a2 \approx \mathcal{P}(a)$$

□

—46—

Přirozená čísla v teorii množin

Přirozená čísla zavádíme do teorie množin způsobem, jenž pochází od von Neumanna: přirozené číslo je množina všech menších přirozených čísel. Tedy:

- 0 je prázdná množina $\emptyset$
- 1 je jednoprvková množina $\{0\} = \{\emptyset\}$
- 2 je dvouprvková množina $\{0, 1\} = \{\emptyset, \{\emptyset\}\}$
- 3 je tříprvková množina $\{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, atd.

  ...
- n je tedy n-prvková množina $\{0, \ldots, n-1\}$
- $n+1$ je tedy $n+1$-prvková množina $\{0, \ldots, n\} = n \cup \{n\}$

Dále se budeme věnovat tomu, zda a jak lze definovat množinu **všech přirozených čísel**.

—47—

Induktivní množiny

Řekneme, že množina z je *induktivní*, jestliže

$$\emptyset \in z \wedge (\forall x)(x \in z \to x \cup \{x\} \in z).$$

Libovolná induktivní množina tak zřejmě obsahuje každé konkrétní přirozené číslo n, zkonstruované dle von Neumanna.

Tvrzení: *Existuje nejmenší induktivní množina (v uspořádání inkluzí* $\subseteq$*).*

Důkaz. Axiom nekonečna zaručuje existenci nějaké induktivní množiny z_0. Položme $\omega = \bigcap\{z \subseteq z_0 \ ; \ z \text{ je induktivní}\}$. ω je induktivní, neboť $\emptyset$ je prvkem všech induktivních podmnožin množiny z_0 a je-li $y \in \omega$, je $y \in z$ a tedy i $y \cup \{y\} \in z$ pro každou induktivní $z \subseteq z_0$, tudíž $y \cup \cup \{y\} \in \omega$. Dále, ω je *nejmenší* ind. množina, neboť je-li z_1 induktivní, je $z_0 \cap z_1$ také induktivní; jelikož $z_0 \cap z_1 \subseteq z_0$, je $\omega \subseteq z_0 \cap z_1$, a tedy $\omega \subseteq z_1$. □

—48—

Množina přirozených čísel

Množinou přirozených čísel nazýváme nejmenší induktivní množinu a značíme ji ω, případně $\mathbb{N}$. Je to tedy nejmenší množina obsahující $\emptyset$ a uzavřená na operaci *„následníka“* $x \cup \{x\}$ (odpovídá operaci $+1$).

Na množině ω budeme definovat operace součtu, součinu. S jejich pomocí lze zavést další základní pojmy aritmetiky přirozených čísel. Ukážeme, že pro prvky ω platí princip indukce, jenž umožňuje dokázat všechna tvrzení známá z elementární aritmetiky.

Prvkům množiny ω budeme říkat *přirozená čísla v teorii množin*, krátce *přirozená čísla*.

Uvědomme si však, že přirozená o nichž mluvíme v meta-jazyce (např. ve větě „formule φ má n volných proměnných“ nejsou objekty teorie množin. Říkáme jim *metamatematická přirozená čísla*.

—49—

Každému metamatematickému číslu n odpovídá nějaké přirozené číslo $\overline{n}$ v teorii množin. Získáme je n-násobnou aplikací operace následníka na $\emptyset$, čili $\overline{n} = \underbrace{S(\ldots(S}_{n\text{-krát}}(\emptyset))\ldots)$, kde $S(x) = x \cup \{x\}$.

Na opačný vztah obecně nelze spoléhat: z principu kompaktnosti v logice plyne, že teorie množin rozšířená o novou konstantu c a axiomy

$$c \in \omega \wedge c \notin \overline{n}$$

pro každé (metamatematické) n, je bezesporná.

Nevyhneme se tak možnosti, že do ω padne i nějaký prvek, jenž není tvaru $\overline{n}$ pro žádné konkrétní metamatematické n.

S tím je třeba se smířit. Podstatné je, že se prvky množiny ω v teorii množin „chovají“ jako přirozená čísla.

—50—

Tvrzení (*Princip matematické indukce*):

(dvě alternativní formulace)

1. *Nechť $\varphi(x)$ je formule jazyka teorie množin. Pak platí*

$$(\varphi(\emptyset) \wedge (\forall x \in \omega)(\varphi(x) \to \varphi(x \cup \{x\}))) \to (\forall x \in \omega)\varphi(x)$$

2. *Nechť $z \subseteq \omega$ taková, že $\emptyset \in z$ a pro každé $x \in z$ je $x \cup \{x\} \in z$. Pak $z = \omega$.*

Důkaz. 1. Množina $y = \{x \in \omega \,;\, \varphi(x)\}$ je induktivní, tudíž $\omega \subseteq y$. Současně $y \subseteq \omega$ z definice.

2. Opět, z je induktivní, tedy $\omega \subseteq z$. Z předpokladu $z \subseteq \omega$, čili $\omega = z$. □

—51—

Uspořádání přirozených čísel

Označme $\leq$ relaci definovanou na množině ω vztahem

$$x \leq y \leftrightarrow (x = y \vee x \in y).$$

Tvrzení: *$(\omega, \leq)$ je dobré (a tedy lineární) uspořádání; je diskrétní, nemá největší prvek, jeho nejmenším prvkem je číslo 0 a $(\omega, \in)$ je odpovídající ostré uspořádání.*

Dále $(\forall x, y \in \omega)(x \leq y \leftrightarrow x \subseteq y)$.

Připomeňme, že lineární uspořádání $(A, \leq)$ je diskrétní, má-li každý prvek x, který není minimální, bezprostředního předchůdce (tj. existuje největší z prvků menších než x) a každý prvek x, který není maximální, má bezprostředního následníka (tj. existuje nejmenší z prvků větších než x).

Tvrzení dokážeme, nejprve ale dokážeme lemma...

—52—

Lemma: *Pro každé $x \in \omega$ platí:*

1. $x \neq 0 \to 0 \in x$,
2. $(\forall y \in \omega)(x \leq y \to x \subseteq y)$,
3. $(\forall y \in \omega)(x \in y \to x \cup \{x\} \leq y)$,
4. $x \notin x$

Důkaz. 1. Indukcí: je-li $x = 0$, není co dokazovat. Je-li $0 \in x$, je zjevně $0 \in x \cup \{x\}$.

2. Pro $x = y$ je to triviální; pro $x \in y$ indukcí dle y: pro $y = 0$ není co dokazovat. Platí-li to pro y a je-li $x \in y \cup \{y\}$, je buď $x \in y$ a pak dle indukčního předpokladu $x \subseteq y$, nebo $x = y$. V obou případech $x \subseteq y \subseteq y \cup \{y\}$.

3. Zvolme $x \in \omega$ libovolně, ale pevně. Formuli dokazujeme indukcí dle y. Je-li $y = 0$, není co dokazovat. Nechť formule platí pro y, dokážeme ji pro $y \cup \{y\}$. Nechť $x \in y \cup \cup \{y\}$. Pak buď $x = y$, odkud $x \cup \{x\} = y \cup \{y\}$, nebo $x \in y \neq x$ a tedy dle indukčního předpokladu $x \cup \{x\} \leq y$, odkud z definice $x \cup \{x\} \in y \cup \{y\}$.

4. Indukcí: pro $x = 0$ to platí. Nechť $x \notin x$. Kdyby $x \cup \{x\} \in x \cup \{x\}$, pak buď $x \cup \{x\} \in x$ odkud dle 2. a 3. $x \cup \{x\} \subseteq x$, nebo $x \cup \{x\} = x$. V obou případech $x \in x$, spor s indukčním předpokladem. □

—53—

Tvrzení: *$(\omega, \leq)$ je dobré (a tedy lineární) uspořádání; je diskrétní, nemá největší prvek, jeho nejmenším prvkem je číslo 0 a $(\omega, \in)$ je odpovídající ostré uspořádání. Navíc pro $x, y \in \omega$ je $x \leq y$ právě když $x \subseteq y$.*

Důkaz. $\leq$ je reflexivní z definice. Dle bodu 2 lemmatu, $x \leq y$ implikuje $x \subseteq y$. Je-li $x \leq y \leq z$ a $x \neq y$, pak $x \in y \subseteq z$, čili $x \in z$ a tedy $x \leq z$. Tudíž je $\leq$ tranzitivní. Slabá anti-symetrie plyne z tranzitivity a bodu 4 lemmatu. Kdyby totiž $x < y < x$, pak by speciálně $x \in y \subseteq x$, tudíž $x \in x$, spor.

Že $(\omega, \leq)$ je dobré, neboli že každá neprázdná podmnožina $u \subseteq \omega$ má $\leq$-nejmenší prvek, ukážeme sporem: Nechť u nemá $\leq$-nejmenší prvek. Označme v množinu všech minorant množiny u, tj. $v = \{x \in \omega\ ;\ (\forall y \in u)(x \leq y)\}$. Zřejmě $u \cap v = \emptyset$ (prvek průniku by byl nejmenší v u). Ze stejného důvodu $0 \in v$. Nechť $x \in v$. Pak pro každé $y \in u$ platí $x \in y$ (kdyby $x = y$, byl by $x \in u \cap v$). Dle bodu 2. lemmatu $x \cup \{x\} \leq y$, čili $x \cup \{x\} \in v$. Z principu indukce tedy $v = \omega$ a tedy $u = \emptyset$, spor.

$(\omega, \leq)$ je tedy lineární. Když $x \subseteq y$, je $x \leq y$, neb jinak $y < x$ a tedy $y \in y$, spor. $(\omega, \leq)$ nemá největší prvek, neboť $x < x \cup \{x\}$. Je diskrétní, neboť je-li $0 \neq x \in \omega$, pak existuje $y \in x$ tak, že $x = y \cup \{y\}$ (jinak by množina x byla induktivní). Kdyby existovalo $y < z < y \cup \{y\}$, pak $y \neq z$, a tedy $z \in y$, čili $y < z < y$, spor. □

—54—

Další číselné obory v teorii množin

K zavedení operací sčítání, násobení a umocňování na ω se vrátíme později.

Obor celých čísel $\mathbb{Z}$ zavedeme např. jako množinu $\omega \cup (\{1\} \times (\omega - \{0\}))$, přičemž prvek tvaru $\langle 1, x\rangle$, kde $0 \neq x \in \omega$, interpretujeme jako číslo $-x$. Operace na $\mathbb{Z}$ se zavedou jako vhodná rozšíření operací na ω.

Obor racionálních čísel lze zavést např. faktorizací množiny $\mathbb{Z} \times (\omega - \{0\})$, podle kongruence $\sim$ definované vztahem $\langle a, b\rangle \sim \langle c, d\rangle \leftrightarrow ad = bc$. Třídu této ekvivalence tvaru $[\langle a, 1\rangle]_\sim$, kde $a \in \mathbb{Z}$, navíc obvykle ztotožňujeme právě s číslem a.

Reálná čísla se v teorii množin obvykle konstruují na základě čísel racionálních, a to například pomocí tzv. *Dedekindových řezů*. Konstrukci reálných čísel probírat nebudeme.

—55—

Konečné množiny

Definice: Množina x je *konečná*, píšeme $\mathrm{Fin}(x)$, jestliže existuje $n \in \omega$ tak, že $x \approx n$. Množina je *nekonečná*, není-li konečná,

Třídu všech konečných množin značíme Fin, tj. $\mathrm{Fin} = \{x\ ;\ \mathrm{Fin}(x)\}$.

Tvrzení: *Každá induktivní množina je nekonečná.*

Důkaz. Je-li x induktivní, je $x \approx x - \{\emptyset\}$ (zobrazení $y \mapsto y \cup \{y\}$ dosvědčuje subvalenci $x \preccurlyeq x - \{\emptyset\}$). Dále indukcí: je-li $x \approx \emptyset$, je $x = \emptyset$ a x tedy není induktivní. Nechť $n \in \omega$, přičemž žádné $x \approx n$ není induktivní. Kdyby existovala induktivní množina $y \approx n \cup \{n\}$, pak zřejmě $n \approx x - \{\emptyset\}$ a tedy $n \approx x$, spor. □

—56—

Několik jednoduchých tvrzení o konečných množinách

1. $\mathrm{Fin}(x) \Rightarrow (\forall y)\mathrm{Fin}(x \cup \{y\})$

Důkaz. Snadno indukcí podle $n \approx x$. □

2.Princip indukce pro konečné množiny

$$(\emptyset \in A \wedge (\forall x \in A)(\forall y)(x \cup \{y\} \in A)) \rightarrow \mathrm{Fin} \subseteq A$$

Důkaz. Nechť A splňuje předpoklad implikace. Indukcí podle $n \in \omega$ snadno ověříme, že pro $x \approx n$ platí $x \in A$. □

3. $x \subseteq n \Rightarrow \mathrm{Fin}(x)$

Důkaz. Indukcí: pro $n = 0$ triviální, je-li $x \subseteq n \cup \{n\}$, je buď $x \subseteq n$, pak použijeme indukční předpoklad, nebo dle indukčního předpokladu $\mathrm{Fin}(x - \{n\})$ a tedy $\mathrm{Fin}(x)$ dle 1. □

—57—

4. $\mathrm{Fin}(x) \wedge \mathrm{Fin}(y) \Rightarrow \mathrm{Fin}(x \cup y)$

Důkaz. Indukcí podle $n \approx y$, pomocí 1. □

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

Důkaz. Indukcí pro konečné množiny. Zřejmě $\mathrm{Fin}(\mathcal{P}(\emptyset))$, neboť $\mathcal{P}(\emptyset) = \{\emptyset\}$. Zbývá dokázat, že je-li $\mathrm{Fin}(a)$ a $\mathrm{Fin}(\mathcal{P}(a))$, pak pro libovolné b je $\mathrm{Fin}(\mathcal{P}(a \cup \{b\}))$. To plyne z 4. a toho, že $\mathcal{P}(a \cup \{b\}) = \mathcal{P}(a) \cup c$, kde $c = \{x \cup \{b\}\ ;\ x \in \mathcal{P}(a)\} \approx \mathcal{P}(a)$, a tedy $\mathrm{Fin}(c)$. □

6. $\mathrm{Fin}(a) \wedge \mathrm{Fin}(b) \to \mathrm{Fin}(a \times b)$

Důkaz. ihned z 5. a toho, že $a \times b \subseteq \mathcal{P}(\mathcal{P}(a \cup b))$. □

7. $\mathrm{Fin}(a) \wedge \mathrm{Fin}(b) \to \mathrm{Fin}({}^a b))$

—58—

Důkaz. ihned z 5. a toho, že ${}^a b \subseteq \mathcal{P}(a \times b)$. □

8. $(\mathrm{Fin}(x) \wedge (\forall z \in x)\mathrm{Fin}(z)) \to \mathrm{Fin}(\bigcup x)$

Důkaz. Indukcí pro konečné množiny. Pro $x = \emptyset$ triviálně. Platí-li dále tvrzení pro nějakou konečnou množinu x, jejíž všechny prvky jsou konečné, platí i pro $x \cup \{y\}$, kde y je konečná, neboť $\bigcup(x \cup \{y\}) = y \cup \cup \bigcup x$ a pravá strana je konečná dle indukčního předpokladu a 4. □

9. $(\forall n, m \in \omega)(n \approx m \to n = m)$

Důkaz. Indukcí dle n. Pro $n = 0$ je tvrzení triviální. Nechť n splňuje formuli $(\forall m \in \omega)(n \approx m \to n = m)$. Dokážeme, že ji splňuje i $n \cup \{n\}$, a to indukcí dle m. Pro $m = 0$ neplatí $n \cup \{n\} \approx m$, tedy implikace platí triviálně. Nechť implikace platí pro m a nechť $n \cup \cup \{n\} \approx m \cup \{m\}$. Buď $f : n \cup \{n\} \to m \cup \{m\}$ bijekce. Případnou

—59—

záměnou funkčních hodnot f v bodech n a $f^{-1}(m)$ získáme bijekci $f' : n \cup \{n\} \to m \cup \{m\}$ takovou, že $f'(n) = m$. Pak $f' \restriction n$ je bijekce n a m, tedy $n \approx m$; a podle indukčního předpokladu $n = m$. Tudíž $n \cup \{n\} = m \cup \{m\}$. □

10. $(n \in \omega \wedge x \subset n) \to x \prec n$

Důkaz. Indukcí: pro $n = 0$ triviální; nechť implikace platí pro n a nechť $x \subset n \cup \{n\}$. Je-li $x - \{n\} \subset n$, je $x - \{n\} \prec n$ dle indukčního předpokladu a tedy $x \prec n \cup \{n\}$. V opačném případě zbývá možnost $x = n$, pro níž platí $x \preccurlyeq n \cup \{n\}$ triviálně a $n \not\approx n \cup \{n\}$ dle 9. □

11. Je-li $y \subset x$ a $y \approx x$, je x nekonečná.

Důkaz. Plyne z 10. □

—60—

Tvrzení 11. vyslovuje důležitou vlastnost konečných množin, totiž že jejich vlastní část je vždy menší než celek.

Toto tvrzení navrhnul jako definici konečnosti množiny Dedekind. V Zermelo-Fraenkelově teorii množin však (bez přidání dalšího axiomu, např. axiomu výběru) *nelze dokázat* opačnou implikaci, tj. tvrzení

> Množina, jejíž každá vlastní část má mohutnost menší než celek, je konečná.

Problém spočívá v tom, že obecně nejsme s to k dané nekonečné množině x nalézt $y \subset x$ a bijekci y na x (přestože pro všechny „konkrétní“ nekonečné množiny, jako je třeba ω, taková zobrazení nalézt umíme).

—61—

Zavedení operací na ω

Z předchozího plyne, že sjednocení, kartézský součin i množinová mocnina dvou konečných množin jsou tedy konečné množiny. Každá konečná množina má mohutnost právě jednoho přirozeného čísla. Operace *sčítání*, *násobení* a *mocnění* proto zavádíme následujícími vztahy. Pro $n, m, k \in \omega$:

$$\begin{aligned} n + m = k &\quad\leftrightarrow\quad k \approx n \uplus m, \\ n \cdot m = k &\quad\leftrightarrow\quad k \approx n \times m, \\ n^m = k &\quad\leftrightarrow\quad k \approx {}^m n. \end{aligned}$$

V každém z nich je číslo k, udávající výsledek uvedené operace, určeno jednoznačně (díky tvrzení 9.)

—62—

Snadno se ověří, že pro přirozená čísla v teorii množin s výše uvedenými operacemi a uspořádáním, platí všechny axiomy Peanovy aritmetiky.

Na druhou stranu jsou známa tvrzení o přirozených číslech, jež jsou dokazatelná v teorii množin, ale v Peanově aritmetice je nelze dokázat ani vyvrátit. Nahradíme-li však v teorii množin axiom nekonečna jeho negací, situace se změní. V takové „teorii konečných množin“ jsou o přirozených číslech dokazatelná právě tatáž tvrzení jazyka aritmetiky, jako v Peanově aritmetice.

To poukazuje na zajímavý fakt, totiž že až zkoumáním nekonečných množin lze získat některé poznatky o konečných množinách (potažmo přirozených číslech), jež by nám jinak zůstaly skryty.

—63—

Spočetné a nespočetné množiny

Řekneme, že množina je (nekonečně) *spočetná*, má-li stejnou mohutnost jako množina přirozených čísel.

Řekneme, že množina je *nejvýše spočetná*, je-li buďto konečná nebo spočetná.

Množina je *nespočetná*, je-li nekonečná, ale není spočetná.

Příklad: $\mathcal{P}(\omega)$ je nespočetná

Důkaz. Dle Cantorovy věty $\omega \prec \mathcal{P}(\omega)$. □

—64—

Příklad: $\omega \times \omega \approx \omega$ (Důsledek: ${}^{\omega}\omega \approx {}^{\omega}2$)

Důkaz. Využijeme Cantor-Bernsteinovy věty. Zřejmě $f : \omega \to \omega \times \omega$ definované předpisem $f(n) = \langle n, n \rangle$ je prosté, tudíž $\omega \preccurlyeq \omega \times \omega$.

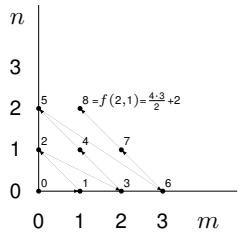
Naopak, zvolme dvě různá prvočísla p, q, např. $p = 2$ a $q = 3$. Zobrazení $g : \omega \times \omega \to \omega$ definujme jako $g(\langle m, n \rangle) = p^n \cdot q^m$. Ze známé věty o jednoznačnosti rozkladu na prvočísla plyne, že g je prosté, tudíž $\omega \times \omega \preccurlyeq \omega$.

Dokázali jsme obě subvalence, tudíž $\omega \times \omega \approx \omega$. □

Jiný důkaz. Přímo sestrojíme bijekci $\omega \times \omega$ a ω jako

$$f(\langle n, m \rangle) = \frac{(n + m + 1)(n + m)}{2} + n.$$

Že jde o bijekci se musí formálně ověřit, patrné to je však ihned z obrázku vpravo. □



—65—

Tvrzení: *1. Sjednocení konečného počtu nejvýše spočetných množin je nejvýše spočetná množina.*

2. Sjednocení konečně mnoha množin je nekonečné právě když aspoň jedna z nich je nekonečná.

Důkaz. 1. Stačí dokázat, že pro nejvýše spočetné množiny x, y je $x \cup y$ nejvýše spočetné, odkud již tvrzení plyne indukcí dle počtu sjednocovaných množin. Dle předpokladu existují prostá zobrazení $f : x \to \omega$ a $g : y \to \omega$. Zobrazení $h : x \cup y \to \omega$ definované předpisem

$$h(a) = \begin{cases} 2 \cdot f(a) & \text{pro } a \in x \\ 2 \cdot g(a) + 1 & \text{pro } a \in y - x \end{cases}$$

je zjevně prosté, tudíž $x \cup y \preccurlyeq \omega$.

2. Plyne z tvrzení 8. o konečných množinách, že sjednocení konečně mnoha konečných množin je konečné. □

—66—

Tvrzení, že i **sjednocení spočetně mnoha nejvýše spočetných množin je spočetné**, nelze v teorii množin obecně rozhodnout bez nějaké formy tzv. *axiomu výběru*, o němž se zmíníme později. Lze však dokázat:

Příklad: Je-li y spočetná a $\langle f_x ; x \in y \rangle$ je soubor prostých zobrazení takových, že $f_x : x \to \omega$, pak $\bigcup y$ je nejvýše spočetné.

Důkaz. Buď $g : y \to \omega$ prosté. Pro $a \in \bigcup y$ buď $h(a) = \langle f_x(a), g(x) \rangle$, kde $x \in y$ volíme tak, aby $a \in x$ a $(\forall x' \in y)(a \in x' \to g(x') \leq g(x))$. Pak $h : \bigcup y \to \omega \times \omega$ je prosté zobrazení. $\bigcup y$ je tudíž nejvýše spočetná. □

Rozdíl mezi shora uvedeným tvrzením a tímto příkladem je v tom, že v příkladu je předem zadán systém zobrazení svědčících o spočetnosti množin $x \in y$. Ke každé jednotlivé množině $x \in y$ sice můžeme díky spočetnosti nějaké prosté zobrazení $f_x : x \to \omega$ zvolit (existenční kvantifikátor), ovšem ve zcela obecném spočetném případě nám vybrat f_x pro všechna $x \in y$ naráz, umožní až zmíněný axiom výběru.

—67—

Příklad: $\mathbb{Z}$, $\mathbb{Q}$ jsou spočetné, jak plyne snadno z jejich konstrukce a vztahu $\omega \times \omega \approx \omega$.

Příklad: $\mathbb{R}$ je nespočetná a $\mathbb{R} \approx \mathcal{P}(\omega) \approx {}^{\omega}2$.
Mohutnosti množiny ${}^{\omega}2$ se proto říká *mohutnost kontinua*.

Nespočetnost $\mathbb{R}$ lze nahlédnout několika způsoby. Jednou možností je hned dokázat, že $\mathbb{R} \approx \mathcal{P}(\omega)$ a použít Cantorovu větu (provedeme dále).

Ukažme si důkaz pomocí Cantorovy diagonální metody: Předpokládejme, že existuje bijekce $r : \omega \to \mathbb{R}$. Definujme číslo s, dané desetinným rozvojem $0, s_0 s_1 s_2 \ldots$, kde s_n jsou číslice zvolené např. takto: $s_n = 2$, je-li číslice na $n+1$-ním desetinném místě čísla $r(n)$ rovna 5; je-li různá od 5, klademe $s_n = 5$. Pro každé $n \in \omega$ se číslo $r(n)$ a námi právě definované číslo s liší právě na $n+1$ desetinném místě. Tedy $s \notin \operatorname{rng}(r)$. Přitom zjevně $s \in \mathbb{R}$, což je spor s předpokladem, že r je zobrazení na.

—68—

Odvodíme $\mathbb{R} \approx \mathcal{P}(\omega)$.

Každé reálné číslo r je supremem množiny racionálních čísel menších než r. Z toho vyplývá, že zobrazení přiřazující číslu r právě tuto podmnožinu $\mathbb{Q}$ je prosté, a tedy $\mathbb{R} \preccurlyeq \mathcal{P}(\mathbb{Q}) \approx \mathcal{P}(\omega)$.

Obráceně: Víme, že $\mathcal{P}(\omega) \approx {}^{\omega}2$. Stačí tedy ${}^{\omega}2$ prostě zobrazit do $\mathbb{R}$. K tomu stačí, přiřadíme-li každé funkci $f \in {}^{\omega}2$ číslo z intervalu $[0, 1]$ s desetinným rozvojem $r_f = 0, f(0)f(1)f(2)\ldots$, neboli položit $r_f = \sum_{n=0}^{\infty} \frac{f(n)}{10^n}$.

Jsou-li $f, g \in {}^{\omega}2$ různé, liší se jejich hodnoty na nějakém $n \in \omega$ a r_f se tudíž liší od r_g na $n+1$-ním desetinném místě. Zobrazení $f \mapsto r_f$ je tedy prosté. □

Důsledek: $\mathbb{R} \times \mathbb{R} \approx \mathbb{R}$.

—69—

Příklad: Cantorova množina, neboli Cantorovo diskontinuum

Pozměníme-li vzorec z minulého příkladu a funkci $f \in {}^{\omega}2$ přiřadíme nyní číslo $d_f = \sum_{n=0}^{\infty} \frac{2f(n)}{3^n}$, získáme tzv. Cantorovu množinu $D = \{d_f \,;\, f \in {}^{\omega}2\}$.

Je zjevné že $D \subseteq [0,1]$ a že $D \approx {}^{\omega}2$. Je to uzavřená podmnožina $\mathbb{R}$ (tj. je-li $\langle x_n \,;\, n \in \omega\rangle$ posloupnost prvků z D, která má v $\mathbb{R}$ limitu $x = \lim_{n\to\infty} x_n$, pak $x \in D$). Odtud též plyne, že $(D, \leq)$ je úplný svaz. Diskontinuum je této množině přezdíváno proto, že je tzv. *totálně nesouvislá*, což v daném případě populárně řečeno znamená, že mezi každými jejími dvěma prvky leží *„díra“*.

Množinu D si lze představit tak, že z intervalu $[0,1]$ vyjmeme prostřední otevřený interval $(\frac{1}{3}, \frac{2}{3})$, pak vyjmeme prostřední třetiny obou zbylých kusů, atd.

—70—

—71—

To, co zbude jakožto průnik množin získaných v jednotlivých krocích, je právě množina D. Součet délek vylomených intervalů je $\sum_{n=1}^{\infty} \frac{2^{n-1}}{3^n} = \frac{1}{3}\sum_{n=0}^{\infty}(\frac{2}{3})^n = \frac{1}{3}\frac{1}{1-\frac{2}{3}} = \frac{1}{3}\cdot 3 = 1$. Zbylá množina D má tedy Lebesgueovu míru 0.

—72—

Příklad (*Algebraická čísla*): Reálné číslo, jež je kořenem polynomu s celočíselnými koeficienty, tj. splňuje nějakou rovnici tvaru

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0, \quad a_0, \ldots, a_n \in \mathbb{Z}$$

se nazývá *algebraické*. Reálné číslo, které není algebraické se nazývá *transcendentní*.

Všechna racionální čísla jsou zjevně algebraická. Také např. číslo $\sqrt{2}$, které je iracionální, je algebraické, neboť je kořenem rovnice $x^2 - 2 = 0$

Dodnes je známo jen velmi málo (typů) příkladů konkrétních transcendentních čísel, mezi něž patří čísla π a e. Dokázat o nějakém konkrétním čísle, že je transcendentní, je velice obtížné.

Dokázat však, že nějaká transcendentní čísla skutečně existují (a že jich je dokonce velmi mnoho) je, jak uvidíme, poměrně snadné (ačkoli si tohoto způsobu důkazu do doby Cantora nikdo nevšiml).

—73—

Ukážeme, že algebraických čísel je spočetně mnoho. Jelikož $\mathbb{R}$ je nespočetná, plyne z toho, že transcendentních čísel je nespočetně mnoho.

Každý polynom n-tého stupně je dán svými koeficienty. Každý polynom s celočíselnými koeficienty tak můžeme ztotožnit s jistou konečnou posloupností prvků z $\mathbb{Z}$, neboli s nějakým zobrazením $f : n \to \mathbb{Z}$, $n \in \mathbb{Z}$. Rovnice daného typu lze tedy ztotožnit s množinou $\bigcup_{n\in\omega} {}^n\mathbb{Z} \approx \bigcup_{n\in\omega} {}^n\omega$. Ukážeme nejprve, že množina vpravo je spočetná. Nechť p_k značí k-té prvočíslo. Přiřadíme-li funkci $f : n \to \omega$ přirozené číslo $F(f) = p_0^{f(0)} \cdot p_1^{f(1)} \dots \cdot p_{n-1}^{f(n-1)}$, získáme prosté zobrazení uvedené množiny do ω a jsme hotovi.

Nechť K_f značí množinu kořenů polynomu zadaného funkcí $f \in {}^n\mathbb{Z}$. Dle základní věty algebry má polynom stupně n nejvýše n reálných kořenů. Polynom určený f je nejvýše stupně $n-1$, tudíž $K_f \approx m$ pro jisté $m < n$. Existuje právě jedno zobrazení $F_f : K_f \to m$ takové, že $x < y \leftrightarrow F_f(x) < F_f(y)$. Z příkladu, o mohutnosti sjednocení spočetně mnoha nejvýše spočetných množin pak plyne, že $\bigcup\{K_f \,;\, f \in \bigcup_{n\in\omega} {}^n\mathbb{Z}\}$ je spočetná. □

—74—

Příklad: Označme $C(\mathbb{R})$ množinu všech **spojitých** reálných funkcí. Je známo, že každá spojitá funkce $f : \mathbb{R} \to \mathbb{R}$ je jednoznačně určena svými hodnotami na $\mathbb{Q}$, tj. funkcí $f{\restriction}\mathbb{Q} : \mathbb{Q} \to \mathbb{R}$. Odtud plyne, že $C(\mathbb{R}) \preccurlyeq {}^{\mathbb{Q}}\mathbb{R}$. Přitom každá konstantní funkce je spojitá, tedy $\mathbb{R} \preccurlyeq C(\mathbb{R})$. Jelikož $\mathbb{Q} \approx \omega$, $\mathbb{R} \approx {}^{\omega}2$, a $\omega \approx \omega \times \omega$, dostáváme

$$ {}^{\omega}2 \approx \mathbb{R} \preccurlyeq C(\mathbb{R}) \preccurlyeq {}^{\mathbb{Q}}\mathbb{R} \approx {}^{\omega}({}^{\omega}2) \approx {}^{\omega\times\omega}2 \approx {}^{\omega}2. $$

Všude tedy platí $\approx$. Spojitých reálných funkcí je proto stejně jako reálných čísel. To je poměrně překvapivé, uvědomíme-li si, že všech reálných funkcí je ${}^{\mathbb{R}}\mathbb{R} \approx \mathcal{P}(\mathbb{R})$ a dle Cantorovy věty $\mathbb{R} \prec \mathcal{P}(\mathbb{R})$. V tomto smyslu se spojitost jeví jako dosti ojedinělá vlastnost funkcí.

Úkol: *Zkuste jako důsledek právě dokázaného tvrzení o spojitých reálných funkcích dokázat, že existuje reálná funkce, jejíž graf protne graf každé spojité reálné funkce.*

—75—

Dobrá uspořádání

Připomeňme, že uspořádání $(A, \leq)$ je *dobré*, jestliže každá neprázdná podmnožina $x \subseteq A$ má $\leq$-nejmenší prvek.

V dobrých uspořádáních tudíž neexistuje nekonečná klesající posloupnost.

Víme, že množina přirozených čísel je dobře ostře uspořádaná relací $\in$, jež na ω definuje kanonické ostré uspořádání. Jelikož každá podmnožina dobrého uspořádání je sama dobře uspořádaná, je dobře uspořádané též každé přirozené číslo.

Rovněž každé konečné lineární uspořádání je dobré, což plyne z toho, že uspořádání přirozených čísel je dobré.

—76—

Přirozená čísla jsme zavedli tak, že prvky každého $m \in \omega$ jsou právě všechna čísla menší než m. Speciálně, je-li $n \in m$, je $n \subseteq m$. Totéž však platí pro samu množinu ω ($m \in \omega \to m \subseteq \omega$) a rovněž pro množiny $\omega + 1 = \omega \cup \cup\{\omega\}$, $\omega + 2 = (\omega + 1) \cup \{\omega + 1\}$, atd., tj. pro množiny získané z ω operací následníka. Řada $0, 1, 2 \dots, \omega, \omega + 1, \omega + 2, \dots$ tak přirozeně prodlužuje řadu $0, 1, 2, \dots$.

Můžeme jít ještě dál a definovat $\omega + \omega = \omega \cdot 2 = \bigcup\{\omega + n \,;\, n \in \omega\}$ a řadu dále produžovat tak, že v izolovaných krocích užíváme operace následníka, v limitních sjednocení. Řada pokračuje:

$0, 1, 2 \dots, \omega, \omega{+}1, \omega{+}2, \dots, \omega{\cdot}2, \omega{\cdot}2{+}1, \omega{\cdot}2{+}2, \dots \omega{\cdot}3, \dots, \omega{\cdot}4 \dots$
$\dots, \omega{\cdot}\omega = \omega^2, \dots, \omega^3, \dots\dots, \omega^\omega = \bigcup_{n\in\omega} \omega^n, \dots\dots, \omega^{\omega^\omega}, \dots, \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}, \dots$

Všechna tato tzv. *„transcendentní čísla“* jsou stále jen spočetné množiny. (Např. $\omega^\omega = \bigcup_{n\in\omega} \omega^n$ je spočetné, neboť je to spočetné sjednocení spočetných množin; **Pozor:** neplést s ${}^{\omega}\omega \approx {}^{\omega}2 \approx \mathcal{P}(\omega)$, což je nespočetná množina!). Transcendentní čísla tohoto typu však pokračují i za hranicí spočetnosti.

—77—

Ordinální čísla

Definice: Řekneme, že třída A je *tranzitivní*, jestliže $\bigcup A \subseteq A$, neboli, když pro každé $x \in A$ platí $x \subseteq A$, neboli $(y \in x \wedge x \in A) \to y \in A$.

Tranzitivním množinám na kterých je relace $\in$ navíc dobré ostré uspořádání, říkáme *ordinální čísla* či krátce *ordinály*.

Třídu všech ordinálních čísel značíme $\mathbf{On}$.

Ordinální čísla prodlužují obor přirozených čísel a matematickou indukci směrem k nekonečným množinám.

Ordinální čísla bývá zvykem označovat malými řeckými písmeny.

—78—

Každé přirozené číslo je ordinál, stejně jako množiny ω, $\omega + 1$, $\omega + 2$, apod. uvedené výše.

Program:

Ukážeme, že relace $\in$ určuje na celém $\mathbf{On}$ dobré ostré uspořádání.

Na $\mathbf{On}$ dále zavedeme operace sčítání, násobení a umocňování, jež se na ω budou shodovat s operacemi, jež jsme pro přirozená čísla zavedli dříve.

Ordinální čísla představují typy všech dobrých uspořádání. Ukážeme totiž, že každé dobré ostré uspořádání $(A, <)$, kde A je množina, lze izomorfně zobrazit na $(\alpha, \in)$, kde α je nějaký ordinál.

—79—

1. *Pro každé $\alpha \in \mathbf{On}$ platí $\alpha \notin \alpha$.*

Důkaz. Kdyby $\alpha \in \alpha$, nebylo by uspořádání $(\alpha, \in)$ ostré. □

2. *Prvky ordinálního čísla jsou ordinální čísla, tj. $\mathbf{On}$ je tranzitivní třída.*

Důkaz. Buď α ordinál a $x \in \alpha$. Jelikož α je tranzitivní množina, je $x \subseteq \subseteq \alpha$, a x je tedy také dobře uspořádáno relací $\in$. Zbývá ukázat, že x je tranzitivní. Je-li $z \in y \in x$, plyne z tranzitivity α, že $y \in \alpha$, a tedy též $z \in \alpha$. Ovšem $\in$ je na α ostré uspořádání a tudíž speciálně tranzitivní relace, tudíž $z \in x$. □

—80—

3. *Jsou-li α, β ordinální čísla, pak $\alpha \subseteq \beta$ právě tehdy, když $\alpha \in \beta$ nebo $\alpha = \beta$.*

Důkaz. Je-li $\alpha \in \beta$, je $\alpha \subseteq \bigcup \beta \subseteq \beta$.

Naopak, nechť $\alpha \subseteq \beta$ a $\alpha \neq \beta$. Pak $\beta - \alpha \neq \emptyset$ a existuje nejmenší prvek γ množiny $\beta - \alpha$. Ukážeme, že $\alpha = \gamma$, odkud již plyne $\alpha \in \beta$.

Je-li $\delta \in \gamma$, je $\delta \in \beta$ a navíc $\delta \in \alpha$, jelikož γ je $\in$-nejmenší prvek $\beta - \alpha$. Tudíž $\gamma \subseteq \alpha$. Je-li naopak $\delta \in \alpha$, je též $\delta \in \beta$ a nutně platí jeden ze vztahů $\gamma \in \delta$, $\gamma = \delta$ či $\delta \in \gamma$, neboť $\in$ je ostré lineární uspořádání na β. Je zřejmé, že žádný z prvních dvou vztahů nastat nemůže, jelikož $\delta \in \alpha$, zatímco $\gamma \notin \alpha$ (neb $\gamma \in \beta - \alpha$), tudíž $\delta \in \gamma$ a $\gamma \supseteq \alpha$, čímž je dokázána i druhá potřebná inkluze. □

4. *Je-li α ordinální číslo je $(\alpha, \subseteq)$ dobré uspořádání.*

Důkaz. Plyne bezprostředně z 2. a 3. □

—81—

5. $(\mathbf{On}, \in)$ *je dobré ostré uspořádání a* $(\mathbf{On}, \subseteq)$ *je odpovídající dobré neostré uspořádání.*

Důkaz. Že $(\mathbf{On}, \in)$ je ostré uspořádání plyne ihned z tranzitivity ordinálů a bodu (1).

Linearita $\in$ na $\mathbf{On}$: Nechť $\alpha, \beta \in \mathbf{On}$, $\alpha \neq \beta$. Není-li $\alpha \in \beta$, neplatí podle 3. ani $\alpha \subseteq \beta$ a existuje tudíž nejmenší prvek $\gamma \in \alpha - \beta$. Pak $\gamma \subseteq \beta$, neboť je-li $\delta \in \gamma$, je $\delta \in \alpha \cap \beta$. Jelikož $\gamma \notin \beta$, je podle 3. nutně $\gamma = \beta$, a tedy $\beta \in \alpha$.

$\in$ je dobré: Buď $x \subseteq \mathbf{On}$ neprázdná a $\alpha \in x$. Ukážeme, že má minimální prvek. Ten je díky linearitě nejmenší. Je-li $\alpha \cap x = \emptyset$, je α zřejmě $\in$-minimální v x. Je-li naopak $\alpha \cap x \neq \emptyset$, pak existuje $\in$-nejmenší prvek γ množiny $\alpha \cap x$, jenž je díky tranzitivitě α $\in$-minimální v x.

Tvrzení (5) nyní plyne bezprostředně z dokázaného a z (3). □

—82—

Na $\mathbf{On}$ tedy můžeme definovat dobré uspořádání $\leq$ předpisem

$$\alpha \leq \beta \quad \overset{\text{df}}{\leftrightarrow} \quad \alpha \in \beta \vee \alpha = \beta.$$

Relace $\leq$ na $\mathbf{On}$ splývá s $\subseteq$ a odpovídající ostrá relace $<$ s relací $\in$.

6. $\mathbf{On}$ *je vlastní třída.*

Důkaz. Třída $\mathbf{On}$ je dle (2) tranzitivní, a dle (5) dobře ostře uspořádaná relací náležení. Kdyby $\mathbf{On}$ byla množina, byla by ordinálním číslem, a tedy by platilo $\mathbf{On} \in \mathbf{On}$. To je ve sporu s (1). □

—83—

Minima a suprema v On

7. *Platí:*

a) Je-li $\emptyset \neq X \subseteq \mathbf{On}$ *třída, je* $\bigcap X$ *ordinál a* $\leq$*-nejmenší prvek* X*.*

b) Je-li $\emptyset \neq x \subseteq \mathbf{On}$ *množina, je* $\bigcup x$ *ordinál a supremum množiny* x *v uspořádání* $(\mathbf{On}, \leq)$*.*

Důkaz. Ad a) Je-li $\alpha \in X$, má $X \cap (\alpha \cup \alpha)$ nejmenší prvek β, neb je to množina. Zřejmě $\beta \subseteq \gamma$ pro každé $\gamma \in X$, je to tedy nejmenší prvek v X a $\beta = \bigcup X$.

Ad b) Analogicky: $\bigcup x$ je tranzitivní množina dobře uspořádaná relací $\in$, tudíž ordinál. Je to $\leq$-majoranta množiny x, neboť pro $\alpha \in x$ platí $\alpha \subseteq \subseteq \bigcup x$. Je to nejmenší majoranta, neboť je-li β taktéž majoranta x, platí pro každý prvek $\alpha \in x$ $\alpha \subseteq \beta$, tudíž $\bigcup x \subseteq \beta$. □

—84—

Prvním ordinálním číslem v uspořádání $\leq$ je prázdná množina $\emptyset$, tedy přirozené číslo 0. Dále následují přirozená čísla (prvky ω) $1, 2, \ldots$ v obvyklém pořadí.

Následníkem ordinálního čísla α je ordinální číslo $\alpha + 1 = \alpha \cup \{\alpha\}$, jež je nejmenším ordinálním číslem větším než α.

Říkáme, že ordinální číslo je *limitní*, není-li následníkem žádného ordinálního čísla. Číslům, která nejsou limitní říkáme *izolovaná*.

Limitní ordinální číslo je sjednocením (a tedy supremem) všech čísel, která je předcházejí, tedy $\alpha = \bigcup \alpha$ (pro izolovaná to neplatí, neboť $\bigcup(\alpha + 1) = \alpha$). V tomto smyslu je i 0 limitní ordinál, všechna ostatní přirozená čísla jsou izolovaná. Nejmenší limitní ordinál větší než 0 je ω, což je supremum množiny přirozených čísel.

—85—

Transfinitní indukce

Následující princip rozšiřuje matematickou indukci na ordinální čísla.

8. Princip transfinitní indukce. *Je-li A třída ordinálních čísel taková, že pro každý ordinál α platí $\alpha \subseteq A \to \alpha \in A$, pak $A = \mathbf{On}$.*

Podmínku $\alpha \subseteq A \to \alpha \in A$ lze též formulovat takto:

i) $0 \in A$,

ii) $\alpha \in A \to \alpha + 1 \in A$ *(izolovaný krok),*

iii) je-li $\alpha > 0$ limitní a $(\forall \beta < \alpha)\beta \in A$, pak $\alpha \in A$ (limitní krok).

Důkaz. Sporem: Buď $A \subseteq \mathbf{On}$ třída splňující $\alpha \subseteq A \to \alpha \in A$ pro všechna $\alpha \in \mathbf{On}$, taková že $A \neq \mathbf{On}$. Existuje nejmenší prvek α třídy $\mathbf{On} - A$. Zřejmě $\alpha \subseteq A$, čili $\alpha \in A$, spor! □

—86—

Transfinitní rekurze

9. Konstrukce transfinitní rekurzí. *Nechť G je zobrazení definované na celém $\mathbf{V}$ (konstruující zobrazení) a nechť $D \in \mathbf{On}$ nebo $D = \mathbf{On}$. Potom existuje právě jedno zobrazení F definované na D tak, že pro každé $\alpha \in D$ platí $F(\alpha) = G(F{\restriction}\alpha)$.*

Konstrukce rekurzí (konečnou či transfinitní) je v matematice velmi běžná. Jejím výsledkem je jistá posloupnost množin indexovaná ordinály (zde daná funkcí F) taková, že hodnotu každého jejího prvku zjistíme nějakým předem daným předpisem (jeho roli zde hraje konstruující funkce G) na základě přecházejících prvků posloupnosti, jejichž hodnoty již známe (tj. na základě $F{\restriction}\alpha$).

Konstrukce může být buď neomezená, nebo omezená, tedy skončit u nějakého ordinálního čísla. V druhém případě nás ve výsledku někdy zajímá celá posloupnost, jindy třeba jen poslední zkonstruovaný prvek.

—87—

Příklad: Funkci $x!$ proměnné x (x *faktoriál*) definujeme na ω rekurzivním předpisem $n! = 1$ je-li $n = 0$ a $(n+1)! = n! \cdot (n+1)$ pro $n > 0$.

Roli D tedy hraje ordinál ω a roli G funkce:

$$G(f) = \begin{cases} 1 & \text{je-li } f = \emptyset \\ f(n) \cdot (n+1) & \text{je-li } n \text{ maximum z } \omega \cap \mathrm{dom}(f) \\ 0 & \text{jinak (tento případ při konstrukci nenastane)} \end{cases}$$

—88—

Důkaz věty o konstrukci transfinitní rekurzí

Uvažujme třídu Y všech funkcí f, jejichž definičním oborem je nějaké ordinální číslo $\delta \subseteq D$ a pro něž platí

$$\alpha \in \mathrm{dom}(f) \quad \to \quad f(\alpha) = G(f{\restriction}\alpha) \tag{2}$$

O třídě Y dokážeme následující dvě tvrzení:

a) $(Y, \subseteq)$ je lineární uspořádání

b) Pro každé $\alpha \in D$ existuje $f \in Y$ tak, že $\alpha \in \mathrm{dom}(f)$.

Z nich již snadno plyne, že $F = \bigcup Y$ je hledané zobrazení.
Ad a). Buďte $f, g \in Y$ a označme $\delta_f = \mathrm{dom}(f)$ a $\delta_g = \mathrm{dom}(g)$. Podle definice Y jsou δ_f, δ_g ordinály. Předpokládejme BÚNO, že $\delta_f \leq \delta_g$ a označme $z = \{\alpha \in \delta_f \ ; \ f(\alpha) \neq g(\alpha)\}$. Je-li $z = \emptyset$, je $f \subseteq g$. V opačném případě buď γ nejmenší prvek množiny z. Pak ovšem $f(\alpha) = g(\alpha)$ pro každé $\alpha \in \gamma$, tedy $f{\restriction}\gamma = g{\restriction}\gamma$. Tudíž $f(\gamma) = G(f{\restriction}\gamma) = G(g{\restriction}\gamma) = g(\gamma)$ dle (5), spor.

—89—

Ad b). Označme $D' = \bigcup\{\mathrm{dom}(f)\ ;\ f \in Y\}$.

Předpokládejme, že $D - D' \neq \emptyset$, vyvodíme spor. Buď γ nejmenší prvek třídy $D - D'$. Zřejmě $\gamma \subseteq D'$. Díky a) platí, že

$$f = \bigcup\{g \in Y\ ;\ \mathrm{dom}(g) \in \gamma\}$$

je funkce splňující (5) a z volby γ je zřejmé, že $\mathrm{dom}(f) = \gamma$. Speciálně $f \in Y$. Položíme-li nyní $f' = f \cup \{\langle \gamma, G(f{\restriction}\gamma)\rangle\}$, je zřejmě $f' \in Y$, $\gamma \in \mathrm{dom}(f') = \gamma + 1$ a tudíž $\gamma \in D'$. Spor! □

—90—

Věta (*o ordinálních typech*): *Buď $(A, \sqsubseteq)$ dobré uspořádání. Je-li A množina, existuje právě jedno $\alpha \in \mathbf{On}$ tak, že uspořádání $(A, \sqsubseteq)$ a $(\alpha, \leq)$ jsou izomorfní. Je-li A vlastní třída a uspořádání $\leq$ je navíc úzké, tj. pro každé $x \in A$ je $\{y \in A\ ;\ y \leq x\}$ množina, je $(A, \sqsubseteq)$ izomorfní s $(\mathbf{On}, \leq)$. V obou případech je uvedený izomorfismus určen jednoznačně.*

Důkaz. Můžeme předpokládat, že $A \neq \emptyset$. Hledaný izomorfismus se získá transfinitní rekurzí přes $\mathbf{On}$, přičemž konstruující funkci G definujeme například takto:

$$G(f) = \begin{cases} \min_{\sqsubseteq}(A - \mathrm{rng}(f)) & \text{pro } A - \mathrm{rng}(f) \neq \emptyset \\ \min_{\sqsubseteq}(A) & \text{jinak.} \end{cases}$$

Buď F funkce získaná touto rekurzí. Označme

$$X = \{\alpha \in \mathrm{dom}(F)\ ;\ \alpha = 0 \vee F(\alpha) \neq \min_{\sqsubseteq}(A)\}.$$

Pak $F{\restriction}X$ je hledaný izomorfismus. Jednoznačnost: je-li F' jiný takový izomorfismus pak pro nejmenší ordinál γ splňující $F(\gamma) \neq F'(\gamma)$ platí

$$F'(\gamma) = \min_{\sqsubseteq}(A - \mathrm{rng}(F'{\restriction}\gamma)) = G(F'{\restriction}\gamma) = G(F{\restriction}\gamma) = F(\gamma), \text{ spor! } \square$$

—91—

DĹŻsledek:

*Jsou-li $\alpha, \beta \in \mathbf{On}$ a $\alpha \neq \beta$, pak $(\alpha, \leq)$ a $(\beta, \leq)$ **nejsou izomorfní**.*

Je-li dobré uspořádání $(A, \sqsubseteq)$ izomorfní $(\alpha, \leq)$ pro $\alpha \in \mathbf{On}$, říkáme, že α je *typem dobrého uspořádání* $(A, \sqsubseteq)$ a píšeme $\alpha = \mathrm{type}(A, \sqsubseteq)$.

Na třídě $\mathbf{On} \times \mathbf{On}$ zavádíme takzvané *lexikografické uspořádání* $\leq_{Le}$ takto:

$$\langle \alpha, \beta\rangle \leq_{Le} \langle \gamma, \delta\rangle \quad \overset{\mathrm{df}}{\leftrightarrow} \quad \alpha < \gamma \vee (\alpha = \gamma \wedge \beta \leq \delta).$$

Snadno se nahlédne, že $\leq_{Le}$ je dobré uspořádání na $\mathbf{On} \times \mathbf{On}$.

Na jeho základě zavádíme na třídě ordinálních čísel následujícím způsobem operace *sčítání* a *násobení*:

$$\alpha + \beta = \mathrm{type}(\alpha \uplus \beta, \leq_{Le}) \quad (\alpha \uplus \beta = \{0\} \times \alpha \cup \{1\} \times \beta) \qquad (3)$$

$$\alpha \cdot \beta = \mathrm{type}(\beta \times \alpha, \leq_{Le}) \qquad (4)$$

—92—

Je zřejmé, že uvedené definice jsou v souladu s námi dříve zavedenými operacemi na ω a odpovídá jim i označení následníka ordinálního čísla: $\alpha + 1 = \alpha \cup \{\alpha\}$.

Ordinální součet a součin jsou asociativní, ale **nejsou komutativní**, neboť např. $\omega + 1 \neq 1 + \omega = \omega$ či $\omega + \omega = \omega \cdot 2 \neq 2 \cdot \omega = \omega$.

—93—

Vlastnosti ordinálních operací

Pro $\alpha, \beta, \gamma \in \mathbf{On}$ platí:

$$\alpha \cdot 0 = 0 \cdot \alpha = 0, \quad \alpha \cdot 1 = 1 \cdot \alpha = \alpha, \quad \alpha \cdot 2 = \alpha + \alpha$$

$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ *(distributivita zprava)*

$\alpha < \beta \to \gamma + \alpha < \gamma + \beta$

$\alpha \leq \beta \to \alpha + \gamma \leq \beta + \gamma$

$\gamma > 0 \wedge \alpha < \beta \to \gamma \cdot \alpha < \gamma \cdot \beta,$

$\alpha \leq \beta \to \alpha \cdot \gamma \leq \beta \cdot \gamma$

$\omega \leq \alpha \to (\forall n \in \omega)\, n + \alpha = \alpha$

$(\omega \leq \alpha \wedge \alpha$ je limitní$) \to (\forall n \in \omega)\, n \cdot \alpha = \alpha$

—94—

Mocnina α^β ordinálních čísel α, β se zavádí rekurzí podle β (α je pevné):

1. $\alpha^0 = 1$,
2. $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$,
3. $\alpha^\beta = \bigcup_{\gamma<\beta} \alpha^\gamma$, je-li $\beta > 0$ limitní.

Na přirozených číslech se ordinální mocnina shoduje s tou, již jsme pro ně zavedli dříve.

Pozor: na nekonečných ordinálech ordinální mocnina neodpovídá množinové mocnině.

Ordinál $\omega^\omega = \bigcup_{n\in\omega} \omega^n$ je totiž na rozdíl od množiny ${}^\omega\omega$ spočetný:
Z $\omega \times \omega \approx \omega$ se snadno vyvodí $\omega^n \approx \omega$ a odtud následně i $\omega^\omega \approx \omega$.

—95—

Funkce $F : \mathbf{On} \to \mathbf{On}$ je *normální*, je-li rostoucí a spojitá (tj. $\alpha < \beta \to F(\alpha) < F(\beta)$ a $F(\gamma) = \bigcup_{\alpha<\gamma} F(\alpha)$ pro $\gamma > 0$ limitní).

Indukcí se snadno ověří, že pro normální funkci platí $\alpha \leq F(\alpha)$.

Věta (*O pevném bodě normální funkce*): *Pro každé $\beta \in \mathbf{On}$ má každá normální funkce pevný bod $\alpha > \beta$ ($F(\alpha) = \alpha$).*

Důkaz. Rekurzí definujme $g : \omega \to \mathbf{On}$ tak, že $g(0) = \beta$ a $g(n+1) = F(g(n))$. Buď $\alpha = \bigcup_{n<\omega} g(n)$. Jelikož F je rostoucí, je i g rostoucí, tudíž je α limitní. Ze spojitosti plyne, že $F(\alpha) = \bigcup_{\gamma<\alpha} F(\gamma)$, ovšem pravá strana je zřejmě rovna $\bigcup_{n<\omega} F(g(n)) = \bigcup_{n<\omega} g(n+1) = \alpha$. □

Každá normální funkce má tedy neomezeně mnoho pevných bodů (ty jsou tudíž uspořádny jako $\mathbf{On}$).

Příklad: Jelikož je ordinální mocnina α^α normální funkce, má pevný bod. Nejmenší ordinální číslo α takové, že $\alpha^\alpha = \alpha$ značíme ε ($= \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$).

—96—

Axiom výběru

Zobrazení f je tzv. *selektor na množině x*, jestliže $\mathrm{dom}(f) = x$ a $f(y) \in y$ pro každé $y \in x, y \neq \emptyset$.

Axiom výběru (AC) je tvrzení:

> *Na každé množině existuje selektor.*

Axiom výběru umožňuje pro dané x vybrat naráz z každé neprázdné množiny $y \in x$ po jednom prvku. Podstatné je, že tento výběr **tvoří množinu**.

Ekvivalentně lze axiom výběru také vyjádřit takto:

> *Kartézský součin neprázdného souboru neprázdných množin je neprázdný, tj.* pro soubor množin $\langle x_i \,;\, i \in I\rangle$ platí
>
> $$(I \neq \emptyset \wedge (\forall i \in I)\, x_i \neq \emptyset) \quad \to \quad \bigtimes_{i\in I} x_i \neq \emptyset.$$

—97—

Axiom výběru je nezávislý na axiomech Zermelo-Fraenkelovy teorie množin (nelze jej v ní ani dokázat ani vyvrátit). Uvidíme, že je v ní ekvivalentní s následujícími principy:

Princip dobrého uspořádání:

Každou množinu lze dobře uspořádat.

což znamená, že každou množinu lze prostě zobrazit na nějaký ordinál, neboli její prvky očíslovat ordinálními čísly.

Definice: Buď $(a, \leq)$ uspořádání. Řekneme, že podmnožina $r \subseteq a$ je *řetěz* v uspořádání $(a, \leq)$, je-li relace $\leq$ lineární uspořádání na r.

Princip maximality aneb Zornovo lemma:

Nechť $(a, \leq)$ je uspořádání, jehož každý řetěz má v $(a, \leq)$ majorantu. Pak pro každé $x \in a$ existuje maximální prvek y množiny a takový, že $x \leq y$.

—98—

Ekvivalence AC, WO, a PM

Ukážeme, že v Zermelo-Fraenkelově teorii množin jsou ekvivalentní:

(WO) principu dobrého uspořádání

(AC) axiomu výběru

(PM) principu maximality

(WO)→(AC)

Je-li x neprázdná množina, buď $\leq$ dobré uspořádání $\bigcup x$. Pak zobrazení $f : x \to \bigcup x$ definované předpisem $f(y) = \min_{\leq} y$ pro $y \in x$ je zjevně selektor na x.

—99—

(AC)→(PM)

Buď $(a, \leq)$ uspořádání, jehož každý řetěz má v $(a, \leq)$ majorantu. Hledáme maximální prvek nad daným $x \in a$. Buď g selektor na $\mathcal{P}(a)$. Pro řetěz r v $(a, \leq)$ označme $\mathrm{maj}(r)$ množinu všech jeho majorant a pro $y \in a$ označme $a_y = \{z \in a \,;\, y < z\}$. Transfinitní rekurzí definujme $F : \mathbf{On} \to b$ takto:

$$\begin{aligned} F(0) &= x, \\ F(\alpha) &= g(\mathrm{maj}(F''\alpha)) \text{ pro } \alpha > 0 \text{ limitní, a} \\ F(\alpha+1) &= \begin{cases} g(a_{F(\alpha)}) & \text{je-li } a_{F(\alpha)} \neq \emptyset, \\ F(\alpha) & \text{jinak.} \end{cases} \end{aligned}$$

Funkce F je neklesající, přesněji: zprvu rostoucí a od určitého α konstantní (nemůže být rostoucí všude, neb $\mathbf{On}$ je vlastní třída a b množina). Pro každé α tedy tvoří $F''\alpha$ řetěz. Buď α nejmenší ordinál, pro který existuje $\beta < \alpha$ tak, že $F(\alpha) = F(\beta)$. Tento α je izolovaný, a tedy $\alpha = \beta + 1$, neb je-li F rostoucí na limitním α, je $F(\alpha)$ větší než kterýkoli prvek z $F''\alpha$. Množina $a_{F(\beta)}$ je tedy prázdná a tudíž je $F(\beta)$ maximální prvek $(a, \leq)$. Přitom $x = F(0) \leq F(\beta)$.

—100—

(PM)→(WO)

Dokazujeme, že danou a lze dobře uspořádat. Položme

$$b = \{o \subseteq a \times a \,;\, o \text{ je dobré uspořádání (části } a)\}.$$

Je $\emptyset \in b$, tedy $b \neq \emptyset$. Ukážeme, že $(b, \trianglelefteq)$, kde $o \trianglelefteq o'$ pokud uspořádání o' prodlužuje o, splňuje předpoklady PM; je-li pak o maximální prvek b, je to dobré uspořádání na celém a, neb jinak existuje $x \in a - \mathrm{dom}(o)$ a $o' = o \cup \cup \{\langle x, x\rangle\} \cup \{\langle y, x\rangle; y \in \mathrm{dom}(o)\}$ je zjevně dobré usp. prodlužující o.

Nechť r je řetěz v b. Pak $o = \bigcup r$ je dobré uspořádání a je to majoranta řetězu r v $(b, \trianglelefteq)$. Je totiž $o_1 \trianglelefteq o$ pro každé $o_1 \in r$, neb je-li $x \in \mathrm{dom}(o_1)$ a $\langle y, x\rangle \in o$, pak $\langle y, x\rangle \in o_2$ pro nějaké $o_2 \in r$. Jelikož $o_1 \trianglelefteq o_2$ nebo $o_2 \trianglelefteq o_1$ a $x \in \mathrm{dom}(o_1)$, je $\langle y, x\rangle \in o_1$. Konečně, o je dobré uspořádání, neb je-li $u \subseteq \mathrm{dom}(o)$ a $x \in u$, je $x \in \mathrm{dom}(o_1)$ pro nějaké $o_1 \in r$. Nejmenší prvek množiny $u \cap \{y \,;\, \langle y, x\rangle \in o\} = u \cap \{y \,;\, \langle y, x\rangle \in o_1\}$ v uspořádání o_1 je nutně nejmenší prvek u v uspořádání o (ověřte podrobně!). □

—101—

Nějaká forma axiomu výběru je nutná k důkazu řady důležitých vět v moderní algebře, analýze a dalších matematických oborech (některé z nich jsou s ním dokonce ekvivalentní). Jsou to např. tvrzení:

- *Každý vektorový prostor má bázi.*
- *Existuje lebesgueovsky neměřitelná množina v* $\mathbb{R}$.
- *Lebesgueova míra na* $\mathbb{R}$ *je* σ*-aditivní*
- *Každé těleso lze algebraicky zúplnit.*
- *Je-li* f *reálná funkce a pro každou posloupnost* $\{a_n\}_{n\in\omega}$ *platí*

$$\lim_{n\to\infty} a_n = a \quad\to\quad \lim_{n\to\infty} f(a_n) = f(a),$$

pak f *je spojitá v bodě* a. *(Tj., že Heineho definice spojitosti v bodě implikuje běžnou Cauchyho* $\varepsilon\delta$*-definici spojitosti v bodě. Mimochodem, důkaz analogické implikace pro spojitost na intervalu axiom výběru nevyžaduje).*

AC je ekvivalentní tvrzení, že relace subvalence je trichotomická na $\mathbf{V}$, tj. pro každé dvě množiny x, y platí $x \preccurlyeq y$ nebo $y \preccurlyeq x$.

—102—

Lebesgueova míra λ_n na $\mathbb{R}^n$ je jednoznačně určená míra na nejmenší úplné σ-algebře obsahující všechny n-rozměrné kvádry, tj. množiny tvaru

$$[a_1, b_1] \times \ldots \times [a_n, b_n],$$

která je invariantní vůči posunutí a splňuje $\lambda_n([0,1]^n) = 1$.

Věta (*AC*): *Existuje lebesgueovsky neměřitelná množina v* $\mathbb{R}$.

Důkaz. Označme $\sim$ ekvivalenci na $\mathbb{R}$ definovanou předpisem $x \sim y \leftrightarrow x - y \in \mathbb{Q}$. Každá třída $[x]_\sim$ je zřejmě spočetná. Z (AC) plyne, že existuje selektor f na $[0,1]/\sim$; položme $V = \mathrm{rng}(f)$. Nechť $\{q_n \;;\; n \in \omega\}$ je očíslování $\mathbb{Q} \cap [0,1]$ a $V_n = V + q_n = \{x + q_n \;;\; x \in V\}$. Předpokládejme, že V je měřitelná (vyvodíme spor). Množiny V_n jsou zřejmě vzájemně disjunktní, $\lambda_1(V_n) = \lambda_1(V)$ (invariance vůči posunutí) a platí $[0,1] \subseteq \bigcup_{n\in\omega} V_n \subseteq [-1,2]$.

Tudíž díky σ-aditivitě λ_1 platí $1 \le \sum_{n\in\omega} \lambda_1(V_n) = \lambda_1(\bigcup_{n\in\omega} V_n) \le 3$. Z první nerovnosti plyne $\lambda_1(V) > 0$, odkud ovšem $\sum_{n\in\omega} \lambda_1(V_n) = \infty$, což je ve sporu s druhou nerovností. V tedy není měřitelná. □

—103—

Příklad: Každý vektorový prostor má bázi.

Připomeňme, že $B \subseteq V$ je bází vektorového prostoru V nad tělesem T, jestliže

1. B je *lineárně nezávislá* množina vektorů tj. z $\sum_{i=1}^n r_i v_i = 0$, kde $v_i \in B$ a $r_i \in T$, plyne $r_1 = r_2 = \cdots = r_n = 0$,
2. B *generuje* celý prostor V, tj. $\overline{B} = V$, kde

$$\overline{X} = \left\{ \sum_{i=1}^n r_i v_i \;;\quad v_i \in X,\, r_i \in T,\, 1 \le i \le n,\, n \in \mathbb{N} \right\}.$$

Důkaz. Použijeme axiom výběru ve formě Zornova lemmatu.

Označme

$$\mathcal{Z} = \{X \;;\; X \text{ je lineárně nezávislá množina}\}.$$

$\mathcal{Z}$ je neprázdná (např. $\emptyset \in \mathcal{Z}$) a částečně uspořádaná inkluzí.

—104—

Je zřejmé, že sjednocení řetězu lineárně nezávislých množin je lineárně nezávislá množina. Je-li totiž $\mathcal{X} \subseteq \mathcal{Z}$ řetěz v uspořádání $(\mathcal{Z}, \subseteq)$ (tj. uspořádání $(\mathcal{X}, \subseteq)$ je lineární) a pro nějaká $v_i \in \bigcup \mathcal{X}$, $r_i \in T$ platí $\sum_{i=1}^n r_i v_i = 0$, pak každý vektor v_i je prvkem nějakého $X_i \in \mathcal{X}$, $1 \le i \le n$. Díky linearitě uspořádání $(\mathcal{X}, \subseteq)$ je jedna z těchto konečně mnoha množin X_i největší v inkluzi. Označme ji X_j. Pak tedy $v_i \in X_j$ pro každé $1 \le i \le n$. Ovšem X_j je lineárně nezávislá množina, tudíž $r_1 = r_2 = \cdots = r_n = 0$.

Každý řetěz $\mathcal{X}$ má tudíž v $\mathcal{Z}$ majorantu (a to $\bigcup \mathcal{X}$). Tím jsou ověřeny předpoklady Zornova lemmatu, dle něhož má tudíž $\mathcal{Z}$ maximální prvek, označme ho B. Ukážeme $\overline{B} = V$. Kdyby to neplatilo, pak by existoval nějaký $v \in V - \overline{B}$. Pak ovšem $B \cup \{v\}$ je lineárně nezávislá množina, tedy $B \cup \{v\} \in \mathcal{Z}$ ve sporu s maximalitou B. Buď totiž $rv + \sum_{i=1}^n r_i v_i = 0$. Kdyby $r \neq 0$, pak by platilo $v = -\sum_{i=1}^n \frac{r_i}{r} v_i$, čili $v \in \overline{B}$, což je spor. Tudíž $r = 0$ a tedy $\sum_{i=1}^n r_i v_i = 0$. Z lineární nezávislosti B pak plyne i $r_1 = r_2 = \cdots = r_n = 0$. □

—105—

Příklad: Je-li f reálná funkce a pro každou posloupnost $\{a_n\}_{n\in\omega}$ platí

$$\lim_{n\to\infty} a_n = a \quad \to \quad \lim_{n\to\infty} f(a_n) = f(a),$$

pak f je spojitá v bodě a.

Důkaz. Využijeme axiom výběru (AC). Postupujeme sporem. Předpokládejme, že předpoklad o limitách platí, přesto je f nespojitá v bodě a, tj.

$$(\exists\varepsilon > 0)(\forall\delta > 0)(\exists y)(|a - y| < \delta \wedge |f(a) - f(y)| \geq \varepsilon). \qquad (5)$$

(negace definice spojitosti). Zafixujme ε a pro každé $n > 0$ zvolme na základě (5) jedno y_n z intervalu $(a - \frac{1}{n}, a + \frac{1}{n})$ tak, aby $|f(a) - f(y_n)| \geq \varepsilon$. Zde užíváme AC. Formálně je zobrazení $n \mapsto y_n$ selektorem na množině

$$\{\{y\,;\, |a - y| < \frac{1}{n} \wedge |f(a) - f(y)| \geq \varepsilon\}\,;\, n \in \mathbb{N}\}.$$

Je zřejmé, že $\lim_{n\to\infty} y_n = a$, ovšem $\lim_{n\to\infty} f(y_n) \neq f(a)$, neboť všechny $f(y_n)$ jsou od $f(a)$ vzdáleny přinejmenším o ε. □

—106—

Cvičení

Jako aplikace axiomu výběru, principu dobrého uspořádání, případně konstrukce transfinitní rekurzí, se můžete pokusit dokázat následující pozoruhodná (leč poněkud neužitečná) tvrzení:

1. Existuje funkce $f : \mathbb{Q} \to \mathbb{Q}$, nabývající na každém otevřeném intervalu racionálních čísel všech hodnot.
2. Pro danou spočetnou množinu přímek P v rovině $\mathbb{R}^2$, existuje spočetná množina $M \subseteq \mathbb{R}^2$, s níž má každá přímka z P právě dva společné body.
3. Existuje množina bodů v rovině (mohutnosti kontinua), s níž má každá přímka v rovině právě dva společné body.
4. Existuje funkce $f : \mathbb{R}^2 \to \mathbb{R}$, nabývající na každé kružnici v $\mathbb{R}^2$ (s nenulovým poloměrem) všech reálných hodnot.

—107—

Axiom výběru byl zprvu řadou matematiků a logiků odmítán pro jeho nekonstruktivní povahu: na rozdíl od ostatních axiomů postuluje existenci množiny (selektoru), aniž by ukázal, jak ji lze sestrojit (což je ovšem do jisté míry též problém axiomu potence).

Pomocí axiomu výběru lze získávat množiny značně „nekonstruktivní“ povahy, viz již zmíněnou neměřitelnou podmnožinu $\mathbb{R}$.

Dnes se však axiom výběru (až na úzce vyhraněné obory) využívá zcela běžně (v některých odvětvích matematiky dokonce natolik automaticky a nevědomky, že by v nich bylo značně obtížné oddělit ta tvrzení, jež se o něj nutně opírají).

—108—

Banach-Tarského Paradox

Na závěr kapitoly o axiomu výběru uveďme jeden příklad určený spíše pro pobavení (ale též k tomu, abychom viděli, že z axiomu, jenž nám může připadat poměrně přirozený a praktický, vyplývají i velmi podivuhodné důsledky, odporující naší bezprostřední intuici):

Tvrzení: *Plnou kouli (v $\mathbb{R}^3$) o poloměru 1 lze rozdělit na 5 částí, tak, že ze vzniklých částí lze složit celé dvě plné koule o poloměru 1.*

Podobná tvrzení platí i pro další typy těles a dimenze větší než 3.

Nezkoušejte to doma, nepovede se vám to! Pomocí nože takto žádné těleso nerozdělíte. Přinejmenším proto, že potřebné *„kusy“* jsou (pochopitelně) Lebesgueovsky neměřitelné.

—109—

Kardinální čísla

Ukázali jsme, že ordinální čísla reprezentují typy dobrých uspořádání množin.

Nyní popíšeme třídu $\mathbf{Cn}$ tzv. *kardinálních čísel*, jež budou reprezentovat typy mohutností všech množin, které lze dobře uspořádat.

Za předpokladu **axiomu výběru** (resp. s ním ekvivalentního principu dobrého uspořádání) tedy **kardinální čísla budou typy mohutností všech množin**, tj. každá množina bude mít mohutnost právě jednoho kardinálního čísla.

Připomeňme, že již nyní víme, že každá konečná množina má mohutnost nějakého (právě jednoho) přirozeného čísla $n \in \omega$. To znamená, že **prvky ω jsou typy mohutností konečných množin**. Tento koncept nyní rozšíříme.

—110—

Třída kardinálních čísel

$$\mathbf{Cn} = \{\alpha \in \mathbf{On}\ ;\ (\forall \beta \in \mathbf{On})(\beta < \alpha \to \neg(\beta \approx \alpha))\}.$$

$\mathbf{Cn}$ sestává z právě těch ordinálních čísel, jež nelze prostě zobrazit na žádné menší ordinální číslo. Jinými slovy, $\mathbf{Cn}$ obsahuje nejmenší prvek z každé rozkladové třídy $\mathbf{On}/\!\approx$.

Indukcí lze snadno dokázat, že $\omega \subseteq \mathbf{Cn}$ a $\omega \in \mathbf{Cn}$.

Prvky třídy $\mathbf{Cn}$ se nazývají *kardinální čísla* či krátce *kardinály*.

$\mathbf{Cn}^\infty$ označuje třídu nekonečných kardinálů, neboli $\mathbf{Cn}^\infty = \mathbf{Cn} - \omega$. Kardinální čísla budeme označovat písmeny $\kappa, \lambda, \mu, \nu, \ldots$.

Je-li x množina a $x \approx \kappa \in \mathbf{Cn}$, píšeme $|x| = \kappa$ a číslo κ nazýváme *mohutností* či *kardinalitou* množiny x.

—111—

Tvrzení: *Nechť $\emptyset \neq X \subseteq \mathbf{Cn}$. Pak:*

1. *$\bigcap X \in \mathbf{Cn}$ a je to nejmenší prvek třídy X v uspořádání $(\mathbf{Cn}, \leq)$,*
2. *Je-li X množina, je $\bigcup X \in \mathbf{Cn}$ a je to supremum množiny X v $(\mathbf{Cn}, \leq)$.*

Důkaz. Víme, že $\bigcap X$ je nejmenší ordinál v X, náleží tedy do X a je to proto kardinální číslo. Tím je průnik odbyt.

Víme dále, že je-li X množina, je $\gamma = \bigcup X$ ordinál, jenž je supremem množiny X v $\mathbf{On}$. Stačí proto ukázat, že je to kardinál. Sporem. Předpokládejme, že $\gamma \notin \mathbf{Cn}$. Existuje tedy $\alpha < \gamma$, $\alpha \approx \gamma$. Pak ale $\alpha \in \kappa$ pro nějaké $\kappa \in X$. Tedy $\alpha \subseteq \kappa \subseteq \gamma$, a tedy $\alpha \approx \kappa$, což není možné, neb $\kappa \in \mathbf{Cn}$. □

—112—

Tvrzení: *Neexistuje největší kardinální číslo.*

Důkaz. Předpokládáme-li AC, stačí užít Cantorovy věty. Z něj (a principu dobrého uspořádání) totiž plyne $\kappa < |\mathcal{P}(\kappa)|$.

Tvrzení však platí i bez AC. Sporem: Nechť κ je největší kardinál.

Pro $\alpha \in \mathbf{On}$ označme R_α množinu všech dobrých uspořádání na κ podle typu α. Je-li $\alpha \geq \kappa$, lze α prostě zobrazit na κ (nejmenší $\alpha > \kappa$, pro které by to nešlo, by bylo samo kardinální, což je ve sporu s maximalitou κ). Z toho plyne, že pro $\alpha \geq \kappa$ je $R_\alpha \neq \emptyset$.

Každé uspořádání na κ je relace na κ, tedy $R_\alpha \subseteq \mathcal{P}(\kappa \times \kappa)$, jinými slovy $R_\alpha \in \mathcal{P}(\mathcal{P}(\kappa \times \kappa))$. Přitom pro $\alpha \neq \beta$ je $R_\alpha \cap R_\beta = \emptyset$, neboť, jak víme, uspořádání žádných dvou ordinálních čísel nejsou izomorfní. Spec. $R_\alpha \neq R_\beta$.

Zobrazení R přiřazující každému prvku α vlastní třídy $\mathbf{On} - \kappa$ neprázdnou množinu R_α je tedy prosté. Sestrojili jsme tedy prosté zobrazení vlastní třídy $\mathbf{On} - \kappa$ do množiny $\mathcal{P}(\mathcal{P}(\kappa \times \kappa))$, což není možné — spor. □

—113—

DĹŽsledek: $\mathbf{Cn}$ *je vlastní třída.*

Jelikož $\mathbf{Cn} \subseteq \mathbf{On}$, je $\mathbf{Cn}$ sama dobře ostře uspořádaná relací $\in$. Protože je $\mathbf{Cn}$ vlastní třída, jde o uspořádání typu $\mathbf{On}$, neboli $(\mathbf{On}, \in) \cong (\mathbf{Cn}, \in)$.

Následník kardinálu κ je nejmenší kardinál větší než κ, značíme jej κ^+. Kardinál κ je *izolovaný*, je-li sám následníkem nějakého kardinálu; jinak je *limitní*.

Pozor: tyto pojmy na $\mathbf{On}$ a $\mathbf{Cn}$ nesplývají:

U přirozených čísel sice ano: 0 je limitní jakožto ordinál i kardinál, zatímco každé $n \geq 1$ je izolované (jakožto ordinál i kardinál). Ovšem všechna nekonečná kardinální čísla (včetně izolovaných) jsou limitní ordinály (je totiž zřejmé, že izolovaný ordinál tvaru $\alpha \cup \{\alpha\}$, kde α je nekonečné, má stejnou mohutnost jako α a nemůže proto být kardinálem).

Při použití pojmů souvisejících s uspořádáním tedy musíme dbát na to, zda dané číslo chápeme jako ordinální, tedy v kontextu uspořádání $(\mathbf{On}, \leq)$, nebo jako číslo kardinální, v kontextu $(\mathbf{Cn}, \leq)$.

—114—

Funkce Alef $\aleph$

Rovněž *třída všech nekonečných kardinálních čísel* $\mathbf{Cn}^\infty$ je vlastní, je tudíž také uspořádána dle typu $\mathbf{On}$.

Jednoznačně určený izomorfismus dobrých úzkých uspořádání $(\mathbf{Cn}^\infty, \leq)$ a $(\mathbf{On}, \leq)$ označujeme prvním písmenem hebrejské abecedy, $\aleph$ (Alef).

Funkci $\aleph$ lze definovat též transfinitní rekurzí, a to předpisem

$$\aleph(\alpha) = \min_{\leq}(\mathbf{Cn}^\infty - \aleph''\alpha).$$

Místo $\aleph(\alpha)$ píšeme obvykle $\aleph_\alpha$.

Chceme-li zdůraznit, že číslo $\aleph_\alpha$ chápeme ordinálně, tj. jako prvek $\mathbf{On}$, píšeme místo $\aleph_\alpha$ symbol ω_α.

Platí: $\aleph_0 = \omega$ a je-li $\kappa = \aleph_\alpha$, je $\kappa^+ = \aleph_{\alpha+1}$. Kardinální číslo $\aleph_\alpha$ je limitní, právě když α je limitní ordinál. Dále $\alpha \leq \omega_\alpha$.

—115—

Tvrzení: *Funkce $\aleph$ je normální, neboli rostoucí ($\alpha < \beta \to \aleph_\alpha < \aleph_\beta$) a spojitá ($\aleph_\lambda = \sup\{\aleph_\beta \,;\, \beta < \lambda\}$ pro limitní ordinál λ)*

Důkaz. Že je rostoucí je zřejmé z definice. Je dále zřejmé, že $\aleph_\lambda$ je majoranta množiny $u = \{\aleph_\beta \,;\, \beta < \lambda\}$. Že je to nejmenší majoranta dokážeme sporem:

Nechť $\kappa < \aleph_\lambda$ je rovněž majorantou u. Z limitnosti λ plyne, že κ je nekonečné, tedy $\kappa = \aleph_\beta$ pro nějaké $\beta < \lambda$. Pak ovšem $\beta + 1 < \lambda$, a tedy $\kappa = \aleph_\beta < \aleph_{\beta+1} \in u$, což je ve sporu s tím, že κ majorizuje u. □

DĹŽsledek: *Funkce $\aleph$ má pevné body (dle věty o pevném bodu pro normální funkce), tj. existují $\xi = \aleph_\xi$. Pro takové ξ pak platí $\xi \approx \xi \cap \mathbf{Cn}$, neboli „pod ξ leží stejný počet ordinálů jako kardinálů“.*

—116—

Maximo-lexikografické uspořádání

Maximo-lexikografické uspořádání $\leq_{MLe}$ na třídě $\mathbf{On} \times \mathbf{On}$ je definováno vztahem

$$\begin{aligned}&\langle\alpha_1, \beta_1\rangle \leq_{MLe} \langle\alpha_2, \beta_2\rangle \leftrightarrow \\ &\quad \max\{\alpha_1, \beta_1\} < \max\{\alpha_2, \beta_2\} \vee \\ &\quad (\max\{\alpha_1, \beta_1\} = \max\{\alpha_2, \beta_2\} \wedge \langle\alpha_1, \beta_1\rangle \leq_{Le} \langle\alpha_2, \beta_2\rangle).\end{aligned}$$

$(\mathbf{On} \times \mathbf{On}, \leq_{MLe})$ je dobré a úzké uspořádání (je tudíž typu $\mathbf{On}$).

➠ Kterou z uvedených vlastností nemá uspořádání $\leq_{Le}$, jež jsme na $(\mathbf{On} \times \mathbf{On})$ zavedli dříve?

—117—

Tvrzení: *Pro každé* $\alpha \in \mathbf{On}$ *platí* $\aleph_\alpha \times \aleph_\alpha \approx \aleph_\alpha$.

Důkaz. Buď $X = \{\alpha \in \mathbf{On} \ ; \ \aleph_\alpha \times \aleph_\alpha \approx \aleph_\alpha\}$. Podle principu transfinitní indukce stačí dokázat, že $\alpha \subseteq X$ implikuje $\alpha \in X$. Buď tedy $\alpha \subseteq X$ a η ordinální typ uspořádání $(\aleph_\alpha \times \aleph_\alpha, \leq_{MLe})$. Zřejmě $\eta \approx \aleph_\alpha \times \aleph_\alpha$. Dokážeme, že $\eta = \aleph_\alpha$.

Kdyby $\eta < \omega_\alpha$, pak by $\eta \prec \aleph_\alpha \preccurlyeq \aleph_\alpha \times \aleph_\alpha \approx \eta$, což není možné. Nechť naopak $\omega_\alpha < \eta$. Je-li f izomorfismus $(\eta, \leq)$ a $(\aleph_\alpha \times \aleph_\alpha, \leq_{MLe})$, je $f(\aleph_\alpha) = \langle \gamma, \delta \rangle \in \aleph_\alpha \times \aleph_\alpha$ pro nějaká $\gamma, \delta \in \aleph_\alpha$.

Buď $\beta = \max\{\gamma, \delta\}+1$. Pak $\beta \in \aleph_\alpha$, tedy speciálně $|\beta| < \aleph_\alpha$, a dále $f''\aleph_\alpha \subseteq \beta \times \beta$, tedy $\aleph_\alpha \leq |\beta \times \beta|$. Podle indukčního předpokladu však $|\beta \times \beta| = |\beta| < \aleph_\alpha$, což je spor. Zbývá tedy jedině možnost $\eta = \omega_\alpha$. Dokázali jsme, že $\alpha \in X$. □

—118—

Z AC a předchozího tvrzení plyne, že pro každou nekonečnou množinu a platí $a \approx a \times a$.

Od této chvíle **pracujeme v teorii množin s axiomem výběru**.

Na třídě $\mathbf{Cn}$ definujeme operace *sčítání*, *násobení* a *umocňování* takto:

$$\kappa + \lambda = |\kappa \uplus \lambda|, \quad \kappa \cdot \lambda = |\kappa \times \lambda|, \quad \kappa^\lambda = |{}^\lambda\kappa|.$$

Operace kardinálního součtu a součinu jsou zřejmě asociativní a komutativní. Buďte $\lambda > \kappa > 0$ a $\lambda \in \mathbf{Cn}^\infty$; pak:

$$\lambda \preccurlyeq \kappa \uplus \lambda \preccurlyeq 2 \times \lambda \preccurlyeq \lambda \times \lambda \approx \lambda$$
$$\lambda \preccurlyeq \kappa \times \lambda \preccurlyeq \lambda \times \lambda \approx \lambda$$

Jsou-li tedy $\kappa, \lambda > 0$ kardinální čísla, z nichž alespoň jedno je nekonečné, pak

$$\kappa + \lambda = \kappa \cdot \lambda = \max\{\kappa, \lambda\}.$$

Na přirozených číslech kardinální operace sčítání, násobení i umocňování splývají s obvyklými.

—119—

Některé zákony kardinální aritmetiky

1. $|x \uplus y| = |x| + |y|, |x \times y| = |x| \cdot |y|, |x|^{|y|} = |{}^y x|$
2. $2^\kappa = |\mathcal{P}(\kappa)| > \kappa$,
3. $0 \neq \kappa_1 \leq \kappa_2 \wedge \lambda_1 \leq \lambda_2 \to \kappa_1^{\lambda_1} \leq \kappa_2^{\lambda_2}$,
4. $\kappa^{\mu+\nu} = \kappa^\mu \cdot \kappa^\nu$,
5. $(\kappa^\mu)^\nu = \kappa^{\mu \cdot \nu}$.
6. $\kappa^0 = 1, 1^\lambda = 1, \lambda \neq 0 \to 0^\lambda = 0$,
7. $0 < n \in \omega \leq \kappa \to \kappa^n = \kappa$,
8. $(2 \leq \kappa \leq \lambda \wedge \omega \leq \lambda) \to \kappa^\lambda = 2^\lambda$.

—120—

Součet souboru kardinálů a mohutnost sjednocení

Součet souboru $\langle \kappa_i \ ; \ i \in I \rangle$ kardinálních čísel je definován vztahem

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

Tvrzení: *Je-li* $\langle \kappa_i \ ; \ i \in I \rangle$ *soubor nenulových kardinálů a* I *nebo některé z* κ_i *je nekonečné, pak*

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

Důkaz. Označme $\kappa = \sup\{\kappa_i \ ; \ i \in I\}$. Zřejmě $\kappa \leq \sum_I \kappa_i$, neboť uvedená suma majorizuje množinu $\{\kappa_i \ ; \ i \in I\}$. Jelikož $\kappa_i \geq 1$ pro každé $i \in I$, platí dále $I \preccurlyeq \sum_I \kappa_i$, tedy celkem $\max\{|I|, \kappa\} \leq \sum_I \kappa_i$.

Obráceně: zřejmě $\sum_I \kappa_i \leq I \times \kappa \approx |I| \cdot \kappa = \max\{|I|, \kappa\}$. □

Je-li $\langle x_i \ ; \ i \in I \rangle$ soubor množin, platí $|\bigcup_I x_i| \leq \sum_I |x_i|$. Jsou-li navíc x_i po dvou disjunktní, pak $|\bigcup_I x_i| = \sum_I |x_i|$. Z předešlého tvrzení navíc vyplývá, že je-li $\kappa \in \mathbf{Cn}^\infty$, $|I| \leq \kappa$ a $|x_i| \leq \kappa$ pro každé $i \in I$, pak $|\bigcup_I x_i| \leq \kappa$.

—121—

Součin souboru kardinálních čísel

Připomeňme, že součin souboru množin $\langle x_i \,;\, i \in I\rangle$ je množina

$$\bigtimes_{i\in I} x_i = \{f \,;\, f \text{ je zobrazení, } \mathrm{dom}(f) = I \text{ a } (\forall i \in I) f(i) \in x_i\}.$$

Součin souboru kardinálních čísel $\langle \kappa_i \,;\, i \in I\rangle$ definujeme jako

$$\prod_{i\in I} \kappa_i = |\bigtimes_{i\in I} \kappa_i|$$

Je-li $\kappa_i = \kappa$ pro každé $i \in I$, pak $\prod_{i\in I} \kappa_i = \kappa^{|I|}$.

Věta (*Königova nerovnost*): *Jsou-li κ_i, λ_i kardinální čísla taková, že $\kappa_i < \lambda_i$ pro každé $i \in I \neq \emptyset$, potom*

$$\sum_{i\in I} \kappa_i < \prod_{i\in I} \lambda_i$$

Jedná se o zobecnění Cantorovy nerovnosti $x \prec \mathcal{P}(x)$ (pro $\kappa_i = 1$, $\lambda_i = 2$ totiž Königova nerovnost dává $|I| < 2^{|I|} = |\mathcal{P}(I)|$).

—122—

Lemma: *Je-li $\lambda_i \geq 2$ pro každé $i \in I$, pak $\sum_{i\in I} \lambda_i \leq \prod_{i\in I} \lambda_i$*

Důkaz. Pro $|I| \leq 2$ je tvrzení snadné. Nechť $|I| > 2$. Zobrazíme prostě $S = \bigcup_{i\in I}(\{i\} \times \lambda_i)$ do $P = \bigtimes_{i\in I} \lambda_i$. Dle předpokladu, $\{0,1\} \subseteq \lambda_i$ pro každé $i \in \lambda$. Dvojici $\langle i, \alpha\rangle \in S$ přiřadíme funkci $f_{i,\alpha} \in P$ definovanou např. takto:

$$f_{i,0}(j) = \begin{cases} 1 & \text{když } i \neq j \\ 0 & \text{když } i = j \end{cases}$$

a pro $\alpha > 0$

$$f_{i,\alpha}(j) = \begin{cases} 0 & \text{když } i \neq j \\ \alpha & \text{když } i = j \end{cases}$$

Snadno se ověří, že toto přiřazení je prosté. □

—123—

Důkaz Königovy nerovnosti. Jelikož $\kappa_i < \lambda_i$, jsou všechna λ_i nenulová. Pokud pro nějaké $i \in I$ je $\lambda_i = 1$, je $\kappa_i = 0$. Členy s indexem i tedy nepřispívají ani do součtu na levé straně, ani do součinu na pravé straně, proto je můžeme vypustit. Lze tedy předpokládat, že $\lambda_i \geq 2$ pro každé $i \in I$.

Dle lematu tudíž $\sum_I \kappa_i \leq \sum_I \lambda_i \leq \prod_I \lambda_i$. Předpokládejme, že nastává rovnost (vyvodíme spor).

Z rovnosti plyne, že existuje disjunktní rozklad množiny $\bigtimes_I \lambda_i$ na množiny X_i pro $i \in I$ tak, že $|X_j| = \kappa_j$. Tedy $\bigcup_I X_i = \bigtimes_I \lambda_i$.

Diagonálním trikem, podobným důkazu Cantorovy věty, sestrojíme funkci $g \in \bigtimes_I \lambda_i$, jež neleží v žádné X_i, čímž dostaneme spor:

Pro každé $i \in I$ buď $Y_i = \{f(i) \,;\, f \in X_i\}$. Je tedy $Y_i \subseteq \lambda_i$. Pak $|Y_i| \leq |X_i| = \kappa_i < \lambda_i$. Hodnoty z Y_i tudíž nevyčerpají celé λ_i a můžeme definovat $g(i) = \min(\lambda_i - Y_i)$ pro každé $i \in I$. Pro každé $i \in I$ tak máme $g(i) \notin Y_i$, tedy $g \notin X_i$. Odtud $g \notin \bigcup_I X_i$, ačkoli zjevně $g \in \bigtimes_I \lambda_i$. Spor. □

—124—

O mohutnosti kontinua

Kardinální číslo $2^{\aleph_0}$ nazýváme (ve shodě s dřívější definicí) *mohutností kontinua*. Někdy se značí symbolem $\mathfrak{c}$. Víme, že

$$|\mathcal{P}(\omega)| = |{}^{\omega}2| = |{}^{\omega}\omega| = |\mathbb{R}| = \mathfrak{c}.$$

Z Cantorovy věty vyplývá, že

$$\aleph_0 < \mathfrak{c} \quad \text{tedy} \quad \mathfrak{c} \geq \aleph_1.$$

Rovnost $\mathfrak{c} = \aleph_1$ se nazývá *hypotéza kontinua* (CH). Říká, že mezi mohutností přirozených a reálných čísel není už žádná mohutnost, neboli, že každá podmnožina množiny reálných čísel je buď konečná, spočetná, nebo mohutnosti kontinua.

Hypotézu kontinua nelze v Zermelo-Fraenkelově teorii s axiomem výběru rozhodnout (tj. ani dokázat ani vyvrátit).

Totéž platí i o dalším průběhu funkce $2^{\aleph_\alpha}$. Je například bezesporné předpokládat, že $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ pro každé $\alpha \in \mathbf{On}$ (tzv. *zobecněná hypotéza kontinua*, GCH) , ovšem to je jen jedna z nepřeberného množství bezesporných možností.

—125—

Kardinální čísla – dodatek

Kardinál κ je *regulární*, nelze-li jej vyjádřit jako sjednocení méně než κ množin menších než κ, tj.

$$(|I| < \kappa \wedge (\forall i \in I)|x_i| < \kappa) \to |\bigcup_{i\in I} x_i| < \kappa.$$

V opačném případě je κ *singulární*. Příkladem singulárního kardinálu je $\aleph_\omega = \bigcup_{n\in\omega} \aleph_n$.

Za předpokladu AC jsou všechny izolované kardinály (tj. kardinály tvaru κ^+) regulární (plyne z $\kappa \cdot \kappa = \kappa$).

Nespočetný kardinál, který je současně limitní a regulární, se nazývá *slabě nedosažitelný*.
Existenci takových kardinálů nelze v ZFC (=ZF+AC) dokázat ani vyvrátit.

—126—

Axiom regularity

Zermelo-Fraenkelova axiomatika (ZF) obsahuje *Axiom regularity* neboli *fundovanosti*, jenž jsme dosud neuvedli (ani nepotřebovali). Ten říká, že neexistuje posloupnost $\{x_n\}_{n\in\omega}$ množin splňující $x_0 \ni x_1 \ni x_2 \ni \ldots$.

Ekvivalentně lze tento axiom vyjádřit rovností $\mathbf{WF} = \mathbf{V}$, kde $\mathbf{WF}$ je třída, kterou získáme transfinitně opakovanou operací potence, se nazývá *fundované jádro*:

$$\begin{aligned} \mathbf{WF} &= \bigcup_{\alpha\in\mathbf{On}} V_\alpha, \text{ kde} \\ V_0 &= \emptyset, \\ V_{\alpha+1} &= \mathcal{P}(V_\alpha), \\ V_\lambda &= \bigcup_{\alpha<\lambda} V_\alpha \text{ pro } \lambda \text{ limitní.} \end{aligned}$$

—127—

- Axiom regularity rozděluje množiny do přehledné hierarchie V_α. Pro každou množinu x lze najít nejmenší α takové, že $x \subseteq V_\alpha$; Potom $x \in V_{\alpha+1} - V_\alpha$. Toto α se značí $\varrho(x)$.
- Všechny V_n pro $n \in \omega$ jsou konečné množiny.
- Pro každý ordinál α platí $\varrho(\alpha) = \alpha$.
- Tzv. „běžná“, tj. klasická matematika (číselné obory $\mathbb{R}, \mathbb{C}$, Eukleidovské prostory, funkce, operátory, funkcionály) se *„vejde“* do konečně mnoha pater za V_ω (s rezervou tedy do $V_{\omega+\omega}$).
- Konstrukce univerza iterováním potence závisí na dalších faktorech:
  - Jak vypadá $\mathbf{On}$? (*„Jak je dlouhé?“*)
  - Jaké části x získáme operací $\mathcal{P}(x)$?
    Víme jen, že obsahuje všechny části, jež lze vydělit formulí, tj. části tvaru $\{y \in x\ ;\ \varphi(y)\}$.

—128—

Konstruovatelné množiny

Konstruovatelné univerzum $\mathbf{L}$ je obor množin definovaný transfinitní rekurzí takto:

$$\begin{aligned} \mathbf{L} &= \bigcup_{\alpha\in\mathbf{On}} L_\alpha, \text{ kde} \\ L_0 &= \emptyset, \\ L_{\alpha+1} &= \mathrm{Def}(L_\alpha), \\ L_\lambda &= \bigcup_{\alpha<\lambda} L_\alpha \text{ pro } \lambda \text{ limitní,} \end{aligned}$$

kde

$$\mathrm{Def}(x) = \{\{y \in x\ ;\ \langle x, \in\rangle \models \Phi(y, \bar z)\}\ ;\ \bar z \in x \wedge \Phi \text{ je formule}\}$$

přičemž $\bar z$ značí nějakou (formální) n-tici $z_1, \ldots, z_n$ a rovněž pojmy *„být formule“* a „$\models$“ jsou vyjádřeny formálně v jazyce ZF.

—129—

- V $\mathbf{L}$ v α-tém kroku přidáváme jen ty množiny, které lze definovat z množin již zkonstruovaných. Přidáváme tedy jen to, co je nutné. Každá množina v L_α je určena jednoznačně tzv. konstruující funkcí def. na α.
- Uvnitř univerza $\mathbf{L}$ (stejně jako v $\mathbf{WF}$) platí všechny axiomy ZF.
- Uvnitř univerza $\mathbf{L}$ platí rovnost $\mathbf{V} = \mathbf{L}$ (každá množina je konstruovatelná). Tzv. *axiom konstruovatelnosti*.
- Za předpokladu $\mathbf{V} = \mathbf{L}$ lze celé univerzum dobře uspořádat: lexikograficky se uspořádají konstruující funkce jednotlivých množin.
- Z $\mathbf{V} = \mathbf{L}$ tedy plyne AC.
- $\mathbf{V} = \mathbf{L}$ dále implikuje zobecněnou hypotézu kontinua (GCH): $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

Jinými metodami lze popsat univerza ZF, v nichž AC a/nebo GCH neplatí.

—130—

Potřebujeme opravdu axiom výběru?

Podívejme se znovu na aplikaci AC v důkazu tvrzení:
Funkce $f : \mathbb{R} \to \mathbb{R}$ *splňující* $\lim_{n\to\infty} f(a_n) = f(a)$ *pro každou posloupnost* $\{a_n\}_{n\in\omega}$ *konvergující k* a *je spojitá v* a.

Je-li f nespojitá v bodě a dle obvyklé $\varepsilon\delta$-definice, užíváme AC k výběru posloupnosti $\{a_n\}_{n\in\omega}$, jejíž obrazy nekonvergují k $f(a)$.

V praxi, je-li f nějak „rozumně“ zadaná, budu schopen posloupnost $\{a_n\}_{n\in\omega}$ přímo definovat na základě konkrétní znalosti f, a tedy se obejdu bez AC. Ostatně v univerzu konstruovatelných množin je axiom výběru dokazatelný.

AC je třeba chápat jako mocný teoretický princip, který nám umožňuje řešit řadu úloh jednotně a obecně bez ohledu na konkrétní danost.

—131—

Je ZF bezesporná teorie?

1. Nevíme, věříme že ano (pracujeme v ní dlouho, spor jsme nenašli).
2. Víme ale, že si její bezesporností nikdy nebudeme jisti neb ji nelze dokázat (řekneme si proč).
3. Pracujeme pouze s tzv. relativní bezesporností, např.: je-li ZF bezesporná, je ZF+AC bezesporná.

Je ZF úplná teorie? (Předpokládáme-li její bezespornost)

1. Není (např. AC, CH, GCH, jakož i ohromné množství dalších známých principů, jsou na ní nezávislé – nelze je v ZF dokázat ani vyvrátit).
2. Je to ještě horší: žádná rekurzivně axiomatizovaná teorie obsahující elementární aritmetiku přirozených čísel není úplná.
3. Tudíž ZF ani **nelze zúplnit** přidáním konečné nebo rekurzivně vyčíslitelné množiny axiomů.

Totéž platí i pro další možné axiomatizace teorie množin.

—132—

Meze formální metody

1. Logika 1. řádu je úplná (neplést s úplností teorie!!). Tj. formule, která platí v každém modelu dané teorie, je v ní dokazatelná (a naopak).
2. Löwenheim-Skolemova věta: bezesporná teorie ve spočetném jazyce má aspoň jeden nejvýše spočetný model.
3. Skolemův paradox: ZF je teorie ve spočetném jazyce, musí tedy mít (je-li bezesporná) spočetný model $\mathcal{V}$. Uvnitř $\mathcal{V}$ lze zkonstruovat množinu reálných čísel; ta je částí $\mathcal{V}$ a tudíž spočetná.
   Množina reálných čísel je ale přece nespočetná !?
4. Množina *„reálných čísel ve smyslu* $\mathcal{V}$*“* je nespočetná *„ve smyslu* $\mathcal{V}$*“*, ale *„zevně“* je spočetná (jako $\mathcal{V}$). Nejde o tutéž spočetnost!
5. Pojmy jako množina, spočetnost, mohutnost, dokonce konečnost jsou relativní.

—133—

6. Věta o kompaktnosti říká, že teorie T vzniklá rozšířením ZF o konstantu c a axiomy $\underline{n} < c$, kde $\underline{n}$ je term definující množinu odpovídající přirozenému číslu n, je bezesporná (je-li ZF bezesporná).
7. V každém modelu této teorie T pak existují přirozená čísla, jež jsou z našeho (metamatematického) pohledu nekonečná, ovšem ve smyslu daného modelu jsou konečná (splňují formální definici konečnosti).
8. Pojem (meta-matematické) konečnosti se liší od konečnosti formální (ve smyslu teorie). Může se lišit i mezi různými modely téže teorie.

—134—

1. Gödelova věta o neúplnosti

Říká toto:

Pro každou formální axiomatizovanou teorii T obsahující alespoň elementární (např. Robinsonovu) aritmetiku lze zkonstruovat aritmetické tvrzení, jež je pravdivé, ale v T nedokazatelné.

Jinými slovy, taková teorie nemůže být současně úplná a bezesporná.

Axiomatizovanost znamená, že množina mimologických axiomů musí být vyčíslitelná (tj. existuje algoritmus rozhodující, zda daná formule je či není axiomem dané teorie).

—135—

Princip důkazu: je založen na paradoxu lháře a self-referenci (tvrzení o sobě – opět forma *diagonální metody*). V elementární aritmetice nejprve zakódujeme jazyk a zformalizujeme pojmy formule a důkazu. Dále dokážeme diagonální lemma: *„pro libovolnou formuli $\varphi(x)$ existuje formule ϑ tak, že $\vartheta \leftrightarrow \varphi(\ulcorner\vartheta\urcorner)$“*, kde $\ulcorner\vartheta\urcorner$ značí term pro přirozené číslo, jež je formálním kódem formule ϑ.

Jsou-li důsledky T o přirozených číslech pravdivé, stačí nyní pomocí diagonálního lemmatu najít formuli η, která říká (je ekvivalentní s tvrzením) *„neexistuje důkaz η v T“*.

Kdyby byla η dokazatelná v T, byla by pravdivá, a tedy nedokazatelná v T (spor). Tedy je η nedokazatelná (a proto i pravdivá).

Pro teorie, jež obsahují aritmetiku, ale tvrdí o číslech i nepravdivá tvrzení, lze použít formuli η: *„pro každý důkaz η v T existuje kratší důkaz $\neg\eta$“*.

—136—

2. Gödelova věta o neúplnosti

Je-li T formální axiomatizovaná teorie obsahující alespoň elementární aritmetiku a základní pravdy o dokazatelnosti, nelze v T dokázat formální bezespornost T.

Důsledky: nelze dokázat bezespornost Peanovy aritmetiky v ní samé; nelze dokázat bezespornost ZF v ZF, atp.

Přidáme-li k ZF axiom *„ZF je bezesporná“*, získáme teorii T, jejíž bezespornost opět nelze v T ověřit.

Z Gödelovy věty plyne, že bezespornost Peanovy aritmetiky ani žádné silnější teorie nelze dokázat finitními prostředky.

—137—

Logika 2. řádu

Obsahuje v sobě logiku 1. řádu.

Jazyk obsahuje vedle proměnných 1. řádu pro individua *proměnné 2. řádu* pro množiny individuí a symbol $\in$ pro náležení (tzv. monadická logika) resp. pro n-ární predikáty a funkce (plná logika 2. řádu), které lze také kvantifikovat.

Dvě možné sémantiky:

V obou případech se vychází ze struktury 1. řádu.

Standardní sémantika: proměnné 2. řádu nabývají všech možných hodnot na dané struktuře, tj. např. proměnné pro množiny individuí nabývají všech prvků potence nosiče dané struktury.

Henkinova sémantika: proměnné 2. řádu nabývají hodnot z nějakého daného oboru (jen nějaká podmnožina potence).

—138—

Logika 2. řádu se standardní sémantikou

- je silnější než logika 1. řádu
  Např. Peanova aritmetika 2. řádu s axiomem indukce tvaru
  $$(\forall X)[(0 \in X \wedge (\forall n)(n \in X \to n+1 \in X)) \to (\forall n) n \in X]$$
  je úplná a $\mathbb{N}$ je (až na izomorfismus) její jediný model.
  Podobně: v teorii uspořádaných archimedovských těles lze na rozdíl od logiky 1. řádu vyjádřit axiom o existenci suprema omezené množiny a tím jednoznačně axiomatizovat reálná čísla.
- nelze pro ni sestrojit dedukční systém, který by byl úplný
  (to je také důsledek 1. Gödelovy věty)

Logika 2. řádu s Henkinovou sémantikou

- má úplný dedukční systém
- lze převést na logiku 1. řádu (je tedy stejně silná)