Poznámka: Tento text vzniká jako materiál k přednášce Logika a teorie množin na MFF UK v Praze. Jelikož jde o text ve fázi vzniku, obsahuje jistě řadu nedostatků, které budou průběžně odstraňovány, stejně jako se text bude obsahově rozrůstat. Budu rád, pokud mě o nalezených chybách informujete na petrglivicky@gmail.com.

LOGIKA A TEORIE MNOŽIN

verze pro ZS 2016/17

Petr Glivický[1]

[1]petrglivicky@gmail.com, 2012-2017

Kapitola 2

Teorie množin

2.1 Úvod

Teorie množin tvoří dnes rámec, ve kterém je možné formalizovat (téměř) veškerou matematiku. Každou matematickou disciplínu je tedy možné interpretovat jako součást teorie množin. Metaforicky bývá proto teorie množin označována za svět matematiky.

V teorii množin je každý matematický objekt (např. funkce, vektorový prostor, číslo 1) množinou a všechny vztahy mezi objekty jsou vztahy množinové, vyjádřitelné pouze pomocí relace „být prvkem“ ($\in$). Poznamenejme, že „množinová definice“ pojmu je v mnoha případech (např. u již zmíněné funkce) obecnější než definice předmnožinové. Díky tomu vedl vznik teorie množin k rozvoji mnoha matematických disciplín daleko za hranice jejich původního oboru.

Naivní (též Cantorova) teorie množin, vytvořená Georgem Cantorem v 70. letech 19. století, vycházela z intuitivního pojetí množiny jako dobře vymezeného souboru libovolných objektů. Šlo tedy o teorii neformální, založenou na intuici. Oproti tomu axiomatická teorie množin je dána svojí axiomatikou, tj. seznamem axiomů. O existenci a vlastnostech množin se pak usuzuje pouze z těchto axiomů. Přitom toto usuzování je precizováno v rámci formální predikátové logiky.

V průběhu 20. století bylo v reakci na problémy, v nichž se ocitla naivní Cantorova teorie množin, vytvořeno několik různých axiomatizací teorie množin. Kromě dnes nejužívanejší Zermelo-Fraenkelovy (ZF) také například teorie Gödel-Bernaysova (GB) a Kelley-Morseova (KM). V řadě kandidátů na nahrazení Cantorovy teorie musíme zmínit též Russellovu teorii typů, která však není axiomatizací teorie množin. Zermelo-Fraenkelovu teorii ZF s axiomatikou rozšířenou o jeden další axiom, tzv. axiom výběru (AC), značíme ZFC a nazýváme ji Zermelo-Fraenkelova teorie množin s axiomem výběru.

V této přednášce se budeme zabývat výhradně Zermelo-Fraenkelovou teorií množin s axiomem výběru. Použijeme-li spojení „teorie množin“, míníme tím obvykle (není-li uvedeno jinak) právě teorii ZFC.

2.2 Základní pojmy syntaxe predikátové logiky

Jak již bylo řečeno, teorie ZFC, jíž se budeme zabývat, je teorií axiomatickou, formalizovanou pomocí predikátové logiky. Nastíníme proto nyní některé potřebné pojmy ze syntaxe predikátové logiky. Všechny tyto pojmy budou upřesněny v kapitole týkající se predikátové logiky.

2.2.1 Jazyk

Jazyk je zadán seznamem symbolů, kde u každého symbolu je určen jeho druh – relační či funkční – a četnost (arita) $n \in \mathbb{N}$ (značící počet argumentů, které symbol přijímá). Symboly uvedené v tomto seznamu se nazývají mimologické. Kromě nich každý jazyk obsahuje symboly logické, které tvoří nekonečně mnoho symbolů pro proměnné ($x, y, z, \ldots$), symboly pro logické spojky ($\neg$, $\rightarrow$,

$\&$, $\vee$, $\leftrightarrow$), kvantifikátory ($\forall$, $\exists$) a případně ještě pomocné symboly (závorky). Pokud není řečeno jinak, je symbolem každého jazyka též symbol $=$.

2.2.2 Formule, teorie

Správně utvořená tvrzení ze symbolů jazyka se nazývají *formule* tohoto jazyka. *Teorii* ztotožňujeme s její axiomatikou, tj. se seznamem nějakých formulí, které nazýváme axiomy této teorie.

Příklad 2.2:1. Jazyk L lze zadat například následovně: $L = \langle 0, 1, +, \cdot, < \rangle$, kde symboly $0, 1$ jsou nulární (tj. četnosti 0) funkční, $+, \cdot$ binární (tj. četnosti 2) funkční a $<$ binární relační. Výrazy $0 < x$, $\neg(x = y) \rightarrow (1 + y < 0 \cdot x)$ či $(\forall x)(\exists y)(x = y + 1 \,\&\, x \cdot x < 0)$ jsou pak příklady formulí jazyka L.

2.3 Axiomatika Zermelo-Fraenkelovy teorie množin

Uvedeme nyní axiomatiku Zermelo-Fraenkelovy teorie množin (ZF). Axiomu výběru, který spolu se ZF tvoří teorii ZFC se budeme věnovat později.

2.3.1 Jazyk ZF

ZF je teorie v jazyce $L = \langle \in \rangle$, kde $\in$ je binární relační symbol. Jazyk $L = \langle \in \rangle$ se nazývá jazyk teorie množin, či též $\in$-jazyk (čteme „epsilon-jazyk“). Formule jazyka teorie množin nazýváme také $\in$-formule (čteme „epsilon-formule“), často též jen formule.

Symbol $\in$ interpretujeme jako relaci „být prvkem“, tj. $x \in y$ čteme „(množina) x je prvkem (množiny) y“. Individua, která si představujeme pod proměnnými $x, y, z, u, v, \ldots$ nazýváme množiny. Pojem „množina“ tedy užíváme jen jako jazykovou figuru pro srozumitelnější vyjádření zamýšleného významu formulí; nepřikládáme mu žádný hlubší význam a nijak ho dále nespecifikujeme. Axiomatická teorie množin tedy (na rozdíl od teorie naivní) vůbec neodpovídá na otázku: „Co je to množina?“

Úmluva o značení

V průběhu přenášky budeme definovat různé další symboly (např. $\subseteq, \emptyset, \cap, \cup, \ldots$) a používat je v zápisech formulí. Přísně vzato, formule obsahující jiný mimologický symbol než $\in$, není formulí jazyka teorie množin. Použití nějakého nově definovaného symbolu proto budeme chápat jen jako zkratku za $\in$-formuli, která vznikne nahrazením všech užitých nových symbolů jejich definicemi (v $\in$-jazyce).

Značí-li $\sqsubset$ nějaký symbol pro binární relaci (např. $=$, $\in$, $\subseteq$, $\ldots$), zavádíme pro něj následující zkratky. Formule $x \sqsupset y$ je zkratkou za $y \sqsubset x$ a $x \not\sqsubset y$ je zkratkou za $\neg(x \sqsubset y)$. Můžeme tedy psát např. $x \neq y$, $x \ni y$ či dokonce $x \not\ni y$.

2.3.2 Třídy

Je-li φ nějaká $\in$-formule a x proměnná vyskytující se ve φ, pak zápis $\{x; \varphi(x)\}$ čteme „soubor všech (množin) x, pro něž platí $\varphi(x)$“ a nazýváme ho *třída* (daná formulí $\varphi(x)$). Třídy dále značíme obvykle velkými písmeny latinské abecedy. Je-li X třída $\{x; \varphi(x)\}$, pak zápis $y \in X$ čteme „(množina) y je prvkem třídy X“ a chápeme ho jako zkratku za formuli $\varphi(y)$. Podobně, je-li Y třída $\{x; \psi(x)\}$, pak zápis $X = Y$ čteme „(třídy) X a Y se rovnají“ a chápeme ho jako zkratku za formuli $(\forall x)(\varphi(x) \leftrightarrow \psi(x))$.

Třídy jsou tedy entity jiného druhu než množiny – zatímco množiny chápeme jako základní objekty naší teorie, třídy jsou pouhé formální zápisy, kterých užíváme ve vyjadřování se o množinách ve formě zkratek za $\in$-formule. Narozdíl od zápisů $x \in y$ a $x \in Y$ tak zápisy $X \in Y$ či $X \in y$ pro třídy X, Y a množiny x, y nemají žádný smysl, neboť jsme jejich významy nijak nedefinovali (a ani bychom žádným rozumným způsobem definovat nemohli). Třídy tedy nemohou být (ani nebýt) prvky jiných tříd ani množin.

Pro každou množinu z je $Z = \{x; x \in z\}$ třída mající tytéž prvky jako množina z. Třídu Z pak s množinou z ztotožňujeme, píšeme $z = Z$ a říkáme také, že třída Z je množinou nebo naopak, že množina z je třídou. Každá množina je tedy třídou, avšak nikoli naopak. Třída, která není množinou se nazývá *vlastní třída.*

Pozorování 2.3:1 (Russellův paradox)**.** *Třída* $M = \{x; x \notin x\}$ *je vlastní.*

Důkaz. Předpokládejme pro spor, že $M = m$ pro nějakou množinu m. Pak ovšem

$$m \in m \Leftrightarrow m \in M \Leftrightarrow m \notin m,$$

kde první ekvivalence platí díky $m = M$ a druhá plyne z definice třídy M. To je zjevný spor. □

Třída $\{x; x = x\}$ obsahuje jako své prvky všechny množiny. Značíme ji $\mathbf{V}$ a nazýváme *univerzální třída.* Z axiomů teorie ZF (konkrétně například z instance axiomu vydělení pro formuli $x \notin x$ nebo též z axiomu fundovanosti) vyplývá, že $\mathbf{V}$ je vlastní třída.

2.3.3 Axiomy ZF

Představíme nyní postupně axiomy teorie ZF. Pro přehlednost uvádíme na tomto místě seznam všech axiomů s jejich tradičními názvy a intuitivním významem. Přesné znění axiomu je uvedeno vždy v jemu příslušející pasáži v následujícím textu. Simultánně s výkladem jednotlivých axiomů budeme postupně zavádět některé elementární pojmy teorie množin.

axiom existence:	„Existuje alespoň jedna množina.“
axiom extenzionality:	„Množiny, které mají stejné prvky, se rovnají.“
schéma axiomů vydělení:	„Vydělením těch prvků nějaké množiny, které splňují danou množinovou vlastnost, vznikne množina.“
axiom dvojice:	„Pro každé dvě množiny existuje dvouprvková množina, která má za prvky právě je.“
axiom sjednocení:	„Sjednocením množiny množin vznikne množina.“
axiom potence:	„Existuje množina všech podmnožin dané množiny.“
schéma axiomů nahrazení:	„Obraz množiny v daném množinově definovaném zobrazení je množina.“
axiom nekonečna:	„Existuje alespoň jedna nekonečná množina.“
axiom fundovanosti:	„Neexistuje nekonečný klesající $\in$-řetězec.“

Axiom existence

Znění:	$(\exists x) x = x$
Význam:	„Existuje alespoň jedna množina.“

Axiom postuluje existenci nějaké množiny. Je dokazatelný v čisté predikátové logice a lze ho tedy z axiomatiky ZF vynechat. Uvádíme ho pouze z historických důvodů.

Axiom extenzionality

Znění:	$(\forall x)(\forall y)((\forall u)(u \in x \leftrightarrow u \in y) \rightarrow x = y)$
Význam:	„Množiny, které mají stejné prvky, se rovnají.“

Opačná implikace, tj. „pokud se množiny rovnají, pak mají stejné prvky“ je dokazatelná v čisté predikátové logice. Tento axiom vyjadřuje důležitou vlastnost, kterou od množin očekáváme, totiž to, že množina je jednoznačně určena tím, které prvky obsahuje.

Říkáme, že třída X je *podtřída* třídy Y a píšeme $X \subseteq Y$, pokud každý prvek X je také prvkem Y, tj. pokud platí $(\forall u)(u \in X \to u \in Y)$. Je-li třída X množinou, používáme namísto termínu podtřída též termín *podmnožina*. Je-li $X \subseteq Y$ a $X \neq Y$, nazýváme X *vlastní podtřídou* Y a píšeme $X \subsetneq Y$. Je-li navíc X množinou, pak mluvíme o *vlastní podmnožině*. (Poznamenejme, že souvislost termínu „vlastní podtřída“ s dříve definovaným pojmem „vlastní třída“ je čistě jazyková. Speciálně tedy vlastní podtřída nemusí být vlastní třídou.) Z axiomu extenzionality vyplývá

$$x \subseteq y \,\&\, y \subseteq x \to x = y.$$

Schéma axiomů vydělení

Znění:	$(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow (u \in x \,\&\, \varphi(u)))$ pro každou formuli $\varphi(u)$ neobsahující proměnnou z
Význam:	„Vydělením těch prvků nějaké množiny, které splňují danou množinovou vlastnost φ, vznikne množina.“
Sestrojená množina:	$\{u \in x; \varphi(u)\} = \{u; u \in x \,\&\, \varphi(u)\}$

Schéma vydělení není jediným axiomem, nýbrž vyjadřuje nekonečně mnoho různých axiomů naráz – pro každou formuli φ jeden, nazývaný instance schématu vydělení pro φ. Instance schématu vydělení pro formuli φ říká, že pro každou množinu x soubor všech prvků x, o nichž φ platí, tvoří množinu. Omezení tohoto vydělování na prvky nějaké již předem dané množiny x je zde podstatné. Bez něj by totiž bylo možné získat množinu implikující spor v teorii množin (např. formulí φ: $u \notin u$ bychom dospěli k Russellovu paradoxu (Pozorování 2.3:1)).

Množina z získaná vydělením prvků z x formulí $\varphi(u)$ podle příslušné instance schématu vydělení existuje jediná – to plyne z axiomu extenzionality. Značíme ji dále

$$\{u \in x; \varphi(u)\},$$

což čteme „množina všech u z x, takových, že platí $\varphi(u)$.“

Je snadné nahlédnout, že schéma axiomů vydělení vyjadřuje právě skutečnost, že každá podtřída množiny je množinou, tj. že množiny nemají podtřídy, které jsou vlastní třídy.

Prázdná množina je taková množina z, která nemá žádné prvky, tj. neexistuje u s $u \in z$. Prázdnou množinu značíme symbolem $\emptyset$. Toto značení je korektní pouze za předpokladu, že existuje právě jedna množina, která je prázdná. To ovšem vyplývá snadno následovně: Existence prázdné množiny plyne z instance schématu vydělení pro formuli $u \neq u$. Množina x, z níž vydělujeme, existuje dle axiomu existence. Řečeno stručněji, je

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

To, že je prázdná množina jediná, je důsledkem axiomu extenzionality.

Axiom dvojice

Znění:	$(\forall x)(\forall y)(\exists z)(\forall u)(u \in z \leftrightarrow u = x \vee u = y)$
Význam:	„Pro každé dvě množiny existuje dvouprvková množina, která má za prvky právě je.“
Sestrojená množina:	$\{x, y\} = \{u; u = x \vee u = y\}$

Axiom dvojice je konstrukčním axiomem. Jako konstrukční označujeme axiom, jenž udává způsob, jakým můžeme z již vytvořených množin zkonstruovat množinu další, a to „složitější“, tj. takovou, která není nutně částí žádné z původních množin (a tedy není možné ji sestrojit použitím schématu vydělení).

Množinu mající právě dva prvky x a y značíme $\{x, y\}$ a nazýváme *(neuspořádaná) dvojice* množin x a y. Existence množiny $\{x, y\}$ pro každé dvě množiny x, y plyne z axiomu dvojice, její jednoznačnost z axiomu extenzionality. Platí (dle definice a axiomu extenzionality)

$$\{x, y\} = \{y, x\}, \qquad \{x, y\} = \{u, v\} \leftrightarrow (x = u \,\&\, y = v) \vee (x = v \,\&\, y = u).$$

Místo $\{x,x\}$ píšeme $\{x\}$ a říkáme, že to je *jednoprvková množina* s prvkem x. Je

$$\{x\} = \{y\} \leftrightarrow x = y,$$

avšak obecně $x \neq \{x\}$ (např. $\emptyset \neq \{\emptyset\}$, jelikož $\emptyset \in \{\emptyset\}$ a tedy $\{\emptyset\}$ není prázdná). Poznamenejme, že důsledkem axiomu fundovanosti je dokonce $(\forall x)(x \neq \{x\})$.

Axiom sjednocení

Znění:	$(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow (\exists y)(y \in x \,\&\, u \in y)$
Význam:	„Sjednocením množiny množin vznikne množina.“
Sestrojená množina:	$\bigcup x = \{u; (\exists y)(y \in x \,\&\, u \in y)\}$

Axiom sjednocení je konstrukčním axiomem. Je-li x již vytvořená množina s prvky $y, y', \ldots$ (libovolně mnoha), pak dle axiomu sjednocení existuje množina z, jejímiž prvky jsou právě prvky náležející alespoň jedné z množin $y, y', \ldots$.

Je-li x množina, množinu z nazýváme *sjednocením* x a značíme $\bigcup x$, pokud $u \in z$, právě když $u \in y$ pro nějaký prvek $y \in x$. Existence $\bigcup x$ plyne z axiomu sjednocení, jednoznačnost z axiomu extenzionality. Místo $\bigcup\{x,y\}$ píšeme $x \cup y$ a říkáme, že to je *sjednocení množin* x a y. Užíváme zde axiomy dvojice a sjednocení.

Pro množinu x definujeme její *průnik* značený $\bigcap x$ jako množinu z obsahující právě ty množiny u (z $\bigcup x$), které jsou prvkem každé množiny $y \in x$, tj. $u \in \bigcap x$ právě když $u \in y$ pro každý prvek $y \in x$. Skutečnost, že průnikem jakékoli množiny x je opět množina plyne z axiomů sjednocení a vydělení; je totiž $\bigcap(x) = \{u \in \bigcup(x); (\forall y)(y \in x \to u \in y)\}$. Místo $\bigcap\{x,y\}$ píšeme $x \cap y$ a říkáme, že to je *průnik množin* x a y.

Definujeme též, obecněji, sjednocení a průnik třídy X jako $\bigcup X = \{u; (\exists y)(y \in X \,\&\, u \in y)\}$ resp. $\bigcap X = \{u; (\forall y)(y \in X \to u \in y)\}$. Axiom sjednocení pak vyjadřuje skutečnost, že je-li X množinou, je $\bigcup X$ také množinou. Poznamenejme, že $\bigcap X$ je množinou pro každou neprázdnou třídu X – to plyne ze schématu axiomů vydělení, neboť pro libovolné $w \in X$ je $\bigcap X = \{u \in w; (\forall y)(y \in X \to u \in y)\}$. Naopak $\bigcap \emptyset = \mathbf{V}$.

Již máme definovány symboly $\emptyset$, $\{x\}$ a $\{x,y\}$ pro prázdnou, jednoprvkovou a dvouprvkovou množinu s určenými prvky. Pomocí axiomu sjednocení můžeme definovat n-prvkovou množinu pro libovolné n přirozené následující induktivní definicí: Pro $n \geq 3$ se *n-prvková množina* s vzájemně různými prvky $x_1, \ldots, x_n$ definuje jako $\{x_1, \ldots, x_n\} = \{x_1, \ldots, x_{n-1}\} \cup \{x_n\}$.

Poznámka 2.3:2. Přirozená čísla n z předchozího odstavce jsou chápána intuitivně, jako čísla $0, 1, 2, \ldots$ (tj. $0, 1, 2$ a tak dále). Přitom význam výrazů „$\ldots$“ či „a tak dále“ nikterak nespecifikujeme. Takováto přirozená čísla nejsou množiny (zavedení přirozených čísel v teorii množin si ukážeme později), stojí mimo námi budovanou formální teorii množin v oblasti pojmů, jež chápeme intuitivně. Abychom je odlišili od přirozených čísel zkonstruovaných uvnitř teorie množin, nazýváme čísla $0, 1, 2, \ldots$ *metapřirozená čísla.*

Říkáme-li tedy výše, že definujeme $\{x_1, \ldots, x_n\}$ pro každé přirozené číslo $n \geq 3$, myslíme tím právě metapřirozená n, tj. to, že definujeme $\{x_1, x_2, x_3\}$, $\{x_1, x_2, x_3, x_4\}$, $\{x_1, x_2, x_3, x_4, x_5\}$ a tak dále.

Axiom potence

Znění:	$(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow u \subseteq x)$
Význam:	„Existuje množina všech podmnožin dané množiny.“
V $\in$-jazyce:	$(\forall x)(\exists z)(\forall u)(u \in z \leftrightarrow (\forall v)(v \in u \to v \in x))$
Sestrojená množina:	$\mathcal{P}(x) = \{u; u \subseteq x\}$

Axiom potence lze chápat jako konstrukční axiom. Na rozdíl od dalších konstrukčních axiomů (dvojice a sjednocení) však axiom potence „konstruuje“ množinu obsahující i prvky, které ještě nebyly explicitně sestrojeny (ne každá podmnožina x byla již dříve sestrojena pomocí jiných axiomů).

V tomto ohledu se podobá spíše axiomům „existenčním“, kterými jsou axiomy existence a nekonečna (a některé instance schématu nahrazení). Tato vlastnost axiomu potence zapříčinila, že v počátcích axiomatické teorie množin měli proti němu někteří matematici výhrady a pochybnosti o jeho správnosti.

Množinu mající za prvky všechny podmnožiny dané množiny x nazýváme *potence* x a značíme $\mathcal{P}(x)$. Jinými slovy $u \in \mathcal{P}(x)$ právě když $u \subseteq x$. Její existenci postuluje axiom potence. Jednoznačnost plyne z axiomu extenzionality. Zřejmě platí

$$\emptyset \in \mathcal{P}(x),\ x \in \mathcal{P}(x),\ \{u_1, \dots, u_n\} \in \mathcal{P}(x) \text{ pro } u_1, \dots, u_n \in x.$$

Schéma axiomů nahrazení

Znění:	$(\forall u)(\forall v)(\forall w)(\varphi(u,v) \,\&\, \varphi(u,w) \to v = w) \to$ $\to (\forall x)(\exists z)(\forall v)(v \in z \leftrightarrow (\exists u)(u \in x \,\&\, \varphi(u,v)))$ pro každou formuli $\varphi(u,v)$ neobsahující proměnné w ani z.
Význam:	„Obraz množiny v daném množinově definovaném zobrazení je množina.“

Schéma axiomů nahrazení sestává z nekonečně mnoha samostatných axiomů, instancí schématu nahrazení, jedné pro každou formuli $\varphi(u,v)$. První část axiomu nahrazení vyjadřuje předpoklad, že $\varphi(u,v)$ „určuje (parciální) zobrazení $u \mapsto v$“, tj. že ke každému u existuje nejvýše jedno v, pro něž $\varphi(u,v)$. Druhá část pak říká, že nahradíme-li prvky u nějaké množiny x jim přiřazenými prvky v, vznikne tímto nahrazením množina. Podobně jako u axiomu vydělení i zde je omezení nahrazování na nějakou již dříve vytvořenou množinu klíčové a jeho vypuštění by vedlo ke sporu.

Poznámka 2.3:3. Povšimněte si, že schéma axiomů vydělení je důsledkem schématu axiomů nahrazení. Skutečně: instance schématu vydělení pro formuli $\psi(u)$ vyplývá z instance schématu nahrazení pro formuli $\varphi(u,v):\ u = v \,\&\, \psi(u)$. Schéma axiomů vydělení lze tedy z axiomatiky ZF vynechat; uvádíme ho však z historických důvodů. Totéž platí pro axiom dvojice – ten vyplývá ze schématu nahrazení a axiomu potence následovně: $\{\emptyset, \{\emptyset\}\} = \mathcal{P}(\mathcal{P}(\emptyset))$ je množina dle axiomu potence; pro dané množiny a, b je pak existence dvojice $\{a, b\}$ zajištěna instancí schématu nahrazení pro formuli $\varphi(u,v) : (u = \emptyset \,\&\, v = a) \vee (u = \{\emptyset\} \,\&\, v = b)$ aplikované na množinu $x = \{\emptyset, \{\emptyset\}\}$, přičemž podformuli $u = \{\emptyset\}$ lze snadno vyjádřit bez použití jednotice $\{\emptyset\}$ (pojem jednotice jsme zavedli až pomocí axiomu dvojice).

Axiom nekonečna

Znění:	$(\exists z)(\emptyset \in z \,\&\, (\forall u)(u \in z \to u \cup \{u\} \in z))$
Význam:	„Existuje alespoň jedna nekonečná množina.“
V $\in$-jazyce:	$(\exists z)((\exists u)(u \in z \,\&\, (\forall v)\neg(v \in u)) \,\&$ $\& \,(\forall u)(u \in z) \to (\exists w)(w \in z \,\&\, (\forall y)(y \in w \leftrightarrow y \in u \vee y = u)))$

Axiom nekonečna je axiom čistě „existenční“, podobného charakteru jako axiom existence. Postuluje existenci nekonečné množiny z. Nekonečnost je přitom vyjádřena induktivně, tj. tím, že jednak $\emptyset \in z$ (první krok) a pro každý prvek $u \in z$ je také jeho „následník“ $u \cup \{u\}$ prvkem z (indukční krok); zřejmě $u \cup \{u\}$ je různé od u. Speciálně máme tedy v z následující prvky $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, …

Axiom nekonečna se zásadně liší od všech předchozích axiomů (snad s výjimkou axiomu existence). Postuluje existenci aktuálně nekonečné množiny, aniž by dával jakýkoli návod, jak tuto množinu vytvořit z již dříve vytvořených množin. Jde tedy o velice silný axiom, který přidává k teorii množin popsaných předchozími axiomy celé nové „patro“ množin nekonečných. Opodstatnění platnosti (či bezespornosti) tohoto axiomu je hluboce netriviální a otázka jeho přijetí či odmítnutí se stala předmětem mnoha zásadních historických sporů mezi významnými matematiky a filosofy.

Uvidíme později, že množina z postulovaná axiomem nekonečna obsahuje všechna přirozená čísla (po té, co je v teorii množin zavedeme) a že množina všech přirozených čísel je nejmenší množinou z splňující vlastnost uvedenou pro množinu z v axiomu nekonečna.

Axiom fundovanosti (regularity)

Znění:	$(\forall x)(x \neq \emptyset \rightarrow (\exists u)(u \in x \,\&\, u \cap x = \emptyset))$
Význam:	„Neexistuje nekonečný klesající $\in$-řetězec.“ „Každá neprázdná množina má $\in$-minimální prvek.“
V $\in$-jazyce:	$(\forall x)((\exists v)(v \in x) \rightarrow (\exists u)(u \in x \,\&\, (\forall w)(w \in u \rightarrow \neg(w \in x))))$

Axiom fundovanosti omezuje bohatost množinového univerza tím, že zakazuje některé typy množin či jejich posloupností. Například množina x taková, že $x = \{x\}$ (x je svým vlastním jediným prvkem) porušuje podmínku ve znění axiomu. Podobně též například množina y s vlastností $y \in y$ či množina x obsahující prvky $u_1, u_2, \ldots$ splňující $u_{i+1} \in u_i$ vedou ke sporu s axiomem fundovanosti.

Pro naprostou většinu praktických aplikací teorie množin je platnost či neplatnost axiomu fundovanosti nepodstatná. V průběhu celé přednášky tento axiom ani jedenkrát nepoužijeme. Uvádíme ho pouze z historických důvodů.

Poznámka 2.3:4. Z výše uvedeného vyplývá, že mnohé z axiomů, jež jsme uvedli, jsou v axiomatice teorie ZF nadbytečné, neboť vyplývají z axiomů ostatních. Ve skutečnosti bychom mohli celý výklad teorie množin v tomto textu provést v teorii obsahující pouze axiomy extenzionality, sjednocení, potence, nekonečna a schéma axiomů nahrazení. Pokud k tomuto výčtu přidáme ještě axiom fundovanosti (který z ostatních nevyplývá, avšak my ho nebudeme pro náš výklad potřebovat), pak je vzniklá teorie ekvivalentní s námi uvedenou axiomatikou ZF.

2.4 Množinová reprezentace matematiky

Teorie ZF poskytuje rámec, v němž je možné formalizovat téměř veškerou matematiku. Abychom tohoto cíle dosáhli, musíme stanovit, které množiny budou reprezentovat matematické objekty, o jejichž formalizaci se snažíme, a to tak, aby množinové vztahy mezi těmito reprezentacemi (dokazatelné z axiomů ZF) odpovídaly vztahům, které o objektech na neformální úrovni očekáváme. Musíme tak například definovat, která množina je funkcí, přirozeným číslem či vektorovým prostorem, a to tak, aby intuitivní vlastnosti funkcí, přirozených čísel a vektorových prostorů byly dokazatelné o příslušných množinách v teorii ZF.

V dalším výkladu již nebudeme vždy zdůrazňovat, na základě jakých axiomů definované množiny existují a proč jsou určeny jednoznačně. Nabádáme však čtenáře, aby si jako cvičení existenci a jednoznačnost každé nově definované množiny z axiomů ZF dokázal.

2.4.1 Základní množinové (a třídové) pojmy a vztahy

V následujících odstavcích zavedeme některé základní množinové operace a vztahy. Často budeme tyto operace a vztahy definovat obecněji pro třídy namísto množin. To, že jde v takovém případě skutečně o obecnější definice, je dáno faktem, že každá množina je také třídou.

Třídové operace

Pro třídy X, Y definujeme třídy $X \cup Y = \{u; u \in X \vee u \in Y\}$, $X \cap Y = \{u; u \in X \,\&\, u \in Y\}$ a $X - Y = \{u; u \in X \,\&\, u \notin Y\}$ a nazýváme je po řadě *sjednocení*, *průnik* a *rozdíl tříd* X a Y. Jsou-li X, Y množiny, pak jejich sjednocení průnik i rozdíl jsou též množinami. Navíc takto definované sjednocení a průnik dvou množin se shodují s definicemi uvedenými dříve (v diskuzi k axiomu sjednocení). *Doplněk* (též *komplement*) třídy X, značený $-X$ je, třída $\mathbf{V} - X$. Povšimněte si, že doplněk množiny může být vlastní třída (např. $-\emptyset = \mathbf{V}$).

Dále uvádíme výčet některých základních vlastností právě definovaných operací:

Lemma 2.4:1. *Pro všechny třídy X, Y, Z platí:*

1. *(Komutativita)* $X \cup Y = Y \cup X$, $X \cap Y = Y \cap X$,
2. *(Asociativita)* $(X \cup Y) \cup Z = X \cup (Y \cup Z)$, $(X \cap Y) \cap Z = X \cap (Y \cap Z)$,
3. *(Distributivita)* $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$, $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$,
4. *(de Morganova pravidla)* $X - (Y \cup Z) = (X - Y) \cap (X - Z)$, $X - (Y \cap Z) = (X - Y) \cup (X - Z)$.

Důkaz. Plyne bezprostředně z definic. Ponecháváme ho jako cvičení. □

Uspořádané n-tice a kartézský součin

Chceme definovat pojem uspořádané dvojice (x, y) pro libovolné dvě množiny x, y. Aby si nějaká množina (x, y) zasloužila označení „uspořádaná dvojice množin x a y", musí jistě splňovat

$$(x, y) = (u, v) \leftrightarrow (x = u \,\&\, y = v). \tag{2.1}$$

Naopak, kdykoli definujeme (x, y) tak, že (2.1) bude platit, můžeme ji označit za uspořádanou dvojici x a y.

Definujeme proto *uspořádanou dvojici* (x, y) jako $\{\{x\}, \{x, y\}\}$. (Intuitivně: $\{x, y\}$ stanovuje, které dvě množiny v uspořádané dvojici leží, a $\{x\}$ určuje, která z nich je první v pořadí.) Je snadné nahlédnout, že vlastost (2.1) je pro tuto definici splněna.

Obecněji, pro n přirozené, zavádíme pojem uspořádané n-tice následovně:

- *uspořádaná* 0*-tice* je $\emptyset$,
- *uspořádaná* 1*-tice* s členem x je $(x) = x$,
- pro $n \geq 2$ *uspořádaná* n*-tice* množin $x_1, \ldots, x_n$ je $(x_1, \ldots, x_n) = ((x_1, \ldots, x_{n-1}), x_n)$.

Tato definice je induktivní – pro $n > 2$ je n-tice definována pomocí již definovaných pojmů $(n-1)$-tice a dvojice. Zde, stejně jako dále, pod pojmem přirozené číslo n myslíme číslo metapřirozené (viz poznámku 2.3:2).

Třídu $X \times Y = \{(x, y); x \in X \,\&\, y \in Y\}$ nazýváme *kartézský součin* tříd X a Y. Jsou-li X, Y množiny, pak $X \times Y$ je také množina – to plyne ze schématu vydělení ($X \times Y$ je vyděleno z $\mathcal{P}(\mathcal{P}(X \cup Y))$, což je množina díky axiomům potence, dvojice a sjednocení).

Pro třídu X a n přirozené definujeme *kartézskou mocninu* $X^n = \{(x_1, \ldots, x_n); x_1 \in X \,\&\, \ldots \,\&\, x_n \in X\}$. Lze snadno nahlédnout, že $X^0 = \{\emptyset\}$, $X^1 = X$ a $X^n = X \times \ldots \times X$ pro $n \geq 2$, kde na pravé straně je n kopií X.

Relace

Relace je každá třída R uspořádaných dvojic, tj. $R \subseteq \mathbf{V}^2$. Je-li $(x, y) \in R$, píšeme místo toho často $R(x, y)$ či xRy a říkáme, že relace R platí o x a y.

Relace jsou formalizací vztahů mezi objekty v teorii množin. V následujících případech budeme užívat množinu $\mathbb{N}$ všech přirozených čísel (spolu se základními vztahy a operacemi na $\mathbb{N}$), kterou zadefinujeme až v následujících kapitolách:

Příklad 2.4:2.

1. $R_< = \{(m, n); m, n \in \mathbb{N} \,\&\, m < n\}$ je relace uspořádání na množině přirozených čísel $\mathbb{N}$, tj. platí $R_<(m, n)$ právě když $m < n$.
2. $R_d = \{(m, n); m, n \in \mathbb{N} \,\&\, (\exists a \in \mathbb{N})(a \cdot m = n)\}$ je relace dělitelnosti na $\mathbb{N}$, tj. platí $R_d(m, n)$ právě když $m|n$.
3. $R_\in = \{(x, y); x \in y\}$ je relace $\in$ („epsilon") na univerzální třídě $\mathbf{V}$. (Povšimněte si, že symbol $\in$ jazyka teorie množin formálně vzato není relací.)

4. $R_{\subseteq} = \{(x,y); x \subseteq y\}$ je relace inkluze na univerzální třídě $\mathbf{V}$.

5. Pro každou třídu X jsou $\emptyset$ a X^2 relace na X.

Třídy dom(R)= $\{x; (\exists y)((x,y) \in R)\}$ a rng(R)= $\{y; (\exists x)((x,y) \in R)\}$ nazýváme *definiční obor* (též *domain*) a *obor hodnot* (též *range*) relace R. Je-li R množina, pak dom(R) i rng(R) jsou množiny díky schématu vydělení (vyděluje se z množiny $\bigcup\bigcup R$).

Inverzní relace k relaci R je relace R^{-1}= $\{(y,x); (x,y) \in R\}$. Je-li R množina, pak R^{-1} také (například podle schématu nahrazení).

Obraz třídy X v relaci R je třída $R''X$=$R[X]$= $\{y; (\exists x)(x \in X \,\&\, (x,y) \in R)\}$. *Vzor* třídy Y v relaci R je třída $R^{-1}{''}Y$=$R^{-1}[Y]$= $\{x; (\exists y)(y \in Y \,\&\, (x,y) \in R)\}$. Je snadno vidět, že vzor Y v relaci R je totožný s obrazem Y v relaci R^{-1} inverzní k R (proto také uvedené značení pro vzor nekoliduje se značením pro obraz a inverzní relaci).

Restrikce (také *zúžení*) relace R na třídu Z je $R \restriction Z$= $\{(x,y) \in R; x \in Z\}$.

Složení relací R a S (v tomto pořadí) je relace $R \circ S = \{(x,z); (\exists y)((x,y) \in R \,\&\, (y,z) \in S)\}$.

Příklad 2.4:3. Pro relace z příkladu 2.4:2 platí:

1. Definiční obor a obor hodnot relace $R_<$ jsou dom$(R_<) = \mathbb{N}$ a rng$(R_<) = \mathbb{N} - \{0\}$.

2. Pro inverzní relaci k relaci $R_<$ platí $R_<^{-1}(m,n)$, právě když $m > n$.

3. Obrazy množin $\{2\}$ a $\{1\}$ v relaci R_d jsou $R_d[\{2\}] = \{n; n \in \mathbb{N} \text{ sudé}\}$ respektive $R_d[\{1\}] = \mathbb{N}$.

4. Vzor množiny $\{u,v\}$ v relaci $R_\in$ je $R_\in^{-1}[\{u,v\}] = u \cup v$.

5. Restrikce relace X^2 na třídu $Z \subseteq X$ je $R \restriction Z = Z \times X$.

6. Pro složení relace $R_<$ se sebou samou platí $(R_< \circ R_<)(m,n)$, právě když $n - m \geq 2$.

Poznámka 2.4:4. Skládání relací je (narozdíl od speciálního případu skládání funkcí) relativně složitá operace – abychom rozhodli, zda dvojice (x,z) leží v $R \circ S$, musíme projít potenciálně všechna y, pro která $(x,y) \in R$, a u každého ověřit, zda $(y,z) \in S$. Implementace skládání relací na počítači je v důsledku toho výpočetně složitá operace. Je proto zajímavé, že existuje velmi jednoduchý „analogový“ způsob skládání relací: Předpokládejme pro názornost, že $R, S \subseteq [0,1]^2$, kde $[0,1]$ značí uzavřený interval reálných čísel. Uvažme jednotkovou krychli $[0,1]^3$ a zakresleme R do její stěny $x \times y$ (tj. stěny určené osami x a y) a S do stěny $y \times z$. Promítneme-li pak R i S z těchto stěn kolmo do vnitřku krychle a podíváme se na průnik těchto průmětů kolmo ze stěny $x \times z$, tvar, který na stěně $x \times z$ uvidíme, bude právě $R \circ S$.

Funkce

Zavedeme pojem funkce jako speciální případ relace, která splňuje podmínku jednoznačnosti: každé x z definičního oboru je v relaci právě s jedním y z oboru hodnot. Řečeno přesněji:

Funkce či též *zobrazení* je každá relace R splňující

$$(\forall x, y, y')(((x,y) \in R \,\&\, (x,y') \in R) \to y = y').$$

Jelikož každá funkce je relace, všechny pojmy definované pro relace (definiční obor, obor hodnot, inverzní relace, obraz a vzor množiny, restrikce a složení) jsou automaticky zavedeny i pro funkce. Je-li F funkce, značíme pro každé $x \in$ dom(F) jediné y splňující $(x,y) \in F$ jako $F(x)$. Je potom rng$(F) = \{F(x); x \in \text{dom}(F)\}$. Zápisem $F : X \to Y$ pro třídy X, Y myslíme, že F je funkce, dom$(F) = X$ a rng$(F) \subseteq Y$.

Funkce F se nazývá *prostá* (též *injektivní*), pokud $F(u) = F(u') \to u = u'$ pro všechna $u, u' \in$ dom(F). Funkce $F : X \to Y$ je *na* množinu Y (též *surjektivní*), pokud rng$(F) = Y$. Funkce $F : X \to Y$ je *bijekce* (též *bijektivní* funkce) z X na Y, pokud je prostá a na Y. Je-li F prostá, pak relace F^{-1} je také funkce. Nazýváme ji *inverzní funkce* k funkci F.

Příklad 2.4:5.

1. Pro každou třídu X je relace $id_X = \{(x, x); x \in X\}$ funkce (nazýváme ji identita na X). Platí $id_X(x) = x$ a dále $id_X : X \to X$ je bijekce a $id_X^{-1} = id_X$.
2. $\emptyset$ je funkce.
3. Žádná z relací $R_<, R_d, R_\in, R_\subseteq$ z příkladu 2.4:2 není funkce, neboť nesplňuje podmínku jednoznačnosti.

Index