Úvod do matematické logiky a teorie množin

Petr Kůrka

Vznik logiky má původ v rozhovoru. Vyslovím-li nějaké tvrzení, které partner bezprostředně nepřijme, musím pro něj uvést nějaké argumenty nebo ho jinak doložit. Logika se snaží postihnout, kdy je tato argumentace vedena korektně a kdy ne. Logika jako metoda správného rozumového uvažování má ale svá omezení. Tato omezení poznáváme na paradoxech. Paradoxy jsou logické úvahy vedoucí k závěrům, které nám připadají podivné nebo nepřijatelné. Často je tomu tak proto, že jsou založeny na nějakých nevyslovených předpokladech. Řešení nebo vysvětlení paradoxů pak spočívá v nalezení takových skrytých předpokladů.

Mnoho paradoxů je založeno na jevu samovztažnosti. Řekl-li Kréťan Epimenidés, že Kréťané stále lžou, lze tento výrok vztáhnout i na Epimenida, a tím ho zpochybnit. Tato samovztažnost působí překvapivě, nevede však k logickému sporu. Vede jen k tomu, že Epimenidův výrok odmítneme jako nepravdivý. Kréťané nelžou stále, ale jenom někdy. Silnější verzi Epimenidova paradoxu dostaneme, prohlásíme-li

"Věta, kterou právě říkám, je nepravdivá."

Tato věta nemůže být ani pravdivá ani nepravdivá. Jedno z východisek spočívá v tom, že tuto větu nebudeme považovat za výrok a odmítneme se jí v logice zabývat. Epimenidův paradox má mnoho variant. Jedna z nich vypráví o holiči, který si napsal nad dveře, že holí všechny muže v městě, kteří se neholí sami. Jinou verzí je paradoxní definice

"Nejmenší přirozené číslo, které nelze popsat větou s méně než dvaceti slovy."

Epimenidův paradox a jeho moderní verze se stal velmi plodným v logice a teorii množin dvacátého století. Ukazuje nám, čemu se v logice musíme vyhnout abychom se nedostali do sporu.

V matematice se používá formalizovaná verze logiky. Matematické věty a důkazy lze zapsat v umělém jazyce, který se nazývá **predikátový počet**. Predikát vyjadřuje, že nějaký objekt má nějakou vlastnost (jednočetný predikát) nebo že dva nebo více objektů jsou v nějakém vztahu (vícečetné predikáty). Dalšími prvky predikátového počtu jsou kvantifikátory, které vyjadřují, že nějakou vlastnost mají všechny objekty určitého typu (obecný kvantifikátor) nebo aspoň nějaký (existenční kvantifikátor). Matematická logika se zabývá studiem predikátového počtu a jeho vlastnostmi jako je dokazatelnost či bezespornost. Jádrem tohoto přístupu je **axiomatická metoda**. Nejjednodušší matematické principy, které nám připadají intuitivně zřejmé, prohlásíme za axiomy a hledáme další matematická tvrzení, která z nich lze odvodit. Pro každou matematickou oblast lze takto budovat příslušnou teorii s axiomy specifickými pro tuto oblast.

Privilegované postavení mezi matematickými teoriemi zaujímá **teorie množin**. Vznikla v devatenáctém století jako studium vlastností nekonečna, zejména srovnáváním různých velikostí nekonečna. Ukázalo se však, že v teorii množin lze modelovat i jiné matematické teorie tak, že se každému matematickému objektu přiřadí určitá množina, která ho reprezentuje. V tomto smyslu je teorie množin základem matematiky, na kterém lze budovat další matematické disciplíny.

1 Výrokový počet

Výrok chápeme jako tvrzení, o kterém lze říci zda je pravdivé nebo nepravdivé. V matematické logice se zabýváme výroky o matematických objektech: číslech, bodech, přímkách, vektorech, množinách. Příklady výroků jsou

$$3 < 5, \quad 7 \text{ je prvočíslo}, \quad 8 \text{ je prvočíslo}, \quad 1 + 1 = 3$$

První dva výroky jsou pravdivé, druhé dva jsou nepravdivé. Místo o pravdivosti či nepravdivosti mluvíme také o **pravdivostní hodnotě výroku**: 0 je-li nepravdivý a 1 je-li pravdivý.

1.1 Logické spojky

Z výroků sestavujeme složitější výroky pomocí logických spojek negace $\neg$, konjunkce $\&$, disjunkce $\vee$, implikace $\rightarrow$ a ekvivalence $\equiv$. Logické spojky chápeme jako operace na množině pravdivostních hodnot $\{0, 1\}$. Jsou definovány tabulkou

p	$\neg p$
0	1
1	0

p	q	$p \,\&\, q$	$p \vee q$	$p \rightarrow q$	$p \equiv q$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Například výroky

$$(3 < 4) \,\&\, (4 < 5), \ \ (3 < 4) \vee (4 < 3), \ \ (4 < 3) \rightarrow (5 < 4)$$

jsou pravdivé a výroky

$$(3 < 4) \rightarrow (5 < 4), \ \ (3 = 4) \vee (4 < 3)$$

jsou nepravdivé.

Logické spojky negace, konjunkce, disjunkce, implikace a ekvivalence jsou nejčastěji používané ale nikoliv jediné možné. Dvoučetná logická spojka je dána čtveřicí nul a jedniček, kterým jsou přiřazeny všechny možné kombinace dvou proměnných, tj. $00, 01, 10, 11$. Je tedy celkem 16 dvoučetných logických spojek, mezi nimi jsou však i jednočetné binární spojky (identita jedné z proměnných a její negace) a také 0-četné spojky, identická pravda (se samými jedničkami), kterou značíme **true** a identická nepravda se samými nulami, kterou značíme **false**.

Některé složené výroky jsou pravdivé nezávisle na tom z jakých výroků jsou sestaveny. Je-li p jakýkoliv výrok, pravdivý či nepravdivý, je $p \rightarrow p$ vždy pravdivý. Říkáme, že p je **výroková proměnná** a $p \rightarrow p$ je formule, která je tautologie. **Formule** jsou výrazy sestavené z výrokových proměnných pomocí logických spojek. Říkáme, že formule je **tautologie**, je-li pravdivá při jakékoliv pravdivostní hodnotě svých proměnných. Například $p \ \& \ p$ je formule která není tautologie: je-li p nepravdivé, není pravdivé ani $p \ \& \ p$. Říkáme, že formule je **sporná**, pokud není pravdivá při žádné pravdivostní hodnotě svých proměnných, tj. je-li negací tautologie. Příklad sporné formule je $p \ \& \ \neg p$. Říkáme, že formule je **splnitelná**, pokud je pravdivá alespoň při jedné pravdivostní hodnotě svých proměnných, tj. pokud není sporná.

1.2 Syntax výrokového počtu

Ve formálním systému výrokové logiky se formule chápou jako řetězce znaků. Pravidla, která stanovují jak se tyto formule vytváří, se nazývají **syntaktická**. Výrokový počet definuje umělý jazyk (podobně jako jazyky programovací) a syntaktická pravidla jsou obdobou gramatiky živých jazyků.

Syntaktická pravidla v prvé řadě stanoví **abecedu**, tj. znaky, ze kterých se formule vytváří. Mezi tyto znaky patří logické spojky, malá písmena pro výrokové proměnné a závorky. Abeceda výrokového počtu je tedy množina

$$A = \{\neg, \ \& \ , \vee, \rightarrow, \equiv, (,), a, b, \ldots, y, z\}$$

Jako výrokové proměnné většinou používáme jednotlivá malá písmena latinské abecedy. Protože však uvažujeme formule s libovolným počtem proměnných, připustíme jako proměnné také řetězce malých písmen.

Definice 1
1. Každý řetězec sestavený z malých písmen je výroková proměnná.
2. Každá výroková proměnná je formule.
3. Je-li φ formule, je $\neg\varphi$ formule.
4. Jsou-li φ, ψ formule, jsou také $(\varphi \ \& \ \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$ a $(\varphi \equiv \psi)$ formule.

Například řetězce p, abc jsou výrokové proměnné a tedy také formule. Další formule jsou $((p \vee q) \rightarrow p)$, $(\neg ab \rightarrow c)$, $\neg(a \ \& \ b)$, zatímco řetězce $\neg \rightarrow$, $ab \rightarrow$

formule nejsou. Otázka, které řetězce jsou formule a které nikoliv je algoritmicky rozhodnutelná: existuje algoritmus, který přečte na vstupu řetězec abecedy A a rozhodne, zda je tento řetězec formule či nikoliv. Tento algoritmus je založen na rekurzivním použití definice formule.

Řetězec znaků $p \to p$ není formule: chybí zde vnější závorky. Nebudeme však naší definici dodržovat úplně striktně a tyto vnější závorky budeme vynechávat. Přijmeme-li precedenční konvence, můžeme také vynechávat některé vnitřní závorky. Není-li pořadí operací stanoveno závorkami, má negace přednost před konjunkcí a disjunkcí a ty mají přednost před implikací a ekvivalencí. Formuli $((p \,\&\, q) \to p)$ budeme tedy psát jednodušeji $p \,\&\, q \to p$.

1.3 Sémantika výrokového počtu

Významem prvků umělého jazyka se zabývá jeho **sémantika**. Význam formule je zobrazení, které přiřazuje pravdivostním hodnotám jejích výrokových proměnných pravdivostní hodnotu dané formule. Má-li daná formule φ n výrokových proměnných, představuje tedy zobrazení z množiny $\{0,1\}^n$ n-tic nul a jedniček do množiny $\{0,1\}$. Formule je tautologie, jestliže toto zobrazení je identicky rovné jedné, tj. pokud pravdivostní hodnota formule je 1 pro každou kombinaci pravdivostních hodnot jejích výrokových proměnných. Pravdivostní funkci formule vyhodnocujeme tabulkou, ve které řádky odpovídají kombinacím pravdivostních hodnot výrokových proměnných a sloupce odpovídají podformulím dané formule. Například pro formuli $(p \to q) \equiv (\neg q \to \neg p)$ sestavíme tabulku

pq	$p \to q$	$\neg q$	$\neg p$	$\neg q \to \neg p$	$(p \to q) \equiv (\neg q \to \neg p)$
00	1	1	1	1	1
01	1	0	1	1	1
10	0	1	0	0	1
11	1	0	0	1	1

V posledním sloupci jsou samé jednotky, to znamená, že formule je tautologie. Také otázka, zda daná formule je tautologie, či nikoliv, je algoritmicky rozhodnutelná. Algoritmus, který tuto úlohu rozhoduje, v dané formuli nalezne všechny její výrokové proměnné, a vyhodnotí její pravdivostní hodnotu při všech možných hodnotách těchto proměnných.

Některé tautologie vyjadřují důležité principy důkazů matematických vět. Právě uváděná tautologie vyjadřuje princip důkazu sporem. Chceme-li dokázat že z p plyne q, předpokládáme že platí, $\neg q$ a snažíme se odvodit $\neg p$ které je ve sporu s p. Sám princip sporu je tautologie $\neg(p \,\&\, \neg p)$. Nemůže platit výrok p a současně jeho negace $\neg p$. Duální tautologie je zákon vyloučeného třetího $p \vee \neg p$, buď platí p nebo jeho negace. Dvojí negací se pravdivostní hodnota nemění, $\neg\neg p \equiv p$. Další důležité tautologie mají podobu algebraických identit.

Chápeme-li totiž množinu pravdivostních hodnot $\{0, 1\}$ jako algebraickou strukturu, hraje ekvivalence roli rovnosti a implikace roli nerovnosti. Všimeme si, že výrok $(p \equiv q)$ platí právě když $p = q$ (tj. p a q mají stejnou pravdivostní hodnotu), a $p \rightarrow q$ platí právě když $p \leq q$. Konjunkce je v této algebraické struktuře operace minima a disjunkce operace maxima. Proto disjunkce a konjunkce mají podobné ale duální vlastnosti. Například pro ně platí komutativní a asociativní zákony a mezi nimi platí zákony distributivní. Negací se navzájem převádí podle de Morganových pravidel. Uveďme si některé důležité tautologie.

$\neg\neg p \equiv p$	dvojí negace
$(p \rightarrow q) \equiv (\neg q \rightarrow \neg p)$	důkaz sporem
$\neg(p \mathbin{\&} \neg p)$	princip sporu
$p \vee \neg p$	princip vyloučeného třetího
$(p \rightarrow q) \mathbin{\&} (q \rightarrow r) \rightarrow (p \rightarrow r)$	transitivita implikace
$(p \rightarrow q) \mathbin{\&} (q \rightarrow p) \equiv (p \equiv q)$	antisymetrie implikace
$(p \mathbin{\&} q) \equiv (q \mathbin{\&} p)$	komutativní zákon konjunkce
$(p \vee q) \equiv (q \vee p)$	komutativní zákon disjunkce
$((p \mathbin{\&} q) \mathbin{\&} r) \equiv (p \mathbin{\&} (q \mathbin{\&} r))$	asociativní zákon konjunkce
$((p \vee q) \vee r) \equiv (p \vee (q \vee r))$	asociativní zákon disjunkce
$p \mathbin{\&} (q \vee r) \equiv (p \mathbin{\&} q) \vee (p \mathbin{\&} r)$	distributivní zákon
$p \vee (q \mathbin{\&} r) \equiv (p \vee q) \mathbin{\&} (p \vee r)$	
$p \mathbin{\&} q \rightarrow p$	vlastnost minima
$p \mathbin{\&} q \rightarrow q$	
$p \rightarrow p \vee q$	vlastnost maxima
$q \rightarrow p \vee q$	
$\neg(p \mathbin{\&} q) \equiv (\neg p \vee \neg q)$	de Morganův zákon
$\neg(p \vee q) \equiv (\neg p \mathbin{\&} \neg q)$	
$\neg(p \rightarrow q) \equiv (p \mathbin{\&} \neg q)$	negace implikace
$p \vee q \equiv (\neg p \rightarrow q)$	
$(p \rightarrow q) \equiv \neg p \vee q$	

1.4 Disjunktní normální forma

Pomocí tautologií lze formule upravovat podobně jako algebraické výrazy a přitom zjednodušovat. Při některých aplikacích je vhodné vyjádřit danou formuli v nějakém předepsaném tvaru. Jedním takovým tvarem je disjunktní normální forma. Je to disjunkce konjuncí, které jsou sestaveny z výrokových proměnných případně z jejich negací. Pro dvě proměnné p a q uvažujme čtyři konjunkce

pq	$(\neg p \mathbin{\&} \neg q)$	$(\neg p \mathbin{\&} q)$	$(p \mathbin{\&} \neg q)$	$(p \mathbin{\&} q)$
00	1	0	0	0
01	0	1	0	0
10	0	0	1	0
11	0	0	0	1

Každá z těchto konjunkcí je pravdivá právě při jediné kombinaci pravdivostních hodnot p a q, prvá pro 00, druhá pro 01, třetí pro 10 a čtvrtá pro 11, tedy právě v jednom řádku tabulky. Je-li nyní φ libovolná formule s dvěma proměnnými je ekvivalentní disjunkci některých těchto konjunkcí a sice právě těch, v jejímž řádku má φ jednotky. Tedy například

$$\begin{array}{rcl} (p \equiv q) & \equiv & (\neg p \,\&\, \neg q) \vee (p \,\&\, q) \\ (p \rightarrow q) & \equiv & (\neg p \,\&\, \neg q) \vee (\neg p \,\&\, q) \vee (p \,\&\, q) \end{array}$$

Na takovouto disjunktní normální formu lze převést každou formuli výrokového počtu.

2 Predikátový počet

Základní syntaktické prvky predikátového počtu jsou predikáty, operace a konstanty. Predikáty vyjadřují vlastnosti matematických objektů případně jejich vztahy. Dvoučetný predikát nerovnosti $<$ vyjadřuje vztah mezi dvěma čísly. Jednočetný predikát "býti prvočíslem" vyjadřuje vlastnost čísel. V geometrii se používá dvoučetný predikát "bod x leží na přímce p", teorie množin je založena na dvoučetném predikátu náležení $x \in y$, tj. množina x je prvkem množiny y. V každé matematické oblasti pracujeme s predikátem rovnosti $=$.

Operace přiřazují matematickým objektům jiné matematické objekty. V algebře pracujeme s dvoučetnými aritmetickými operacemi jako je sčítání a násobení. Jednočetná operace je například faktoriál. Jsou také 0-četné operace, tj. konstanty. V algebře za konstanty často volíme 0 a 1 protože mají vyjímečné vlastnosti vzhledem ke sčítání a násobení.

Formule predikátového počtu vypovídají o vztazích v matematických strukturách. Strukturu chápeme jako množinu, na které jsou dány nějaké operace a vztahy odpovídající studovaným predikátům. Budeme se zabývat zejména algebraickými strukturami jeko je struktura $\mathbb{N}$ přirozených čísel, struktura $\mathbb{Z}$ celých čísel, struktura $\mathbb{Q}$ racionálních čísel a struktura $\mathbb{R}$ reálných čísel. Ve všech těchto strukturách jsou definovány operace sčítání a násobení a predikáty rovnosti a nerovnosti. Existují také konečné struktury. Pro každé přirozené číslo $n > 0$ uvažujeme strukturu $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ zbytkových tříd modulo n. Sčítání a odčítání je v ní definováno modulo n, uspořádání nerovnostmi $0 < 1 < \cdots < n-1$. Například ve struktuře $\mathbb{Z}_3$ je sčítání a násobení definováno tabulkami

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Pojmy množiny a struktury zatím chápeme intuitivně. Přesněji je vymezíme až se budeme zabývat teorií množin.

Základní, neboli **atomární** formule predikátového počtu sestávají z predikátů vztažených na nějaké konstanty, proměnné nebo aritmetické výrazy z nich sestavené. Takovéto aritmetické výrazy nazýváme **termy**. Například $x+1$ nebo $(x+y)*z$ jsou termy a $x+y=y+x$ nebo $x<0$ jsou atomární formule. Z atomárních formulí vytváříme složitější pomocí logických spojek a **kvantifikátorů**: Obecný kvantifikátor $\forall$ vyjadřuje, že nějaké tvrzení platí pro všechny objekty (dané struktury). Existenční kvantifikátor $\exists$ vyjadřuje, že existuje aspoň jeden objekt s touto vlastností. Například formule $(\forall x)(x \geq 0)$ vyjadřuje, že každé číslo je větší nebo rovno nule. To platí ve struktuře přirozených čísel, ale ne ve struktuře celých čísel. To zapisujeme

$$\mathbb{N} \models (\forall x)(x \geq 0), \quad \mathbb{Z} \not\models (\forall x)(x \geq 0)$$

Pro určení pravdivosti formulí je důležité rozlišení mezi volnými a vázanými proměnnými formule. Volné proměnné jsou ty, které nejsou kvantifikovány. Například ve formuli $x < z \rightarrow (\exists y)(x < y < z)$ jsou proměnné x a z volné, proměnná y je vázaná. Formule $x+y=y+x$ má pouze volné proměnné x a y. Formule $(\forall x)(\exists y)(x<y)$ má pouze vázané proměnné x a y. Formule budeme vytvářet tak, aby žádná proměnná nebyla ve formuli současně volná a vázaná. Například $(x>0)\ \&\ (\exists x)(x<0)$ za formuli považovat nebudeme. Místo ní použijeme formuli $(x>0)\ \&\ (\exists y)(y<0)$.

2.1 Syntax predikátového počtu

Také v predikátovém počtu se definují formule jako určité řetězce symbolů. Symboly pro predikáty, operace a konstanty volíme podle toho, jakou matematickou strukturou se zabýváme. Jako příklad si uvedeme predikátový počet pro algebraické struktury s konstantami 0, 1, dvoučetnými operacemi $+$, $*$ a dvoučetnými predikáty $<$ a $=$. Seznam

$$\mathcal{L} = \{0, 1, +, *, <, =\}$$

těchto konstant, operací a predikátů se nazývá **jazyk**. Formule predikátového počtu obsahují symboly jazyka $\mathcal{L}$ a další symboly jako logické spojky, kvantifikátory a malá písmena. Celá abeceda symbolů je tedy

$$A = \{0, 1, +, *, <, =, \neg, \ \&\ , \vee, \rightarrow, \equiv, \forall, \exists, (,), a, b, \ldots, y, z\}$$

Malá písmena opět slouží pro vytváření proměnných, tyto proměnné však zastupují čísla, nebo prvky algebraických struktur, nikoliv výroky.

Před vlastní definicí formulí se zavádí termy, což jsou výrazy sestavené z proměnných a konstant pomocí aritmetických operací. Jejich obdobou v programovacích jazycích jsou aritmetické výrazy.

Definice 2
1. Každý řetězec malých písmen je proměnná.

2. Každá proměnná je term.
3. Konstanty 0 *a* 1 *jsou termy.*
4. Jsou-li s, t, *termy, jsou* $(\mathsf{t}+\mathsf{s})$ *a* $(\mathsf{t}*\mathsf{s})$ *termy.*

Příklady termů jsou řetězce $((x*y)+1)$, $(1+1)$. Naopak řetězce $+*$ nebo $\neg 0$ termy nejsou. Závorky používáme proto aby pořadí operací bylo jednoznačné. Nebudeme však naší definici dodržovat striktně a pokud nebude hrozit nedorozumění, budeme některé závorky vynechávat. Uvedené termy tedy zapíšeme jednodušeji $x*y+1$ nebo $1+1$. Přijímáme opět precedenční konvenci, podle které se nejdříve vykonávají operace násobení a poté sčítání.

Pomocí predikátů se z termů vytvářejí atomární formule. Z atomárních formulí se vytvářejí složitější formule pomocí logických spojek a kvantifikátorů. Současně s definicí formule také vymezujeme, které proměnné jsou ve formuli volné a které vázané.

Definice 3

1. *Jsou-li* s *a* t *termy, jsou* $(\mathsf{s}<\mathsf{t})$ *a* $(\mathsf{s}=\mathsf{t})$ *(atomární) formule. Každá proměnná, která se vyskytuje v atomární formuli, je v ní volná. Žádná proměnná v ní není vázaná.*
2. *Je-li* φ *formule, je* $\neg\varphi$ *formule. Formule* $\neg\varphi$ *má stejné volné proměnné i stejné vázané proměnné jako* φ.
3. *Nechť* φ *a* ψ *jsou formule takové, že žádná proměnná není volná v* φ *a vázaná v* ψ *nebo naopak. Pak* $(\varphi \,\&\, \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$ *a* $(\varphi \equiv \psi)$ *jsou formule. Proměnná je v těchto formulích volná, je-li buď volná v* φ *nebo v* ψ. *Proměnná je v těchto formulích vázaná, je-li buď vázaná v* φ *nebo v* ψ.
4. *Je-li* φ *formule a* x *proměnná, která je volná v* φ, *jsou* $(\forall\mathsf{x})\varphi$ *a* $(\exists\mathsf{x})(\varphi)$ *formule. Proměnná je v těchto formulích volná, je-li volná v* φ *a různá od* x. *Proměnná je v těchto formulích vázaná, je-li buď vázaná v* φ *nebo je to* x.
5. *Říkáme, že formule je otevřená, nemá-li vázané proměnné. Formule je sentence, nemá-li volné proměnné.*

Formule $x+y=y+x$ je otevřená, má pouze volné proměnné. Formule $1+1>0$ je otevřená sentence, nemá ani volné ani vázané proměnné. Formule

$$(\forall x)(\forall z)((x<z) \rightarrow (\exists y)((x<y) \,\&\, (y<z)))$$

vyjadřuje, že mezi každými dvěma čísly existuje třetí. Je to sentence, všechny její proměnné jsou v ní vázané. Také v zápise formulí budeme vynechávat závorky, pokud nevznikne nejednoznačnost. Následují-li po sobě dva kvantifikátory stejného typu, nebudeme znak kvantifikátoru opakovat. Uvedenou formuli pak zapíšeme

$$(\forall x, z)(x<z \rightarrow (\exists y)(x<y<z))$$

Obdobou volných proměnných jsou parametry počítačového programu. Formule vyjadřuje nějaké tvrzení o svých volných proměnných. Vázané proměnné jsou obdobou pomocných proměnných programu, které jsou uživateli skryty. Uvažujeme-li o nějaké formuli φ, která má volné proměnné $\mathsf{x}_1, \ldots, \mathsf{x}_n$ (a případně další volné proměnné), zapisujeme ji $\varphi(\mathsf{x}_1, \ldots, \mathsf{x}_n)$. Tím naznačujeme, že volné proměnné hrají roli parametrů. Řecké písmeno φ tedy používáme jako proměnnou pro formule. Zápis $\varphi(x)$ znamená, že φ je nějaká formule, která má volnou proměnnou x a případně další volné proměnné. Symboly t a s používáme podobně jako proměnné pro termy a $\mathsf{x}_1, \ldots, \mathsf{x}_n$ používáme jako proměnné pro proměnné.

Je-li $\varphi(\mathsf{x})$ formule, která má volnou proměnnou x (a případně další volné proměnné) a je-li t term, značíme $\varphi(\mathsf{t})$ formuli, která vznikne tak, že každý výskyt proměnné x nahradíme termem t. Aby přitom nedošlo ke změně významu, je nutné, aby t neobsahoval proměnné vázané v φ. V tomoto případě říkáme, že term t je **substituovatelný** za proměnnou x do formule φ. Například je-li

$$\varphi(x) \equiv (\exists u)(x < u < 0),$$

je $\varphi(0) \equiv (\exists u)(0 < u < 0)$ a $\varphi(y+1) \equiv (\exists u)(y+1 < u < 0)$. Pokud bychom však dosadili za x term $u+1$, dostali bychom formuli $\varphi(u+1) \equiv (\exists u)(u+1 < u < 0)$ se zcela jiným významem. Term $u+1$ není substituovatelný za x do formule $(\exists u)(0 < u < x)$.

2.2 Sémantika predikátového počtu

Podobně jako pro formule výrokového počtu, chceme i pro formule predikátového počtu stanovit, zda jsou pravdivé či nepravdivé. Pravdivost formulí predikátového počtu však závisí na tom, o jakých matematických objektech hovoří. Například formule $(\exists x)(x < 0)$ je pravdivá ve strukturách $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$, není však pravdivá ve struktuře $\mathbb{N}$ ani v žádném $\mathbb{Z}_n$. I v rámci jedné struktury pravdivost nebo platnost formule závisí na hodnotě jejích proměnných. Formule $x > 0$ platí pro 1 ale neplatí pro 0.

Pro určení pravdivosti či nepravdivosti formulí nejprve určíme hodnoty termů. Hodnota termu t s proměnnými $\mathsf{x}_1, \ldots, \mathsf{x}_n$ závisí na tom jakou hodnotu mají tyto proměnné. Je-li $\mathbb{M}$ struktura a $a_1, \ldots, a_n$ její prvky je

$$\mathsf{t}[\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n]_{\mathbb{M}}$$

prvek struktury $\mathbb{M}$ který získáme, dosadíme-li do termu t za proměnné x_i prvky a_i. Například ve struktuře $\mathbb{N}$ je

$$((x+1)*y)[x:2, y:3]_{\mathbb{N}} = 9, \ \ ((x+1)*y)[x:3, y:2]_{\mathbb{N}} = 8$$

Pravdivost formulí závisí na hodnotě jejich volných proměnných. Pro formuli φ s volnými proměnnými $\mathsf{x}_1, \ldots, \mathsf{x}_n$, strukturu $\mathbb{M}$ a $a_1, \ldots, a_n$ její prvky budeme definovat vztah

$$\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models \varphi$$

že formule φ platí ve struktuře $\mathbb{M}$ při hodnotách a_i proměnných x_i.

Nechť $(\mathsf{t} < \mathsf{s})$ nebo $(\mathsf{t} = \mathsf{s})$ je atomární formule s proměnnými $\mathsf{x}_1, \ldots, \mathsf{x}_n$. Pak

$$\begin{aligned} &\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models (\mathsf{t} < \mathsf{s}) \text{ právě když} \\ &\qquad \mathsf{t}[\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n]_{\mathbb{M}} < \mathsf{s}[\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n]_{\mathbb{M}} \end{aligned}$$

$$\begin{aligned} &\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models (\mathsf{t} = \mathsf{s}) \text{ právě když} \\ &\qquad \mathsf{t}[\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n]_{\mathbb{M}} = \mathsf{s}[\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n]_{\mathbb{M}} \end{aligned}$$

Například $\mathbb{N}, [x : 2, y : 3] \models (x * x > y)$ protože $(x * x)[x : 2, y : 3]_{\mathbb{N}} = 4$ a $y[x : 2, y : 3]_{\mathbb{N}} = 3$. Proměnné $\mathsf{x}_1, \ldots, \mathsf{x}_n$ se nemusí všechny vyskytovat v obou termech t a s. Proměnné navíc zde však nevadí, hodnota termu na nich nezávisí. Podobně

$$\mathbb{N}, [x : 3, y : 7] \models (x * x > y), \quad \mathbb{N}, [x : 3, y : 9] \not\models (x * x > y)$$

Zde $\not\models$ znamená, že formule není splněna.

Platnost formulí vytvořených logickými spojkami se definuje stejně jako ve výrokovém počtu. Je-li φ formule s volnými proměnnými $\mathsf{x}_1, \ldots, \mathsf{x}_n$ a $a_1, \ldots, a_n \in \mathbb{M}$, pak

$$\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models \neg\varphi \text{ právě když } \mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \not\models \varphi$$

Je-li $\varphi \mathbin{\&} \psi$ formule, jejíž všechny volné proměnné jsou $\mathsf{x}_1, \ldots, \mathsf{x}_n$, pak

$$\begin{aligned} &\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models (\varphi \mathbin{\&} \psi) \text{ právě když} \\ &\qquad \mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models \varphi \text{ a } \mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models \psi \end{aligned}$$

a podobně pro další logické spojky. Nakonec význam kvantifikátorů. Nechť φ je formule s volnými proměnnými $\mathsf{x}, \mathsf{x}_1, \ldots, \mathsf{x}_n$ a $a_1, \ldots, a_n \in \mathbb{M}$. Pak

$$\begin{aligned} &\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models (\forall \mathsf{x})\varphi \text{ právě když pro každé } a \in \mathbb{M}, \text{ platí} \\ &\qquad \mathbb{M}, [\mathsf{x} : a, \mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models \varphi \\ &\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models (\exists \mathsf{x})\varphi \text{ právě když existuje } a \in \mathbb{M}, \text{ pro které} \\ &\qquad \mathbb{M}, [\mathsf{x} : a, \mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models \varphi \end{aligned}$$

Jestliže formule je sentence, její platnost nezávisí na hodnotách žádných proměnných, závisí pouze na struktuře. Má-li fomule volné proměnné, říkáme že platí v nějaké struktuře, platí-li v ní pro všechny možné hodnoty jejích volných proměnných.

Definice 4 *Formule φ s volnými proměnnými $\mathsf{x}_1, \ldots, \mathsf{x}_n$ platí ve struktuře $\mathbb{M}$ ($\mathbb{M} \models \varphi$), jestliže pro každé prvky $a_1, \ldots, a_n$ struktury $\mathbb{M}$ platí*

$$\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models \varphi$$

To znamená
$$\mathbb{M} \models \varphi \text{ právě když } \mathbb{M} \models (\forall \mathsf{x}_1)\cdots(\forall \mathsf{x}_n)\varphi$$
Formuli $(\forall \mathsf{x}_1)\dots(\forall x_n)\varphi$ nazýváme **uzávěrem** formule φ. Formule je tedy platná v nějaké struktuře právě když je v ní platný její uzávěr.

Má-li struktura $\mathbb{M}$ konečný počet prvků, je zjištění platnosti sentencí v této struktuře algoritmizovatelné: stačí probrat všechny možné hodnoty, kterých její proměnné mohou nabývat. Z tabulky sčítání ve struktuře $\mathbb{Z}_3$ například zjistíme, že toto sčítání nezávisí na pořadí, takže $\mathbb{Z}_3 \models (x + y = y + x)$, a tedy také $\mathbb{Z}_3 \models (\forall x)(\forall y)(x + y = y + x)$.

Ukážeme dále, že ve struktuře $\mathbb{Z}_3$ existují opačné prvky.

$$\begin{array}{lcl}
\mathbb{Z}_3, [x:0, y:0] \models (x+y=0), & \text{tedy} & \mathbb{Z}_3, [x:0] \models (\exists y)(x+y=0) \\
\mathbb{Z}_3, [x:1, y:2] \models (x+y=0), & \text{tedy} & \mathbb{Z}_3, [x:1] \models (\exists y)(x+y=0) \\
\mathbb{Z}_3, [x:2, y:1] \models (x+y=0), & \text{tedy} & \mathbb{Z}_3, [x:2] \models (\exists y)(x+y=0)
\end{array}$$

Odtud již
$$\mathbb{Z}_3 \models (\forall x)(\exists y)(x + y = 0)$$

V nekonečných strukturách takto platnost formulí ověřovat nemůžeme, protože by to znamenalo vyšetřit nekonečně mnoho možností. Nevíme s jistotou, zda pro přirozená čísla platí komutativní zákon, tj. zda $\mathbb{N} \models x + y = y + x$, věříme tomu však na základě naší představy o přirozených číslech. V logické výstavbě matematiky mají takováto zřejmá leč nevykazatelná tvrzení charakter axiomů, které přijímáme a z nich odvozujeme složitější tvrzení.

Cvičení. Rozhodněte, zda pro $n > 1$ platí
1. $\mathbb{Z}_n \models x * (y + z) = x * y + x * z$
2. $\mathbb{Z}_n \models (\forall x)(\exists y)(x + y = 0)$
3. $\mathbb{Z}_n \models (\exists y)(\forall x)(x + y = 0)$
4. $\mathbb{Z}_n \models (\forall x)(x \neq 0 \to (\exists y)(x * y = 1))$
5. $\mathbb{Z}_n \models x < y \to x + z < y + z$
6. $\mathbb{Z}_n \models (\forall x)(\exists y)(y > x)$
7. $\mathbb{Z}_n \models (\exists x)(\exists y)(\exists z)(x \neq y \neq z \neq x)$

2.3 Logicky pravdivé formule

Přestože obecně platnost formulí v nekonečných strukturách nelze přímo ověřovat, u mnohých formulí to možné je. Mezi ně patří všechny tautologie.

Definice 5 *Formule φ predikátového počtu je tautologie, jestliže vznikne z nějaké tautologie ψ výrokového počtu tak, že v ní každou výrokovou proměnnou nahradíme nějakou formulí predikátového počtu.*

Například $p \rightarrow p$ je tautologie výrokového počtu, takže formule

$$(x > 0) \rightarrow (x > 0), \quad \text{nebo} \quad (\exists x)(x + 1 = 0) \rightarrow (\exists x)(x + 1 = 0)$$

jsou tautologie predikátového počtu. Tyto formule platí pro každé ohodnocení svých proměnných nejen ve struktuře $\mathbb{N}$, ale dokonce v každé myslitelné struktuře, ať jsou aritmetické operace a nerovnosti definovány jakkoliv. Takové formule nazýváme logicky pravdivé.

Definice 6 *Říkáme, že formule φ je logicky pravdivá, jestliže platí v každé neprázdné struktuře.*

$$\models \varphi \quad \textit{jestliže} \ \mathbb{M} \models \varphi \quad \textit{pro každou neprázdnou strukturu} \ \mathbb{M}$$

Každá tautologie je logicky pravdivá. Například každá formule tvaru $\varphi \;\&\; \psi \rightarrow \varphi$, kde φ, ψ jsou libovolné formule, je tautologie a tedy logicky pravdivá. Tautologie však nejsou jediné logicky pravdivé formule. Například pro každou formuli $\varphi(x, y)$ (s volnými proměnnými x a y) je

$$\models (\forall x)(\forall y)\varphi(x, y) \equiv (\forall y)(\forall x)\varphi(x, y)$$

logicky pravdivá formule, ale není to tautologie. Je totiž $\mathbb{M} \models (\forall x)(\forall y)\varphi(x, y)$ právě když pro všechna $a, b \in \mathbb{M}$ platí $\mathbb{M}, [x : a, y : b] \models \varphi(x, y)$, a to platí právě když $\mathbb{M} \models (\forall y)(\forall x)\varphi(x, y)$. Obdobně lze zaměňovat pořadí existenčních kvantifikátorů, takže

$$\models (\exists x)(\exists y)\varphi \equiv (\exists y)(\exists x)\varphi$$

Zajímavější je záměna obecného a existenčního kvantifikátoru. Zde ekvivalence neplatí. Je například

$$\mathbb{Z}_3 \models (\forall x)(\exists y)(x + y = 0), \quad \text{ale} \quad \mathbb{Z}_3 \not\models (\exists y)(\forall x)(x + y = 0)$$

V opačném směru však implikace platí

Tvrzení 7 (Záměna pořadí kvantifikátorů)

$$\models (\exists y)(\forall x)\varphi(x, y) \rightarrow (\forall x)(\exists y)\varphi(x, y)$$

Důkaz: Nechť $x, y, z_1, \ldots, z_n$ jsou volné proměnné formule φ. Nechť $\mathbb{M}$ je struktura, $c_1, \ldots, c_n$ prvky $\mathbb{M}$ a

$$\mathbb{M}, [z_1 : c_1, \ldots, z_n : c_n] \models (\exists y)(\forall x)\varphi(x, y)$$

takže existuje prvek b struktury $\mathbb{M}$, takový že

$$\mathbb{M}, [y : b, z_1 : c_1, \ldots, z_n : c_n] \models (\forall x)\varphi(x, y)$$

Pro každé $a \in \mathbb{M}$ je tedy $\mathbb{M}[x : a, y : b, z_1 : c_1, \ldots, z_n : c_n] \models \varphi(x, y)$, takže

$$\mathbb{M}, [x : a, z_1 : c_1, \ldots, z_n : c_n] \models (\exists y)\varphi$$

a

$$\mathbb{M}, [z_1 : c_1, \ldots, z_n : c_n] \models (\forall x)(\exists y)\varphi(x, y)$$

Pro každé $c_1, \ldots, c_n$ je tedy

$$\mathbb{M}, [z_1 : c_1, \ldots, z_n : c_n] \models (\exists y)(\forall x)\varphi(x, y) \rightarrow (\forall x)(\exists y)\varphi(x, y)$$

takže $\models (\exists y)(\forall x)\varphi(x, y) \rightarrow (\forall x)(\exists y)\varphi(x, y)$ je logicky pravdivá formule. □

Z tohoto argumentu také vidíme, proč neplatí opačná implikace. Jestliže pro každé $a \in \mathbb{M}$ existuje $b \in \mathbb{M}$ pro které $\mathbb{M}, [x : a, y : b] \models \varphi$, tato b mohou být pro různá a různá. Nemusí existovat b, s kterým by φ platila pro všechna a.

Další důležité logicky pravdivé formule jsou De Morganova pravidla, která ukazují, jak se neguje kvantifikovaná formule.

Tvrzení 8 (de Morganova pravidla)

$$\begin{aligned} &\models \quad \neg(\forall x)\varphi(x) \equiv (\exists x)\neg\varphi(x) \\ &\models \quad \neg(\exists x)\varphi(x) \equiv (\forall x)\neg\varphi(x) \end{aligned}$$

Důkaz: Nechť $\mathfrak{y}_1, \ldots, \mathfrak{y}_n$ jsou volné proměnné formule $(\forall x)\varphi$, nechť $\mathbb{M}$ je struktura a $b_1, \ldots, b_n$ její prvky. Je-li

$$\mathbb{M}, [\mathfrak{y}_1 : b_1, \ldots, \mathfrak{y}_n : b_n] \models \neg(\forall x)\varphi(x)$$

pak $\mathbb{M}, [\mathfrak{y}_1 : b_1, \ldots, \mathfrak{y}_n : b_n] \not\models (\forall x)\varphi(x)$ a existuje $a \in \mathbb{M}$, pro které

$$\mathbb{M}, [x : a, \mathfrak{y}_1 : b_1, \ldots, \mathfrak{y}_n : b_n] \not\models \varphi(x)$$

takže

$$\mathbb{M}, [x : a, \mathfrak{y}_1 : b_1, \ldots, \mathfrak{y}_n : b_n] \models \neg\varphi(x)$$

Je tedy $\mathbb{M}, [\mathfrak{y}_1 : b_1, \ldots, \mathfrak{y}_n : b_n] \models (\exists x)\neg\varphi(x)$. Dokázali jsme

$$\mathbb{M}, [\mathfrak{y}_1 : b_1, \ldots, \mathfrak{y}_n : b_n] \models \neg(\forall x)\varphi(x) \rightarrow (\exists x)\neg\varphi(x)$$

Podobně pro opačnou implikaci. Druhé (duální) tvrzení z toho plyne použitím na formuli $\neg\varphi$.

De Morganova pravidla můžeme považovat za jakési "nekonečné tautologie", díváme-li se na obecný kvantifikátor jako na nekonečnou konjunkci a na existenční kvantifikátor jako na nekonečnou disjunkci. Uvažujme konečnou strukturu $\mathbb{M}$ a předpokládejme, že všechny její prvky $a_1, \ldots, a_n$ jsou také konstanty jazyka

$\mathcal{L}$. Taková situace nastává pro náš algebraický jazyk $\mathcal{L}$ u struktury $\mathbb{Z}_2 = \{0, 1\}$. Pak

$$\begin{aligned} \mathbb{M} &\models (\forall x)\varphi(x) \equiv \varphi(a_1) \,\&\, \cdots \,\&\, \varphi(a_n) \\ \mathbb{M} &\models (\exists x)\varphi(x) \equiv \varphi(a_1) \vee \cdots \vee \varphi(a_n) \end{aligned}$$

V konečné struktuře de Morganova pravidla predikátového počtu odpovídají de Morganovým pravidlům výrokového počtu.

$$\begin{aligned} \neg(\forall x)\varphi(x) &\equiv \neg(\varphi(a_1) \,\&\, \cdots \,\&\, \varphi(a_n)) \equiv (\neg\varphi(a_1) \vee \cdots \vee \neg\varphi(a_n)) \\ &\equiv (\exists x)\neg\varphi(x) \end{aligned}$$

Chápeme-li obecný kvantifikátor jako zobecněnou konjunkci a existenční kvantifikátor jako zobecněnou disjunkci, nahlédneme jakým způsobem komutují kvantifikátory s konjunkcí a disjunkcí.

Tvrzení 9 *Následující formule jsou logicky pravdivé:*

$$\begin{aligned} (\forall x)(\varphi(x) \,\&\, \psi(x)) &\equiv (\forall x)\varphi(x) \,\&\, (\forall x)\psi(x) \\ (\exists x)(\varphi(x) \,\&\, \psi(x)) &\rightarrow (\exists x)\varphi(x) \,\&\, (\exists x)\psi(x) \\ (\forall x)\varphi(x) \vee (\forall x)\psi(x) &\rightarrow (\forall x)(\varphi(x) \vee \psi(x)) \\ (\forall x)\varphi(x) \,\&\, (\forall x)\psi(x) &\equiv (\forall x)(\varphi(x) \,\&\, \psi(x)) \end{aligned}$$

Opačné implikace v druhém a třetím řádku neplatí. To je okamžitě vidět je-li $\psi \equiv \neg\varphi$, například $\varphi(x) \equiv (x > 0)$. Evidentně neplatí formule

$$\begin{aligned} (\exists x)(x > 0) \,\&\, (\exists x)(x \leq 0) &\rightarrow (\exists x)(x > 0 \,\&\, x \leq 0) \\ (\forall x)(x > 0 \vee x \leq 0)) &\rightarrow (\forall x)(x > 0) \vee (\forall x)(x \leq 0) \end{aligned}$$

(Píšmeme zde $x \leq 0$ místo $\neg(x > 0)$.) Obdobně můžeme někdy zaměňovat kvantifikátory s dalšími logickými spojkami.

Tvrzení 10

$$\models (\forall x)(\varphi(x) \rightarrow \psi(x)) \rightarrow ((\forall x)\varphi(x) \rightarrow (\forall x)\psi(x))$$

Důkaz: Použijeme tautologie výrokového počtu

$$(p \rightarrow (q \rightarrow r)) \equiv (p \,\&\, q) \rightarrow r)$$

a převedeme uvažovanou formuli na ekvivalentní

$$\models ((\forall x)(\varphi \rightarrow \psi(x)) \,\&\, (\forall x)\varphi(x)) \rightarrow (\forall x)\psi(x)$$

Je-li $\mathbb{M} \models (\forall x)(\varphi(x) \to \psi(x))$ a $\mathbb{M} \models (\forall x)\varphi(x)$, je pro všechna $a \in \mathbb{M}$,

$$\mathbb{M}, [x : a] \models (\varphi(x) \to \psi(x)), \quad \mathbb{M}, [x : a] \models \varphi(x)$$

a tedy $\mathbb{M}, [x : a] \models \psi(x)$. Z toho již olyne $\mathbb{M} \models (\forall x)\psi(x)$.

Všimněme si, že obrácená implikace neplatí. Ve struktuře celých čísel platí

$$\mathbb{Z} \models (\forall x)(x < 0) \to (\forall x)(0 < x)$$

protože premisa implikace neplatí. Neplatí však $(\forall x)(x < 0 \to 0 < x)$.

Subtilnější je otázka logické pravdivosti formule

$$(\forall x)\varphi(x) \to (\exists x)\varphi(x)$$

Pokud by totiž $\mathbb{M}$ byla prázdná struktura, která nemá žádné prvky, pak tato formule v $\mathbb{M}$ neplatí. Premisa implikace říká, že φ platí pro jakýkoliv prvek struktury. Nemá-li struktura žádný prvek, není co ověřovat, takže premisa $(\forall x)\varphi(x)$ platí. Neplatí však závěr $(\exists x)\varphi(x)$. Tuto paradoxní situaci vyloučíme tak, že budeme uvažovat jen neprázdné struktury, jako v Definici 6. V neprázdných strukturách tato formule platí, takže podle naší definice je logicky pravdivá

$$\models (\forall x)\varphi(x) \to (\exists x)\varphi(x)$$

Vztah mezi obecnou platností a existencí vyjadřují také následující formule.

Tvrzení 11 *Nechť* t *je term substituovatelný za proměnnou x do formule $\varphi(x)$. Pak následující formule jsou logicky pravdivé*

$$\begin{aligned} &\models \quad (\forall x)\varphi(x) \to \varphi(\mathsf{t}) \\ &\models \quad \varphi(\mathsf{t}) \to (\exists x)\varphi(x) \end{aligned}$$

Důkaz: Připomeňme, že term t je substituovatelný za proměnnou x do formule $\varphi(x)$, jestliže t neobsahuje žádnou proměnnou, která je vázaná v φ. Nechť $\mathsf{x}_1, \ldots, \mathsf{x}_n$ jsou všechny proměnné volné ve formuli $\varphi(\mathsf{t})$, $\mathbb{M}$ struktura a $a_1, \ldots, a_n$ její prvky. Protože t neobsahuje jiné proměnné než $\mathsf{x}_1, \ldots, \mathsf{x}_n$, závisí jeho hodnota jenom na $a_1, \ldots, a_n$. Označme $a = \mathsf{t}[\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n]_{\mathbb{M}}$. Jestliže

$$\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models (\forall x)\varphi(x)$$

pak také pro prvek a platí $\mathbb{M}, [x : a, \mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models \varphi(x)$. Z toho plyne

$$\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models \varphi(\mathsf{t})$$

protože v obou případech se za termy dosazují stejné prvky. Dokázali jsme tedy

$$\mathbb{M}, [\mathsf{x}_1 : a_1, \ldots, \mathsf{x}_n : a_n] \models (\forall x)\varphi(x) \to \varphi(\mathsf{t})$$

takže $(\forall x)\varphi(x) \to \varphi(\mathtt{t})$ je logicky pravdivá formule. Druhá formule z ní plyne s použitím tautologie $(p \to q) \equiv (\neg q \to \neg p)$. Je totiž

$$\neg(\exists x)\varphi(x) \equiv (\forall x)\neg\varphi(x) \to \neg\varphi(\mathtt{t})$$

Další logicky pravdivé formule vznikají, jestliže se kvantifikuje logická spojka, jejíž jedna z formulí neobsahuje kvantifikovanou proměnnou.

Tvrzení 12 *Nechť proměnná x se nevyskytuje ve formuli φ. Pak*

$$\models (\forall x)(\varphi \to \psi(x)) \to (\varphi \to (\forall x)\psi(x))$$

Důkaz: Nechť $\mathtt{x}_1, \ldots, \mathtt{x}_n$ jsou všechny volné proměnné formule $(\forall x)(\varphi \to \psi(x))$. Nechť $\mathbb{M}$ je struktura, $a_1, \ldots, a_n \in \mathbb{M}$ a

$$\mathbb{M}, [\mathtt{x}_1 : a_1, \ldots, \mathtt{x}_n : a_n] \models (\forall x)(\varphi \to \psi(x)) \;\&\; \varphi$$

Pak pro všechna $a \in \mathbb{M}$ platí

$$\mathbb{M}, [x : a, \mathtt{x}_1 : a_1, \ldots, \mathtt{x}_n : a_n] \models \varphi \to \psi(x), \quad \text{a} \quad \mathbb{M}, [x : a, \mathtt{x}_1 : a_1, \ldots, \mathtt{x}_n : a_n] \models \varphi$$

takže

$$\mathbb{M}, [x : a, \mathtt{x}_1 : a_1, \ldots, \mathtt{x}_n : a_n] \models \psi(x)$$
$$\mathbb{M}, [\mathtt{x}_1 : a_1, \ldots, \mathtt{x}_n : a_n] \models (\forall x)\psi(x)$$

Je tedy

$$(\forall x)(\varphi \to \psi(x)) \;\&\; \varphi \to (\forall x)\psi(x))$$

a odtud již plyne tvrzení.

Cvičení. Rozhodněte, zda následující formule jsou logicky pravdivé

1. $(\exists x)(\varphi(x) \to \psi(x)) \to ((\exists x)\varphi(x) \to (\exists x)\psi(x))$
2. $((\exists x)\varphi(x) \to (\exists x)\psi(x)) \to (\exists x)(\varphi(x) \to \psi(x))$
3. $(\exists x)(\varphi(x) \equiv \psi(x)) \to ((\exists x)\varphi(x) \equiv (\exists x)\psi(x))$
4. $((\exists x)\varphi(x) \equiv (\exists x)\psi(x)) \to (\exists x)(\varphi(x) \equiv \psi(x))$
5. $(\forall x)(\varphi(x) \equiv \psi(x)) \to ((\forall x)\varphi(x) \equiv (\forall x)\psi(x))$
6. $((\forall x)\varphi(x) \equiv (\forall x)\psi(x)) \to (\forall x)(\varphi(x) \equiv \psi(x))$
7. $(\forall x)(\varphi(x) \to \psi(x)) \to ((\exists x)\varphi(x) \to (\exists x)\psi(x))$
8. $((\forall x)\varphi(x) \to (\forall x)\psi(x)) \to (\exists x)(\varphi(x) \to \psi(x))$

2.4 Teorie

Studujeme-li nějakou matematickou strukturu, nazajímáme se ani tak o logicky pravdivé formule, jako spíše o to, čím je tato struktura charakteristická, které formule platí v ní a neplatí třeba v jiných strukturách. Protože se ale jedná o strukturu nekonečnou, nelze pravdivost formulí ověřovat přímo. Ověřit zda platí $\mathbb{N} \models x + y = y + x$ znamená vyšetřit nekonečně mnoho možností. O pravdivosti této formule jsme nicméně přesvědčeni. Toto přesvědčení se asi opírá o geometrickou představu: přemisťujeme-li nějaké objekty v prostoru a různě je seskupujeme, jejich počet se nezmění. Další důvod je algoritmický. Algoritmus sčítání přirozených čísel (v desetinné soustavě) zřejmě nezáleží na pořadí sčítanců.

V logice mají takováto zřejmá tvrzení povahu axiomů. Předpokládáme, že platí, a snažíme se zjistit, jaké mají všechny důsledky. Soubor takovýchto axiomů nazýváme teorií. Za axiomy teorie přirozených čísel se většinou přijímají algebraické identity jako komutativní a asociativní zákon pro sčítání a násobení a zákon distributivní. Další důležitý axiom je **Princip matematické indukce**. Platí-li nějaké tvrzení pro nulu, a jestliže z jeho platnosti pro x plyne také platnost pro $x + 1$, pak toto tvrzení platí pro všechna přirozená čísla. Takové tvrzení může být libovolná formule $\varphi(x)$ a princip indukce pro $\varphi(x)$ vyjadřuje formule

$$\varphi(0) \mathbin{\&} (\forall x)(\varphi(x) \to \varphi(x+1)) \to (\forall x)\varphi(x)$$

V teorii přirozených čísel se za axiom přijímá každá formule tohoto tvaru, říkáme, že to je **schema axiomů**. Teorie tedy může mít i nekonečně mnoho axiomů, podstatné však je, že lze algoritmicky rozhodnout, která formule je axiom a která ne.

Z axiomů teorie a z logicky pravdivých formulí odvozujeme další formule pomocí dedukčních pravidel. Platí-li například v nějaké struktuře $\mathbb{M} \models \varphi$ a $\mathbb{M} \models \varphi \to \psi$, platí také $\mathbb{M} \models \psi$. Toto dedukční pravidlo se nazývá **pravidlo modus ponens**. **Pravidlo generalizace** říká, že platí-li v nějaké struktuře $\mathbb{M} \models \varphi(x)$, platí v ní také $\mathbb{M} \models (\forall x)\varphi(x)$. Dedukční pravidla modus ponens a generalizace zapisujeme graficky

$$\frac{\varphi,\ \varphi \to \psi}{\psi} \qquad\qquad \frac{\varphi(x)}{(\forall x)\varphi(x)}$$

Některá dedukční pravidla jsou založena na tautologiích. Například pravidlo modus ponens je založeno na tautologii $\varphi \mathbin{\&} (\varphi \to \psi) \to \psi$. Dedukční pravidlo generalizace však na tautologii založeno není, protože $\varphi(x) \to (\forall x)\varphi(x)$ ani není formule. Proměnná x by v ní byla jak volná tak vázaná. Přejmenujeme-li proměnnou x, dostáváme formuli $\varphi(x) \to (\forall y)\varphi(y)$, a ta není ani tautologie ani není logicky platná. Například formule $x < 0 \to (\forall y)(y < 0)$ neplatí ve struktuře $\mathbb{Z}$ pro $x = -1$.

Další dedukční pravidla jsou

$$\frac{\varphi,\ \psi}{\varphi \mathbin{\&} \psi} \qquad\qquad \frac{\varphi \to \chi,\ \psi \to \chi}{\varphi \vee \psi \to \chi}$$

Tím, že vymezíme nějakou teorii (jako soubor axiomů), nevymezíme zpravidla jedinou strukturu. Za axiomy sice přijímáme formule, o kterých předpokládáme, že platí ve struktuktuře, kterou studujeme, mohou však platit i v dalších strukturách. Studujeme-li teorii, studujeme tedy současně všechny struktury, ve kterých platí axiomy této teorie. Takové struktury nazýváme modely teorie.

Definice 13

1. *Teorie je soubor axiomů.*
2. *Struktura $\mathbb{M}$ je model teorie T, jestliže každá formule ψ teorie T platí v $\mathbb{M}$, tj. $\mathbb{M} \models \psi$.*
3. *Říkáme, že formule φ logicky vyplývá z teorie T a píšeme $T \models \varphi$, jestliže v každém modelu $\mathbb{M}$ teorie T platí $\mathbb{M} \models \varphi$.*

$$T \models \varphi \text{ jestliže } \mathbb{M} \models \varphi \text{ pro každý model } \mathbb{M} \text{ teorie } T$$

Pokud chceme vymezit formálně také pojem důkazu, přijmeme za axiomy některé logicky pravdivé formule a stanovíme některá dedukční pravidla. V důkazech pak používáme pouze tyto stanovené axiomy a dedukční pravidla. Uvedeme si jeden takový axiomatický systém, který pracuje pouze s logickými spojkami negace a implikace (ostatní logické spojky se v tomto systému chápou jako zkratky).

Definice 14 *Logický axiom je každá formule následujícího tvaru*
1. $\varphi \to (\psi \to \varphi)$
2. $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$
3. $(\neg\psi \to \neg\varphi) \to ((\neg\psi \to \varphi) \to \psi)$
4. $(\forall x)\varphi(x) \to \varphi(\mathtt{t})$, *pokud* $\mathtt{t}$ *je substituovatelný za* x.
5. $(\forall x)(\varphi \to \psi(x)) \to (\varphi \to (\forall x)\psi(x))$ *kde* x *není volná ve formuli* φ.

2.5 Teorie rovnosti

Predikát rovnosti $=$ má vyjímečné postavení, pokud ho v každé struktuře interpretujeme jako identitu. Vlastnostmi identity se zabývá teorie rovnosti. Její axiomy jsou reflexivita, symetrie a tranzitivita. Rovnost je také kongruencí vzhledem k aritmetickým operacím. To znamená, že rovnají-li se argumenty aritmetické operace, rovná se i její výsledek. Také predikáty nezmění svou pravdivostní hodnotu při záměně stejnými prvky. Pro algebraický jazyk $\mathcal{L} = \{0, 1, +, *, <, =\}$ sestává teorie rovnosti z následujících axiomů

Definice 15 *Axiomy rovnosti jsou následující formule.*

$(x = x)$	*reflexivita*
$(x = y) \to (y = x)$	*symetrie*
$(x = y)\ \&\ (y = z) \to (x = z)$	*tranzitivita*
$(x = y) \to (x + z = y + z)\ \&\ (z + x = z + y)$	*kongruence pro sčítání*
$(x = y) \to (x * z = y * z)\ \&\ (z * x = z * y$	*kongruence pro násobení*
$(x = y)\ \&\ (x < z) \to (y < z)$	*kongruence pro nerovnost*
$(x = y)\ \&\ (z < x) \to (z < y)$	

V teorii rovnosti můžeme například odvodit

$$(x = y) \to (x + z) = (y + z) \to (x + z) * v = (y + z) * v$$

a podobné identity. Obecně, je-li $\mathtt{t}(x)$ term s proměnnou x a $\mathtt{t}(y)$ term který získáme z $\mathtt{t}(x)$ nahrazením x za y, pak lze v teorii rovnosti odvodit

$$(x = y) \to (\mathtt{t}(x) = \mathtt{t}(y))$$

Podobně je-li $\varphi(x)$ formule, lze odvodit

$$(x = y) \,\&\, \varphi(x) \to \varphi(y)$$

Například

$$(x = y) \,\&\, (\exists z > x) \to (\exists z > y)$$

2.6 Další kvantifikátory

Pro přehlednější a kratší zápis matematických tvrzení se predikátový počet rozvíjí ještě o další typy kvantifikátorů. Jsou to zejména omezené kvantifikátory a kvantifikátor jednoznačné existence. Omezený kvantifikátor se nevztahuje na všechny možné hodnoty, ale omezuje je nějakou podmínkou.

Je-li $\varphi(x)$ formule a y proměnná, která není vázaná v $\varphi(x)$, píšeme

$$\begin{aligned} (\forall x < y)\varphi(x) &\equiv (\forall x)((x < y) \to \varphi(x)) \\ (\exists x < y)\varphi(x) &\equiv (\exists x)((x < y) \,\&\, \varphi(x)) \end{aligned}$$

Toto rozšíření syntaxe predikátového počtu můžeme chápat dvěma způsoby. Buďto jsou omezené kvantifikátory pouhé zkratky. Formule, ve kterých se vyskytují, jsou pouze zkrácené zápisy skutečných formulí utvořených podle Definice 3. Druhá možnost je rozšířit syntaktickou definici formulí také o tyto konstrukty. Uvedené ekvivalence, které je vymezují, se pak stanou logicky pravdivými formulemi. Všimněmě si, že také pro omezené kvantifikátory platí de Morganova pravidla

$$\begin{aligned} \neg(\forall x < y)\varphi(x) &\equiv \neg(\forall x)((x < y) \to \varphi(x)) \equiv (\exists x)((x < y) \,\&\, \neg\varphi(x)) \\ &\equiv (\exists x < y)\neg\varphi(x) \end{aligned}$$

Obecně však neplatí formule $(\forall x < y)\varphi(x) \to (\exists x < y)\varphi(x)$ Například v algebraických strukturách neplatí formule

$$(\forall x < 0)(x > 0) \to (\exists x < 0)(x > 0)$$

Další nový kvantifikátor je jednoznačná existence. Formule

$$\varphi(y) \,\&\, \varphi(z) \to y = z$$

vyjadřuje, že neexistují dva různé objekty, které splňují formuli φ. To znamená, že objekt, pro který platí φ, buď vůbec neexistuje nebo existuje právě jeden. Kvantifikátor jednoznačné existence $\exists!$ vyjadřuje, že takový objekt existuje právě jeden. Je tedy

$$(\exists! x)\varphi(x) \equiv (\exists x)\varphi(x) \ \&\ (\forall y)(\forall z)(\varphi(y) \ \&\ \varphi(z) \rightarrow y = z)$$

Například ve struktuře $\mathbb{Z}_3$ (a v každé struktuře $\mathbb{Z}_n$) platí

$$\mathbb{Z}_3 \models (\forall x)(\exists! y)(x + y = 0)$$

To znamená, že každý prvek má právě jeden prvek opačný.

2.7 Definice

Studujeme-li nějakou matematickou strukturu, nevystačíme pouze s těmi predikáty a operacemi, které jsme zavedli na počátku. Nové predikáty a operace se zavádějí pomocí definic, což jsou axiomy speciálního typu. Ve struktuře $\mathbb{N}$ například zavádíme pojem "býti prvočíslem". To je jednočetný predikát. Zvolíme si pro něj nějaký nový znak, například P a přidáme axiom

$$P(x) \equiv (\forall y)(\forall z)(x = y * z \rightarrow (y = 1 \vee z = 1))$$

Dvoučetný predikát $D(x, y)$ vyjadřující, že y je dělitelné x definujeme axiomem

$$D(x, y) \equiv (\exists z)(x * z = y)$$

Takovéto nové predikáty lze definovat libovolnou formulí. Je-li $\varphi(\mathsf{x}_1, \ldots, \mathsf{x}_n)$ formule s n volnými proměnnými, definujeme nový n-četný predikát $\mathcal{P}$ axiomem

$$\mathcal{P}(\mathsf{x}_1, \ldots, \mathsf{x}_n) \equiv \varphi(\mathsf{x}_1, \ldots, \mathsf{x}_n)$$

Zavedení nových operaceí je složitější. Lze je zavést pokud jsou všude definovány a jsou jednoznačné. Například ve struktuře $\mathbb{Z}_3$ (a v každé struktuře $\mathbb{Z}_n$) platí formule

$$\mathbb{Z}_3 \models (\forall x)(\forall y)(\exists! z)(x + z = y)$$

Můžeme tedy zavést novou operaci – odčítání axiomem

$$(\forall x)(\forall y)(x + (y - x) = y)$$

Nově definovaná operace je pak splňuje axiomy rovnosti, tj. platí

$$(x = y) \rightarrow (x - z = y - z), \ \ (x = y) \rightarrow (z - x = z - y)$$

Je totiž

$$\begin{aligned} (x = y) \quad &\rightarrow \quad z + (x - z) = x = y = z + (y - z) \rightarrow (x - z = y - z) \\ (x = y) \quad &\rightarrow \quad x + (z - x) = z = y + (z - y) = x + (z - y) \rightarrow (z - x = z - y) \end{aligned}$$

Obecně, je-li $\varphi(x, y, z)$ formule s třemi volnými proměnnými a jestliže platí

$$(\forall x)(\forall y)(\exists! z)\varphi(x, y, z)$$

lze zavést novou binární operaci F definicí

$$(\forall x)(\forall y)\varphi(x, y, F(x, y))$$

Obdobně lze zavést nové jednočetné operace a také nové konstanty. Je-li $\varphi(x)$ formule s jednou volnou proměnnou a jestliže platí $(\exists! x)\varphi(x)$, lze zavést novou konstantu C definicí $\varphi(C)$ a platí $(\forall x)(\varphi(x) \rightarrow x = C)$.

3 Teorie množin

Teorie množin zaujímá v současné matematice významné postavení tím, že jí poskytuje logické základy. Každou matematickou oblast lze vnořit do teorie množin tak, že se každý matematický objekt reprezentuje nějakou množinou. Při studiu matematických objektů není totiž důležité, čím tyto objekty jsou, jak jsou utvořeny, ale jen jaké mají vlastnosti a jaké jsou jejich vzájemné vztahy. Proto stačí, že teorie množin dokáže nabídnout dostatečné množství množin pro konstrukci matematických objektů a má dostatečně bohatou strukturu vztahů. Zdá se, že predikát náležení $\in$ je nejjednodušší matematický vztah, a proto jím lze všechny ostatní matematické vztahy modelovat.

3.1 Univerzum množin

Množinu chápeme jako konečný či nekonečný soubor prvků. Svými prvky je množina jednoznačně určena. Množinu, která má prvky $x_1, \ldots, x_n$, značíme $\{x_1, \ldots, x_n\}$. Speciálně $\{x\}$ je množina, která obsahuje jediný prvek x a $\{\}$ je prázdná množina, která neobsahuje žádný prvek. Tu si označíme symbolem $\emptyset = \{\}$. Další množiny postupně vytváříme z prázdné množiny $\emptyset$. První množina, kterou můžeme utvořit, je množina $\{\emptyset\}$, která obsahuje právě jen prázdnou množinu. Je důležité si uvědomit, že $\emptyset \neq \{\emptyset\}$. Prázdná množina neobsahuje žádný prvek, množina $\{\emptyset\}$ obsahuje jediný prvek a sice právě prázdnou množinu. Nyní již máme tedy dvě množiny $\emptyset$ a $\{\emptyset\}$ a z nich můžeme utvořit novou množinu $\{\{\emptyset\}\}$, která má jediný prvek $\{\emptyset\}$ a množinu $\{\{\emptyset\}, \emptyset\}$, která má dva prvky. Takto vytváříme množiny postupně po úrovních. Na urovni 0 je prázdná množina. Na každé další úrovni se vytvoří všechny množiny z prvků, které byly vytvořeny na úrovních předcházejících.

0:	$\emptyset$	
1:	$\{\emptyset\}$	
2:	$\{\{\emptyset\}\}, \quad \{\emptyset, \{\emptyset\}\}$	
3:	$\{\{\{\emptyset\}\}\}, \quad \{\{\emptyset, \{\emptyset\}\}\}$	jednoprvkové množiny
	$\{\emptyset, \{\{\emptyset\}\}\}, \quad \{\emptyset, \{\emptyset, \{\emptyset\}\}\}, \quad \{\{\emptyset\}, \{\{\emptyset\}\}\},$	
	$\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \{\{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$	dvouprvkové množiny
	$\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},$	
	$\{\emptyset, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}, \quad \{\{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$	tříprvkové množiny
	$\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$	čtyřprvková množina

Z n prvků lze vytvořit celkem 2^n množin. Pro každý z těchto prvků totiž máme dvě možnosti. Buď ho do uvažované množiny dáme nebo ne a každá volba těchto možností určuje jinou množinu. Například ze tří prvků a, b, c lze vytvořit množiny

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$$

Označíme-li a_n počet množin vytvořených celkově na úrovních 0 až n, je $a_0 = 1$, $a_1 = 2$, $a_2 = 4$, $a_3 = 2^4 = 16$ a $a_{n+1} = 2^{a_n}$. Takto můžeme pokračovat pro všechny úrovně číslované přirozenými čísly. Počet množin přitom velmi rychle roste.

Všechny takto utvořené množiny jsou konečné, mají konečný počet prvků. V mnoha oblastech matematiky s konečnými množinami vystačíme a omezíme se pouze na teorii konečných množin. V jiných oblastech však pracujeme i s nekonečnými množinami jako je množina přirozených čísel nebo množina reálných čísel. Představíme-li si, že máme vytvořeny množiny na všech konečných úrovních, můžeme z nich vytvářet nekonečné množiny, například množinu

$$\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \{\{\{\{\emptyset\}\}\}\} \ldots\}$$

Tato množina se objevuje teprve na nekonečné úrovni. Z ní a z jiných konečných či nekonečných množin lze sestavovat další množiny, a tak lze pokračovat dál k vyšším a vyšším nekonečným úrovním. Tyto úrovně odpovídají tzv. ordinálním číslům, která zobecňují čísla přirozená. Všechny takto vytvořené množiny tvoří soubor, které nazýváme univerzum množin. Univerzum množin tvoří strukturu pro predikát náležení $\in$. Za axiomy teorie množin budeme přijímat formule, o kterých věříme, že v tomto univerzu množin platí. Celé toto univerzum však již za množinu považovat nemůžeme, dostali bychom se do logického sporu.

3.2 Axiomy specifikace

Univerzum množin popsané v minulém odstavci, spolu s množinovými operacemi jako je průnik, sjednocení, budeme nyní popisovat formulemi v predikátového počtu. Základní jazyk $\mathcal{L} = \{\in\}$ sestává z jediného binárního predikátu $\in$ náležení. Jako proměnné budeme používat malá i velká písmena latinské abecedy. Formule $x \in y$ znamená že (množina) x náleží, či je prvkem množiny y. Její negaci zapisujeme $x \notin y \equiv \neg(x \in y)$. Jazyk teorie množin budeme postupně rozšiřovat o další predikáty, operace a konstanty. Nejprve zavedeme dvoučetné predikáty rovnosti $=$ a inkluze $\subseteq$, $\subset$. Množina je určena svými prvky, dvě množiny se tedy rovnají, mají-li stejné prvky.

Definice 16

$$\begin{aligned} x = y &\equiv (\forall u)(u \in x \equiv u \in y) \\ x \subseteq y &\equiv (\forall u)(u \in x \rightarrow u \in y) \\ x \subset y &\equiv x \subseteq y \,\&\, x \neq y \end{aligned}$$

Nerovnost $x \neq y$ zde znamená $\neg(x = y)$. Vlastnosti rovnosti jako reflexita, symetrie a transitivita plynou již přímo z této definice, není třeba je přijímat jako nové axiomy rovnosti. Inkluze má vlastnosti částečného uspořádání, tj. reflexivitu, tranzitivitu a antisymetrii

Tvrzení 17

1. $x = x$	*reflexivita*
2. $(x = y) \rightarrow (y = x)$	*symetrie*
3. $(x = y) \,\&\, (y = z) \rightarrow (x = z)$	*tranzitivita*
4. $x \subseteq x$	*reflexivita*
5. $(x = y) \equiv (x \subseteq y) \,\&\, (y \subseteq x)$	*antisymetrie*
6. $(x \subseteq y) \,\&\, (y \subseteq z) \rightarrow (x \subseteq z)$	*tranzitivita*

Důkaz: Z definice rovnosti dostáváme dosazením y za x

$$(x = x) \equiv (\forall u)(u \in x \equiv u \in x)$$

Na pravé straně je uzávěr tautologie, tedy logicky pravdivá formule, takže $x = x$. Symetrie rovnosti plyne z tautologie $(u \in x \equiv u \in y) \equiv (u \in y \equiv u \in x)$ a podobně pro tranzitivitu.

Z definice rovnosti plyne formule

$$x = y \rightarrow (u \in x \equiv u \in y)$$

která vyjadřuje, že rovnost se vzhledem k druhému argumentu predikátu náležení chová jako kongruence. Podobnou vlastnost pro proměnnou u ve formuli $(u \in x)$ však nemáme a přijmeme ji jako první axiom

Axiom 1 (Axiom rovnosti) $(u = v) \rightarrow (u \in x \equiv v \in x)$

Existenci prázdné množiny zaručíme axiomem

Axiom 2 (Axiom prázdné množiny) $(\exists z)(\forall u)(u \notin z)$

Pomocí definice rovnosti ukážeme, že prázdná množina existuje jediná.

Tvrzení 18 $(\exists! z)(\forall u)(u \notin z)$

Důkaz: Je třeba ukázat, že každé dvě množiny, které nemají žádný prvek, jsou si rovny, tj.

$$(\forall u)(u \notin z) \mathbin{\&} (\forall u)(u \notin w) \rightarrow (z = w)$$

To plyne z Definice 16 a logicky pravdivé formule

$$\begin{aligned}(\forall u)(u \notin z) \mathbin{\&} (\forall u)(u \notin w) &\equiv (\forall u)(u \notin z \mathbin{\&} u \notin w)\\ &\rightarrow (\forall u)(u \in z \equiv u \in w)\end{aligned}$$

Protože existuje právě jedna množina, která nemá žádné prvky, můžeme ji označit novou konstantou $\emptyset$.

Definice 19 (Prázdná množina) $(\forall u)(u \notin \emptyset)$

Dalším axiomem zaručíme existenci množiny utvořené z jediného prvku.

Axiom 3 (Axiom jednotice)

$$(\forall x)(\exists z)(\forall u)(u \in z \equiv u = x)$$

Opět snadno dokážeme, že taková množina existuje jediná, tj.

$$(\forall x)(\exists! z)(\forall u)(u \in z \equiv u = x)$$

takže definujeme jednočetnou operaci

Definice 20 (Jednotice)

$$(\forall x)(\forall u)(u \in \{x\} \equiv u = x)$$

Podobně bychom mohli zaručit existenci dvojice a trojice, to však lze zaručit najednou pomocí axiomu sjednocení dvou množin

Axiom 4 (Axiom sjednocení)

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

Taková množina existuje jediná:

$$(\forall x)(\forall y)(\exists! z)(\forall u)(u \in z \equiv u \in x \vee u \in y)$$

a nazýváme ji sjednocení $z = x \cup y$. To je další definice

Definice 21 (Sjednocení)

$$(\forall x)(\forall y)(\forall u)(u \in x \cup y \equiv u \in x \vee u \in y)$$

Složením těchto operací nyní definujeme operaci dvojice $\{x,y\} = \{x\} \cup \{y\}$. Je ovšem $\{x,x\} = \{x\}$. Podobně definujeme trojici $\{x,y,z\} = \{x,y\} \cup \{z\}$ a obecně n-tici.

Axiomy prázdné množiny, jednotice a sjednocení zaručují existenci všech konečných množin vytvořených z prázdné množiny. Existenci nekonečných množin zatím zaručenu nemáme, ale také jsme jejich existenci nevyloučili.

Mohlo by se zdát, že přinejmenším pro práci s konečnými množinami již máme dostatečně silné prostředky. Avšak již tak jednoduchou a potřebnou operaci jako je průnik dvou množin z těchto axiomů neodvodíme, přestože uvnitř univerza konečných množin průnik každých dvou množin existuje. Potíž je s případnými nekonečnými množinami, pro které průnik existovat nemusí.

Operaci průniku lze jistě zavést dalším axiomem a tak pokračovat pro další množinové operace. Nabízí se ale obecnější postup. Množiny často vytváříme tak, že seskupíme všechny objekty, které mají určitou vlastnost, tj. splňují určitou formuli. Je-li $\varphi(u)$ formule s volnou proměnnou u (a případně s dalšími volnými proměnnými), chceme sestrojit množinu, do které patří všechny objekty (množiny) u, pro které $\varphi(u)$ platí. To je axiom

$$(\exists z)(\forall u)(u \in z \equiv \varphi(u))$$

Všimněme si, že axiomy prázdné množiny, jednotice a sjednocení jsou jeho speciální případy pro formule

$\varphi(u) \equiv u \neq u \equiv \mathbf{false}$	prázdná množina
$\varphi(u) \equiv u = x$	jednotice
$\varphi(u) \equiv (u \in x) \vee (u \in y)$	sjednocení

Ve své plné obecnosti je však tento axiom sporný. Existovala by podle něj také množina všech množin a ta by musela obsahovat sama sebe. To je v rozporu s naším intuitivním pojetím množin, logicky sporné to však ještě být nemusí. Do sporu se však dostaneme, chceme-li utvořit množinu těch množin, které neobsahují samu sebe, tj. použijeme-li ho na formuli $\varphi(u) \equiv u \notin u$. Kdyby existovala množina z, obsahující všechny prvky s vlastností φ, tj.

$$(\forall u)(u \in z \equiv u \notin u)$$

pak dosazením z za u dostáváme spor $z \in z \equiv z \notin z$. Všimněme si, že tento Russellův paradox teorie množin je založen na Epimenidově paradoxu lháře. Východisko z tohoto paradoxu spočívá v oslabení axiomu specifikace. Máme-li již utvořenou nějakou množinu x, vydělíme z ní ty prvky, které splňují formuli φ a z nich sestavíme novou množinu.

Axiom 5 (Schema axiomů specifikace)

$$(\exists z)(\forall u)(u \in z \equiv u \in x \,\&\, \varphi(u))$$

kde $\varphi(u)$ je libovolná formule, která neobsahuje proměnnou z.

Množina z je axiomem specifikace určena jednoznačně. Platí

$$(\forall u)(u \in z \equiv u \in x \ \&\ \varphi(u)) \ \&\ (\forall u)(u \in w \equiv u \in x \ \&\ \varphi(u)) \to z = w$$

takže

$$(\exists! z)(\forall u)(u \in z \equiv u \in x \ \&\ \varphi(u))$$

Každá formule $\varphi(u)$ tedy určuje množinovou operaci, jejíž četnost je počet volných proměnných formule φ. Tuto množinovou operaci značíme $\{u \in x :\ \varphi(u)\}$,

Definice 22

$$u \in \{u \in x :\ \varphi(u)\} \equiv u \in x \ \&\ \varphi(u)$$

Formule $\varphi(u) \equiv u \in y$ a $\varphi(u) \equiv u \notin y$ tak určují množinový průnik a rozdíl

Definice 23

$$\begin{aligned} x \cap y &= \{u \in x :\ u \in y\} \\ x \setminus y &= \{u \in x :\ u \notin y\} \end{aligned}$$

Operace průniku a sjednocení splňují podobné vlastnosti jako konjunkce a disjunkce ve výrokovém počtu. Množinový rozdíl $\setminus$ je analogií logické spojky $\varphi \ \&\ \neg\psi$. Snadno ověříme identity

$$\begin{aligned} x \cap y &= y \cap x \\ x \cap (y \cup z) &= (x \cap y) \cup (x \cap z) \\ x \setminus (y \cap z) &= (x \setminus y) \cup (x \setminus z) \end{aligned}$$

Důkazy takovýchto identit se převádí na odpovídající tautologie predikátového počtu. Například

$$\begin{aligned} u \in (x \setminus (y \cap z)) &\equiv u \in x \ \&\ u \notin (y \cap z) \equiv (u \in x) \ \&\ (u \notin y \vee u \notin z) \\ &\equiv (u \in x \vee u \notin y) \ \&\ (u \in x \vee u \notin z) \\ &\equiv u \in (x \setminus y) \cup (x \setminus z) \end{aligned}$$

Omezení axiomu specifikace zamezuje sice sporu, některé potřebné množinové operace nám ale nezaručí. Zejména se jedná o potenční množinu a obecné sjednocení. Potenční množina $\mathcal{P}(x)$ množiny x sestává z množiny všech jejích podmnožin, například $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Obecné sjednocení $\mathcal{U}(x)$ množiny x je sjednocení všech jejích prvků, například $\mathcal{U}(\{a, b\}) = a \cup b$. V obou těchto případech nemáme k dispozici množinu, ze které bychom mohli prvky $\mathcal{P}(x)$ nebo $\mathcal{U}(x)$ vybírat. Potřebujeme tedy ještě dva případy (neomezeného) axiomu vydělení pro formule $\varphi(u) \equiv u \subseteq x$ a $\varphi(u) \equiv (\exists v)(u \in v \in x)$.

Axiom 6 (Axiom potenční množiny)

$$(\forall x)(\exists z)(\forall u)(u \in z \equiv u \subseteq x)$$

Definice 24

$$(\forall x)(\forall u)(u \in \mathcal{P}(x) \equiv u \subseteq x)$$

Platí $\mathcal{P}(\emptyset) = \{\emptyset\}$ a $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. Aplikujeme-li operaci potence na prázdnou množinu n-krát, dostaneme všechny konečné množiny úrovně menší než n. Je-li x množina utvořená na úrovni n, je $\mathcal{P}(x)$ množina utvořená na úrovni $n+1$.

Axiom 7 (Axiom obecného sjednocení)

$$(\forall x)(\exists z)(\forall u)(u \in z \equiv (\exists v)(u \in v \in x))$$

Definice 25

$$(\forall x)(\forall u)(u \in \mathcal{U}(x) \equiv (\exists v)(u \in v \in x))$$

Je $\mathcal{U}(\emptyset) = \emptyset$ ale také $\mathcal{U}(\{\emptyset\}) = \emptyset$ a obecněji $\mathcal{U}(\{x\}) = x$, neboť

$$u \in \mathcal{U}(\{x\}) \equiv (\exists v)(u \in v \in \{x\}) \equiv (\exists v)(u \in v = x) \equiv u \in x$$

Sjednocení konečné množiny x lze ekvivalentně vyjádřit operací $\cup$ tak že postupně sjednotíme všechny prvky množiny x. Je-li x množina utvořená na úrovni $n+1$, je $\mathcal{U}(x)$ množina utvořená na úrovni n. Operace potence a obecného sjednocení jsou do jisté míry k sobě inverzní. Je totiž

Tvrzení 26 $\mathcal{U}(\mathcal{P}(x)) = x \subseteq \mathcal{P}(\mathcal{U}(x))$.

Důkaz plyne přímo z definice těchto dvou operací:

$$\begin{array}{rcl}
u \in \mathcal{U}(\mathcal{P}(x)) & \rightarrow & (\exists v)(u \in v \in \mathcal{P}(x)) \rightarrow (\exists v)(u \in v \subseteq x) \\
& \rightarrow & u \in x \\
u \in x & \rightarrow & u \in \{u\} \subseteq x \rightarrow u \in \{u\} \in \mathcal{P}(x) \\
& \rightarrow & u \in \mathcal{U}(\mathcal{P}(x)) \\
u \in x & \rightarrow & (\forall v)(v \in u \rightarrow v \in \mathcal{U}(x)) \rightarrow u \subseteq \mathcal{U}(x) \\
& \rightarrow & u \in \mathcal{P}(\mathcal{U}(x))
\end{array}$$

Obrácená inkluze $\mathcal{P}(\mathcal{U}(x)) \subseteq x$ neplatí. Například pro $x = \{\{a\}\}$ je

$$\mathcal{P}(\mathcal{U}(\{\{a\}\})) = \mathcal{P}(\{a\}) = \{\emptyset, \{a\}\} \neq \{\{a\}\}$$

Další vztahy dostáváme pro průnik a sjednocení

Tvrzení 27

$$\begin{array}{rcl}
\mathcal{U}(x \cup y) & = & \mathcal{U}(x) \cup \mathcal{U}(y) \\
\mathcal{U}(x \cap y) & \subseteq & \mathcal{U}(x) \cap \mathcal{U}(y) \\
\mathcal{P}(x \cup y) & \supseteq & \mathcal{P}(x) \cup \mathcal{P}(y) \\
\mathcal{P}(x \cap y) & = & \mathcal{P}(x) \cap \mathcal{P}(y)
\end{array}$$

Analogicky jako obecné sjednocení uvažujeme obecný průnik množiny jako průnik všech jejích prvků. Obecný průnik množiny je částí jejího obecného sjednocení, existence obecného průniku tedy plyne z axiomu specifikace.

Definice 28

$$\mathcal{I}(x) = \{u \in \mathcal{U}(x) : (\forall v \in x)(u \in v)\}$$

Zřejmě $\mathcal{I}(\emptyset) = \emptyset$ a také $\mathcal{I}(\mathcal{P}(x)) = \emptyset$, neboť $\mathcal{I}(\emptyset) \subseteq \mathcal{U}(\emptyset) = \emptyset$ a $\mathcal{P}(x)$ obsahuje prázdnou množinu. Neplatí však tvrzení $u \in \mathcal{I}(x) \equiv (\forall v \in x)(u \in v)$, speciálně neplatí pro $x = \emptyset$, neboť v tomto případě je formule na pravé straně splněna pro všechna u. Platí však

$$u \in \mathcal{I}(x) \equiv (\forall v \in x)(u \in v) \ \& \ x \neq \emptyset$$

Cvičení. Nejděte příklady množin pro které platí

1. $\mathcal{U}(x) \subseteq x$
2. $\mathcal{U}(x) \not\subseteq x$
3. $x \subseteq \mathcal{P}(x)$
4. $x \not\subseteq \mathcal{P}(x)$

Určete zda platí
5. $\mathcal{U}(x) \subseteq y \rightarrow x \subseteq \mathcal{P}(y)$
6. $x \subseteq \mathcal{P}(x) \rightarrow \mathcal{U}(x) \subseteq x$
7. $x \subseteq \mathcal{U}(y) \rightarrow \mathcal{P}(x) \subseteq y$
8. $\mathcal{P}(x) \subseteq y \rightarrow x \subseteq \mathcal{U}(y)$
9. $\mathcal{P}(x \setminus y) = \mathcal{P}(x) \setminus \mathcal{P}(y)$
10. $\mathcal{U}(\mathcal{I}(x)) = \mathcal{I}(\mathcal{U}(x))$
11. $\mathcal{P}(\mathcal{I}(x)) = \mathcal{I}(\mathcal{P}(x))$

3.3 Axiom regularity

Dosud přijaté axiomy nevylučují možnost, aby nějaká množina byla svým vlastním prvkem. Anomálie tohoto druhu vyloučíme obecnějším axiomem.

Axiom 8 (Axiom regularity)

$$(\forall x \neq \emptyset)(\exists y \in x)(x \cap y = \emptyset)$$

Je-li x neprázdná množina univerza množin konstruovaném z prázdné množiny, zvolíme za y takovou množinu z x, která má nejnižší úroveň (kteroukoliv množinu nejnižší úrovně). Prvky množiny y pak mají úroveň nižší než y, takže nenáleží do x.

Tvrzení 29 $u \notin u$

Důkaz: Předpokládejme sporem, že pro nějaké u platí $u \in u$. Utvořme množinu $x = \{u\}$. Protože $u \in x$, x je neprázdná a podle axiomu regularity existuje $y \in x$ pro které $y \cap x = \emptyset$. Z toho ale plyne $y = u$ a $u \in y \cap x$, takže $y \cap x$ není neprázdná a to je spor. □

Axiom regularity je obecnější než právě dokázané tvrzení. Znemožňuje také konečné (i nekonečné) cykly v relaci náležení. Například

Tvrzení 30 $\neg(u \in v \;\&\; v \in u)$

Důkaz: Předpokládejme sporem $u \in v \in u$ a utvořme množinu $x = \{u, v\}$. Tato množina je neprázdná tedy existuje $y \in x$ pro které $x \cap y = \emptyset$. Je-li $y = u$, je $v \in x \cap y$. Je-li $y = v$, je $u \in x \cap y$. V každém případě je tedy množina $x \cap y$ neprázdná a to je spor. □

3.4 Kartézský součin a relace

Důležitá množinová operace je kartézský součin dvou množin, který je tvořen uspořádanými dvojicemi prvků daných množin. Dvojice $\{u, v\}$ je neuspořádaná. Platí $\{u, v\} = \{v, u\}$, nezáleží zde na pořadí. Za uspořádanou dvojice prvků zvolíme takovou množinovou operaci, kde na pořadí vždy záleží. Nejjednodušeji ji definujeme předpisem

Definice 31 (Uspořádaná dvojice) $\langle u, v\rangle = \{\{u\}, \{u, v\}\}$

Tvrzení 32 $\langle u, v\rangle = \langle x, y\rangle \rightarrow u = x \;\&\; v = y$.

Důkaz: Rozeznáváme dva případy.
1. Je-li $u = v$, je $\langle u, v\rangle = \{\{u\}, \{u, u\}\} = \{\{u\}\}$. Protože

$$\{x, y\} \in \langle x, y\rangle = \langle u, v\rangle = \{\{u\}\},$$

je $\{x, y\} = \{u\}$, takže $x = y = u = v$.
2. Je-li $u \neq v$, je $\{x\} \neq \{u, v\}$. Protože $\{x\} \in \langle x, y\rangle = \{\{u\}, \{u, v\}\}$, je $\{x\} = \{u\}$ a tedy $x = u$. Protože $\{u, v\} \in \langle u, v\rangle = \{\{x\}, \{x, y\}\}$, je $\{u, v\} = \{x, y\}$, a tedy $y = v$. □

Pomocí uspořádané dvojice lze také definovat uspořádané trojice atd.

$$\langle u, v, w\rangle = \langle u, \langle v, w\rangle\rangle,\ \langle u_1, \ldots, u_n\rangle = \langle u_1, \langle u_2, \ldots, u_{n-1}\rangle\rangle$$

Kartézský součin $X \times Y$ množin X a Y je sestaven ze všech uspořádaných dvojic $\langle u, v\rangle$, kde $u \in X$ a $v \in Y$. Abychom mohli kartézský součin definovat pomocí axiomu specifikace, potřebujeme sestrojit množinu, do které všechny tyto dvojice patří. Je

$$\begin{aligned} u \in X \;\&\; v \in Y &\rightarrow \{u\}, \{u, v\} \subseteq X \cup Y \rightarrow \{u\}, \{u, v\} \in \mathcal{P}(Y \cup X) \\ &\rightarrow \langle u, v\rangle \subseteq \mathcal{P}(X \cup Y) \rightarrow \langle u, v\rangle \in \mathcal{P}(\mathcal{P}(X \cup Y)) \end{aligned}$$

Existenci množiny $\mathcal{P}(\mathcal{P}(X \cup Y))$ již máme zajištěnu, takže můžeme definovat

Definice 33 (Kartézský součin)

$$X \times Y = \{w \in \mathcal{P}(\mathcal{P}(X \cup Y)) : (\exists u \in X)(\exists v \in Y)(w = \langle u, v\rangle)\}$$

Použili jsme tedy axiom specifikace s formulí

$$\varphi(w) \equiv (\exists u \in X)(\exists v \in Y)(w = \langle u, v\rangle).$$

Definici kartézského součinu zapíšeme stručněji

$$X \times Y = \{\langle u, v\rangle \in \mathcal{P}(\mathcal{P}(X \cup Y)) : u \in X \;\&\; v \in Y\}$$

Kartézský součin tří a více množin definujeme v souladu s definicí uspořádaných trojic a n-tic

$$X \times Y \times Z = X \times (Y \times Z)$$

Obecně jsou množiny $(X \times Y) \times Z$ a $X \times (Y \times Z)$ různé, asociativní zákon zde neplatí.

Kartézský součin umožňuje modelovat nějaký vztah mezi prvky dvou množin jako množinu těch dvojic, které jsou v daném vztahu. Takovým množinám říkáme **relace**. Vlastnost $\mathbf{Rel}$ "býti relací" definujeme jako nový predikát

Definice 34 $\mathbf{Rel}(R) \equiv (\exists X)(\exists Y)(R \subseteq X \times Y)$

Definiční obor relace R tvoří prvky množiny X, které jsou v relaci s nějakým prvkem množiny Y. Abychom mohli definovat definiční obor jako novou množinovou operaci pomocí axiomu specifikace, potřebujeme znát množinu, ze které máme tyto prvky vybírat. Je-li $\langle u, v\rangle \in R$, je $u, v \in \{u, v\} \in \langle u, v\rangle \in R$, takže $\{u, v\} \in \mathcal{U}(R)$ a $u, v \in \mathcal{U}(\mathcal{U}(R))$. **Definiční obor** $\mathcal{D}(R)$ a **obor hodnot** $\mathcal{R}(R)$ je tedy

Definice 35

$$\begin{aligned}\mathcal{D}(R) &= \{u \in \mathcal{U}(\mathcal{U}(R)) : (\exists v)(\langle u, v\rangle \in R)\}\\ \mathcal{R}(R) &= \{v \in \mathcal{U}(\mathcal{U}(R)) : (\exists u)(\langle u, v\rangle \in R)\}\end{aligned}$$

Množinové operace $\mathcal{D}$ a $\mathcal{R}$ jsou definovány pro každou množinu, používají se ale především pro relace. Relace je každá množina, která obsahuje pouze uspořádané dvojice. Množiny $\{\emptyset\}$ ani $\{\{\emptyset\}\}$ tedy nejsou relace, zatímco $\{\{\{\emptyset\}\}\} = \{\langle\emptyset, \emptyset\rangle\}$ relace je. Také $\emptyset$ je relace, protože $\emptyset \times \emptyset = \emptyset$.

Tvrzení 36

$$\mathbf{Rel}(R) \equiv (\forall w \in R)(\exists u)(\exists v)(w = \langle u, v\rangle)$$

Důkaz: Je-li $\mathbf{Rel}(R)$, existují množiny X, Y takové že $R \subseteq X \times Y$, takže každý prvek R je uspořádaná dvojice.
Naopak, je-li každý prvek R uspořádaná dvojice, platí $R \subseteq \mathcal{D}(R) \times \mathcal{R}(R)$. □

Další (dvoučetná) množinová operace je **obraz** $R[A]$ množiny A při relaci R. Je to množina všech prvků, které jsou v relaci R s nějakým prvkem z A. **Restrikce** $R|X$ relace R na množinu X vznikne omezením definičního oboru R na množinu X (nebo její podmnožinu). **Inverzní relaci** R^{-1} dostaneme z R záměnou pořadí jejích uspořádaných dvojic. Je to jednočetná množinová operace. **Složení relací** $R \circ S$ je dvoučetná operace.

Definice 37

$$\begin{aligned}
R[A] &= \{v \in \mathcal{U}(\mathcal{U}(R)) : (\exists u \in A)(\langle u, v\rangle \in R)\} \\
R|X &= \{\langle u, v\rangle \in R : u \in X\} \\
R^{-1} &= \{w \in \mathcal{R}(R) \times \mathcal{D}(R) : (\exists u)(\exists v)(w = \langle u, v\rangle \ \&\ \langle v, u\rangle \in R)\} \\
S \circ R &= \{z \in \mathcal{D}(R) \times \mathcal{R}(S) : (\exists u, v, w)(\langle u, v\rangle \in R \ \&\ \langle v, w\rangle \in S \ \&\ z = \langle u, w\rangle)\}
\end{aligned}$$

Poslední dva vzorce lze psát jednodušeji (bez proměnných w a z)

$$\begin{aligned}
R^{-1} &= \{\langle u, v\rangle \in \mathcal{R}(R) \times \mathcal{D}(R) : \langle v, u\rangle \in R\} \\
S \circ R &= \{\langle u, w\rangle \in \mathcal{D}(R) \times \mathcal{R}(S) : (\exists v)(\langle u, v\rangle \in R \ \&\ \langle v, w\rangle \in S)\}
\end{aligned}$$

Operace inverze a složení jsou definovány pro všechny množiny, dobrý smysl ale mají jen pro relace. Navzájem jsou všechny tyto množinové operace svázány mnoha vztahy. Například $\mathbf{Rel}(R) \to (R^{-1})^{-1} = R$, ale obecně (pro každou množinu R) platí jen slabší vztah $(R^{-1})^{-1} \subseteq R$. Je-li totiž $w \in (R^{-1})^{-1}$, pak existují u, v taková že $w = \langle v, u\rangle$ a $\langle u, v\rangle \in R^{-1}$, takže $w \in R$. Naopak R však může obsahovat prvky, které nejsou dvojicemi a neobjeví se tedy v množině $(R^{-1})^{-1}$. Další identity nebo inkluze se vztahují k operacím průniku sjednocení a složení

$$\begin{aligned}
(R^{-1})^{-1} &\subseteq R \\
(S \circ R)^{-1} &= R^{-1} \circ S^{-1} \\
R[A \cup B] &= R[A] \cup R[B] \\
R[A \cap B] &\subseteq R[A] \cap R[B] \\
(S \circ R)[A] &= S[R[A]] \\
A \subseteq B &\to R[A] \subseteq R[B]
\end{aligned}$$

Všechny tyto identity se dokazují přímo z definice. Například

$$\begin{aligned}
z \in (S \circ R)^{-1} &\equiv (\exists u, w)(z = \langle w, u\rangle \ \&\ \langle u, w\rangle \in S \circ R) \\
&\equiv (\exists u, v, w)(z = \langle w, u\rangle \ \&\ \langle u, v\rangle \in R \ \&\ \langle v, w\rangle \in S) \\
&\equiv (\exists u, w)(z = \langle w, u\rangle \ \&\ \langle w, u\rangle \in R^{-1} \circ S^{-1}) \\
&\equiv z \in R^{-1} \circ S^{-1}
\end{aligned}$$

Speciálním případem relace je **funkce**, která každému prvku svého definičního oboru přiřazuje právě jeden prvek oboru hodnot. Tříčetný predikát $f : A \longrightarrow B$ znamená, že f je funkce s definičnim oborem A jejíž obor hodnot je podmnožina B. Říkáme, že funkce $f : A \longrightarrow B$ je **prostá** nebo **injektivní**, je-li f^{-1} také funkce. Říkáme, že funkce $f : A \longrightarrow B$ je **na** nebo **surjektivní**, je-li $\mathcal{R}(f) = B$. Funkce $f : A \longrightarrow B$ je **bijektivní**, je-li prostá a na.

Definice 38

$$\begin{aligned} \mathsf{Fnc}(f) &\equiv \mathsf{Rel}(f) \;\&\; (\forall u \in \mathcal{D}(f))(\exists! v \in \mathcal{R}(f))(\langle u, v\rangle \in f) \\ \mathsf{In}(f) &\equiv \mathsf{Fnc}(f) \;\&\; \mathsf{Fnc}(f^{-1}) \\ f : A \longrightarrow B &\equiv \mathsf{Fnc}(f) \;\&\; \mathcal{D}(f) = A \;\&\; \mathcal{R}(f) \subseteq B \end{aligned}$$

Hodnotu funkce f na prvku $u \in \mathcal{D}(f)$ značíme $f(u)$. V případě, že f není funkce pokládáme $f(u) = \emptyset$, tedy

$$\begin{array}{ll} f(u) = v & \text{pokud} \quad \langle u, v\rangle \in f \;\&\; (\forall w)(\langle u, w\rangle \in f \rightarrow v = w) \\ f(u) = \emptyset & \text{jinak} \end{array}$$

Další množinová operace je mocnina

Definice 39

$$x^y = \{f \in \mathcal{P}(x \times y) : \; f : y \rightarrow x\}$$

Je to množina všech funkcí z množiny y do množiny x. Pokud x je m-prvková množina a y je n-prvková množina, má x^y právě m^n prvků.

3.5 Ekvivalence množin

Dvě konečné množiny jsou stejně velké, mají-li stejný počet prvků. V tomto případě existuje vzájemně jednoznačná funkce, která prvkům jedné množiny přiřazuje prvky druhé množiny. V tomto smyslu budeme chápat i velikost nebo mohutnost nekonečných množin.

Definice 40 *Říkáme, že množiny X, Y mají stejnou mohutnost, nebo že jsou ekvivalentní ($X \approx Y$), jestliže existuje vzájemně jednoznačná funkce z X na Y. Existuje-li vzájemně jednoznačná funkce z X do Y, říkáme, že X má menší nebo rovnou mohutnost než Y.*

$$\begin{aligned} X \approx Y &\equiv (\exists f)(\mathcal{D}(f) = X \;\&\; \mathcal{R}(f) = Y \;\&\; \mathsf{Fnc}(f) \;\&\; \mathsf{Fnc}(f^{-1})) \\ X \preceq Y &\equiv (\exists f)(\mathcal{D}(f) = X \;\&\; \mathcal{R}(f) \subseteq Y \;\&\; \mathsf{Fnc}(f) \;\&\; \mathsf{Fnc}(f^{-1})) \end{aligned}$$

Například pro každé množiny u, v jsou jednoprvkové množiny $\{u\}, \{v\}$ ekvivalentní, protože $\{\langle u, v\rangle\} : \{u\} \rightarrow \{v\}$ je vzájemně jednoznačná funkce z $\{u\}$ na $\{v\}$. Množinové operace kartézského součinu a mocniny množin připomínají aritmentické operace násobení a umocňování (obdobou aritmetického součtu je sjednocení disjunktních množin). Mnoho aritmetických identit platí i pro množiny, nahradíme-li rovnost ekvivalencí. Například množiny $X \times Y$ a $Y \times X$ jsou obecně různé, jsou však ekvivalentní. V tomto smyslu je kartézský součin komutativní a asociativní.

Tvrzení 41 *Pro každé množiny X, Y, Z platí*
1. $X \times Y \approx Y \times X$,
2. $(X \times Y) \times Z \approx X \times (Y \times Z)$
3. $Z^X \times Z^Y \approx Z^{X \cup Y}$ *pokud* $X \cap Y = \emptyset$
4. $(X \times Y)^Z \approx X^Z \times Y^Z$
5. $(Z^Y)^X \approx Z^{Y \times X}$.
6. $\{a, b\}^X \approx \mathcal{P}(X)$ *pokud* $a \neq b$.

Důkaz:1. Funkce F definovaná předpisem $F(\langle u, v\rangle) = \langle v, u\rangle$ je vzájemně jednoznačná funkce z $X \times Y$ na $Y \times X$. Podrobněji, F je definována formulí

$$F = \{w \in (X \times Y) \times (Y \times X) : \ (\exists u \in X)(\exists v \in Y)(w = \langle\langle u, v\rangle, \langle v, u\rangle\rangle)\}$$

2. Funkce F definovaná předpisem $F(\langle\langle u, v\rangle, w\rangle) = \langle u, \langle v, w\rangle\rangle$ je vzájemně jednoznačná funkce z $X \times (Y \times Z)$ na $(X \times Y) \times Z$.
3. Definujme funkci $F : Z^{X \cup Y} \to Z^X \times Z^Y$ předpisem $F(f) = \langle f|X, f|Y\rangle$. Zde $f : X \cup Y \to Z$ je funkce a $f|X$, $f|Y$ její restrikce na množiny X a Y. Inverzní funkce je definována předpisem $F^{-1}(\langle g, h\rangle) = g \cup h$. Zde je nutný předpoklad $X \cap Y = \emptyset$, protože jinak by $g \cup h$ nemusela být funkce.
4. Definujme vzájemně jednoznačnou funkci $F : X^Z \times Y^Z \to (X \times Y)^Z$ předpisem $F(\langle f, g\rangle)(w) = \langle f(w), g(w)\rangle$. Zde $f : Z \to X$, $g : Z \to Y$ a $F(\langle f, g\rangle) : Z \to X \times Y$.
5. Definujme vzájemně jednoznačnou funkci $F : (Z^Y)^X \to Z^{X \times Y}$ předpisem $F(f)(\langle u, v\rangle) = f(u)(v)$. Zde $f : X \to Y^Z$, $u \in X$, $f(u) : Y \to Z$, $v \in Y$ a $f(u)(v) \in Z$.
6. Definujme vzájemně jednoznačnou funkci $F : \{a, b\}^X \to \mathcal{P}(X)$ předpisem $F(f) = \{u \in X : \ f(u) = a\}$.

Kromě kartézského součinu dvou množin se v teorii množin uvažuje také kartézský součin nekonečného souboru množin. Na rozdíl od operací průniku a skednocení, u kartézského součinu záleží na pořadí množin, které spolu násobíme. Proto se zavádí pojem **souboru množin** indexovaného nějakou množinou I. Všimneme si nejprve, že jsou-li $a \neq b$ libovolné množiny a $I = \{a, b\}$, platí pro každé množiny Y, Z

$$Y \times Z \approx \{f : I \to Y \cup Z : \ f(a) \in Y \ \& \ f(b) \in Z\}$$

Vzájemně jednoznačná funkce F mezi těmito množinami je dána předpisem $F(\langle u, v\rangle) = \{\langle a, u\rangle, \langle b, v\rangle\}$.

Souborem množin indexovaných indexovou množinou I nazýváme libovolnou funkci X s neprázdným definičním oborem I. V našem případě je $X(a) = Y$ a $X(b) = Z$. Soubor množin zapisujeme symbolicky $(X_i)_{i \in I}$. Prvky $i \in I$ používáme jako indexy, $X_i = X(i)$. Kartézský součin souboru $(X_i)_{i \in I}$ definuje jako množinu všech funkcí, které každému indexu $i \in I$ přiřazují nějaký prvek X_i

$$\prod_{i \in I} X_i = \{f : I \to \mathcal{U}(\mathcal{R}(X)) : (\forall i \in I)(f(i) \in X_i)\}$$

Jsou-li všechny množiny $X_i = Y$ stejné, dostáváme mocninu

$$\prod_{i \in I} Y = \{f : I \to Y\} = Y^I$$

Podobně zapisujeme sjednocení a průnik souboru množin $(X_i)_{i \in I}$

$$\begin{aligned} \bigcup_{i \in I} X_i &= \mathcal{U}(\mathcal{R}(X)) = \{u : (\exists i \in I)(u \in X_i)\} \\ \bigcap_{i \in I} X_i &= \mathcal{I}(\mathcal{R}(X)) = \{u : (\forall i \in I)(u \in X_i)\} \end{aligned}$$

3.6 Uspořádání a ekvivalence

Říkáme, že R je relace na množině X, je-li $R \subseteq X \times X$. Speciálně diagonální relace na dané množině X definujeme předpisem

Definice 42

$$\Delta(X) = \{\langle u, u \rangle \in \mathcal{P}(\mathcal{P}(X)) : u \in X\}$$

Zřejmě $\Delta(X)^{-1} = \Delta(X)$ a $\Delta(X) \circ \Delta(X) = \Delta(X)$. Je-li R libovolná relace na X, je $\Delta(X) \circ R = R \circ \Delta(X) = R$.

Definice 43 *Nechť $R \subseteq X \times X$ je relace na X.*
1. R je reflexivní, je-li $\Delta(X) \subseteq R$, tj.

$$(\forall u \in X)(\langle u, u \rangle \in R)$$

2. R je symetrická, je-li $R^{-1} = R$, tj.

$$(\forall u, v)(\langle u, v \rangle \in R \to \langle v, u \rangle \in R)$$

3. R je antisymetrická, je-li $R \cap R^{-1} = \Delta(X)$, tj.

$$(\forall u, v)(\langle u, v \rangle \in R \;\&\; \langle v, u \rangle \in R \to u = v)$$

4. R je tranzitivní, je-li $R \circ R \subseteq R$, tj.

$$(\forall u, v, w)(\langle u, v \rangle \in R \;\&\; \langle v, w \rangle \in R \to \langle u, w \rangle \in R)$$

5. R je úplná, je-li $R \cup R^{-1} = X \times X$,

$$(\forall u, v)(\langle u, v \rangle \in R \vee \langle v, u \rangle \in R)$$

Relace R na množině X, která je reflexivní, transitivní a antisymetrická se nazývá **částečné uspořádání**. Je-li navíc úplná, nazývá se **lineární uspořádání**. Pro každou množinu x je $\mathcal{P}(x)$ částečně uspořádána inkluzí, to znamená, že

$$\{\langle u,v\rangle \in \mathcal{P}(x)\times\mathcal{P}(x) :\ u\subseteq v\}$$

je částečné uspořádání na $\mathcal{P}(x)$.

Relace R na množině X, která je reflexivní, symetrická a tranzitivní se nazývá ekvivalence. Relace ekvivalence mají jednoduchou strukturu. Určují rozklad množiny X na třídy vzájemně ekvivalentních prvků.

Definice 44 *Nechť R je relace ekvivalence na X. Řekneme, že neprázdná množina $A\subseteq X$ je třída ekvivalence relace R, jestliže $R[A]=A$ a $A\times A\subseteq R$, tj.*

$$(\forall u\in A)(\forall v)(v\in A\equiv\langle u,v\rangle\in R)$$

Tvrzení 45 *Nechť R je relace ekvivalence na X.*
1. Každé dvě různé třídy ekvivalence jsou disjunktní (tj. jejich průnik je $\emptyset$).
2. Každý prvek $a\in X$ náleží právě do jedné třídy ekvivalence.

Důkaz: 1. Předpokládejme, že $A,B\subseteq X$ jsou dvě třídy ekvivalence, které nejsou disjunktní, tj. mají společný prvek $a\in A\cap B$. Je-li $u\in A$, pak $\langle a,u\rangle\in R$ a tedy $a\in B$. Dokázali jsme $A\subseteq B$. Analogicky ukážeme $B\subseteq A$.
2. Je-li $a\in X$, položme

$$A=\{u\in x :\ \langle a,u\rangle\in R\}$$

Protože R je reflexivní, je $a\in A$ a A je třída ekvivalence. Z (1) plyne, že a náleží do jediné třídy ekvivalence. □

Nechť R je relace ekvivalence na X. Položme

$$\begin{aligned} X/R &= \{A\in\mathcal{P}(X) :\ R[A]=A \,\&\, A\times A\subseteq R\}\\ \pi &= \{\langle a,A\rangle\in X\times(X/R) :\ a\in A\}\end{aligned}$$

Pak $\pi : X\longrightarrow X/R$ je surjektivní funkce. Množina X/R tříd ekvivalence se nazývá **faktorová množina** X podle R a funkce π se nazývá **faktorizace**. Konstrukce faktorové množiny se často používá, chceme-li ztotožnit ekvivalentní prvky. Je-li přitom na množině X nějaká struktura (aritmetické operace nebo relace), snažíme se jí přenést na faktorovou množinu. K tomu je třeba, aby ekvivalence R byla kongruencí vzhledem k této struktuře. Ukážeme si to na příkladě jednočetné funkce.

Definice 46 *Nechť R je ekvivalence na X a $f:X\to X$ funkce. Říkáme, že R je kongruence pro f, jestliže platí*

$$(\forall u,v\in X)(\langle u,v\rangle\in R\ \rightarrow\ \langle f(u),f(v)\rangle\in R)$$

Je-li R kongruence pro f, položme

$$f/R=\{\langle A,B\rangle\in(X/R)\times(X/R) :\ (\exists a\in A)(\exists b\in B)(\langle a,b\rangle\in f)\}$$

Je-li $a \in X$ a $A = \pi(a)$ příslušná třída ekvivalence, je $(f/R)(A) = \pi(f(a))$. To znamená, že $(f/R) \circ \pi = \pi \circ f$. Říkáme, že komutuje diagram zobrazení

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ \downarrow \pi & & \downarrow \pi \\ X/R & \xrightarrow{f/R} & X/R \end{array}$$

3.7 Struktury

Prostředky teorie množin, které máme nyní k dispozici umožňují zavést pro daný jazyk (seznam predikátů, operací a konstant) pojem struktury pro tento jazyk. Například struktura pro jazyk $\mathcal{L} = \{=\}$ obsahující jediný dvoučetný predikát rovnosti je každá dvojice $\mathbb{M} = \langle X, R \rangle$, kde X je neprázdná množina a $R \subseteq X \times X$ je dvoučetná relace na X. Modely teorie rovnosti (s axiomy reflexivity, symetrie a transitivity) jsou právě struktury $\langle X, R \rangle$, kde R je relace ekvivalence na X. Struktura pro jazyk $\mathcal{L} = \{=, \mathsf{f}\}$, kde f je jednočetná operaci, je každá uspořádaná trojice $\mathbb{M} = \langle X, R, f \rangle$, kde X je neprázdná množina, $f : X \to X$ je funkce a $R \subseteq X \times X$ je ekvivalence na X, která je kongruence pro $f : X \to X$. V teorii rovnosti (odstavec 2.5) přibývá ještě axiom kongruence pro f

$$x = y \to \mathsf{f}(x) = \mathsf{f}(y)$$

a modely teorie rovnosti jsou struktury $\langle X, R, f \rangle$, kde R je relace kongruence pro f. Podobně struktura pro jazyk $\mathcal{L} = \{0, 1, +, *, <, =\}$ je každá množina tvaru $\mathbb{M} = \langle M, C_0, C_1, F_+, F_*, R_<, \Delta(M) \rangle$, kde
1. $M \neq \emptyset$ je neprázdná množina
2. $C_0, C_1 \in M$,
3. $F_+, F_* : M \times M \to M$ jsou dvoučetné funkce na M,
4. $R_< \subseteq M \times M$ je dvoučetná relace.

4 Aritmetické struktury

4.1 Ordinální čísla

Struktura $\mathbb{N}$ přirozených čísel je jeden z nejdůležitějších matematických objektů. V teorii množin lze přirozená čísla sestrojit velmi elegantním způsobem. Ztotožníme číslo 0 s prázdnou množinou $\emptyset$ a každé další číslo s množinou všech přirozených čísel menších. Definujeme tedy nové konstanty $0, 1, 2, 3 \ldots$

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \quad 4 = \{0, 1, 2, 3\}, \ldots$$

Číslo n je tedy množina, která má právě n prvků. V univerzu množin se objeví právě na n-té úrovni. Při této reprezentaci můžeme ihned definovat nerovnosti mezi přirozenými čísly vztahy

$$\begin{aligned} n < m &\equiv n \in m \\ n \leq m &\equiv n \subseteq m \end{aligned}$$

Operaci následníka definujeme předpisem $n+1 = n \cup \{n\}$. Je totiž $1 = \emptyset \cup \{\emptyset\}$, takže $1 = 0+1$, $2 = 1 \cup \{1\} = 1+1$, $3 = 2+1$, atd. Abychom mohli sestrojit množinu přirozených čísel, je třeba přirozená čísla charakterizovat nějakou vlastností. Definujme nejprve nový predikát $\mathbf{Ord}(x)$, který vymezuje obecnější ordinální čísla. Přirozená čísla jsou konečná ordinální čísla. Pokud existují nekonečné množiny (jejich existenci jsme dosud nezaručili žádným axiomem), existují také nekonečná ordinální čísla.

Definice 47 *Množina x je ordinální číslo, platí-li*

$$\mathbf{Ord}(x) \equiv (\forall u \in x)(u \subseteq x) \ \ \& \ \ (\forall u, v \in x)((u \in v) \vee (u = v) \vee (v \in u))$$

První podmínku lze ekvivalentně vyjádřit pomocí operace obecného sjednocení a potenční množiny

$$(\forall u \in x)(u \subseteq x) \quad \equiv \quad \mathcal{U}(x) \subseteq x \quad \equiv \quad x \subseteq \mathcal{P}(x)$$

Ukážeme si nejprve že přirozená čísla $0, 1, 2, 3, 4, \ldots$ jsou čísly ordinálními.

Tvrzení 48
1. $\mathbf{Ord}(0)$
2. $\mathbf{Ord}(x) \rightarrow \mathbf{Ord}(x \cup \{x\})$.

Důkaz: 1. platí triviálně.
2. Předpokládejme $\mathbf{Ord}(x)$. Je-li $u \in x \cup \{x\}$, je buď $u \in x$ a pak $u \subseteq x \subseteq x \cup \{x\}$ nebo $u = x$ a pak $u \subseteq \{x\}$. V obou případech je tedy $u \subseteq x \cup \{x\}$.
Nechť $u, v \in x \cup \{x\}$. Rozeznáváme čtyři případy
a. $u, v \in \{x\}$ $\rightarrow$ $u = v$.
b. $u \in \{x\}$, $v \in x$ $\rightarrow$ $v \in u$.
c. $u \in x$, $v \in \{x\}$ $\rightarrow$ $u \in v$.
d. $u, v \in x$ $\rightarrow$ $u \in v$ nebo $v \in u$ nebo $u = v$ □

Tvrzení 49
1. $\mathbf{Ord}(x)$ & $\mathbf{Ord}(y) \rightarrow \mathbf{Ord}(x \cap y)$
2. $\mathbf{Ord}(x)$ & $y \in x \rightarrow \mathbf{Ord}(y)$
3. $\mathbf{Ord}(x)$ & $\mathbf{Ord}(y)$ & $y \subset x \rightarrow y \in x$

1. Důkaz je triviální. Je-li $u \in x \cap y$, je $u \subseteq x$ a $u \subseteq y$ takže $u \subseteq x \cap y$. Podobně je-li $u, v \in x \cap y$, je $u, v \in x$ takže buď $u \in v$ nebo $u = v$ nebo $v \in u$.
2. Podle definice $y \subseteq x$. Ukážeme, že pro $u \in y$ je $u \subseteq y$. Je-li $v \in u$, pak $u \in x$, $u \subseteq x$ a $v \in x$. Protože také $y \in x$, je

$$(v \in y) \vee (v = y) \vee (y \in v).$$

Ale ani $v = y$ ani $y \in v$ nenastává podle axiomu regularity (tvrzení 30). Je tedy $v \in y$. Dokázali jsme tedy $u \in y \rightarrow u \subseteq y$.
Je-li $u, v \in y$, je $u, v \in x$ a nastává jedna z možností $u \in v$, $u = v$, $v \in u$.
3. Podle předpokladu je množina $x \setminus y \subseteq x$ neprázdná, takže podle axiomu regularity existuje z, pro které

$$z \in x \setminus y \ \& \ z \cap (x \setminus y) = \emptyset \rightarrow z \subseteq x \ \& \ z \subseteq y.$$

Ukážeme, že platí obrácená inkluze $y \subseteq z$. Nechť $u \in y$. Protože $u, z \in x$, je buď $z \in u$ nebo $z = u$ nebo $u \in z$. Ale $z \in u$ implikuje $z \in y$ protože $u \subseteq y$ a $z = u$ rovněž implikuje $z \in y$ protože $u \in y$. Avšak $z \in y$ je ve sporu s $z \in (x \setminus y)$, takže nastává třetí možnost $u \in z$. Ukázali jsme tedy $y = z$. Protože $z \in x$, je $y \in x$. □

Je-li x ordinální číslo, definujme na x relaci

$$\{(v, u) \in x \times x : \ v \in u \vee v = u\}$$

Z Tvrzení 49 plyne, že tato relace je lineární uspořádání na x. Vlastnost linearity platí i mezi každými dvěma ordinálními čísly.

Tvrzení 50 *Je-li* $\mathbf{Ord}(x)$ *a* $\mathbf{Ord}(y)$, *nastává právě jedna z možností*

$$(x \in y) \vee (x = y) \vee (y \in x)$$

Důkaz: Dvě z těchto možností současně nastat nemohou podle Axiomu regularity. Podle Tvrzení 49 je $\mathbf{Ord}(x \cap y)$. Rozeznáváme čtyři možnosti.
1. $x \cap y = x$, $x \cap y = y$. Pak $x = y$.
2. $x \cap y = x$, $x \cap y \subset y$. Pak $x \cap y \in y$ podle Tvrzení 49, takže $y \in x$.
3. $x \cap y \subset x$, $x \cap y = y$. Pak $y = x \cap y \in x$.
4. $x \cap y \subset x$, $x \cap y \subset y$. Pak $x \cap y \in x$ a $x \cap y \in y$, takže $x \cap y \in x \cap y$ a to je spor s Tvrzením 29. □

Tvrzení 51 *Sjednocení každé množiny ordinálních čísel je ordinální číslo.*

$$(\forall y \in x)\mathbf{Ord}(y) \rightarrow \mathbf{Ord}(\mathcal{U}(x))$$

Důkaz: 1. Nechť $y \in \mathcal{U}(x)$, takže existuje z, pro které $y \in z \in x$. Protože $\mathbf{Ord}(z)$, je $y \subseteq z$. Pro každé $w \in y$ je tedy $w \in z \in x$ a tedy $w \in \mathcal{U}(x)$. Ukázali jsme $y \subseteq \mathcal{U}(x)$.
2. Nechť $u, v \in \mathcal{U}(x)$. pak existují ordinální čísla y, z, pro která $u \in y \in x$ a $v \in z \in x$. Podle Tvrzení 49.2 je $\mathbf{Ord}(u)$ a $\mathbf{Ord}(v)$. Podle tvrzení 50 je buď $u \in v$ nebo uv nebo $v \in u$. □

4.2 Přirozená čísla

Pokud existuje množina všech přirozených čísel $\omega = \{\emptyset, 1, 2, 3, 4, \ldots\}$, je také ordinálním číslem, platí $\mathbf{Ord}(\omega)$. To je důsledek tvrzení 50. Z našich dosavadních axiomů však existenci nekonečných množin nelze odvodit. Chceme-li pracovat s množinou přirozených čísel, musíme přijmout další axiom. Ten musí vystihnout nějakou vlastnost, která je charakteristická pro nekonečné množiny, nebo alespoň nějakou vlastnost množiny ω, kterou tato množina nesdílí s přirozenými čísly. Jedna taková vlastnost je, že nemá předchůdce. Neexistuje množina x, pro kterou $\omega = x \cup \{x\}$. Taková ordinální čísla se nazývají limitní. Prázdná množina sice také nemá předchůdce, za limitní jí však nepovažujeme.

Definice 52

$$\mathbf{Lim}(x) \equiv \mathbf{Ord}(x) \ \ \& \ \ x \neq \emptyset \ \ \& \ \ \neg(\exists y)(x = y \cup \{y\})$$

Existují-li limitní ordinální čísla, existuje jeich nekonečně mnoho. Je-li totiž x limitní ordinální číslo, je $x+1 = x \cup \{x\}$ také ordinální číslo, $x+2 = (x+1)+1$ také a množina $x \cup \{x, x+1, x+2, \ldots\}$ je další limitní ordinální číslo. Množina přirozených čísel je charakterizována tím, že je nejmenším limitním ordinálním číslem

Axiom 9 (Axiom nekonečna)

$$(\exists z)(\mathbf{Lim}(z) \ \& \ (\forall y \in z)\neg\mathbf{Lim}(y))$$

Tvrzení 53

$$(\exists! z)(\mathbf{Lim}(z) \ \& \ (\forall y \in z)\neg\mathbf{Lim}(y)$$

Důkaz: Předpokládejme, že z a w splňují obě vlastnosti axiomu nekonečna. Protože jsou to ordinální čísla, podle tvrzení 50 platí $w \in z$ nebo $w = z$ nebo $z \in w$. Avšak $w \in z$ vede ke sporu, protože w je limitní ordinální číslo a z neobsahuje limitní ordinální čísla. Podobně vede ke sporu $z \in w$, takže $w = z$. □

Množina postulovaná axiomem nekonečna tedy existuje jediná a označíme si ji novou konstantou ω

Definice 54 $\mathbf{Lim}(\omega) \ \& \ (\forall y \in \omega)\neg\mathbf{Lim}(y)$

Proměnné pro přirozená čísla (prvky ω) budeme značit $n, m, p, \ldots$. Na množině ω definujeme uspořádání předpisem

$$n < m \equiv n \in m, \ \ n \leq m \equiv n < m \vee n = m$$

Důležitá vlastnost množiny přirozených čísel je princip matematické indukce. Ten lze formulovat dvěma způsoby. První formulace říká, že každá neprázdná podmnožina přirozených čísel má nejmenší prvek. To je přímo axiom regularity použitý na ω: $(\forall x \subseteq \omega)(x \neq \emptyset \rightarrow (\exists n \in x)(n \cap x = \emptyset)$. Je-li ale $n \in x \subseteq \omega$, platí

$$n \cap x = \emptyset \equiv (\forall m \in x)(m \notin n) \equiv (\forall m \in x)(n \leq m)$$

a odtud

$$(\forall x \subseteq \omega)(x \neq \emptyset \rightarrow (\exists n \in x)(\forall m \in x)(n \leq m))$$

Druhá formulace Principu matematické indukce se týká vlastností přirozených číslech vyjádřených formulemi. Platí-li nějaká formule pro 0 a plyne-li z její platnosti pro n také platnost pro $n+1$, platí pro všechna přirozená čísla.

Věta 55 (Princip matematické indukce) *Je-li $\varphi(x)$ formule pak*

$$\varphi(0) \mathbin{\&} (\forall n \in \omega)(\varphi(n) \rightarrow \varphi(n+1)) \rightarrow (\forall n \in \omega)\varphi(n)$$

Důkaz: Podle axiomu specifikace utvořme množinu

$$y = \{n \in \omega : \neg\varphi(n)\}$$

Je-li tato množina neprázdná, má nejmenší prvek m. Protože platí $\varphi(0)$, je $m \neq 0$. Protože m není limitní, má předchůdce $m = n+1$. Protože m je nejmenší prvek y, n do y nenáleží a platí $\varphi(n)$. Podle předpokladu platí i $\varphi(m)$ a to je spor. □

Naopak z principu matematické indukce plyne, že každá neprázdná podmnožina přirozených čísel má nejmenší prvek. Předpokládejme sporem, že $\emptyset \neq x \subseteq \omega$ je neprázdná a nemá nejmenší prvek. Uvažujme formuli

$$\varphi(n) \equiv (\forall m \leq n)(m \notin x)$$

Pak $\varphi(0) \equiv 0 \notin x$ a to platí protože jinak by 0 byl nejmenší prvek x. Pokud $n \in \omega$, $\varphi(n)$ a $\neg\varphi(n+1)$, pak $n+1$ je nejmenší prvek x a to je spor. Platí tedy $(\forall n \in \omega)(\varphi(n) \rightarrow \varphi(n+1)$, takže podle principu matematické indukce $(\forall n \in \omega)\varphi(n)$ a z toho plyne $x = \emptyset$.

K přirozeným číslům umíme přičítat jednotku podle vzorce $n+1 = n \cup \{n\}$. Přičítání dvojky tedy definujeme $n+2 = (n+1)+1$ a podobně můžeme definovat přičítání každé konstanty. Vzorec pro součet $n+m$ dvou přirozených čísel ale nemáme. Aritmetickou operaci sčítání zavedeme jako funkci $f : \omega \times \omega \rightarrow \omega$. Lze ji určit jednoznačně rekurentním vztahem $f(n, 0) = n$, $f(n, m+1) = f(n, m) + 1$. Je třeba však dokázat existenci a jednoznačnost funkce s těmito vlastnostmi. Učiníme tak obecně pro libovolnou rekurentní definici.

Věta 56 (Věta o rekurentní definici) *Nechť X je libovolná množina, $a \in X$ a $g : X \rightarrow X$ je funkce. Pak existuje jediná funkce $f : \omega \rightarrow X$ pro kterou platí*

$$f(0) = a, \quad (\forall n \in \omega)(f(n+1) = g(f(n)))$$

Důkaz: Ukážeme si nejprve, že funkce s požadovanými vlastnostmi existuje jediná. Předpokládejme sporem, že existují dvě různé funkce $f_1, f_2 : \omega \to X$, které obě splňují požadovanou vlastnost. Utvořme množinu

$$Y = \{n \in \omega : f_1(n) \neq f_2(n)\}$$

Protože f_1, f_2 jsou různé funkce, je $Y \subseteq \omega$ neprázdná a má tedy nejmenší prvek m. Protože $f_1(0) = a = f_2(0)$, je $m \neq 0$ a má tedy předchůdce $m = p + 1$. Protože $p \notin Y$, je $f_1(p) = f_2(p)$ a podle předpokládaných vlastností funkcí f_1, f_2 také $f_1(p+1) = f_2(p+1)$ a to je spor.
Ukážeme nyní existenci funkce f tak že budeme uvažovat funkce s danou rekurentní vlastností definované pouze na nějakém přirozeném čísle. Například každá z funkcí

$$h_1 = \{\langle 0, a\rangle\}, \quad h_2 = \{\langle 0, a\rangle, \langle 1, g(a)\rangle\}, \quad h_3 = \{\langle 0, a\rangle, \langle 1, g(a)\rangle, \langle 2, g(g(a))\rangle\}$$

splňuje rekurentní vztah, jejich definiční obory jsou $\mathcal{D}(h_1) = 1$, $\mathcal{D}(h_2) = 2$ a $\mathcal{D}(h_3) = 3$. Sestrojíme množinu všech takovýchto funkcí

$$\begin{aligned} H \;=\; & \{h \subseteq \omega \times X : \mathbf{Fnc}(h) \;\&\; \mathcal{D}(h) \in \omega \;\&\; h(0) = a \;\&\; \\ & (\forall n)(n + 1 \in \mathcal{D}(h) \to h(n+1) = g(h(n))\} \end{aligned}$$

Množina H obsahuje funkce h_1, h_2, h_3, atd. Položme $f = \mathcal{U}(H)$ a ukažme, že f splňuje tvrzení věty. Uvažujme formuli

$$\varphi(n) \equiv (\exists! x)(\langle n, x\rangle \in f)$$

Protože $f_1 \in H$, je $\langle 0, a\rangle \in f$. Protože pro každé $h \in H$ je $h(0) = a$, je a jediný prvek s touto vlastností, tj. platí $\varphi(0)$. Předpokládejme, že platí $\varphi(n)$. Existuje tedy $x \in X$ pro které $\langle n, x\rangle \in f$ a existuje $h \in H$ pro které $h(n) = x$. Pak $h' = h \cup \langle n + 1, g(x)\rangle$ je funkce, $h' \in H$, takže $\langle n + 1, g(x)\rangle \in f$. Protože pro každé $h \in H$ je $h(n) = x$ je $y = g(x)$ jediný prvek, pro který platí $\langle n + 1, y\rangle \in f$. Dokázali jsme tedy $\varphi(n) \to \varphi(n + 1)$, takže podle principu matematické indukce $(\forall n \in \omega)\varphi(n)$. To znamená že $f : \omega \to X$ je funkce. Protože $h_1 \in H$, je $f(0) = a$. Pro každé $n \in \omega$ existuje $h \in H$ pro které $n + 1 \in \mathcal{D}(h)$ a $f(n + 1) = h(n + 1) = g(h(n)) = g(f(n))$. Funkce f tedy má požadované vlastnosti. □

Podle Věty o rekurentní definici například setsrojíme funkci $f(n) = n + n$ rekurentním vztahem $f(0) = 0$, $f(n + 1) = (f(n) + 1) + 1$. Pro definici sčítání jako dvoučetné funkce potřebujeme rekurentní definice závislé na parametru.

Věta 57 (Rekurentní definice s parametrem) *Nechť X, Y jsou libovolné množiny, $g_0 : Y \to X$, $g_1 : Y \times X \to X$ funkce. Pak existuje jediná funkce $f : Y \times \omega \to X$ pro kterou platí*

$$f(y, 0) = g_0(y), \quad (\forall n \in \omega)(f(y, n + 1) = g_1(y, f(y, n))$$

Důkaz je analogický jako u předcházející věty. Hledaná funkce se sestrojí jako $f = \mathcal{U}(H)$, kde

$$\begin{aligned} H &= \{h \subseteq (Y \times \omega) \times X : (\exists n \in \omega)(\mathcal{D}(h) = Y \times n) \ \& \\ &\quad (\forall y \in y)(h(y, 0) = g_0(y)), \ \& \\ &\quad (\forall \langle y, m+1 \rangle \in \mathcal{D}(h))(h(y, m+1) = g_1(y, h(y, m)))\} \end{aligned}$$

Volíme-li nyní funkce $g_0 : \omega \to \omega$, kde $g_0(n) = n$ a $g_1 : \omega \times \omega \to \omega$, kde $g_1(n, m) = m + 1$, platí pro $f : \omega \times \omega \to \omega$, $f(n, 0) = n$, $f(n, m+1) = f(n, m) + 1$. Funkční hodnotu $f(n, m)$ budeme značit, jak je obvyklé, $n+m$. Všechny vlastnosti sčítání lze odvodit (matematickou indukcí) z rekurentního vztahu

$$n + 0 = n, \quad n + (m+1) = (n+m) + 1$$

Ukážeme nejprve asociativní zákon

Tvrzení 58 $(\forall n, m, p \in \omega)((n+m) + p = n + (m+p))$

Důkaz: Indukcí podle p. Pro $p = 0$ je

$$(n+m) + 0 = n + m = n + (m+0)$$

Je-li $(n+m) + p = n + (m+p)$, je také

$$\begin{aligned} (n+m) + (p+1) &= ((n+m) + p) + 1 = (n + (m+p)) + 1 \\ &= n + ((m+p) + 1) = n + (m + (p+1)) \end{aligned}$$

Důkaz komutativního zákona je trochu složitější

Tvrzení 59 $(\forall n, m \in \omega)(n + m = m + n)$

1. Dokážeme nejprve $n + 0 = 0 + n$.
Pro $n = 0$ vztah platí. Je-li $n + 0 = 0 + n$, je

$$(n+1) + 0 = n + 1 = (0+n) + 1 = 0 + (n+1)$$

2. Ukážeme $n + 1 = 1 + n$.
Pro $n = 0$ je $0 + 1 = 1 = 1 + 0$. Je-li $n + 1 = 1 + n$, je

$$(n+1) + 1 = (1+n) + 1 = 1 + (n+1)$$

3. Je-li $n + m = m + n$, je

$$\begin{aligned} (n+1) + m &= n + (1+m) = n + (m+1) = (n+m) + 1 = (m+n) + 1 \\ &= m + (n+1) \end{aligned}$$

Volíme-li $g_0(n) = 0$, $g_1(n, m) = m + n$, dostáváme funkci násobení $f(n, m) = n * m$. Všechny algebraické identity pro násobení a sčítání lze matematickou indukcí dokázat z rekurentního vztahu

$$n * 0 = 0, \quad n * (m + 1) = n * m + n$$

Také další aritmetické operace jako faktoriál nebo mocninu lze závést obdobnými rekurentními vztahy. Můžeme tedy definovat strukturu přirozených čísel jako $\mathbb{N} = \langle \omega, 0, 1, f, g, R, \Delta(\omega) \rangle$, kde f, g jsou funkce sčítání a násobení sestrojené výše a

$$R = \{\langle n, m \rangle \in \omega \times \omega : \ n \leq m\}$$

je relace nerovnosti.

4.3 Celá a racionální čísla

Rozšíření čísel přirozených na čísla celá je motivováno snahou čísla odčítat, což ve struktuře přirozených čísel není vždy možné. Podobně rozšíření celých čísel na racionální je motivováno snahou čísla dělit. Obě konstrukce jsou analogické. Celá čísla můžeme chápat jako formální výrazy $n - m$, kde $n, m \in \omega$. Dva takové formální výrazy mohou reprezentovat stejné záporné číslo, například je $2 - 3 = 4 - 5 = 0 - 1$. Formální výraz $n - m$ kódujeme jako uspořádanou dvojici $\langle n, m \rangle$, ztotožňujeme však dvojice které reprezentují stejné záporné číslo. Uvažujme relaci $\approx$ na $\omega \times \omega$ danou předpisem

$$\langle n, m \rangle \sim \langle p, q \rangle \equiv n + q = p + m$$

Snadno dokážeme, že $\sim$ je ekvivalence na $\omega \times \omega$ a množinu celých čísel definujeme jako faktorovou množinu $\mathbb{Z} = (\omega \times \omega)/\sim$. Aritmetické operace sčítání, násobení a dělení definujeme nejprve na $\omega \times \omega$ předpisem

$$\begin{aligned}
\langle n, m \rangle + \langle p, q \rangle &= \langle n + p, m + q \rangle \\
\langle n, m \rangle - \langle p, q \rangle &= \langle n + q, m + p \rangle \\
\langle n, m \rangle * \langle p, q \rangle &= \langle n * p + m * q, m * p + n * q \rangle
\end{aligned}$$

Tyto aritmetické operace jsou kongruence vzhledem k ekvivalenci $\sim$, to znamená, že ekvivalentní prvky mají ekvivalentní součty, rozdíly a násobky. Například

$$\langle n, m \rangle \sim \langle p, q \rangle \rightarrow \langle n, m \rangle + \langle r, s \rangle \sim \langle p, q \rangle + \langle r, s \rangle$$

Pro celá čísla $a, b, c \in \mathbb{Z}$, tj. třídy ekvivalence $a, b, c \subseteq \omega \times \omega$ pak položíme

$$a + b = c \equiv (\exists u \in a)(\exists v \in b)(\exists w \in c)(u + v = w)$$

a podobně pro další aritmetické operace.

Racionální čísla sestrojíme jako formální zlomky, tj. jako dvojice čísel celých.

Protože nelze nulou dělit, položíme $A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ a definujeme ekvivalenci $\sim$ na A předpisem

$$\langle n, m \rangle \sim \langle p, q \rangle \equiv n * q = p * m$$

Množina racionálních čísel je faktorová množina $\mathbb{Q} = \mathbb{Z}/\sim$.

4.4 Reálná čísla

Racionální čísla lze sčítat, odčítat, násobit a dělit, nelze je však vždy odmocňovat. Rozšířit racionální čísla o všechny odmocniny racionálních čísel lze podobným způsobem jakým jsme sestrojili čísla celá a racionální. Ale ani v této struktuře bychom neměli čísla transcendentní jako π nebo e. Obecné reálné číslo vymezíme, určíme-li všechna racionální čísla, která jsou menší než ono. Reprezentujeme je tedy speciálními množinami racionálních čísel, které nazýváme řezy

Definice 60 *Řez je neprázdná množina racionálních čísel, různá od $\mathbb{Q}$ taková, že s každým prvkem obsahuje všechny prvky menší a nemá největší prvek. Množina A je tedy řez, je-li*

$$\emptyset \subset A \subset \mathbb{Q} \ \ \& \ \ (\forall x \in A)(\forall y < x)(y \in A) \ \ \& \ \ (\forall x \in A)(\exists y > x)(y \in A)$$

Každé racionální číslo $a \in \mathbb{Q}$ určuje řez $A_a = \{x \in \mathbb{Q} : \ x < a\}$. Druhá odmocnina ze dvou je reprezentována řezem

$$A = \{x \in \mathbb{Q} : \ x < 0 \vee x * x < 2\}$$

Množinu reálných čísel můžeme definovat jako množinu řezů racionálních čísel. Na této množině lze definovat všechny aritmetické operace. Například součet dvou řezů definujeme předpisem

$$A + B = \{a + b : \ a \in A \ \& \ b \in B\}$$

Poněkud složitější je odčítání. Pokud $A = A_a = \{x \in Q : \ x < a\}$, definujeme opačný řez předpisem

$$-A_a = \{x \in \mathbb{Q} : \ x < -a\}$$

Pokud A je iracionální, tj. různý od každého A_a, definujeme řez opačný předpisem

$$-A = \{x \in \mathbb{Q} : \ -x \notin A\}$$

Podobně lze definovat násobení a dělení reálných čísel, je třeba však rozenávat různé případy kdy jsou argumenty kladné či záporné, racionální či iracionální.

Alternativní způsob zavedení reálných čísel využívá Bolzano-Cauchyovu větu, podle které posloupnost reálných čísel má limitu právě když je cauchyovská. Reálná čísla můžeme ztotožnit s cauchyovskými posloupnostmi racionálních čísel.

Posloupnost racionálních čísel ja každá funkce $a : \omega \to \mathbb{Q}$. Hodnotu posloupnosti v čísle n (její n-tý člen) značíme $a_n = a(n)$. Posloupnost a je cauchyovská, platí-li

$$(\forall \varepsilon \in \mathbb{Q}^+)(\exists n \in \omega)(\forall m, p \geq n)(|a_m - a_p| < \varepsilon)$$

Zde $\mathbb{Q}^+$ je množina kladných racionálních čísel. Na množině C cauchyovských posloupností definujeme ekvivalenci $\sim$ předpisem

$$a \sim b \equiv (\forall \varepsilon \in \mathbb{Q}^+)(\exists n \in \omega)(\forall m \geq n)(|a_m - b_m| < \varepsilon)$$

Množina reálných čísel je faktorová množina $\mathbb{R} = C/\sim$. Aritmetické operace definujeme nejprve na množině C po složkách

$$\begin{aligned}
(a+b)_n &= a_n + b_n \\
(a*b)_n &= a_n * b_n \\
(a-b)_n &= a_n - b_n \\
(a/b)_n &= a_n / b_n
\end{aligned}$$

Snadno ukážeme, že součet, součin a rozdíl cauchyovských posloupností je opět cauchyovská posloupnost. Pro podíl to platí pouze v případě že b_n není ekvivalentní nulové posloupnosti. Ekvivalence $\sim$ je kongruencí pro všechny tyto aritmetické operace, takže jsou jednoznačně definovány i na faktorové množině $\mathbb{R}$.

5 Mohutnosti množin

V odstavci 3.5 jsme definovali ekvivalenci a subvalenci množin. Existuje-li vzájemně jednoznačné obrazení z X na Y, říkáme, že X má stejnou mohutnost jako Y ($X \approx Y$) nebo že množiny X a Y jsou ekvivalentní. Existuje-li prosté zobrazení z X do Y, říkáme, že X má menší nebo rovnou mohutnost než Y ($X \preceq Y$).

Definice 61 *1. Množina X je konečná, je-li ekvivalentní nějakému přirozenému číslu $n \in \omega$.*
2. Množina X je spočetná, je-li ekvivalentní množině ω.

Paradoxním jevem v teorii mohutností je, že nekonečná množina má stejnou mohutnost jako některé její vlastní části. Například množina přirozených čísel ω má stejnou mohutnost jako množina sudých čísel

$$A = \{n \in \omega : (\exists m \in \omega)(n = 2 * m)\}$$

Funkce $f : \omega \to A$ definovaná předpisem $f(n) = 2 * n$ je vzájemně jednoznačná. Také obě množiny $\mathbb{Z}$ a $\mathbb{Q}$ jsou spočetné. To plyne z toho, že množina $\omega \times \omega$ je spočetná. Vzájemně jednoznačná funkce $f : \omega \times \omega \to \omega$ může být definována předpisem

$$f(n,m) = \frac{(n+m)*(n+m+1)}{2} + n$$

	0	1	2	3
0	0	2	5	9
1	1	4	8	
2	3	7		
3	6			

5.1 Cantor-Bernsteinova věta

Vztah subvalence $x \preceq y$ je zřejmě tranzitivní. Je-li $x \preceq y$ a $y \preceq z$, existují prosté funkce $f : x \to y$ a $g : y \to z$ a jejich složení je prostá funkce $g \circ f : x \to z$, takže $x \preceq z$. Cantor-Bernsteinova věta říká, že vztah subvalence je antisymetrický. Pro důkaz této věty si nejprve zavedeme pojem **iterace** funkce. Nechť $g : X \to X$ je funkce a uvažujme funkce $g_0 : X \to X$, $g_1 : X \times X \to X$ dané předpisy $g_0(x) = x$, $g_1(y,x) = g(x)$. Podle věty o rekurentní definici s parametrem existuje jediná funkce $f : X \times \omega \to X$ splňující

$$f(x,0) = x, \quad f(x,n+1) = g(f(x,n))$$

Pro pevné $n \in \omega$ označme $g^n : X \to X$ funkci definovanou $g^n(x) = f(x,n)$. Pak

$$g^0(x) = x, \quad g^{n+1}(x) = g(g^n(x))$$

Funkce g^n se nazývá n-tá iterace funkce g. Je to složení funkce g se sebou samou n-krát.

Tvrzení 62 (Cantor-Bernsteinovo lemma) *Je-li $Z \subseteq Y \subseteq X$ a $X \approx Z$, je $X \approx Y$.*

Důkaz: Podle předpokladu existuje vzájemně jednoznačná funkce $f : X \to Z$. Protože $Z \subseteq X$, existuje n-tá iterace funkce f. Položme

$$M = \{f^n(x) : \ x \in X \setminus Y, n \in \omega\} \subseteq (X \setminus Y) \cup Z$$

Definujme funkci $g : X \to Y$ předpisem

$$g(a) = \begin{cases} f(a) & \text{pokud} \quad a \in M \\ a & \text{pokud} \quad a \in X \setminus M \end{cases}$$

Ukážeme, že g je prostá funkce. Nechť $a, b \in X$, $a \neq b$.
Je-li $a, b \in X \setminus M$, je $g(a) = a \neq b = g(b)$.
Je-li $a, b \in M$, je $g(a) = f(a) \neq f(b) = g(b)$.
Je-li $a \in M$, $b \in X \setminus M$, je $g(a) = f(a) \in M$, a $g(b) = b \in X \setminus M$, takže

$g(a) \neq g(b)$.
Ukážeme $\mathcal{R}(g) = Y$. Je-li $a \in Y \setminus M$, je $a = g(a) \in \mathcal{R}(g)$. Je-li $a \in Y \cap M$, je $a = f^n(c)$ pro nějaké $n \in \omega$ a $c \in X \setminus Y$. Protože $a \neq c$, je $n > 0$, takže $a = g(f^{n-1}(c)) \in \mathcal{R}(g)$. $\square$

Věta 63 (Cantor-Bernsteinova věta) *Vztah subvalence $\preceq$ je antisymetrický*

$$X \preceq Y \;\&\; Y \preceq X \quad \rightarrow \quad X \approx Y$$

Důkaz: Nechť $f : X \rightarrow Y$ a $g : Y \rightarrow X$ jsou prostá zobrazení. Pak $g \circ f[X] \subseteq g[Y] \subseteq X$ a $X \approx g \circ f[X]$, takže, podle Cantor-Bersteinova lemma, $X \approx g[Y] \approx Y$. $\square$

5.2 Nespočetné množiny

Množina reálných čísel již spočetná není. Ukážeme si, že již jednotkový interval $[0,1] = \{x \in \mathbb{R} : \; 0 \leq x \leq 1\}$ není spočetný. Každé číslo $x \in [0,1]$ lze psát v binárním rozvoji $x = 0.x_0x_1x_2\ldots$, tj. existují binární číslice $x_i \in \{0,1\}$ tak, že x je nekonečný součet

$$x = \frac{x_0}{2} + \frac{x_1}{2^2} + \frac{x_2}{2^3} + \cdots$$

Tvrzení 64 *Jednotkový interval* $[0,1]$ *není spočetný.*

Předpokládejme sporem, že jednotkový interval je spočetný a nechť $a : \omega \rightarrow [0,1]$ je posloupnost všech čísel jednotkového intervalu. Pišme každé číslo a_i v binárním rozvoji

$$\begin{aligned} a_0 &= 0.a_{00}a_{01}a_{02}\ldots \\ a_1 &= 0.a_{10}a_{11}a_{12}\ldots \\ a_2 &= 0.a_{20}a_{21}a_{22}\ldots \end{aligned}$$

Sestrojme reálné číslo $b = 0.b_0b_1b_2\ldots$ předpisem $b_i = 1 - a_{ii}$. Protože $b_0 \neq a_{00}$, $b \neq a_0$. Protože $b_i \neq a_{ii}$, $b \neq a_i$. Číslo b se tedy v posloupnosti a nevyskytuje a to je spor.

Diagonální metodu použitou v tomto důkazu lze zobecnit. Ukážeme si obecně, že žádná množina není ekvivalentní své potenční množině.

Věta 65 *Pro každou množinu x je $x \preceq \mathcal{P}(x)$ ale $x \not\approx \mathcal{P}(x)$.*

Důkaz: Funkce $g = \{\langle y, \{y\}\rangle : \; y \in x\}$ je vzájemně jednoznačné zobrazení z x do $\mathcal{P}(x)$, takže $x \preceq \mathcal{P}(x)$.
Předpokládejme, že $f : x \rightarrow \mathcal{P}(x)$ je vzájemně jednoznačné surjektivní zobrazení. Definujme množinu $y = \{u \in x : \; u \notin f(u)\}$. Protože $y \subseteq x$, existuje $v \in x$, takové, že $y = f(v)$. Ale

$$v \in y \equiv v \notin f(v) = y \equiv v \notin y$$

a to je spor. □

Množina $\mathcal{P}(\omega)$ je tedy nekonečná a nespočetná množina. Říkáme, že má **mohutnost kontinua**. Množina $\mathcal{P}(\mathcal{P}(x))$ má ovšem ještě větší mohutnost než $\mathcal{P}(x)$. Vidíme že možných mohutností nekonečných množin je nekonečně mnoho. Nevíme však, zda v této hierarchii nekonečných mohutností nejsou některé mohutnosti přeskočeny, například zda existuje nespočetná množina reálných čísel, která má menší mohutnost než množina všech reálných čísel. Tento problém byl dlouhou dobu otevřený až jej v šedesátých letech vyřešil Leonard Cohen překvapujícím způsobem. Existenci takové množiny nelze z axiomů teorie množin ani dokázat ani vyvrátit. Existenci takové množiny lze přijmout jako nový axiom, stejně tak je ale možné přijmout jeho negaci.

5.3 Axiom výběru

Další žádoucí vlastnost v teorii množin je srovnatelnost množin podle mohutnosti. Platí pro každé dvě množiny x a y buď $x \preceq y$ nebo $y \preceq x$? Ze stávajících axiomů toto tvrzení neplyne. Je třeba přidat dva nové axiomy. První, axiom substituce, se týká vytváření nových množin jako obrazů množin při množinových operacích. Uvažujme formuli $\varphi(u,v)$ takovou, že platí $(\forall u)(\exists! v)\varphi(u,v)$. Formule φ reprezentuje množinovou operaci. Axiom substituce požaduje, aby obraz každé množiny při této operaci byl také množinou. Je formulován za slabšího předpokladu, že pro každé u existuje nejvýše jedno v, pro které $\varphi(u,v)$.

Axiom 10 (Schema axiomů substituce)

$$(\forall u,v,w)(\varphi(u,v)\ \&\ \varphi(u,w) \rightarrow v = w)\ \rightarrow\ (\forall x)(\exists y)(\forall v)(v \in y \equiv (\exists u \in x)\varphi(u,v))$$

Zde tedy můžeme chápat y jako obraz x při zobrazení φ.

Axiom výběru postuluje existenci funkce, která z neprázdných množin vybírá nějaké jejich prvky.

Definice 66 *Říkáme, že fukce f je selektor na množině x, pokud platí*

$$\mathbf{Sel}(f,x) \equiv \mathbf{Fnc}(f)\ \&\ \mathcal{D}(f) = x\ \&\ (\forall y \in x)(y \neq \emptyset\ \rightarrow\ f(y) \in y)$$

Funkce f je tedy selektor na x, pokud z každé neprázdné množiny $y \in x$ vybírá nějaký její prvek. Existence selektorů je intuitivně přijatelný princip, přesto však z dosavadních axiomů neplyne a přijmeme ho jako další axiom.

Axiom 11 (Axiom výběru) *Pro každou množinu existuje její selektor.*

$$(\forall x)(\exists f)\mathbf{Sel}(f,x)$$

Věta 67 *Pro každou množinu existuje s ní ekvivalentní ordinální číslo.*

$$(\forall x)(\exists y)(\mathbf{Ord}(y)\ \&\ x \approx y)$$

Idea důkazu spočívá v tom, že vybíráme z množiny x postupně jeden prvek za druhým a přiřazujeme je nejprve přirozeným a potom dalším ordinálním číslům. Axiom substituce zaručuje, že tento proces se na některém ordinálním čísle zastaví. Nechť F je selektor na množině $\mathcal{P}(x)$. Položme $f(0) = F(x)$, $f(1) = F(x \setminus \{f(0)\}) = F(x \setminus f[1])$ a pro každé přirozené číslo n

$$f(n) = F(x \setminus \{f(0), \ldots, f(n-1)\}) = F(x \setminus f[n])$$

Je-li x n-prvková množina, je $f[n] = x$, a f je vzájemně jednoznačné zobrazení $n \in \omega$ na x. Je-li x nekonečné, položíme také $f(\omega) = F(x \setminus f[\omega])$ a stejně pro všechna následující ordinální čísla, dokud množinu x nevyčerpáme. Ve formálním důkazu sestrojujeme množinu G funkcí, které jsou takto definovány na nějakém ordinálním čísle a požadovanou funkci f sestrojíme jako obecné sjednocení G.
Důkaz věty: Uvažujme formuli $\varphi(u, g)$

$$\begin{aligned}\varphi(u,g) \quad \equiv \quad & (\exists\alpha)(\mathbf{Ord}(\alpha) \mathbin{\&} \mathcal{D}(g) = \alpha + 1 \mathbin{\&} u = g(\alpha)) \mathbin{\&} \\ & (\forall\gamma \in \mathcal{D}(g))(g(\gamma) = F(x \setminus f[\gamma]))\end{aligned}$$

Ukážeme, že formule φ reprezentuje jednoznačnou funkci, tj.

$$\varphi(u,g) \mathbin{\&} \varphi(u,h) \rightarrow g = h$$

Nechť $\mathcal{D}(h) = \beta + 1$ a předpokládejme $\alpha \leq \beta$. Položme

$$\gamma = \min\{\delta \in \alpha + 1 : \; g(\delta) \neq h(\delta)\}$$

Pak $g[\gamma] = h[\gamma]$, takže $g(\gamma) = F(x \setminus g[\gamma]) = F(x \setminus h[\gamma]) = h(\gamma)$ a to je spor. Je tedy $u = g(\alpha) = h(\alpha)$, takže $\beta = \alpha$ a $g = h$. Za předpokladu $\beta \leq \alpha$ je důkaz obdobný. Podle axiomu nahrazení pro množinu x platí

$$(\exists G)(\forall g)(g \in G \equiv (\exists u \in x)\varphi(u,g))$$

Položme $f = \mathcal{U}(G)$. Zřejmě $\mathcal{D}(f)$ je ordinální číslo a pro každé $\gamma \in \mathcal{D}(f)$ je

$$f(\gamma) = F(x \setminus f[\gamma]) \in x \setminus f[\gamma]$$

takže f je prostá funkce. Předpokládejme sporem, že $\mathcal{R}(f) \subset x$. Pak $u = F(x \setminus \mathcal{R}(f)) \in x \setminus \mathcal{R}(f)$. Položíme-li $g = f \cup \{\langle \mathcal{D}(f), u \rangle\}$, je $g \in G$ a tedy $u \in \mathcal{R}(f)$ a to je spor. Obor hodnot funkce f je tedy celé x, takže f je vzájemně jednoznačná funkce z x na nějaké ordinální číslo. □

Věta 68 *Každé dvě množiny jsou srovnatelné.*

$$x \preceq y \;\vee\; y \preceq x$$

Důkaz: Existují ordinální čísla $\alpha \approx x$ a $\beta \approx y$ a buď $\alpha \subseteq \beta$ nebo $\beta \subseteq \alpha$. □

6 Historické poznámky

Logiku jako nauku o rozumovém myšlení založil Aristotelés (384 - 322 př.n.l.) Paradoxy logického myšlení odkryl Zénón Elejský (asi 490 - 430 př.n.l.). Systematickým vyhledáváním paradoxů se zabývala Megarská škola vedená Eukleidem z Megar (450-380 př.n.l. - odlišný od Eukleida Základů). Aristetolova logika zásadním způsobem ovlivninla antickou geometrii. Hledalo se odvození geometrie z prvních počátků, nabízelo se však více alternativ, jak tyto počátky vymezit. Systematickou stavbu antické geometrie zachytil Eukleidés (činný kolem roku 300 př.n.l.) ve svých Základech. Jsou založeny na axiomatické metodě. Některé evidentní geometrické poznatky se prohlásí za předpoklady - axiomy a postuláty - a ostatní se z nich odvozují logickou cestou.

V Eukleidově systému má speciální postavení jeho pátý postulát o rovnoběžkách. Je-li v rovině dána přímka a bid který leží mimo ni, axiom postuluje existenci jediné rovnoběžky s danou přímkou procházející daným bodem. Mnoho matematiků se snažilo dokázat pátý postulát z ostatních Eukleidových axiomů. Tyto snahy byly neúspěšné a v devatenáctém století se ukázalo, že to není možné. Existují alternativní neeukleidovské geometrie, ve kterých pátý postulát neplatí. Navzájem nezávisle je objevili Carl Friedrich Gauss (1777-1855), János Bolyai (1802-1860) a Nikolaj Ivanovič Lobačevskij (1793-1856). I oni se pokoušeli dokázat pátý postulát, dospěli však závěru, že to není možné, že je stejně dobře možné přijmout za axiom jeho negaci a nedospět přitom ke sporu. V Lobačevského geometrii lze vést daným bodem nekonečně mnoho rovnověžek s danou přímkou a součet úhlů v každém trojúhelníku je menší než dva pravé.

Možnost takové geometrie později potvrdil Eugenio Beltrami (1835 - 1900) konstrukcí jejího modelu. Geometrické termíny jako bod, úsečka, úhel nebo shodnost není nutno interpretovat tím způsobem, jaký známe z eukleidovské geometrie. Dáme-li jim jiný obsah a budou-li i nadále splněny všechny axiomy, budou v tomto novém světě platit i všechny dokázané věty. Beltramiho model neeukleidovské geometrie (planimetrie) je vnitřek nějakého kruhu v eukleidovské rovině. Za body a úsečky v novém smyslu se považují pouze vnitřní body a úsečky tohoto kruhu. Přitom se měření délek a úseček odlišuje od eukleidovského, takže z hlediska vnitřní geometrie se jedná o nekonečný prostor.

V Beltramiho modelu jsou splněny všechny Eukleidovy axiomy a postuláty kromě pátého. Speciálně lze každou úsečku prodloužit, každé dva body lze spojit úsečkou a kolem každého bodu lze daným poloměrem opsat kružnici (nebude to však eukleidovská kružnice). Pátý postulát však neplatí. Dvě úsečky jsou rovnoběžky, pokud se uvnitř kruhu neprotínají žádná jejich prodloužení; je tedy vidět, že ke každé úsečce lze každým mimo ni ležícím bodem vést nekonečně mnoho rovnoběžek.

Beltramiho model není jen o geometrii ale také o logice geometrie. Ukazuje, že negaci pátého postulátu nelze přivést ke sporu, že neeukleidovská geometrie je **bezesporná**, protože svět který popisuje vskutku existuje. Věříme-li v existenci eukleidovského světa, musíme připustit i možnost neeukleidovského světa.

Beltramiho model nám tedy ukazuje **nezávislost** pátého postulátu. Nelze ho z ostatních axiomů ani dokázat ani vyvrátit.

Logické základy geometrie a metodu modelů přivedl k dokonalosti koncem devatenáctého století David Hilbert (1862 - 1943). Hilbert doplnil nevyslovené Eukleidovy axiomy, pomocí modelů ukázal, že jeho axiomy jsou na sobě navzájem nezávislé, a uvažoval další varianty geometrií. Kladl si také otázku bezespornosti eukleidovské geometrie. Konstruuje její model založený na Descartově analytické metodě. Body reprezentuje jako dvojice reálných čísel (souřadnice) a přímky jako trojice reálných čísel (koeficienty jejich rovnic). Tento důkaz bezespornosti je však založen na předpokladu bezespornosti systému reálných čísel, a tím se otázka bezespornosti pouze přesunula jinam. V problému bezespornosti systému reálných čísel pak hraje kritickou roli problém nekonečna.

Studium nekonečna přineslo další impuls k rozvoji logiky. Antická matematika se nekonečnu vyhýbala. Aristotelés dokazuje, že žádná veličina nemůže být nekonečná, že v oblasti fyziky není nekonečno možné. V matematice připouští pouze potenciální nekonečno. Úsečky lze libovolně prodlužovat, ne však do nekonečna, úsečky lze dělit libovolně dlouho, ne však nekonečně mnohokrát. Řecká matematika, tak jak je prezentována v Eukleidových základech se bez aktuálního nekonečna obešla a tím se dokázala vyhnout mnoha paradoxům.

Do matematiky uvádí aktuální nekonečno až Bernard Bolzano (1781 - 1848) na základě teologických argumentů v knize 'Paradoxy nekonečna'. Bolzano odlišuje tento pojem aktuálně nekonečné množiny od nekonečně velikých infinitesimálního počtu a dokazuje, že existují množiny vskutku nekonečné, například množina všech pravd.

Systematicky rozvinul teorii nekonečných množin Georg Cantor (1845 - 1918). K této problematice se Cantor dostal při zkoumání algebraických čísel roku 1874. Cantor dokazuje, že algebraická čísla, tj. čísla která splňují algebraickou rovnici s celočíselnými koeficienty, lze vzájemně jednoznačně přiřadit přirozeným číslům, to znamená, že je lze seřadit do nekonečné posloupnosti, která je všechny obsahuje. Naproti tomu ale neexistuje posloupnost všech reálných čísel. V každé posloupnosti reálných čísel se některá reálná čísla nevyskytují. Z toho Cantor nově dokazuje, že transcendentální (nealgebraická) čísla existují, a že je jich dokonce nekonečně mnoho v každém intervalu. Pro rozvoj teorie množin byl právě tento důkaz klíčový. Ukazuje totiž, že existují dvě nekonečné množiny, které co do množství nejsou stejné: množina přirozených a množina reálných čísel.

V devatenáctém století se také rozvinula samotná logika díky formálním, algebraickým metodám. Formální přístup je typický pro arabskou matematiku. Zatímco řecká matematika byla založena na náhledu do světa idejí, arabská matematika přináší možnost získávat nové výsledky formální manipulací symbolů. V řecké matematice jsou přirozená čísla chápána jako geometrické veličiny a operace s nimi jako operace geometrické. Vyjádření čísla znakem nebylo podstatné. Naproti tomu arabská matematika propracovává babylónský vynález zápisu čísel v pozičním systému a na něm založené algoritmy sčítání a násobení. Postupujeme-li podle algoritmu, vzdáváme se náhledu. Jednotlivé kroky algoritmu provádíme slepě a mechanicky, jsme-li však pečliví, můžeme se spolehnout na správnost výsledku. Do jisté míry se zde náhled na čísla nahrazuje náhledem na algoritmus.

Snaha o formální vyjádření logiky se objevuje již u středověkých dialektiků např. Petra Abelarda (1079 - 1142), v extrémní formě pak u Raimunda Lulla (1235-1315), který se pokusil o vybudování formalizovaného systému teologie a filosofie. Zkonstruoval dokonce mechanismus, který pomocí otáčivých kol ukazuje formální výsledky sylogistické dedukce. Také Gottfried Wilhem Leibniz (1646-1716) uvažoval "...o abecedě lidského myšlení, ve které by se dalo vyjádřit všechno myslitelné vhodnými kombinacemi a kterou by se myšlení redukovalo na kvazimechanickou operaci procházení seznamů."

Algebraický přístup k logice zavedl George Boole (1815-1864), který definuje **logické operace** (konjunkce, disjunkce, implikace, negace) a ukazuje, že tyto operace splňují určité algebraické zákonitosti analogicky jako v algebře operace číselné.

Formální systém logiky vybudoval Gottlob Frege (1848 - 1925). Frege byl veden snahou vytvořit umělý logický jazyk, který by umožnil vyjádřit všechna matematická fakta bez nepřesností a nejednoznačností jazyka přirozeného. Frege použil Booleovu analýzu logických operací a axiomatický přístup. Jeho největší přínos je však v zavedení predikátů a kvantifikátorů. Tento systém je popsán ve Fregeho spisu 'Begriffsschrift' z roku 1879 a odpovídá dnešnímu predikátovému počtu. Ve Fregeho době nebyla ještě rozpracována axiomatika teorie množin a Frege proto svůj systém dále rozšiřoval a zobecňoval. Roku 1893 publikuje první díl 'Grundgesetze der Arithmetik' a roku 1903 jejich druhý díl, zabývající se teorií reálných čísel. K tomu účelu zavádí proměnné predikáty, které jsou ekvivalentní množinám. (Frege obdivoval Cantorovu teorii množin a obhajoval jí proti jejím kritikům.) Tím se však jeho systém otevírá všem paradoxům teorie množin a Bertrand Russell (1872 -1970) formuloval svůj paradox množiny těch množin, které neobsahují sebe sama, právě v rámci Fregeho systému.

Východisko z této krize základů matematiky hledal David Hilbert v důsledné formalizaci matematiky. Formální pojetí matematiky bylo umožněno objevem neeukleidovských geometrií a jejích modelů. Pojmy přímka a bod nemusí mít jeden jediný význam. Lze jim dát i jiné významy a přitom zůstanou splněny všechny axiomy eukleidovské nebo neeukleidovské geometrie, a tedy i všechny věty z nich odvozené. Toto pojetí rozpracoval Hilbert v díle 'Grundlagen der Geometrie' roku 1898. Hilbert zcela abstrahuje od významu geometrických pojmů a zabývá se pouze jejich logickými vztahy. Říká výslovně, že

> '... musí být možné místo o bodu, přímce a rovině mluvit o stolu, židli a půllitru.' (Grundlagen der Geometrie, [11])

Tím překračuje pojetí Fregeho, který svým predikátovým počtem mluví ještě o zcela určitých matematických objektech. V další fázi po roce 1902 Hilbert reaguje na paradoxy teorie množin. Prosazuje zcela formální pojetí matematiky, abstrahuje nejen od významu primitivních pojmů a vztahů, ale i od významu logických operací. Matematické důkazy a věty se stanou pouhými řetězci symbolů a jejich dokazatelnost závisí jen na tom jakými jsou řetězci, nezávisle na subjektivních soudech matematiků. Navazuje tak na Leibnizův sen mechanického a úplného systému všeho vědění.

Znaky, řetězce a výrazy, na kterých jsou formální systémy založeny, jsou však opět matematické povahy. Tím se ocitáme v logickém kruhu. K vybudování logických základů matematiky potřebujeme znát matematické vlastnosti řetězců a tedy také vlastnosti přirozených čísel. Vystavujeme se tak nebezpečí, že paradoxy nekonečné matematiky se projeví i při budování logického kalkulu. Hilbert tomuto nebezpečí čelí důsledným omezováním se na finitní (konečné) metody. Základy matematiky by měly být vybudovány jen na vlastnostech konečných řetězců.

Je sice možné uvažovat modely formálních teorií, tj. struktury se vztahy, které splňují axiomy teorie, takových struktur však může být více, a jejich znalost není nutným předpokladem k rozvíjení teorie. V tomto pojetí se však stává kritickým problém **bezespornosti**. Teorie je jistě bezesporná, pokud má konečný model, tj. model který lze celý přehlédnout. Není-li tomu tak, zbývá jedině možnost ukázat, že spor nelze obdržet formálními manipulacemi symbolů.

Kromě bezespornosti se nabízejí další žádoucí vlastnosti formálních systémů, a sice **úplnost a rozhodnutelnost**. Formální systém je úplný, jestliže každá sentence (formule bez volných proměnných) buďto je dokazatelná nebo je dokazatelná její negace. Požadujeme-li úplnost, činíme si nárok na úplné poznání nějaké matematické oblasti. Chceme, aby každý matematický problém byl řešitelný. Stejně jako bezespornost, považoval Hilbert i požadavek úplnosti za samozřejmý. Konečně formální matematické systémy nabízí nejslibnější možnost - automatizaci matematických důkazů. Je-li formule a důkaz pouze posloupnost znaků, lze hledat algoritmus, který by pro každou formuli rozhodnoval, zda je dokazatelná, stejně jako algoritmus násobení násobí dvě čísla pouze na základě jejich zápisu. Záměr vybudovat matematiku na formálním logickém systému, který by byl bezesporný, úplný a rozhodnutelný, se označuje jako **Hilbertův program** a Hilbert se mu se svými spolupracovníky věnoval mnoho let.

Rozpracováním Fregeho predikátového počtu se vskutku podařilo sestrojit solidní základy matematiky. Klíčové místo v této struktuře zaujímá teorie množin, ani ne tak pro zachycení pojmu nekonečna, jako pro bohatství vztahů, které lze v teorii množin najít. Axiomatickou teorii množin vypracoval Ernst Zermelo (1871-1953). Později Zermelův axiomatický systém doplnil Adam Abraham Fraenkl (1891-1965) zejména o axiom substituce. Proto se tento axiomatický systém teorie množin nazývá Zermelo-Fraenkelův. Alternativní systém teorie množin vypracovali Kurt Gödel (1906 - 1978) a Paul Bernays. V Gödel-Bernaysově systému vystupují dva druhy objektů - množiny a třídy. Třídy jsou velké soubory množin (jako například třída všech množin), které nemohou být prvky množin ani tříd. To je alternativní řešení Russellova paradoxu. Do teorie množin lze vnořit téměř každou matematickou oblast tak, že každý matematický objekt se reprezentuje nějakou množinou. Logické základy současné matematiky tak spočívají na teorii množin.

Přes tento výrazný úspěch formální metody je ale Hilbertův program nedosažitelný. Jak ukázal Kurt Gödel, zajímavé matematické teorie nejsou ani úplné ani rozhodnutelné, a pokud jsou bezesporné, není možné to o nich dokázat. Formální logika a teorie množin tak matematice poskytují rozumně spolehlivé základy, nikoliv však úplnou jistotu.

Literatura

[1] Aristoteles: První Analytiky. Nakladatelství ČSAV, Praha 1961.

[2] Aristoteles: Druhé Analytiky. Nakladatelství ČSAV, Praha 1962.

[3] Bohuslav Balcar, Petr Štěpánek: Teorie množin, skripta MFF UK, SPN Praha 1974.

[4] Bohuslav Balcar, Petr Štěpánek: Teorie množin, Academia, Praha 1986.

[5] J.Blažek, B.Vojtášková: Teorie množin. skripta PF UJEP, Ústí nad Labem 1994.

[6] Bernard Bolzano: Paradoxy nekonečna. NČSAV, Praha 1963.

[7] Georg Cantor: Gesammelte Abhandlungen. Springer, Berlin 1932.

[8] Eukleides: Základy. JČMF, Praha 1907.

[9] Paul R.Halmos: Naive set theory. D. Van Nostrand Company, Princeton 1960.

[10] Thomas Heath: A History of Greek Mathematics. Oxford University Press, Oxford 1921.

[11] David Hilbert: Grundlagen der Geometrie. B.G.Teubner, Leipzig 1898, 1923.

[12] David Hilbert, Paul Bernays: Grundlagen der Mathematik I. Springer, Heidelberg 1934, 1968.

[13] Jean van Heijenoort: From Frege to Gödel. A Source Book of Mathematical Logic 1879-1931. Harvard Univ. Press, Cambridge 1967.

[14] William Kneale, Martha Kneale: The Development of Logic. Oxford University Press, Oxford 1962.

[15] Elliot Mendelson: Introduction to Mathematical Logic. van Nostrand, Princeton 1964.

[16] Joseph R. Shoenfield: Mathematical Logic. Addison-Wesley, Reading 1967.

[17] Patrick Suppes: Axiomatic set theory. D. Van Nostrand Company, Princeton 1960.

[18] Petr Štěpánek: Matematická logika. Skripta MFF UK, SPN, Praha 1982.

[19] P.Vopěnka, J.Blažek, B.Kussová: Množiny a přirozená čísla, SPN, Praha 1977.

[20] P.Vopěnka: Úhelný kámen evropské vzdělanosti a moci. PRÁH, Praha 2000.

Obsah