Matematický ústav Slezské univerzity v Opavě
Logika a teorie množin
M. Marvan

LOGIKA A TEORIE MNOŽIN

1. Místo úvodu

Tento text je určen posluchačům navštěvujícím přednášku *Logika a teorie množin.* Ve shodě s autorovými preferencemi pojednává zejména o Kelley–Morseově teorii s axiómem výběru a axiomem regularity, méně už o logice. Některé partie jsou prozatímně nahrazeny odkazem na knihu T. Šalát a J. Smítal, *Teória množín*, což v textu označujeme odkazem [TM, n_1–n_2], kde n_1, n_2 jsou čísla stránek, na nichž je příslušná partie vyložena v uvedené knize.

2. Úvod

Teorie množin a matematická logika jsou dvě vzájemně provázané matematické disciplíny. Obě leží v základech moderní matematiky. Jako součásti matematiky obě vznikly v 19. století.

Matematická logika je výsledkem snahy formalizovat proces matematického uvažování. Vytváří a používá jazyk, v němž lze formulovat matematická tvrzení i jejich důkazy. Pojednává obecně o axiomatických teoriích, důkazových metodách, dokazatelnosti, bezespornosti apod. Je nástrojem k rozhodování o pravdivosti v matematice.

Mezi zakladatele náleží Gottlob Frege (1848–1925). Ve spisu *Begriffsschrift* (1879) si položil za cíl odhalit všechny logické principy matematických důkazů. Každý i intuitivně zřejmý krok bylo třeba rozpoznat a popsat jako axiom. V důsledku se aritmetika měla stát částí logiky. Vděčíme mu za zavedení kvantifikátorů $\forall$, $\exists$. Na Fregeho navázali Giuseppe Peano (1858–1932), Bertrand Russel (1872–1970) a další.

Teorie množin je speciální axiomatická teorie, jež dnes leží v základech prakticky všech ostatních matematických disciplín. Její prvotní podobu vytvořil německý matematik Georg Cantor (1845–1918). Významným předchůdcem byl Bernard Bolzano (1781–1848), autor knihy *Paradoxy nekonečna* (1851).

2.1. Naivní teorie množin

Za zakládající publikaci teorie množin lze považovat Cantorův článek z roku 1874, v němž dokazuje existenci nekonečně mnoha transcendentních čísel (v jeho době byla známa pouze dvě transcendentní čísla, e a π). Od počátku byla teorie množin přijímána jako poněkud kontroverzní (odmítali ji např. Kronecker, Brouwer, Poincaré).

K vymezení všech pojmů Cantor používá přirozeného jazyka, jeho dílo neobsahuje žádnou definici množiny. Takto neformálně budovaná teorie se dnes nazývá *naivní teorie množin.* Cantor ji propracoval do značné hloubky; v ohnisku jeho zájmu ležel pojem *mohutnost* množiny. Množiny mají stejnou mohutnost, existuje-li mezi nimi bijekce.

Jakmile Cantor mezi množiny zahrnul i souhrn $\mathfrak{M}$ všech možných mohutností, vyvstal paradox. Ukázalo se, že samotná množina $\mathfrak{M}$ by nutně měla ještě větší mohutnost, neobsaženou v $\mathfrak{M}$. O dva roky dříve, v roce 1887, Burali-Forti objevil podobný paradox v Cantorově teorii ordinálních čísel.

Na Cantora navázal Frege dvousvazkovým dílem *Základní zákony aritmetiky* (*Grundgesetze der Arithmetik*) (1893, 1903). Pátý základní zákon se, v moderním označení, týkal množiny

$$M_\phi = \{X \mid \phi(X)\}$$

všech X, pro něž platí nějaká podmínka $\phi(X)$. Shodou okolností těsně před vydáním druhého svazku Bertrand Russel upozornil na paradox, vznikající ve speciálním případě

$$N = \{X \mid X \notin X\}.$$

Russelův paradox spočívá v tom, že obě možnosti $N \in N$ i $N \notin N$ vedou ke sporu. Vskutku, jestliže $N \in N$, pak musí platit podmínka $N \notin N$. A naopak, jestliže $N \notin N$, pak nesmí platit podmínka $N \notin N$. Jelikož naivní pokusy o vybudování teorie množin nevedly ke zdaru, byla posléze vybudována jako axiomatická teorie.

2.2. Logické paradoxy

Od antických dob jsou známy příklady logických úvah vedoucích k paradoxním závěrům. Výskyt paradoxů v základech matematiky je krajně nežádoucí.

Příklad. Epimenidův paradox. V moderní verzi je obsažen v tvrzení "Tento výrok je nepravdivý." Epimenidés, sám Kréťan, pravil, že Kréťané [za všech okolností] lžou. Paradox nastává, snažíme-li se zjistit, zda je Epimenidův výrok pravdivý.

V Epimenidově paradoxu snadno spatříme logický kruh, protože věta vypovídá o své vlastní (ne)pravdivosti.

Příklad. Holičův paradox. Holič obdržel rozkaz holit všechny muže, kteří se neholí sami. Má holit sám sebe? Tímto způsobem Russel popularizoval svůj paradox zmíněný výše.

Příklad. Grelling–Nelsonův paradox. Rozdělme přídavná jména středního rodu na heterologická a homologická. Přídavné jméno nechť je *homologické*, má-li za všech okolností vlastnost, kterou samo popisuje (například přídavná jména *české, čtyřslabičné, pětislabičné, sedmnáctipísmenné, devatenáctipísmenné* jsou homologická); nechť je *heterologické* v opačném případě. Paradox se vyjeví, pokusíme-li se určit, jaké je přídavné jméno *heterologické*.

Příklad. Berryho paradox. Méně než deseti slovy lze určit jen konečně mnoho čísel. Proto existují čísla, která nelze určit méně než deseti slovy. Nicméně, každá neprázdná podmnožina množiny přirozených čísel má nejmenší prvek. Proto existuje "nejmenší číslo, které nelze určit méně než deseti slovy." Zde vzniká paradox, protože zmíněné číslo je určeno větou o devíti slovech.

Následující příklad ukazuje, že následky může mít logický paradox i v reálném světě.

Příklad. Arbitrův paradox. Dvě společnosti uzavřely smlouvu, v níž se mimo jiné dohodly, že v případě sporu se místo k soudu obrátí na arbitra, který jejich spor rozhodne. Jedna ze společností poté předložila nezpochybnitelné důkazy, že smlouva je od počátku neplatná. Pokud arbitr uzná, že smlouva je od počátku neplatná, pozbude práva spor rozhodnout. Pokud arbitr uzná platnost smlouvy a spor rozhodne, vzhledem k předloženým důkazům platnost smlouvy uznat nemůže.

O logických paradoxech lze všeobecně říci, že vznikají, protože se nějaké výroky uplatňují šířeji, než bylo původně předvídáno a zamýšleno a nakonec vedou k nějaké formě logického kruhu. U lingvistických paradoxů vidíme i směšování jazyka jímž mluvíme s jazykem o němž mluvíme.

3. Axiomatická teorie množin a tříd

V rámci naivní teorie množin vznikl Russelův paradox ohledně definice

$$N = \{X \mid X \notin X\}.$$

Obecně se můžeme ptát, zda lze korektně definovat soubor

$$M_\phi = \{X \mid \phi(X)\}$$

všech množin X, majících nějakou vlastnost $\phi(X)$ a zda je M_ϕ potom množina. Zdá se, že neexistuje žádný jednoduchý způsob, jak rozeznat přípustné vlastnosti $\phi(X)$ od nepřípustných. Východiskem je vybudování axiomatické teorie množin, k čemuž bylo učiněno mnoho pokusů.

Historicky první Zermelo–Fraenkelova teorie (zkráceně **ZF**) vzniku Russelova paradoxu zabraňuje tím, že nepovažuje zápis $N = \{X \mid X \notin X\}$ za korektní definici množiny. V rámci **ZF** N *není* množina; otázka co N *je* zůstává nezodpovězena. V důsledku potom není množinou ani soubor všech množin, načež není množinou ani soubor všech grup, všech topologických prostorů a podobných struktur. Nicméně, i takové soubory mohou být a bývají předmětem matematických úvah, například v teorii kategorií a na ni navazující algebraické topologii. Proto je žádoucí i těmto "nemnožinovým" souborům poskytnout místo v budované teorii.

Ukazuje se, že soubor $\{X \mid \phi(X)\}$ všech množin X s vlastností $\phi(X)$ sám o sobě k paradoxům nevede. Obecně však není množinou, nýbrž je příkladem tak zvané *třídy.* Třídy přirozeně vznikají i v teorii množin samotné (máme třídu všech množin, třídu všech kardinálních čísel, třídu všech ordinálních čísel, které nejsou množinami). Axiomatizujeme-li jen množiny, je za jejich hranicí naprostá terra incognita, axiomatizujeme-li třídy, je tam něco, s čím se dá pracovat.

Třídy jsou axiomatizovány kupříkladu v Gödel—Bernays–von Neumannově teorii a Kelley–Morseově teorii. Rozdíl mezi oběma posledně jmenovanými tkví v tom, že druhá je o něco odvážnější (bude upřesněno níže). Kelley teorii tříd uveřejnil v dodatku ke knize *Obecná topologie* (*General topology*) z roku 1957. S nepodstatnými odchylkami budeme níže budovat právě Kelley–Morseovu teorii.

Při výkladu se budeme snažit, aby čtenář na konci chápal "co si lze dovolit s třídami" a "co si lze dovolit s množinami." Zdůrazněme, že množina je speciální případ třídy.

3.1. Formule

Jazyk teorie tříd používá následující symboly:

1. Symbol $\in$. Čte se "je prvkem" nebo "náleží do" nebo "patří do."
2. Symboly proměnných, což jsou malá i velká písmena latinské abecedy, případně i další symboly kromě symbolů uvedených v bodech 1, 3, 4, 5.
3. Logické spojky $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$.
4. Kvantifikátory $\forall, \exists$.
5. Závorky (,).

Například, x, X, y_1, U_2 jsou symboly proměnných. Označují třídy (a tedy i množiny jako speciální případ tříd). Nadbytečné závorky můžeme vynechat. Postupně budeme některé další užitečné symboly přidávat, např. $=$, $\notin$, $\cap$, $\cup$, $\{$, $\}$, $\emptyset$, 0, 1, 2, 3.

Dále budeme induktivně definovat formule teorie tříd, zkráceně *formule.* Všechny formule budou neprázdné konečné posloupnosti symbolů jazyka teorie tříd. Ne všechny posloupnosti budou formule, protože ne všechny posloupnosti dávají smysl v teorii tříd. Například posloupnost $x \in y$ dává smysl a bude formulí, zatímco $\in x \in$ a $x\forall\exists$ nikoliv.

Současně budeme definovat, které proměnné, vyskytující se ve formuli, jsou *volné* a které jsou *vázané* (každá bude buď volná anebo vázaná, nikoliv obojí). Pravdivost formule bude záležet na hodnotách volných proměnných. Vázané proměnné zase bude možné přejmenovat, podobně jako smíme přejmenovat sčítací index nebo integrační proměnnou.

Samotné formule budeme označovat písmeny řecké abecedy. Naše induktivní definice obsahuje čtyři pravidla $\mathbf{F}_1$ až $\mathbf{F}_4$, která postupně uvedeme. Formulí bude každá posloupnost, která vznikne jako výsledek konečného počtu kroků, spočívajících v uplatnění některého z pravidel $\mathbf{F}_1$ až $\mathbf{F}_4$.

$\mathbf{F}_1$ Každá posloupnost $X \in Y$, kde X, Y jsou proměnné, je formule. Obě proměnné X, Y jsou volné.

Formule zavedená pravidlem $\mathbf{F}_1$ se nazývá *atomická formule*. Jiné atomické formule nezavedeme.

$\mathbf{F}_2$ Je-li ϕ formule, pak i $\neg(\phi)$ je formule. Vázané a volné proměnné jsou u $\neg(\phi)$ tytéž jako u ϕ.

Příklad. Příkladem formule vzniklé podle pravidla $\mathbf{F}_2$ je formule $\neg(X \in Y)$. Obvykle ji zkracujeme na $X \notin Y$. Obě proměnné X, Y jsou volné.

$\mathbf{F}_3$ Je-li ϕ formule a x její volná proměnná, pak $(\forall x)(\phi)$ resp. $(\exists x)(\phi)$ jsou formule. Proměnná x je v obou formulích $(\forall x)(\phi)$ a $(\exists x)(\phi)$ vázaná, ostatní proměnné jsou volné nebo vázané podle toho, zda jsou volné nebo vázané ve formuli ϕ.

Čteme "pro každé x" resp. "existuje x." Uplatněním pravidla $\mathbf{F}_3$ jsme proměnnou x takzvaně *kvantifikovali*, přestala být volnou proměnnou a stala se vázanou.

Příklad. Příkladem formule vzniklé podle pravidla $\mathbf{F}_3$ je

$$(\exists x)\,(x \in X).$$

Ve výchozí atomické formuli $x \in X$ byly obě proměnné volné, ve výsledné formuli je x vázaná a X volná. Smysl formule $(\exists x)\, x \in X$ je, že X je neprázdná.

3.1. Poznámky. 1. Závorky lze vynechávat, pokud to neohrožuje srozumitelnost. Například, pravidlo $\mathbf{F}_3$ vyžaduje, abychom psali $(\exists x)((\exists X)(x \in X))$, ale množství závorek ke srozumitelnosti nepřispívá. Dostatečně srozumitelné jsou i zápisy $(\exists x)(\exists X)(x \in X)$ nebo dokonce $\exists x\, \exists X\, x \in X$ úplně bez závorek. V tomto textu se pokusíme zachovávat rozumné množství závorek, abychom dosáhli dobré srozumitelnosti i bez zavedení explicitních pravidel pro čtení (bez zavedení precedence operací).

2. Lze připustit i vázání proměnných, které se ve formuli vůbec nevyskytují, ale takový kvantifikátor je zbytečný.

Abychom se mohli spolehnout, že proměnná je buď vázáná anebo volná, ale ne obojí, zavedeme slučitelnost formulí.

3.2. Definice. Říkáme, že formule ϕ, ψ jsou *slučitelné*, jestliže každá proměnná, která se vyskytuje v obou formulích, je buď v obou vázaná nebo v obou volná.

$\mathbf{F}_4$ Jsou-li ϕ, ψ slučitelné formule, pak

$$(\phi) \wedge (\psi), \quad (\phi) \vee (\psi), \quad (\phi) \Rightarrow (\psi), \quad (\phi) \Leftrightarrow (\psi)$$

jsou formule; nazývají se *složené* formule. Proměnná je volná resp. vázaná ve složené formuli, je-li volná resp. vázaná v alespoň jedné z formulí ϕ, ψ.

Příklad. Formule $\phi = (\exists x)\, x \in y$ a $\psi = x \in z$ jsou neslučitelné, protože x je jednou vázaná a jednou volná. Zbývající proměnné y, z se vyskytují každá jen v jedné z formulí, a proto nemají na slučitelnost vliv. Potom

$$\phi \wedge \psi = ((\exists x)\, x \in y) \wedge (x \in z)$$

není formule.

3.3. Tvrzení. *Vyskytuje-li se proměnná X ve formuli ϕ, pak je v ní buď volná anebo vázaná, ale nikoliv obojí.*

Důkaz. Tvrzení platí pro atomické formule, neboť v těch se vyskytují pouze volné proměnné. Platí-li tvrzení pro formuli ϕ, platí i pro $\neg\phi$, protože volné a vázané proměnné jsou u obou stejné. Platí-li tvrzení pro formuli ϕ s volnou proměnnou X, platí i pro $(\forall x)(\phi)$ resp. $(\exists x)(\phi)$, protože volné a vázané proměnné jsou u obou stejné, s výjimkou X, která se změnila z volné na vázanou. Platí-li tvrzení pro každou ze slučitelných formulí ϕ, ψ, neexistuje proměnná, která by byla volná v jedné a vázaná v druhé, a proto tvrzení platí i pro složené formule $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \Rightarrow \psi$, $\phi \Leftrightarrow \psi$.

Nejsou-li dvě formule slučitelné, pak libovolnou společnou proměnnou, která je vázaná jen v jedné z formulí, můžeme přejmenovat, tj. označit jiným symbolem tak, aby se nový symbol v druhé formuli nevyskytoval. Takto si lze slučitelnost vždy vynutit. Později ukážeme, že takové přejmenování nemá vliv na pravdivost formule.

Příklad. Uvažujme opět o neslučitelných formulích $\phi = (\exists x)\, x \in y$ a $\psi = x \in z$. Pokud ve formuli ϕ zaměníme x například za u, takže $\phi = (\exists u)\, u \in y$, budou obě formule slučitelné a

$$\phi \wedge \psi = ((\exists u)\, u \in y) \wedge (x \in z)$$

bude formule.

Pro názornost se někdy za symbolem formule uvádějí v závorkách všechny její volné proměnné.

Příklad. Formuli $(\exists x)\, x \in y$ můžeme označit např. ϕ nebo, pro názornost, $\phi(y)$, ale nikoliv $\phi(x, y)$ ani $\phi(y, z)$.

3.2. Pravdivost formulí

Přejděme k otázce pravdivosti formulí ve smyslu klasické logiky se dvěma pravdivostními hodnotami 1 (formule je pravdivá, formule platí) a 0 (formule je nepravdivá, formule neplatí).

O pravdivosti formulí budeme rozhodovat na základě pravdivosti jejich podformulí pomocí pravidel $\mathbf{P}_1$ až $\mathbf{P}_4$, odpovídajících pravidlům $\mathbf{F}_1$ až $\mathbf{F}_4$ pro konstrukci formulí teorie tříd.

- $\mathbf{P}_2$ Formule $\neg\phi$ je pravdivá právě tehdy, když ϕ je nepravdivá.
- $\mathbf{P}_3$ Formule $(\forall x)\, \phi(x)$ je pravdivá právě tehdy, když $\phi(x)$ platí pro všechna x; formule $(\exists x)\, \phi(x)$ je pravdivá právě tehdy, když existuje x takové, že platí $\phi(x)$.
- $\mathbf{P}_4$ Pravdivost formulí $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \Rightarrow \psi$, $\phi \Leftrightarrow \psi$ v závislosti na pravdivosti formulí ϕ, ψ je dána známou tabulkou:

ϕ	ψ	$\phi \wedge \psi$	$\phi \vee \psi$	$\phi \Rightarrow \psi$	$\phi \Leftrightarrow \psi$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Chybějící pravidlo $\mathbf{P}_1$, umožňující posoudit pravdivost atomických formulí, uvedeme později. Kdybychom je mohli uvést již teď, nebylo by třeba budovat axiomatickou teorii, neboť bychom již teď mohli rozhodnout o pravdivosti všech formulí.

Všimněme si, že $\phi \Leftrightarrow \psi$ platí právě tehdy, když mají ϕ a ψ stejné pravdivostní hodnoty. Formule ϕ a ψ jsou pak co do pravdivosti a nepravdivosti zaměnitelné. Řekneme, že formule ϕ, ψ jsou *logicky ekvivalentní*.

V tomto textu budeme logickou ekvivalenci formulí ϕ, ψ vždy vypisovat slovy '$\phi \Leftrightarrow \psi$ platí'. Někdy se k zápisu logické ekvivalence používá symbol '$\equiv$'. Má vlastnost reflexivity ($\phi \equiv \phi$ pro každou formuli ϕ), symetrie (jestliže $\phi \equiv \psi$, pak $\psi \equiv \phi$) a tranzitivity (jestiže $\phi \equiv \psi$ a $\psi \equiv \chi$, pak $\phi \equiv \chi$). Zdůrazněme však, že $\phi \equiv \psi$ není formule teorie tříd (nesmíme směšovat jazyk, kterým mluvíme, s jazykem, o kterém mluvíme).

Formule bez volných proměnných má jednoznačně určenu pravdivostní hodnotu 1 nebo 0; před zjišťováním pravdivostní hodnoty formule s volnými proměnnými je nutno za volné proměnné zvolit nějaké konkrétní třídy.

Nyní již máme shromážděny základní rekvizity pro budování axiomatické teorie tříd. Dále budeme systematicky uvádět jeden axiom za druhým a mezitím zavádět další pomocné pojmy. Kdybychom vypsali všechny axiomy naráz, aniž bychom měli pomocné pojmy k dispozici, byly by velmi komplikované a zcela nesrozumitelné.

Pro jistotu uveďme, že axiomy jsou pokládány za pravdivé formule. Další pravdivé formule (platná tvrzení) z nich odvozujeme pomocí pravidel $\mathbf{P}_2$ až $\mathbf{P}_4$ a dalších standardních důkazových postupů, o nichž předpokládáme, že jsou dostatečně známy a proto je podrobně nevypisujeme. Již dříve jsme v jednom příkladu zavedli symbol $\notin$ tak, aby formule $X \notin Y$ měla stejný smysl jako $\neg(X \in Y)$. Ať za X, Y dosadíme cokoliv, vždy budou mít $X \notin Y$ a $\neg(X \in Y)$ stejnou pravdivostní hodnotu. Vidíme, že $X \notin Y$ a $\neg(X \in Y)$ jsou logicky ekvivalentní.

Zdůrazněme, že $X \notin Y$ není atomická formule, ačkoliv tak na první pohled vypadá. Je to jen stručný zápis pro neatomickou formuli $\neg(X \in Y)$. Pravdivostní hodnota formule $X \notin Y$ je zcela jednoznačně odvoditelná z pravdivostní hodnoty atomické formule $X \in Y$. Další podobné stručné zápisy zavedeme níže.

3.3. Množiny

V axiomatické teorii tříd můžeme a budeme množiny *definovat.*

3.4. Definice. Třída X je *množina*, jestliže existuje třída Y taková, že $X \in Y$. Zapisujeme $X \underline{\in \mathcal{U}}$. Třída, která není množinou, se nazývá *vlastní třída.*

Podtržením zdůrazňujeme, že $\underline{\in \mathcal{U}}$ je (prozatím) nedílný symbol. Brzy zavedeme třídu $\mathcal{U}$ všech množin, přičemž $X \in \mathcal{U}$ a $X \underline{\in \mathcal{U}}$ bude znamenat totéž a podtržení se stane zbytečným.

3.4. Rovnost tříd

Zavedeme ještě jedno označení. Řekneme, že dvě třídy jsou si rovny a zapisujeme $X = Y$, jestliže mají stejné prvky. Zde je formální definice:

3.5. Definice. Třídy X, Y jsou si *rovny*, jestliže platí

$$(\forall U)\,(U \in X \Leftrightarrow U \in Y).$$

Zapisujeme $X = Y$.

V předchozím textu už jsme symbol '$=$' několikrát použili ve smyslu obecné rovnosti či totožnosti formulí nebo tříd. Pro třídy jsme teď zavedli rovnost jako označení pro fakt, že mají stejné prvky, což není ve sporu s dřívějším použitím. Pro formule zůstaneme u neformální definice rovnosti jako totožnosti. Je zřejmé, že totožné formule jsou logicky ekvivalentní, ale ne naopak.

Všimněme si, že je-li U vlastní třída, pak rozhodně neplatí ani $U \in X$ ani $U \in Y$, takže ekvivalence $U \in X \Leftrightarrow U \in Y$ je pravdivá pro všechny vlastní třídy U. Stačí tedy posuzovat ekvivalenci $U \in X \Leftrightarrow U \in Y$ pouze v případě, že U je množina.

Fakticky je "$=$" relace mezi třídami, o níž lze snadno ukázat, že je reflexivní, symetrická a tranzitivní.

Cvičení. Ukažte, že platí

$$(\forall X)\, X = X,$$

$$(\forall X)(\forall Y)\,(X = Y \Rightarrow Y = X),$$

$$(\forall X)(\forall Y)(\forall Z)\,((X = Y \wedge Y = Z) \Rightarrow X = Z).$$

Nápověda: Dokažme první tvrzení. To je ekvivalentní pravdivosti formule

$$(\forall X)(\forall U)\,(U \in X) \Leftrightarrow (U \in X).$$

Jelikož $(U \in X) \Leftrightarrow (U \in X)$ platí pro libovolnou pravdivostní hodnotu atomické formule $U \in X$, je první tvrzení dokázáno.

Podle definice rovnosti tříd má $X = Y$ za následek $U \in X \Leftrightarrow U \in Y$ pro každé U. Odnikud však nevyplývá, že by $X = Y$ mělo za následek i $X \in V \Leftrightarrow Y \in V$ pro každé V. To je nutno postulovat, přičemž tak samozřejmě stačí učinit pro implikaci.

A. Axiom invariance. Platí

$$(\forall X)(\forall Y)(\forall V)\,((X = Y \wedge X \in V) \Rightarrow Y \in V).$$

Slovy: Jestliže $X = Y$, pak z $X \in V$ plyne $Y \in V$.

3.6. Tvrzení. *Nechť $X = Y$ a V je libovolná třída. Pak*

$$X \in V \Leftrightarrow Y \in V.$$

Slovy: $X \in V$ a $Y \in V$ platí nebo neplatí současně.

Důkaz. Z axiomu invariance plynou implikace $X \in V \Rightarrow Y \in V$ a $Y \in V \Rightarrow X \in V$.

3.7. Tvrzení. *Nechť $X = Y$ a $U_1, \ldots, U_n$ jsou libovolné třídy. Pak platí*

$$\phi(X, U_1, \ldots, U_n) \Leftrightarrow \phi(Y, U_1, \ldots, U_n)$$

čili $\phi(X, U_1, \ldots, U_n)$ a $\phi(Y, U_1, \ldots, U_n)$ platí nebo neplatí současně.

Tvrzení dokážeme indukcí vzhledem k délce formule. Délkou formule se rozumí počet znaků ve formuli, sestrojené podle pravidel $\mathbf{F}_1$ až $\mathbf{F}_4$ včetně všech závorek. Je zřejmé, že atomické formule jsou nejkratší (každá sestává ze tří znaků) a každé pravidlo $\mathbf{F}_2$ až $\mathbf{F}_4$ vytváří formule delší než jsou jednotlivé komponenty.

Důkaz. Je-li $\phi(X, U)$ atomická formule $U \in X$, plyne tvrzení z definice rovnosti tříd. Je-li $\phi(X, U)$ atomická formule $X \in U$, plyne tvrzení z axiomu invariance, přesněji, z tvrzení 3.6.

Pro ostatní formule se postupuje indukcí. Předpokládejme, že tvrzení platí pro všechny formule kratší než formule $\phi(X, U_1, \dots, U_n)$.

Nechť je formule $\phi(X, U_1, \dots, U_n)$ tvaru $\neg\psi(X, U_1, \dots, U_n)$ podle pravidla $\mathbf{F}_2$. Jelikož je $\psi(X, U_1, \dots, U_n)$ kratší než $\phi(X, U_1, \dots, U_n)$, platí $\psi(X, U_1, \dots, U_n) \Leftrightarrow \psi(Y, U_1, \dots, U_n)$ podle indukčního předpokladu. Pak ovšem platí $\phi(X, U_1, \dots, U_n) \Leftrightarrow \phi(Y, U_1, \dots, U_n)$.

Nechť je $\phi(X, U_1, \dots, U_n)$ tvaru $(\forall U)\, \psi(X, U, U_1, \dots, U_n)$ nebo $(\exists U)\, \psi(X, U, U_1, \dots, U_n)$ podle pravidla $\mathbf{F}_3$. Opět je $\psi(X, U, U_1, \dots, U_n)$ kratší než $\phi(X, U_1, \dots, U_n)$, a proto platí $\psi(X, U, U_1, \dots, U_n) \Leftrightarrow \psi(Y, U, U_1, \dots, U_n)$ podle indukčního předpokladu. Načež ovšem $\phi(X, U_1, \dots, U_n) \Leftrightarrow \phi(Y, U_1, \dots, U_n)$.

Analogicky ohledně pravidla $\mathbf{F}_4$.

$\mathbf{B}_\phi$. Schéma axiomů specifikace. Buď $\phi(x, U_1, \dots, U_n)$ formule s volnými proměnnými x, $U_1, \dots, U_n$, buď Z proměnná, která se ve ϕ nevyskytuje. Pak je

$$(\forall U_1) \cdots (\forall U_n)(\exists Z)(\forall x)\, [x \in Z \Leftrightarrow (x \underline{\in \mathcal{U}} \wedge \phi(x, U_1, \dots, U_n))]$$

axiom. Slovy: Existuje třída Z, závislá na $U_1, \dots, U_n$, jejíž prvky jsou právě všechny množiny x takové, že platí $\phi(x, U_1, \dots, U_n)$.

Třída Z se nazývá *třída specifikovaná formulí* $\phi(x, U_1, \dots, U_n)$ a označuje se

$$\{x \underline{\in \mathcal{U}} \mid \phi(x, U_1, \dots, U_n)\}.$$

Odtud okamžitě plyne pravidlo pro rozhodování o pravdivosti atomických formulí s pravou stranou $Z = \{x \underline{\in \mathcal{U}} \mid \phi(x, U_1, \dots, U_n)\}$:

$\mathbf{P}_1$ Nechť $Z = \{x \underline{\in \mathcal{U}} \mid \phi(x, U_1, \dots, U_n)\}$ je třída specifikovaná formulí $\phi(x, U_1, \dots, U_n)$. Potom pro každou množinu x platí

$$x \in Z \Leftrightarrow \phi(x, U_1, \dots, U_n).$$

Slovy: Je-li x množina, pak $x \in Z$ je pravdivá právě tehdy, když platí $\phi(x, U_1, \dots, U_n)$.

Požadavek $x \underline{\in \mathcal{U}}$ je důležitý, protože zabraňuje vzniku Russelova paradoxu.

V úvodu jsme se zmínili o dvou variantách teorie tříd, Gödel–Bernays–von Neumannově a Kelley–Morseově. První z nich ve schématu axiomů specifikace připouští jen formule, jejichž proměnnými jsou množiny, zatímco druhá připouští obecné třídy. Gödel–Bernays–von Neumannových axiomů $\mathbf{B}_\phi$ je potom méně než Kelley–Morseových axiomů $\mathbf{B}_\phi$ a naopak, Kelley–Morseových tříd je více než Gödel–Bernays–von Neumannových.

3.5. Univerzální třída

Doposud byl $\underline{\in \mathcal{U}}$ nedělitelný symbol. Nyní zavedeme třídu $\mathcal{U}$ předpisem

$$\mathcal{U} = \{x \underline{\in \mathcal{U}} \mid x = x\}.$$

Zdůrazněme, že nejde o definici kruhem, protože symboly $\mathcal{U}$ na levé straně a $\underline{\in \mathcal{U}}$ na pravé straně jsou různé. Protože formule $x = x$ je vždy pravdivá, je $\mathcal{U}$ třída všech množin. Nazývá se též *univerzální třída* čili *univerzum*. Později ukážeme, že univerzum $\mathcal{U}$ je vlastní třída.

Zápis $x \in \mathcal{U}$ znamená právě tolik, že x je množina, čili právě tolik, co $x \underline{\in \mathcal{U}}$. Nadále budeme používat jen první z nich.

3.6. Prázdná třída

Prázdnou třídu $\emptyset$ zavedeme předpisem

$$\emptyset = \{x \in \mathcal{U} \mid x \neq x\}.$$

Jelikož $x \neq x$ neplatí pro žádnou množinu, neexistuje množina, která by ležela v prázdné třídě, což vysvětluje její název.

3.7. Algebra tříd

Axiom specifikace umožňuje zavést operace s třídami, které jsou přímým zobecněním dobře známých množinových operací:

$$U \cap V = \{x \in \mathcal{U} \mid x \in U \wedge x \in V\},$$
$$U \cup V = \{x \in \mathcal{U} \mid x \in U \vee x \in V\},$$
$$U \setminus V = \{x \in \mathcal{U} \mid x \in U \wedge \neg(x \in V)\}.$$

Máme i unární operaci doplňku třídy

$$\widetilde{U} = \{x \in \mathcal{U} \mid \neg(x \in U)\},$$

kde množinová analogie není, protože doplňkem množiny je vždy vlastní třída.

Cvičení. Ukažte, že platí

$$\begin{aligned} &U \cap \mathcal{U} = U, && U \cup \emptyset = U,\\ &U \cap \emptyset = \emptyset, && U \cup \mathcal{U} = \mathcal{U},\\ &U \cap U = U, && U \cup U = U,\\ &U \cap V = V \cap U, && U \cup V = V \cup U,\\ &(U \cap V) \cap W = U \cap (V \cap W), && (U \cup V) \cup W = U \cup (V \cup W),\\ &(U \cap V) \cup W = (U \cup W) \cap (V \cup W), && (U \cup V) \cap W = (U \cap W) \cup (V \cap W). \end{aligned}$$

Cvičení. Ukažte, že platí

$$\begin{aligned} &\widetilde{\mathcal{U}} = \emptyset, && \tilde{\emptyset} = \mathcal{U},\\ &(U \cap V)^{\sim} = \widetilde{U} \cup \widetilde{V}, && (U \cup V)^{\sim} = \widetilde{U} \cap \widetilde{V},\\ &\widetilde{\widetilde{U}} = U. \end{aligned}$$

Přímé zobecnění má i inkluze.

3.8. Definice. Řekneme, že třída U je *podtřída* třídy V a zapisujeme $U \subseteq V$, jestliže platí formule

$$(\forall x)\,(x \in U \Rightarrow x \in V).$$

Vztah $A \subseteq B$ se nazývá *inkluze. Ostrá inkluze* $A \subset B$ se zavádí formulí

$$A \subset B \Leftrightarrow (A \subseteq B) \wedge (A \neq B).$$

Následující cvičení ukazuje, že $\subseteq$ má vlastnosti uspořádání.

Cvičení. Ukažte, že platí

$$
\begin{aligned}
& U \subseteq U && \text{(reflexivita)},\\
& (U \subseteq V \wedge V \subseteq U) \Rightarrow U = V && \text{(antisymetrie)},\\
& (U \subseteq V \wedge V \subseteq W) \Rightarrow U \subseteq W && \text{(tranzitivita)}.
\end{aligned}
$$

Cvičení. Ukažte, že platí

$$
\begin{aligned}
& \emptyset \subseteq U, && U \subseteq \mathcal{U},\\
& U \subseteq V \Leftrightarrow U \cup V = V, && U \subseteq V \Leftrightarrow U \cap V = U.
\end{aligned}
$$

Je-li U třída, zavádíme *omezené kvantifikátory* $(\exists X \in U)$ a $(\forall X \in U)$ předpisem, že

$$
\begin{aligned}
(\exists X \in U)\, \phi(X, V_1, \dots, V_n) &\Leftrightarrow (\exists X)\, X \in U \wedge \phi(X, V_1, \dots, V_n),\\
(\forall X \in U)\, \phi(X, V_1, \dots, V_n) &\Leftrightarrow (\forall X)\, X \in U \Rightarrow \phi(X, V_1, \dots, V_n).
\end{aligned}
$$

platí pro libovolnou formuli $\phi(X, V_1, \dots, V_n)$.

Sjednocení a průnik třídy množin definujeme předpisem

$$
\begin{aligned}
\bigcup U &= \{x \in \mathcal{U} \mid (\exists X \in U)\, x \in X\}\\
&= \{x \in \mathcal{U} \mid (\exists X)\, (X \in U \wedge x \in X)\},\\
\bigcap U &= \{x \in \mathcal{U} \mid (\forall X \in U)\, x \in X\}\\
&= \{x \in \mathcal{U} \mid (\forall X)\, (X \in U \Rightarrow x \in X)\}.
\end{aligned}
$$

Vidíme, že $\bigcap U$ obsahuje právě ta x, která leží ve všech množinách $X \in U$. Oproti tomu $\bigcup U$ obsahuje právě ta x, která leží v alespoň jedné množině $X \in U$. Možný a obvyklý je též zápis

$$
\bigcup U = \bigcup_{X \in U} X, \qquad \bigcap U = \bigcap_{X \in U} X.
$$

3.9. Tvrzení. *Platí*

$$
\bigcap \emptyset = \mathcal{U}, \qquad \bigcup \emptyset = \emptyset.
$$

Důkaz. Ohledně první rovnosti zřejmě $\bigcap \emptyset \subseteq \mathcal{U}$. Dokažme opačnou inkluzi $\mathcal{U} \subseteq \bigcap \emptyset$. Buď $x \in \mathcal{U}$ libovolná množina. Ale $x \in \bigcap \emptyset$ právě tehdy, když pro každou třídu X platí implikace $X \in \emptyset \Rightarrow x \in X$. Taková implikace ovšem platí, a to z toho důvodu, že předpoklad $X \in \emptyset$ není nikdy pravdivý.

Ohledně druhé rovnosti zřejmě $\emptyset \subseteq \bigcup \emptyset$. Dokažme opačnou inkluzi $\bigcup \emptyset \subseteq \emptyset$. Ale $x \in \bigcup \emptyset$ právě tehdy, když pro každou třídu X platí $X \in \emptyset \wedge x \in X$. Avšak $X \in \emptyset$ neplatí nikdy, a proto $x \in \bigcup \emptyset$ neexistuje, a tudíž $\bigcup \emptyset \subseteq \emptyset$.

Cvičení. Nechť $U \subseteq V$. Ukažte, že pak platí

$$
\bigcup U \subseteq \bigcup V, \qquad \bigcap U \subseteq \bigcap V.
$$

Cvičení. Nechť $x \in X$. Ukažte, že pak platí

$$\bigcap X \subseteq x \subseteq \bigcup X.$$

3.8. Třída všech podmnožin

Třída $\wp U$ všech podmnožin třídy U je definována předpisem

$$\wp U = \{Z \in \mathcal{U} \mid Z \subseteq U\}.$$

Není snad nutno zdůrazňovat, že pokud U je vlastní třída, pak neexistuje třída všech podtříd v U.

C. Dva axiomy ohledně podmnožin.
$\mathbf{C}_1$ Je-li X množina a $Z \subseteq X$, pak Z je množina.
$\mathbf{C}_2$ Je-li X množina, pak $\wp X$ je množina.

Lze ukázat, že axiomy $\mathbf{C}_1$, $\mathbf{C}_2$ lze nahradit jediným. Platí totiž věta

3.10. Tvrzení. *Dvojice axiomů* $\mathbf{C}_1$, $\mathbf{C}_2$ *je ekvivalentní axiomu*

$$\mathbf{C} \qquad (\forall X \in \mathcal{U})(\exists Y \in \mathcal{U})(\forall Z)\,(Z \subseteq X \Rightarrow Z \in Y).$$

Důkaz. Nechť platí axiomy $\mathbf{C}_1$ a $\mathbf{C}_2$. Nechť X je množina. Položme $Y = \wp X$, což je množina podle $\mathbf{C}_2$, přičemž každá podtřída $Z \subset X$ je množina podle $\mathbf{C}_1$, a proto $Z \in \wp X$. Tím je dokázána formule $\mathbf{C}$.

Nechť platí formule $\mathbf{C}$. Nechť X je množina. Pak existuje množina Y taková, že pro každou třídu Z platí implikace $Z \subseteq X \Rightarrow Z \in Y$. Dokažme $\mathbf{C}_1$. Jestliže $Z \subseteq X$, pak $Z \in Y$, a tedy Z je množina a $\mathbf{C}_1$ je dokázáno. Dokažme $\mathbf{C}_2$. Snadno se vidí, že $\wp X \subseteq Y$, načež $\wp X$ je množina, protože Y je množina. Tím je dokázáno $\mathbf{C}_2$.

3.11. Tvrzení. *Univerzum* $\mathcal{U}$ *je vlastní třída.*

Důkaz. Připusťme, že $\mathcal{U}$ je množina. Pak i podtřída $N = \{X \in \mathcal{U} \mid X \notin X\}$ je množina a dostáváme spor $N \in N \Leftrightarrow N \notin N$ (Russelův paradox). Tudíž, $\mathcal{U}$ není množina.

3.9. Existence množin

Všimněme si, že doposud jsme nedokázali existenci ani jedné množiny. Všechny doposud uvedené axiomy připouštějí i možnost, že vůbec žádná třída není množinou, čili možnost, že $\mathcal{U} = \emptyset$.

D. Axiom existence množin.

$$\emptyset \in \mathcal{U},$$

aneb prázdná třída je množina.

Ekvivalentně stačí předpokládat existenci alespoň jedné množiny.

3.12. Tvrzení. *Axiom* $\mathbf{D}$ *a tvrzení*

$$\mathcal{U} \neq \emptyset$$

jsou ekvivalentní.

Důkaz. Je.li $\mathcal{U}$ neprázdná, pak existuje alespoň jedna množina, označme ji U. Jelikož $\emptyset \subseteq U$, je $\emptyset$ rovněž množina podle $\mathbf{C}_1$.

3.13. Tvrzení.

$$\bigcap \mathcal{U} = \emptyset, \qquad \bigcup \mathcal{U} = \mathcal{U}.$$

Důkaz. Ohledně první rovnosti zřejmě $\emptyset \subseteq \bigcap \mathcal{U}$. Dokažme opačnou inkluzi $\bigcap \mathcal{U} \subseteq \emptyset$. Připusťme, že existuje $x \in \bigcap \mathcal{U}$. Jelikož $\emptyset \in \mathcal{U}$, z podmínky $x \in \bigcap \mathcal{U}$ plyne, že x náleží všem množinám, a tedy i prázdné množině, což je spor. Tudíž, $x \in \bigcap \mathcal{U}$ neexistuje.

Ohledně druhé rovnosti zřejmě $\bigcup \mathcal{U} \subseteq \mathcal{U}$. Dokažme opačnou inkluzi $\mathcal{U} \subseteq \bigcup \mathcal{U}$. Buď $x \in \mathcal{U}$ libovolná množina. Ale $x \in \bigcup \mathcal{U}$ právě tehdy, když existuje třída X taková, že $X \in \mathcal{U}$ a $x \in X$. Takové X existuje, například $\wp x$.

3.10. Jednoprvková množina

Je-li x množina, definujeme třídu $\{x\}$ předpisem

$$\{x\} = \{y \in \mathcal{U} \mid y = x\}.$$

Cvičení. Rozhodněte, zda platí
a) $\emptyset \in \{\emptyset\}$;
b) $\emptyset \subseteq \{\emptyset\}$.

3.14. Tvrzení. *Platí*

$$(\forall x \in \mathcal{U})\, \{x\} \in \mathcal{U},$$

aneb je-li x množina, pak i $\{x\}$ je množina.

Důkaz. Nechť x je množina. Platí $x \in \wp x$, protože $x \subseteq x$. Tudíž, $\{x\} \subseteq \wp x$, načež $\{x\}$ je množina, protože $\wp x$ je množina podle $\mathbf{C}_2$.

Množina $\{x\}$ se nazývá *jednoprvková množina s prvkem x.*

Pokud stejný předpis použijeme v případě, že x je vlastní třída, dostaneme $\{x\} = \emptyset$, protože množina y splňující $y = x$ neexistuje. Předpoklad, že x je množina, je lépe ponechat jako ochranu před možným nedorozuměním.

Všimněte si, že už umíme sestrojit nekonečné množství množin $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}$, atd. Každé dvě jsou různé, což snadno zjistíme porovnáním prvků. Například $\emptyset \neq \{\emptyset\}$, protože množina na levé straně nemá žádné prvky a množina na pravé straně prvek má, a sice $\emptyset$. Podobně $\{\emptyset\} \neq \{\{\emptyset\}\}$, protože kdyby platila rovnost $\{\emptyset\} = \{\{\emptyset\}\}$, muselo by o jejich prvcích platit $\emptyset = \{\emptyset\}$, což jsme již vyloučili. Nicméně, všechny zatím konstruovatelné množiny jsou jednoprvkové.

3.15. Definice. Jsou-li x, y množiny, zavedeme třídu

$$\{x, y\} = \{u \in \mathcal{U} \mid u = x \vee u = y\}$$

Je-li $x \neq y$, nazývá se *dvouprvková třída* s prvky x, y nebo též *neuspořádaná dvojice* prvků x, y.

Je-li $x = y$, pak evidentně $\{x, y\} = \{x\} = \{y\}$.

E. Axiom dvojice.

$$(\forall x \in \mathcal{U})(\forall y \in \mathcal{U})(\exists u \in \mathcal{U})(\forall z \in \mathcal{U})\,(z \in u \Leftrightarrow (z = x \vee z = y))$$

čili jsou-li x, y množiny, pak třída $\{x, y\}$ je množina.

F. Axiom sjednocení.

$$(\forall S \in \mathcal{U})\left(\bigcup S \in \mathcal{U}\right).$$

Je-li S množina, pak $\bigcup S$ je množina.

Sjednocováním množiny množin vždy dostaneme zase množinu. To samozřejmě nemusí platit pro sjednocení vlastní třídy množin. Analogii pro průniky nepotřebujeme, protože plyne z axiomu $\mathbf{C}_1$.

Cvičení.

$$X \cup Y = \bigcup\{X, Y\}.$$

Vidíme, že i sjednocení dvou množin je množina (podle axiomu sjednocení).

Všimněme si, že se zásoba prokazatelně existujících množin opět rozšířila, například o

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

atd. Stále však jde o množiny s konečně mnoha prvky (zde vždy se dvěma prvky).

Zřejmě $\{x, y\} = \{x\} \cup \{y\}$. Jsou-li x, y, z množiny, lze analogicky zavést

$$\{x, y, z\} = \{x, y\} \cup \{z\} = \{x\} \cup \{y\} \cup \{z\}.$$

A tak dále.

3.11. Kartézský součin

Kartézský součin je další významná množinová konstrukce, kterou lze bez problémů rozšířit na třídy.

3.16. Definice. Nechť a, b jsou množiny, pak předpisem

$$[a, b] = \{\{a\}, \{a, b\}\}$$

definujeme *uspořádanou dvojici* $[a, b]$.

3.17. Tvrzení. *Jsou-li a, b, c, d množiny, pak $[a, b] = [c, d]$ právě tehdy, když $a = c \wedge b = d$.*

Důkaz. Rozborem možných případů snadno zjistíme, že $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ právě tehdy, když $a = c$ a současně $b = d$.

Uspořádaná dvojice $[a, b]$ je jednoznačně určena zadáním dvou prvků a jejich pořadím, na rozdíl od množiny $\{a, b\}$, která je určena zadáním dvou prvků bez ohledu na pořadí.

3.18. Definice. Jsou-li A, B třídy, definujeme třídu

$$A \times B = \{x \in \mathcal{U} \mid (\exists a \in A)(\exists b \in B)\, x = [a, b]\}$$

všech uspořádaných dvojic $[a, b]$ prvků tříd A, B a nazýváme ji *kartézský součin* tříd A, B.

Běžně se používá i zápis

$$A \times B = \{[a, b] \mid a \in A, b \in B\}.$$

Příklad. $\{\heartsuit, \diamondsuit\} \times \{\spadesuit, \clubsuit\} = \{[\heartsuit, \spadesuit], [\heartsuit, \clubsuit], [\diamondsuit, \spadesuit], [\diamondsuit, \clubsuit]\}$.

Cvičení. 1. Buďte A, B libovolné třídy, buďte $A' \subseteq A$, $B' \subseteq B$ jejich podtřídy. Ukažte, že platí

$$A' \times B' = (A \times B') \cap (A' \times B).$$

2. Buďte A, B libovolné třídy, buďte A', A'' podtřídy třídy A. Dokažte, že platí

$$(A' \cap A'') \times B = (A' \times B) \cap (A'' \times B),$$
$$(A' \cup A'') \times B = (A' \times B) \cup (A'' \times B).$$

3. Buďte A, U libovolné třídy. Dokažte, že platí

$$A \times \bigcap U = \bigcap (A \times U),$$
$$A \times \bigcup U = \bigcup (A \times U).$$

Později dokážeme, že kartézský součin množin je množina, ale neobejdeme se bez dalšího axiomu.

3.12. Relace a zobrazení

Relace a zobrazení mezi třídami se definují úplně stejně jako mezi množinami. Pro úplnost níže uvádíme základní definice, ale důkazy tvrzení ponecháváme jako cvičení.

3.19. Definice. Buďte A, B libovolné třídy. *Relace* (neboli korespondence) mezi třídami A, B je libovolná podtřída kartézského součinu $A \times B$. Je-li $\rho \subseteq A \times B$ relace a jsou-li $a \in A$, $b \in B$ množiny takové, že $[a, b] \in \rho$, pak říkáme, že a je v relaci ρ s b a stručně zapisujeme $a\ \rho\ b$. Relace *na* třídě A je zvláštní případ, kdy $A = B$.

Příklady. 1. Prázdná množina $\emptyset \subseteq A \times B$ je relace mezi třídami A, B. Žádné dva prvky $a \in A$, $b \in B$ nejsou v této relaci.

2. Celá třída $A \times B$ je rovněž relace mezi třídami A, B. Každé dva prvky $a \in A$, $b \in B$ jsou v této relaci.

3. *Identická relace* na třídě A je podtřída $\mathrm{id}_A = \{\, [a, a] \mid a \in A \,\}$. Prvky $a, b \in A$ jsou v této relaci právě tehdy, když $a = b$.

3.20. Definice. Je-li $\rho \subseteq A \times B$ relace mezi třídami A, B, je relace $\rho^{-1} \subseteq B \times A$ mezi třídami B, A definovaná předpisem

$$\rho^{-1} := \{ [b, a] \mid a \; \rho \; b \}$$

se nazývá *opačná relace* k relaci ρ.

Zapamatujte si: $a \; \rho \; b \Leftrightarrow b \; \rho^{-1} \; a$.

3.21. Definice. Buď ρ relace mezi třídami A, B, buď σ relace mezi třídami B, C. Relace $\sigma \circ \rho$ (čti „σ po ρ“) mezi třídami A, C, definovaná předpisem

$$\sigma \circ \rho = \{(a, c) \mid (\exists b \in B)(a \; \rho \; b \wedge b \; \sigma \; c)\},$$

se nazývá *složení relací* ρ a σ.

Cvičení. Buď ρ relace mezi třídami A, B. Pak platí
1. $\rho \circ \mathrm{id}_A = \rho$;
2. $\mathrm{id}_B \circ \rho = \rho$.

Buď navíc σ relace mezi třídami B, C. Pak platí
3. $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$.

Cvičení. 1. Ukažte, že $(\rho^{-1})^{-1} = \rho$.
2. Nechť $\rho \subseteq \rho'$, $\sigma \subseteq \sigma'$. Dokažte, že pak $\rho \circ \sigma \subseteq \rho' \circ \sigma'$.

3.13. Zobrazení

Zobrazení je speciální případ relace mezi třídami A, B.

Definice. Buďte A, B množiny. *Zobrazení* f z třídy A do třídy B je relace $f \subseteq A \times B$, která splňuje podmínku: Pro každý prvek $a \in A$ existuje právě jeden prvek $b \in B$ takový, že platí $[a, b] \in f$.

Intuitivně jde o přiřazení hodnoty: každému prvku z třídy A se přiřadí právě jedna "hodnota" z třídy B. Prvek b se pak obvykle označuje $f(a)$, někdy také f_a. Nazývá se *hodnota* zobrazení f v prvku a nebo také *obraz* prvku a při zobrazení f.

Zápisem $f : A \to B$ vyjadřujeme, že f je zobrazení z třídy A do třídy B. Jiný zápis: $A \xrightarrow{f} B$. Místo $b = f(a)$ často píšeme $f : a \mapsto b$ nebo $a \xmapsto{f} b$.

Zavedeme-li zvláštní kvantifikátor $\exists!$ s významem "existuje právě jeden," lze podmínku na zobrazení zapsat jako

$$(\forall a \in A)(\exists! \, b \in B) \, [a, b] \in f.$$

"Existuje právě jeden" znamená "existuje, a pokud jsou dva, pak jsou stejné," čili

$$(\exists! \, x \in X) \, \phi(x) \Leftrightarrow ((\exists x \in X) \, \phi(x)) \wedge ((\forall x \in X)(\forall x' \in X) \, (\phi(x) \wedge \phi(x')) \Rightarrow x = x').$$

Příklad. Identická relace na třídě A je zobrazení a nazývá se *identické zobrazení.* z třídy A do ní samé a značí se $\mathrm{id}_A : A \to A$. Platí $\mathrm{id}_A(a) = a$ pro každé $a \in A$.

Je-li $A \subseteq X$ podtřída, pak je $\iota_A = \{(a, a) \mid a \in A\}$ zobrazení, které prvku $a \in A$ přiřadí týž prvek $a \in X$: $\iota_{AX}(a) = a$. Zobrazení ι_{AX} se nazývá *vložení* podtřídy.

Cvičení. Buďte $f : A \to B$, $g : B \to C$ dvě zobrazení. Pak je relace $g \circ f$ zobrazení $A \to C$ a

$$(\forall a \in A) \, (g \circ f)(a) = g(f(a)).$$

Zobrazení $g \circ f$ se nazývá *kompozice* zobrazení f, g.

Cvičení. (1) Budiž $f : A \to B$ zobrazení. Pak

$$f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f.$$

(2) Buďte $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení. Pak

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Jak vyplývá z (2), zápis $h \circ g \circ f$ je jednoznačný i při vynechaných závorkách.

Je-li relace $f \subseteq A \times B$ zobrazením $f : A \to B$, neznamená to ještě, že i opačná relace f^{-1} je zobrazením. Je-li prvek $b \in B$ obrazem prvku $a \in A$, pak se prvek a nazývá *vzor prvku b při zobrazení f*. Třída všech vzorů prvku $b \in B$ při zobrazení f se značí $f^{-1}\{b\}$. To jest,

$$f(a) = b \Leftrightarrow a \in f^{-1}\{b\}.$$

Zatímco obraz obecného prvku $a \in A$ vždy existuje a je jediný, vzor prvku $b \in B$ obecně existovat nemusí a nemusí být ani jediný.

Pro obecnou podmnožinu $B' \subseteq B$ definujeme

$$f^{-1}B' = \{a \in A \mid f(a) \in B'\}.$$

Speciálním případem je $f^{-1}\{b\}$ z předchozího odstavce.

3.22. Poznámka. Zdůrazněme, že vzor $f^{-1}\{b\}$ prvku b je třída a může být i vlastní. Uveďme příklad. Přiřadíme-li každé množině množinu prázdnou, dostáváme konstantní zobrazení $\mathcal{U} \to \{\emptyset\}$ a vzorem prvku $\emptyset$ je celá třída $\mathcal{U}$. Následkem toho vzory nemusí tvořit třídu. To je nepříjemné omezení, protože že nějaká kolekce takových vzorů intuitivně existuje a občas s ní i potřebujeme pracovat. Má to i poněkud paradoxální charakter, protože v těch případech, kdy všechny vzory při zobrazení f třídu tvoří, existuje i bijekce mezí ní a obrazem fA. který třídou je. To je slabina naší axiomatizace.

Cvičení. Dokažte, že pro $f \subseteq A \times B$ a $B', B'' \subseteq B$ platí

$$f^{-1}(B' \cap B'') = f^{-1}B' \cap f^{-1}B'',$$
$$f^{-1}(B' \cup B'') = f^{-1}B' \cup f^{-1}B''.$$

3.23. Definice. Zobrazení $f : A \to B$ se nazývá *surjektivní* (*surjekce*) neboli zobrazení *na* třídu B, jestliže má každý prvek $b \in B$ alespoň jeden vzor v A:

$$(\forall b \in B)(\exists a \in A)\, b = f(a).$$

Zobrazení $f : A \to B$ se nazývá *injektivní* (*injekce*) neboli *prosté*, jestliže má každý prvek $b \in B$ nejvýše jeden vzor v A:

$$(\forall a \in A)(\forall a' \in A)\, (f(a) = f(a') \Rightarrow a = a').$$

Zobrazení $f : A \to B$ se nazývá *bijektivní* (*bijekce*), je-li surjektivní a injektivní současně.

Cvičení. Buď $f : A \to B$ zobrazení. Dokažte, že následující podmínky jsou ekvivalentní:
(1) Zobrazení f je bijektivní.
(2) Existuje zobrazení $g : B \to A$ takové, že

$$g \circ f = \mathrm{id}_A, \qquad f \circ g = \mathrm{id}_B .$$

(3) Relace $f^{-1} \subseteq B \times A$ opačná k relaci $f \subseteq A \times B$ je zobrazení.
Zobrazení g s vlastnostmi (2) je opět bijektivní a splývá s relací f^{-1} z (3).

Zobrazení $g = f^{-1}$ z předchozího tvrzení se nazývá *inverzní* k f. Je definováno předpisem:

$$f^{-1}(b) = a \Leftrightarrow b = f(a).$$

Cvičení. Buďte $f : A \longrightarrow B$, $g : B \longrightarrow C$ bijekce. Dokažte, že $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Cvičení. Buďte $f : A \longrightarrow B$, $g : B \longrightarrow C$ dvě zobrazení.
(1) Je-li zobrazení $g \circ f$ injektivní, pak je i zobrazení f injektivní.
(2) Je-li zobrazení $g \circ f$ surjektivní, pak je i zobrazení g surjektivní.
(3) Je-li zobrazení $g \circ f$ bijektivní, pak je i zobrazení g bijektivní.
Dokažte.

Cvičení. Buďte $f : A \longrightarrow B$, $g : A \longrightarrow B$ dvě zobrazení. Dokažte, že platí:
(1) Buď $h : B \longrightarrow C$ injektivní zobrazení takové, že $h \circ f = h \circ g$. Pak $f = g$. Jinými slovy, injektivním zobrazením lze krátit zleva.
(2) Buď $h : D \longrightarrow A$ surjektivní zobrazení takové, že $f \circ h = g \circ h$. Pak $f = g$. Jinými slovy, surjektivním zobrazením lze krátit zprava.

Příklad. Buď $A \subseteq X$ potřída, $\iota_A = \{(a, a) \mid a \in A\}$ přílušné vložení.
Je-li $f : X \longrightarrow Y$ nějaké zobrazení, pak kompozice $f \circ \iota_{AX}$ představuje zobrazení $A \longrightarrow Y$, které se nazývá *zúžení* (též *restrikce* nebo *restrinkce*) zobrazení f na podmnožinu A a značí se $f|_A$:

$$f|_A : A \xrightarrow{\iota_{AX}} X \xrightarrow{f} Y.$$

Všimněte si, že zúžení je dáno týmž předpisem $a \mapsto f(a)$ jako f.
Je-li množina Y obsažena v jiné množině Z, pak existuje i kompozice $\iota_{YZ} \circ f : X \longrightarrow Z$. V tomto případě říkáme, že f vzniká rozšířením oboru hodnot, ale zvláštní dohodnuté označení neexistuje.

Cvičení. Ukažte, že ι_{AX} je injektivní.

Buď $f : X \longrightarrow Y$ zobrazení, buď $A \subseteq X$ podtřída. Položme

$$fA = \{y \in Y \mid (\exists a \in A)\, y = f(a)\},$$

což často zkracujeme

$$fA = \{f(a) \mid a \in A\}.$$

Nazývá se *obraz* podtřídy $A \subseteq X$ při zobrazení f.

Cvičení. Buď $f : X \longrightarrow Y$ zobrazení. Ukažte, že $\bar{f} : X \longrightarrow fX$, $x \mapsto f(x)$, je surjektivní zobrazení a platí $f = \iota_{fX,Y} \circ \bar{f}$.

Je-li A množina, očekávali bychom, že i fA je množina, ale ve skutečnosti je k tomu potřeba zvláštní axiom.

G. Axiom substituce. Je-li $f : X \longrightarrow Y$ zobrazení a X množina, pak fX je množina.

V Zermelo–Fraenkelově axiomatizaci je na tomto místě schema axiomů, v němž hrají roli substituce, odtud název.

Příklad. Označme $\mathcal{U}_1$ třídu všech jednoprvkových množin, které definujeme jako množiny tvaru $\{a\}$, kde a je množina.
Ukažme, že $\mathcal{U}_1$ je vlastní třída. Uvažujme o zobrazení $s : \mathcal{U} \longrightarrow \mathcal{U}_1$, $a \mapsto \{a\}$. Zobrazení s je zřejmě surjektivní i injektivní (proč?), čili bijekce. Existuje proto inverzní zobrazení $t : \mathcal{U}_1 \longrightarrow \mathcal{U}$, $\{a\} \mapsto a$, které je rovněž bijekce. Kdyby $\mathcal{U}_1$ byla množina, pak by nutně i $\mathcal{U} = t\mathcal{U}_1$ byla množina, což, jak víme, není.

3.24. Definice. Nechť I je množina a $F : I \longrightarrow \mathcal{U}$ zobrazení, které každému prvku $i \in I$ přiřadí množinu $F_i \in \mathcal{U}$. Zobrazení $F : I \longrightarrow \mathcal{U}$ se obecně nazývá *systém množin.* Definujeme

$$\bigcup_{i\in I} F_i = \bigcup\{F_i \mid i \in I\} = \bigcup FI,$$

$$\bigcap_{i\in I} F_i = \bigcap\{F_i \mid i \in I\} = \bigcap FI.$$

Axiom substituce spolu s axiomem sjednocení dává následující tvrzení.

3.25. Tvrzení. *Nechť I je množina a $F : I \longrightarrow \mathcal{U}$ zobrazení. Pak*

$$\bigcup_{i\in I} F_i$$

je množina.

Důkaz. Třída $\bigcup FI$ je množina podle axiomu sjednocení, protože FI je množina množin podle axiomu substituce.

Nyní můžeme dokázat, že kartézský součin dvou množin je množina.

3.26. Tvrzení. *Buďte A, B množiny. Pak $A \times B$ je množina.*

Důkaz.

$$A \times B = A \times \bigcup_{b\in B} \{b\} = \bigcup_{b\in B} A \times \{b\},$$

kde $A \times \{b\}$ jsou množiny podle axiomu substituce, protože $A \times \{b\}$ je obrazem množiny A při zobrazení $a \mapsto [a, b]$.

3.27. Definice. Buďte $f : X \longrightarrow Y$ a $g : Y \longrightarrow X$ zobrazení. Jestliže

$$g \circ f = \mathrm{id}_X,$$

pak říkáme, že zobrazení g je *levá inverze* zobrazení f. Jestliže

$$f \circ g = \mathrm{id}_Y,$$

pak říkáme, že zobrazení g je *pravá inverze* zobrazení f.

3.28. Tvrzení. *Buď $f : A \longrightarrow B$ injektivní zobrazení množin, přičemž $A \neq \emptyset$. Pak má f levou inverzi.*

Důkaz. Protože A je neprázdná, existuje $c \in A$. Konstruujme $g : B \longrightarrow A$. Jestliže $b \in fA$, pak má právě jeden vzor, čili existuje a takové, že $f^{-1}\{b\} = \{a\}$. Položíme $g(b) = a$, načež $g(f(a)) = g(b) = a$. Jestliže naopak $b \notin fA$, pak položíme $g(b) = c$. Snadno se vidí, že $g \circ f = \mathrm{id}_A$.

Jiný způsob: Označíme-li

$$g = \{(b, a) \in fA \times A \mid b = f(a)\},$$

(g je ohraničení relace f^{-1} na obraz fA), je g zobrazením $fA \longrightarrow A$ a platí $g \circ f = \mathrm{id}_A$. Nyní dodefinujeme g na prvcích neležících v fA tak, že jim přiřadíme hodnotu c, čímž neporušíme rovnost $g \circ f = \mathrm{id}_A$.

Cvičení. Je předpoklad $A \neq \emptyset$ nutný?

Duální tvrzení, že každé surjektivní zobrazení má pravou inverzi, ze zatím uvedených axiomů nevyplývá. Připomeňme si obvyklý důkaz v rámci naivní teorie množin. Buď $f : X \to Y$ surjektivní zobrazení. Pak má každý prvek $y \in Y$ alespoň jeden vzor $x \in X$ takový, že $f(x) = y$. Pro každé $y \in Y$ vyberme právě jeden ze vzorů a označme jej $g(y)$. Dostáváme zobrazení $g : Y \to X$. Z konstrukce vyplývá, že platí $f \circ g = \mathrm{id}_Y$.

Uvědomme si však, že zatím umíme konstruovat třídy jedině specifikací, tedy nějakou formulí definující onu třídu, čili jednoznačným předpisem. Podtřídu $g \subseteq Y \times X$ jsme však nekonstruovali jednoznačným předpisem, nýbrž jsme pro každé $y \in Y$ libovolně vybrali jeden prvek z neprázdné množiny $f^{-1}\{y\}$.

AC. Axiom výběru. Je-li X množina neprázdných množin, existuje zobrazení $\tau : X \to \bigcup X$ takové, že $(\forall x \in X)\, \tau(x) \in x$.

Zobrazení τ se nazývá výběrové zobrazení, protože vybírá po jednom prvku z každé množiny $x \in X$.

3.29. Tvrzení. *Buď $f : A \to B$ surjektivní zobrazení množin. Pak má pravou inverzi.*

Důkaz. Buď $f : A \to B$ injektivní zobrazení. Pak je $\{f^{-1}\{y\} \mid y \in Y\}$ systém neprázdných množin a podle axiomu výběru existuje výběrové zobrazení τ splňující $\tau(f^{-1}\{y\}) \in f^{-1}\{y\}$. Nyní stačí položit $g(y) = \tau(f^{-1}\{y\})$, aby platilo $g(y) \in f^{-1}\{y\}$, a tedy $f \circ g = \mathrm{id}_Y$.

Axiom výběru byl po staletí používán nevědomky, dokud jej v roce 1904 "neobjevil" Ernst Zermelo (1871–1953). Axiomu výběru umožňuje nekonstruktivní důkazy existence, tedy důkazy, které neposkytují žádný předpis k sestrojení objektu, jehož existence je dokazována. Typickým případem je Brouwerova věta o pevném bodu (každé spojité zobrazení uzavřené koule do sebe sama má pevný bod). S vědomým použitím axiomu výběru byla zpočátku spojena jistá nedůvěra, protože se záhy objevily důkazy některých poněkud paradoxních výsledků, například Banach–Tarského věty, podle níž lze jednotkovou kouli v trojrozměrném Euklidovském prostoru rozložit na konečný počet částí (pět) a z nich použitím shodných transformací sestavit dvě jednotkové koule (části jsou neměřitelné, a proto nejde o skutečný paradox).

Dnes již axiom výběru téměř nikdo nezpochybňuje. Nicméně, libovůle spojená s volbou výběrového zobrazení způsobuje, že "konstrukce" využívající axiom výběru jsou nejednoznačné a neopakovatelné. Přesvědčivé příklady uvedeme v následujícím oddílu (§ 3.14). Proto je zajímavé sledovat, která tvrzení jsou s axiomem výběru ekvivalentní. Příkladem je tvrzení o existenci pravé inverze u surjekcí.

3.30. Tvrzení. *Z posledního tvrzení (existence pravé inverze ke každé surjekci mezi množinami) plyne axiom výběru.*

Důkaz. Buď X množina neprázdných množin. Pak je $X \times \bigcup X$ množina a podtřída

$$E = \left\{[x,a] \in X \times \bigcup X \;\middle|\; a \in x\right\}$$

všech dvojic $[x, a]$ takových, že $a \in x \in X$, je též množina. Uvažujme o zobrazeních

$$p_1 : E \to X, \quad [x,a] \mapsto x,$$
$$p_2 : E \to X, \quad [x,a] \mapsto a.$$

Zobrazení p_1 je surjektivní, protože každá množina $x \in X$ je podle předpokladu neprázdná. Buď q pravá inverze k p_1, čili $p_1 \circ q = \mathrm{id}_X$. Máme $q(x) = [p_1(q(x)), p_2(q(x))] \in E$, načež $p_2(q(x)) \in p_1(q(x)) = x$ pro každé x. Vidíme, že $p_2 \circ q$ je výběrová funkce.

Výběrová funkce pro *konečný* počet objektů existuje i bez axiomu výběru. Snadno ji popíšeme formulí. Například pro jednu neprázdnou množinu x obsahující prvek c je výběrovou funkcí $\{[x, c]\}$.

Cvičení. Bertrand Russel popularizoval axiom výběru výrokem, že je nutný k výběru množiny z nekonečného počtu ponožek, ale není nutný k výběru množiny z nekonečného počtu bot.
Vysvětlete. Nápověda: Ponožky jednoho páru považujeme za nerozlišitelné.

Příklad tvrzení ekvivalentního s axiomem výběru poskytuje také kartézský součin systému množin. Buď $F : I \to \mathcal{U}$, $i \mapsto F_i$, systém množin, kde I je množina. Označme

$$\prod_{i \in I} F_i = \left\{ f : I \to \bigcup_{i \in I} F_i \;\middle|\; \underset{i \in I}{\forall} f(i) \in F_i \right\}.$$

3.31. Tvrzení. *Kartézský součin neprázdné množiny množin je neprázdný.*

Důkaz. Prvek kartézského součinu je totéž co výběrová funkce.

V teorii tříd lze formulovat axiomy silnější než axiom výběru pro množiny. Uvedeme dva, ale nebudeme je používat.

Axiom globálního výběru. Je-li $T = \mathcal{U} \setminus \{\emptyset\}$ třída všech neprázdných množin, existuje zobrazení $\tau : T \to \mathcal{U}$ takové, že $(\forall x \in T)\, \tau(x) \in x$.

Axiom globálního výběru praví, že výběrová funkce existuje i pro vlastní třídy neprázdných množin. Neříká nic nového o *množinách*, pouze o vlastních třídách.
Axiom globálního výběru implikuje, že i kartézský součin vlastní třídy neprázdných množin je neprázdný.

Axiom omezené velikosti. Je-li C vlastní třída, pak existuje bijekce $C \to \mathcal{U}$.

Axiom omezené velikosti praví, že všechny vlastní třídy jsou “stejné” v tom smyslu, že libovolné tvrzení o jedné z nich lze přenést na každou jinou. Přestože je jeho formulace velmi odvážná, není v rozporu s ostatními axiomy.

3.14. Relace ekvivalence

3.32. Definice. Buď $\rho \subseteq A \times A$ relace na třídě A. Relace ρ se nazývá
– *reflexivní*, jestliže pro každé $a \in A$ platí $a \;\rho\; a$;
– *symetrická*, jestliže platí implikace $a \;\rho\; b \Rightarrow b \;\rho\; a$;
– *tranzitivní*, jestliže platí implikace $(a \;\rho\; b \wedge b \;\rho\; c) \Rightarrow a \;\rho\; c$.

Příklady. 1. Identická relace id_A je reflexivní, symetrická i tranzitivní.
2. Relace “$\in$” na univerzální třídě $\mathcal{U}$ není ani reflexivní, ani symetrická, ani tranzitivní.
3. Relace “$\subseteq$” na univerzální třídě $\mathcal{U}$ je reflexivní a tranzitivní, ale není symetrická.

Cvičení. Graf relace na množině můžeme kreslit tak, že prvky množiny A zobrazíme body v rovině a mezi prvky vedeme šipku, jsou-li v relaci. Jak se pozná graf reflexivní resp. symetrické resp. tranzitivní relace?

Cvičení. Najděte chybu v následujícím ,,důkazu“ nepravdivého tvrzení, že každá symetrická a tranzitivní relace ρ je reflexivní: “Je-li $a\ \rho\ b$, pak ze symetrie plyne $b\ \rho\ a$, načež z tranzitivity plyne $a\ \rho\ a$.”

3.33. Definice. Reflexivní, symetrická a tranzitivní relace na třídě se nazývá *relace ekvivalence* (nebo prostě *ekvivalence*, pokud nemůže dojít k záměně s logickou ekvivalencí).

Příklady. 1. Identická relace id_A je ekvivalence na třídě A.

2. Na univerzální třídě $\mathcal{U}$ zavedeme relaci ekvivalence $\sim$ předpisem: $A \sim B$ právě tehdy, když existuje bijekce $A \to B$.

3.34. Definice. Buď ρ ekvivalence na třídě A. Pro libovolné $a \in A$ označme

$$[a]_\rho = \{x \in A \mid a\ \rho\ x\}.$$

Třída $[a]_\rho$ se nazývá *třída rozkladu* podle ekvivalence ρ.

3.35. Tvrzení. Buď ρ ekvivalence na třídě A. Pro libovolné $a \in A$ platí

$$a \in [a]_\rho,$$

$$a\ \rho\ b \Leftrightarrow [a]_\rho = [b]_\rho,$$

$$[a]_\rho \cap [b]_\rho \neq \emptyset \Rightarrow [a]_\rho = [b]_\rho.$$

Navíc, pokud jsou $[a]_\rho$ množiny, platí

$$\bigcup_{a \in A} [a]_\rho = A.$$

3.36. Poznámka. Pokud je alespoň jedna třída $[a]_\rho$ vlastní, není sjednocení $\bigcup_{a\in A}[a]_\rho$ definováno, protože nemáme k dispozici zobrazení $a \mapsto [a]_\rho$.

Každé ekvivalenci na množině přísluší rozklad. Ekvivalenci na vlastní třídě přísluší rozklad jen tehdy, když je každá třída rozkladu množinou.

3.37. Definice. Nechť je každá třída $[a]_\rho$ rozkladu třídy A podle ekvivalence ρ množinou. Třída

$$A/\rho = \{B \in \mathcal{U} \mid (\exists a \in A)\, B = [a]_\rho\} = \{[a]_\rho \mid a \in A\}$$

se nazývá *faktorová třída* podle ekvivalence ρ.

Faktorová třída A/ρ množiny A je opět množina, protože je obrazem množiny A při zobrazení $A \to \mathcal{U}$, $a \mapsto [a]_\rho$.

Cvičení. Nalezněte všechny rozklady na množině $A = \{1, 2, 3\}$ (je jich pět).

Cvičení. Buď ρ ekvivalence na třídě A, buď σ ekvivalence na třídě B. Zaveďme relaci $\gamma = \rho \times \sigma$ na třídě $C = A \times B$ předpisem

$$(a_1, b_1)\ \gamma\ (a_2, b_2) \Leftrightarrow a_1\ \rho\ a_2 \wedge b_1\ \sigma\ b_2.$$

Ukažte, že γ je relace ekvivalence. Ukažte, že třídy ekvivalence γ jsou právě třídy $U \times V$, kde U je třída ekvivalence ρ a V je třída ekvivalence σ.

Podle axiomu výběru lze vytvořit množinu tím, že z každé třídy rozkladu některé množiny vybereme po jednom prvku.

Příklad. V tomto příkladu použijeme množiny $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ reálných, racionálních a celých čísel (vše, co o nic potřebujete vědět, jste se dozvěděli v matematické analýze). Na množině $\mathbb{R}$ zavedeme relaci $\sim_{\mathbb{Q}}$ předpisem

$$x \sim_{\mathbb{Q}} y \Leftrightarrow y - x \in \mathbb{Q}.$$

Snadno se uláže, že $\sim_{\mathbb{Q}}$ je relace ekvivalence. Podle axiomu výběru existuje množina U, která má s

Příklad. *Vitaliho množina* je podmnožina V uzavřeného intervalu $[0,1]$ taková, že pro každé $r \in \mathbb{R}$ existuje právě jedno číslo $v \in V$ takové, že $r - v \in \mathbb{Q}$, kde $\mathbb{Q} \subset \mathbb{R}$ je množina racionálních čísel. Získáme ji výběrem prvků z tříd ekvivalence $r \equiv s \Leftrightarrow r - s \in \mathbb{Q}$. O množinách $\mathbb{Q}$ a $\mathbb{R}$ viz níže.

3.15. Von Neumannova konstrukce přirozených čísel

Zatím uvedené axiomy nemají dost síly, aby prokázaly existenci nekonečné množiny, jakou je třeba množina všech přirozených čísel. Navíc, pokud je naším cílem vybudování matematiky "z ničeho," měli bychom přirozená čísla zkonstruovat jen s použitím těch nástrojů, které nám zatím teorie tříd poskytuje.

Von Neumann navrhl *definovat* přirozené číslo jako množinu všech předcházejících přirozených čísel. Je-li 0 první (nejmenší) přirozené číslo, dostáváme postupně

$$\begin{aligned}
0 &= \emptyset, \\
1 &= \{0\} = \{\emptyset\} \\
2 &= \{0,1\} = \{\emptyset, \{\emptyset\}\} \\
3 &= \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 &= \{0,1,2,3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}
\end{aligned}$$

atd. Vidíme, že platí $1 = 0 \cup \{0\}$, $2 = 1 \cup \{1\}$, $3 = 2 \cup \{2\}$, atd.

3.38. Definice. Řekneme, že množina N je *induktivní*, jestliže platí
(i) $\emptyset \in N$;
(ii) jestliže $n \in N$, pak $n \cup \{n\} \in N$.
Dále,

$$\mathcal{I} = \{N \in \mathcal{U} \mid (\emptyset \in N) \wedge (\forall n)\,(n \in N \Rightarrow n \cup \{n\} \in N)\}$$

se nazývá *třída všech induktivních množin.*

H. Axiom nekonečna.

$$\mathcal{I} \neq \emptyset$$

(třída všech induktivních množin je neprázdná) aneb

$$(\exists N \in \mathcal{U})\,((\emptyset \in N) \wedge (\forall n)\,(n \in N \Rightarrow n \cup \{n\} \in N))$$

(existuje induktivní množina).

Množinu přirozených čísel označujeme $\mathbb{N}$ a definujeme jako průnik všech induktivních množin. Tudíž,

$$\mathbb{N} = \bigcap_{N \in \mathcal{I}} N = \bigcap \mathcal{I},$$

což je množina, protože $\mathbb{N}$ je podtřída alespoň jedné induktivní množiny N, která existuje podle axiomu nekonečna.

Několik prvních přirozených čísel jsme vypsali výše, další lze snadno doplnit. Je-li n přirozené číslo, pak se $n \cup \{n\}$ nazývá *následovník* čísla n a označuje se σn nebo $n+1$.

3.16. Princip matematické indukce

Princip matematické indukce umožňuje dokazovat tvrzení závislá na přirozenám čísle, neboli tvrzení tvaru

$$(\forall n \in \mathbb{N})\, \phi(n).$$

3.39. Tvrzení. *Buď $K \subseteq \mathbb{N}$ množina taková, že platí $0 \in K$ a implikace $n \in K \Rightarrow n+1 \in K$. Pak platí $K = \mathbb{N}$.*

Důkaz. Podle předpokladu je K induktivní, a proto obsahuje průnik všech induktivních množin, čili $\mathbb{N} \subseteq K$. Opačnou implikaci jsme předpokládali, a proto $K = \mathbb{N}$.

3.40. Důsledek. *Buď $\phi(n)$ formule taková, že platí $\phi(0)$ a implikace $\phi(n) \Rightarrow \phi(n+1)$. Pak platí $\phi(n)$ pro všechna $n \in \mathbb{N}$.*

Důkaz. Položíme $K = \{n \in \mathbb{N} \mid \phi(n)\}$.

Princip matematické indukce také umožňuje konstruovat množiny nebo dokonce třídy X_n závislé na přirozeném čísle n. K tomu stačí dokazovat formule tvaru

$$(\forall n \in \mathbb{N})(\exists X_n)\, \phi(n, X_n).$$

V tom případě hovoříme o rekurzívní definici tříd X_n.

Následující axiom vypadá na první pohled záhadně, ale je užitečný tím, že zjednodušuje řadu důkazů.

I. Axiom regularity.

$$(\forall X \in \mathcal{U})\, (X \neq \emptyset \Rightarrow (\exists x \in X)\, x \cap X = \emptyset),$$

čili každá neprázdná množina obsahuje prvek, který je s ní disjunktní.

Axiom regularity vylučuje existenci obtížně představitelných a snadno postradatelných vztahů mezi množinami, jako například $a \in a$ nebo $a \in b \in a$ a podobných.

3.41. Tvrzení. *Neexistuje množina a taková, že $a \in a$.*

Důkaz. Množina $\{a\}$ je neprázdná, a proto existuje podle axiomu regularity takový prvek $b \in \{a\}$, že $b \cap \{a\} = \emptyset$. Jelikož jediným prvkem množiny $\{a\}$ je a, máme $b = a$, a tedy $a \cap \{a\} = \emptyset$. Připusťme, že platí $a \in a$. Pak $a \cap \{a\} = \{a\} \neq \emptyset$, což je spor. Tudíž, $a \notin a$.

Lze definovat množinu obsahující samu sebe, aniž by byla definována kruhem? Je $\{\{\{\cdots\}\}\}$ (tečky označují nekonečné opakování vložených závorek) korektně definovaná množina? Axiom regularity je tu od toho, aby nás podobných bezedných otázek zbavil.

3.42. Tvrzení. *Neexistují množiny a, b takové, že $a \in b$ a $b \in a$.*

Tudíž, ze dvou množin jen jedna může být prvkem druhé.

Důkaz. Množina $\{a, b\}$ je neprázdná, a proto existuje podle axiomu regularity takový prvek $c \in \{a, b\}$, že $c \cap \{a, b\} = \emptyset$. Jsou dvě možnosti. Je-li $c = a$, pak $a \cap \{a, b\} = \emptyset$, a proto $b \notin a$. Je-li $c = b$, pak $b \cap \{a, b\} = \emptyset$, a proto $a \notin b$.

3.43. Tvrzení. *Neexistuje systém množin $\{f_n \mid n \in \mathbb{N}\}$ takový, že $(\forall n \in \mathbb{N})\, f_{n+1} \in f_n$.*

Tudíž, neexistuje nekonečná posloupnost množin $f_0 \ni f_1 \ni f_2 \ni \cdots \ni f_n \ni f_{n+1} \ni \cdots$.

Důkaz. Označme $S = \{f_n \mid n \in \mathbb{N}\}$, což je množina a je neprázdná, a proto existuje podle axiomu regularity takový prvek $s \in S$, že $s \cap S = \emptyset$. Podle konstrukce musí existovat $n \in \mathbb{N}$ takové, že $s = f_n$. Pak ale $f_{n+1} \in f_n$ a současně $f_{n+1} \in S$, což znamená, že $s \cap S \neq \emptyset$, spor.

3.44. Poznámka. Je možné postulovat existenci množin, narušujících axiom regularity, aniž by to bylo bylo ve sporu s ostatními axiomy. Množiny splňující $a \in a$ jsou pak přípustné.

Axiom reularity je posledním axiomem teorie tříd a potažmo teorie množin, který zavádíme. Kapitolu završíme ukázkami, jak vybudovat základy matematické analýzy, protože bez toho by naše počínání nemělo rozumný důvod.

3.17. Aritmetika přirozených čísel

V této části budeme definovat sčítání a násobení přirozených čísel. Následovníka čísla n prozatím budeme označovat σn, od označení $n + 1$ dočasně upustíme.

3.45. Tvrzení. *Neexistuje $m \in \mathbb{N}$ takové, že $\sigma m = 0$.*

Důkaz. Muselo by platit $m \cup \{m\} = \emptyset$, ale levá strana obsahuje m jako prvek a pravá nikoliv.

3.46. Tvrzení. *Nechť $m, n \in \mathbb{N}$ splňují $\sigma n = \sigma m$. Pak $n = m$.*

Jinak řečeno, zobrazení $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$ je injektivní.

Důkaz. Podle předpokladu $n \cup \{n\} = m \cup \{m\}$. Levá strana obsahuje n jako prvek, a proto i pravá, načež $n \in m$ nebo $n \in \{m\}$. Pravá strana obsahuje m jako prvek, a proto i levá, načež $m \in n$ nebo $m \in \{n\}$. Nemůže platit $n \in m$ a $m \in n$ současně, a proto platí $n \in \{m\}$ nebo $m \in \{n\}$. Ve prvním i druhém případě zřejmě $n = m$ a jsme hotovi.

Nyní máme dokázány všechny tzv. Peanovy axiomy, ze kterých lze odvodit všechny aritmetické vlastnosti přirozených čísel.

Každé zobrazení $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ se nazývá binární operace na množině $\mathbb{N}$. Ukažme nyní, jak lze zavést binární operace známé z aritmetiky.

3.47. Tvrzení. *Existuje právě jedno zobrazení $\mathbb{N} \times \mathbb{N} \xrightarrow{+} \mathbb{N}$, splňující*

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

právě jedno zobrazení $\mathbb{N} \times \mathbb{N} \xrightarrow{\cdot} \mathbb{N}$, splňující

$$n \cdot 0 = 0, \quad n \cdot \sigma m = n + (n \cdot m)$$

a právě jedno zobrazení $\mathbb{N} \times \mathbb{N} \xrightarrow{\wedge} \mathbb{N}$, *splňující*

$$n^\wedge 0 = 1, \quad n^\wedge \sigma m = n \cdot (n^\wedge m).$$

Důkaz. Pro každé $n \in \mathbb{N}$ definujme zobrazení $\alpha_n : \mathbb{N} \longrightarrow \mathbb{N}$ rekurzivní formulí

$$\alpha_n(0) = n, \quad \alpha_n(\sigma m) = \sigma\alpha_n(m),$$

zobrazení $\beta_n : \mathbb{N} \longrightarrow \mathbb{N}$ rekurzivní formulí

$$\beta_n(0) = 0, \quad \beta_n(\sigma m) = \alpha_n(\beta_n(m))$$

a zobrazení $\gamma_n : \mathbb{N} \longrightarrow \mathbb{N}$ rekurzivní formulí

$$\gamma_n(0) = 1, \quad \gamma_n(\sigma m) = \beta_n(\gamma_n(m)).$$

Podle tvrzení 3.39 jsou zobrazení α_n, β_n i γ_n definována na celé množině $\mathbb{N}$. Podle tvrzení 3.39, 3.46 a 3.45 jsou definována jednoznačně. Položíme $n + m = \alpha_n(m)$, $n \cdot m = \beta_n(m)$, $n^\wedge m = \gamma_n(m)$.

Nyní dokážeme, že $\sigma n = n + 1$. Máme postupně

$$n + 1 = \alpha_n(1) = \alpha_n(\sigma 0) = \sigma\alpha_n(0) = \sigma n.$$

Cvičení. Ověřte každý krok právě uvedeného důkazu.

Právě definované binární operace $+$, $\cdot$, $^\wedge$ mají všechny vlastnosti operací sčítání, násobení a umocňování přirozených čísel, zejména platí následující formule aritmetiky přirozených čísel:

$$\begin{array}{lll}
a + 0 = a, & a \cdot 1 = a, & \\
a + b = b + a, & a \cdot b = b \cdot a, & \\
a + (b + c) = (a + b) + c, & a \cdot (b \cdot c) = (a \cdot b) \cdot c, & \\
a \cdot (b + c) = (a \cdot b) + (a \cdot c), & a^\wedge(b + c) = (a^\wedge b) \cdot (a^\wedge c), & \\
(a \cdot b)^\wedge c = (a^\wedge c) \cdot (b^\wedge c), & & \\
(a^\wedge b)^\wedge c = a^\wedge(b \cdot c), & & \\
a^\wedge 0 = 1, & a^\wedge 1 = a, & 1^\wedge a = 1.
\end{array}$$

Cvičení. Dokažte indukcí formule aritmetiky přirozených čísel.

3.48. Poznámka. Všimněte si, že při naší definici platí

$$0^0 = 1$$

(přecházíme k obvyklému zápisu umocňování), zatímco *neplatí* $0^a = 0$ pro $a = 0$. Zjednodušuje to mnohé formule. Například zápis

$$a_n x^n + \cdots + a_1 x + a_0 = \sum_0^n a_n x^n$$

je možný jen tehdy, když $0^0 = 1$ a jinak se musí pro $x = 0$ sjednat výjimka.

Rovnost $0^0 = 1$ bude v platnosti i v oboru kardinálních čísel a v oboru ordinálních čísel, které zavedeme později.

Poznámka 3.49 níže je k neurčitým výrazům typu 0^0.

3.18. Celá, racionální a reálná čísla

Nyní zavedeme celá, racionální a reálná čísla. Z konstrukce bude jasné, že tvoří množinu. Aritmetické operace se zavádějí známým způsobem a nebudeme s tím zdržovat výklad.

Dobře známa je konstrukce celých čísel jako dvojic $[+, n]$, kde $n \in \mathbb{N}$, nebo $[-, n]$, kde $n \in \mathbb{N} \setminus \{0\}$ (znaménka $+$ a $-$ jsou symboly různé od symbolů označujících přirozená čísla). Definujeme-li třídu $\mathbb{Z}$ celých čísel jako sjednocení $\big(\{+\} \times \mathbb{N}\big) \cup \big(\{-\} \times (\mathbb{N} \setminus \{0\})\big)$. Je zřejmé, že $\mathbb{Z}$ je množina.

Alternativně můžeme zavést $\mathbb{Z} = (\{+, -\} \times \mathbb{N})/\rho$, kde ρ je relace ekvivalence, jejíž jedinou třídou obsahující více než jeden prvek je $\{[+, 0], [-, 0]\}$ (ztotožňujeme $+0$ a -0).

Konstrukce racionálních čísel jako dvojic p/q nesoudělných čísel, kde $p \in \mathbb{Z}$ a $q \in \mathbb{N} \setminus \{0\}$, je též dobře známa. Třídu $\mathbb{Q}$ racionálních čísel můžeme konstruovat jako faktorovou množinu součinu $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ podle ekvivalence $[p_1, q_1]\ \rho\ [p_2, q_2] \Leftrightarrow p_1 q_2 = p_2 q_1$. Zřejmě je $\mathbb{Q}$ množina.

Dobře známa je konstrukce rálných čísel jako Dedekindových řezů. Zde uvedeme jinou definici pomocí dvojkových rozkladů, čili jako posloupností dvojkových cifer $0, 1$. Reálné číslo

$$a = 0, a_1 a_2 a_3 \ldots = \sum_{i \in \mathbb{N}} a_i 2^{-i}$$

z polouzavřeného intervalu $\mathbb{I} = [0, 1)$ lze ztotožnit se zobrazením $\mathbb{N} \to \{0, 1\} = 2$, a proto je prvkem množiny $2^{\mathbb{N}}$ všech zobrazení $\mathbb{N} \to 2$. Jelikož však

$$0, 111 \ldots = 1, 000 \ldots,$$
$$0, 0111 \ldots = 0, 1000 \ldots$$

atd., je nutno vyloučit posloupnosti, které od některého místa počínaje sestávají ze samých jedniček; budeme jim říkat *nadbytečné* posloupnosti. Každou posloupnost $0, a_1 \ldots a_n 0111 \ldots$ přitom lze nahradit posloupností, $0, a_1 \ldots a_n 1000 \ldots$, která od stejného místa počínaje sestává ze samých nul a jedna nula bezprostředně předcházející samým jedničkám se změní na jednu jedničku bezprostředně předcházející samým nulám. Tudíž, polouzavřený interval $\mathbb{I}$ lze ztotožnit s podmnožinou množiny $2^{\mathbb{N}}$, z níž jsou vynechány nadbytečné posloupnosti ve shora uvedeném smyslu. Množina reálných čísel je pak identifikovatelná se součinem $\mathbb{Z} \times \mathbb{I}$.

3.49. Poznámka. V matematické analýze se 0^0 považuje za neurčitý výraz. Jde ovšem jen o to, že limita typu 0^0 může nabývat libovolných hodnot, to jest, že při $\lim_{x \to c} f(x) = 0$ a $\lim_{x \to c} g(x) = 0$ závisí limita

$$\lim_{x \to c} f(x)^{g(x)}$$

na volbě funkcí $f(x)$ a $g(x)$.

Nijak to není ve sporu se *stanovením* hodnoty 0^0 učiněným výše. Znamená to však, že funkce 0^x je nespojitá v nule (zato x^0 je spojitá a obě být spojité zřejmě nemohou).

Řečené však nebrání jiným autorům považovat 0^0 za nedefinovaný výraz vždy. Je to v pořádku, pokud se nezapomene na všechna nutná opatření, na něž jsme jedním příkladem upozornili v poznámce 3.48.