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 $\phi(X, U_1, \ldots, U_n)$.

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

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

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

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

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

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

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

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

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

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

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

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

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 něž 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.
C$_1$ Je-li X množina a $Z \subseteq X$, pak Z je množina.
C$_2$ Je-li X množina, pak $\wp X$ je množina.

Lze ukázat, že axiomy **C**$_1$, **C**$_2$ lze nahradit jediným. Platí totiž věta

3.10. Tvrzení. *Dvojice axiomů* **C**$_1$, **C**$_2$ *je ekvivalentní axiomu*

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

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

Nechť platí formule **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 **C**$_1$. Jestliže $Z \subseteq X$, pak $Z \in Y$, a tedy Z je množina a **C**$_1$ je dokázáno. Dokažme **C**$_2$. Snadno se vidí, že $\wp X \subseteq Y$, načež $\wp X$ je množina, protože Y je množina. Tím je dokázáno **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* **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 $f : A \longrightarrow B$ vyjadřujeme, že f je zobrazení z třídy A do třídy B. Jiný zápis: $A \xrightarrow{f} B$. Místo $b = f(a)$ často píšeme $f : a \longmapsto b$ nebo $a \overset{f}{\longmapsto} b$.

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 $\mathrm{id}_A : A \longrightarrow A$. 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 $f : A \longrightarrow B$, $g : B \longrightarrow C$ dvě zobrazení. Pak je relace $g \circ f$ zobrazení $A \longrightarrow C$ 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 $a \longmapsto f(a)$ 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 $\bar{f} : X \longrightarrow fX$, $x \longmapsto f(x)$, 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 $s : \mathcal{U} \longrightarrow \mathcal{U}_1$, $a \longmapsto \{a\}$. Zobrazení s je zřejmě surjektivní i injektivní (proč?), čili bijekce. Existuje proto inverzní zobrazení $t : \mathcal{U}_1 \longrightarrow \mathcal{U}$, $\{a\} \longmapsto a$, 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.* Alternativně píšeme $\{F_i\}_{i \in I}$. 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 $a \longmapsto [a, b]$.

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 výběrové zobrazení.

Výběrové zobrazení pro *konečný* počet objektů existuje i bez axiomu výběru. Snadno ji popíšeme formulí. Například pro jednu neprázdnou množinu x obsahující prvek c je výběrovým zobrazením $\{[x, c]\}$.

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 $\{F_i\}_{i \in I}$ systém množin. Označme

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

Prvky kartézského součinu nazýváme I-tice a používáme pro ně příhodný zápis $[f_i]_{i \in I}$, přičemž $f_i \in F_i$.

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

Důkaz. Prvek kartézského součinu je totéž co výběrové zobrazení.

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 výběrové zobrazení 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 $\{f_n\}_{n\in\mathbb{N}}$ 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 $\sigma : \mathbb{N} \to \mathbb{N}$ 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 $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 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 $\mathbb{N}\times\mathbb{N}\stackrel{\cdot}{\longrightarrow}\mathbb{N}$*, splňující*

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

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

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

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

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

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

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

a zobrazení $\gamma_n:\mathbb{N}\to\mathbb{N}$ 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

$$a_nx^n+\cdots+a_1x+a_0=\sum_0^n a_nx^n$$

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 $\mathbb{N} \longrightarrow \{0, 1\} = 2$, a proto je prvkem množiny $2^{\mathbb{N}}$ všech zobrazení $\mathbb{N} \longrightarrow 2$. 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.

4. Mohutnosti

Velmi důležitou relaci ekvivalence představuje ekvivalence $\sim$, kdy dvě množiny A, B považujeme za ekvivalentní právě tehdy, když existuje bijekce $A \longrightarrow B$. Konečné množiny jsou ekvivalentní právě tehdy, když mají stejný počet prvků (dokažte). Ekvivelence je zobecnění "rovnosti počtu prvků" na obecné množiny.

Cvičení. Ukažte, že právě definovaná relace $\sim$ je reflexivní, symetrická a tranzitivní.

Cvičení. Ukažte, že pro libovolnou množinu A platí $A \times A \sim A^2$. (A^2 je množina všech zobrazení z dvouprvkové množiny $2 = \{0, 1\}$ do A.

Důležitý příklad ekvivalence poskytuje následující tvrzení.

4.1. Tvrzení. *Je-li X množina, pak*

$$\wp X \sim 2^X,$$

tj. existuje bijekce mezi množinou $\wp X$ všech podmnožin v X a množinou všech zobrazení z X do dvouprvkové množiny.

Důkaz. Bijekcí je zobrazení $\wp X \longrightarrow 2^X$, které dané podmnožině $A \subseteq X$ přiřadí zobrazení $f_A : X \longrightarrow 2^X$, definované předpisem

$$f_A(x) = \begin{cases} 1, & \text{jestliže } x \in A, \\ 0, & \text{jestliže } x \notin A. \end{cases}$$

Inverzní bijekcí $2^X \longrightarrow \wp X$ je zobrazení, které zobrazení $f : X \longrightarrow 2^X$ přiřadí vzor $f^{-1}\{1\}$ jedničky.

O ekvivalentních množinách pravíme, že mají stejnou *mohutnost.* Nic nám nebrání zavést nějaké symboly pro jednotlivé mohutnosti. Obecně se takové symboly nazývají *kardinální čísla.*

Nabízí se myšlenka definovat mohutnosti jako třídy rozkladu $\mathcal{U}/\!\sim$ podle ekvivalence $\sim$. Prvky rozkladu $\mathcal{U}/\!\sim$, tj. třídy ekvivalence $\sim$, jsou však vesměs vlastní třídy, a proto nemohou být prvky jiných tříd. To je další drobný nedostatek zvolené axiomatizace, který se však dá snadno obejít.

Mohutnost množiny A značíme $\#A$. Podle definice

$$\#A = \#B \Leftrightarrow A \sim B.$$

Pro každé $n \in \mathbb{N}$, množiny ekvivalentní s množinou $n = \{0, \dots, n-1\}$ (ekvivalentně, množiny o n prvcích), nazýváme *n-prvkové množiny.* Třída n-prvkových množin budiž označena $\mathcal{U}_n$. Za příslušné kardinální číslo volíme prostě $n \in \mathbb{N}$, to jest, $\#n = n$.

Množiny náležející sjednocení

$$\bigcup_{n \in \mathbb{N}} \mathcal{U}_n$$

se nazývají *konečné množiny.* Množinu $\mathbb{N}$ ztotožňujeme s množinou *konečných mohutností.* Ostatní mohutnosti se nazývají *nekonečné mohutnosti.*

Množiny ekvivalentní s množinou $\mathbb{N}$ se nazývají *spočetné množiny.* Spočetná mohutnost se označuje symbolem $\aleph_0$ ($\aleph$ je první písmeno hebrejské abecedy a čte se *alef*). Máme tedy $\#\mathbb{N} = \aleph_0$. Ještě se dočkáme nekonečně mnoha dalších alefů (dokonce budou tvořit vlastní třídu) a každá nekonečná mohutnost bude některým alefem.

Příklad. Se spočetnými množinami jste se již seznámili v přednášce z matematické analýzy. Měli byste (nalezením příslušné bijekce) umět ověřit, že

$$\mathbb{N} \sim \mathbb{Z}, \quad \mathbb{N} \sim \mathbb{N} \times \mathbb{N}, \quad \mathbb{N} \sim \mathbb{Q}.$$

Návod: Uspořádejte celá resp. racionální čísla do posloupnosti

Z výsledku plyne, že $\#\mathbb{Z} = \#(\mathbb{N} \times \mathbb{N}) = \#\mathbb{Q} = \aleph_0$.

Zatím nemůžeme definovat třídu kardinálních čísel. Tento nedostatek napravíme později. Předesíláme, že kardinální čísla tvoří vlastní třídu.

4.1. Aritmetika kardinálních čísel

Nyní zavedeme sčítání, násobení a umocňování kardinálních čísel, které bude zobecněním obdobných aritmetických operací s přirozenými čísly. Budeme k tomu potřebovat další výsledky o množinách.

Při sčítání mohutností se používá disjunktní sjednocení množin.

4.2. Definice. Buďte A, B dvě množiny. Množina $(\{0\} \times A) \cup (\{1\} \times B)$ se nazývá *disjunktní sjednocení* množin A, B a značí se $A \sqcup B$.

Snadno se vidí, že množiny $\{0\} \times A$ a $\{1\} \times B$ nemají žádné společné prvky (proč?) a v tom spočívá smysl této konstrukce. Později ji zobecníme na systémy množin.

4.3. Tvrzení. *Buďte A, B dvě disjunktní množiny. Pak $A \cup B \sim A \sqcup B$.*

Důkaz. Zadejme zobrazení $h : A \cup B \to A \sqcup B$ předpisem

$$h(x) = \begin{cases} [0, x], & \text{když } x \in A, \\ [1, x], & \text{když } x \in B. \end{cases}$$

Ukažte jako cvičení, že h je bijekce.

4.4. Tvrzení. *Buďte $A \sim A'$ dvě ekvivalentní množiny a $B \sim B'$ jiné dvě ekvivalentní množiny. Pak*

1° $\quad A \sqcup B \sim A' \sqcup B'$,

2° $\quad A \times B \sim A' \times B'$,

3° $\quad B^A \sim {B'}^{A'}$

jsou ekvivalentní množiny.

Důkaz. Buďte $g_A : A \to A'$ a $g_B : B \to B'$ bijekce.

1° : Zaveďme zobrazení

$$g_A \sqcup g_B : A \sqcup B \to A' \sqcup B'$$

předpisem

$$(g_A \sqcup f_B)(x) = \begin{cases} [0, g_A(a)], & \text{když } x = [0, a] \in \{0\} \times A, \\ [1, g_B(b)], & \text{když } x = [1, b] \in \{1\} \times B. \end{cases}$$

Snadno se ukáže, že $g_A \sqcup g_B$ je bijekce s inverzí ${g_A}^{-1} \sqcup {g_B}^{-1}$. Tudíž, $A \sqcup B$ a $A' \sqcup B'$ jsou ekvivalentní.

2° : Zaveďme zobrazení

$$g_A \times g_B : A \times B \longrightarrow A' \times B'$$

předpisem

$$(g_A \times g_B)(a, b) = [g_A(a), g_B(b)].$$

Snadno se ukáže, že $g_A \times g_B$ je bijekce s inverzí ${g_A}^{-1} \times {g_B}^{-1}$. Tudíž, $A \times B$ a $A' \times B'$ jsou ekvivalentní.

3° . Zobrazení $B^A \longrightarrow {B'}^{A'}$, $f \mapsto g_B \circ f \circ g_A^{-1}$, má inverzi ${B'}^{A'} \longrightarrow B^A$, $h \mapsto g_B^{-1} \circ h \circ g_A$, a proto je bijektivní. Tudíž, B^A a ${B'}^{A'}$ jsou ekvivalentní.

V důsledku posledního tvrzení můžeme zavést sčítání, násobení a umocňování kardinálních čísel předpisy

1° $\quad \#A + \#B = \#(A \sqcup B)$,

2° $\quad \#A \times \#B = \#(A \times B)$,

3° $\quad (\#B)^{(\#A)} = \#(B^A)$.

Jinak řečeno, k daným mohutnostem libovolně vybereme množiny, které je reprezentují, provedeme s nimi odpovídající množinovou operaci a zjistíme mohutnost výsledku.

Cvičení. Přesvědčte se, že $1 + 1 = 2$, $1 \times 2 = 2$, $1^2 = 1$, $2^1 = 2$.

Cvičení. Ukažte, že $\aleph_0 + 1 = \aleph_0 + 2 = \cdots = \aleph_0 + \aleph_0 = \aleph_0$.
Návod: Uspořádávání do posloupnosti.

Cvičení. Ukažte, že ${\aleph_0}^2 = {\aleph_0}^3 = \cdots = \aleph_0$. (Pozor, ${\aleph_0}^{\aleph_0} = \aleph_0$ neplatí!)
Návod: Uspořádávání do posloupnosti.

Pro operace s kardinálními čísly platí obvyklé zákony aritmetiky.

4.5. Tvrzení. *Buďte* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *libovolné mohutnosti. Pak*

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a},$$
$$0 + \mathfrak{a} = \mathfrak{a},$$
$$(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c}),$$
$$\mathfrak{a} \times \mathfrak{b} = \mathfrak{b} \times \mathfrak{a},$$
$$1 \times \mathfrak{a} = \mathfrak{a},$$
$$(\mathfrak{a} \times \mathfrak{b}) \times \mathfrak{c} = \mathfrak{a} \times (\mathfrak{b} \times \mathfrak{c}),$$
$$\mathfrak{a} \times (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \times \mathfrak{b} + \mathfrak{a} \times \mathfrak{c},$$
$$0 \times \mathfrak{a} = 0,$$
$$\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}} \times \mathfrak{a}^{\mathfrak{c}},$$
$$\mathfrak{a}^{\mathfrak{b}\times\mathfrak{c}} = (\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}},$$
$$(\mathfrak{a} \times \mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}} \times \mathfrak{b}^{\mathfrak{c}},$$
$$\mathfrak{a}^0 = 1,$$
$$\mathfrak{a}^1 = \mathfrak{a}.$$

Důkaz. Nechť $\mathfrak{a} = \#A$, $\mathfrak{b} = \#B$, $\mathfrak{c} = \#C$. Jako cvičení nalezněte potřebné bijekce.

Cvičení. Ukažte, že pro každou mohutnost $\mathfrak{m}$ platí $1^{\mathfrak{m}} = 1$, $\mathfrak{m} + \mathfrak{m} = 2 \times \mathfrak{m}$, $\mathfrak{m}^2 = \mathfrak{m} \times \mathfrak{m}$. A pokud $\mathfrak{m} \neq 0$, pak $0^{\mathfrak{m}} = 0$.

Operace s kardinálními čísly mají i analogie pro systémy kardinálních čísel.

4.6. Definice. Buď $\{F_i\}_{i \in I}$ systém množin. Jeho *disjunktní sjednocení* definujeme jako sjednocení

$$\bigsqcup_{i \in I} F_i = \bigcup_{i \in I} (\{i\} \times F_i).$$

Podobně jako u binární operace $\sqcup$ platí, že sjednocované množiny $\{i\} \times F_i$ nemají žádné společné prvky (proč?) a opět v tom spočívá smysl této konstrukce.

4.7. Tvrzení. *Buď $\{F_i\}_{i \in I}$ systém množin po dvou disjunktních, čili takových, že $F_i \cap F_j = \emptyset$, kdykoliv $i \neq j \in I$. Pak $\bigcup_{i \in I} F_i \sim \bigsqcup_{i \in I} F_i$.*

Důkaz. Zadejme zobrazení $h : \bigcup_{i \in I} F_i \to \bigsqcup_{i \in I} F_i$ předpisem

$$h(x) = [i, x], \quad \text{když } x \in F_i.$$

Ukažte jako cvičení, že h je bijekce.

4.8. Tvrzení. *Buďte $F_i \sim F_i'$ systémy ekvivalentních množin. Pak*

1° $$\bigsqcup_{i \in I} F_i \sim \bigsqcup_{i \in I} F_i',$$

2° $$\prod_{i \in I} F_i \sim \prod_{i \in I} F_i'$$

jsou ekvivalentní množiny.

Důkaz. Buďte $g_i : F_i \to F_i'$ bijekce.

1° : Zaveďme zobrazení

$$\bigsqcup_{i \in I} g_i : \bigsqcup_{i \in I} F_i \to \bigsqcup_{i \in I} F_i'$$

předpisem

$$\left(\bigsqcup_{i \in I} g_i\right)(x) = [i, g_i(f)], \quad \text{když } x = [i, f] \in \{i\} \times F_i$$

Snadno se ukáže, že $\bigsqcup_{i \in I} g_i$ je bijekce s inverzí $\bigsqcup_{i \in I} g_i^{-1}$. Odtud tvrzení.

2° : Zaveďme zobrazení

$$\prod_{i \in I} g_i : \prod_{i \in I} F_i \to \prod_{i \in I} F_i'$$

předpisem

$$\left(\prod_{i \in I} g_i\right)([f_i]_{i \in I}) = [g_i(f_i)]_{i \in I}.$$

Snadno se ukáže, že $\prod_{i\in I} g_i$ je bijekce s inverzí $\prod_{i\in I} g_i^{-1}$. Odtud tvrzení.

Při troše velkorysosti můžeme se systémem $\{F_i\}_{i\in I}$ spojit systém kardinálních čísel $\mathfrak{f}_i = \#F_i$ (ignorujeme fakt, že dosud nemáme třídu kardinálních čísel). Díky právě dokázanému tvrzení lze definovat součet a součin systému kardinálních čísel předpisem

$$\sum_{i\in I} \mathfrak{f}_i = \#\bigcup_{i\in I} F_i,$$

$$\prod_{i\in I} \mathfrak{f}_i = \#\prod_{i\in I} F_i.$$

Jde o přímá zobecnění výše definovaných binárních operací '+' a '×' (ty dostáváme pro dvouprvkové systémy množin).

Platí analogie formulí z tvrzení 6.7, zejména

$$\mathfrak{a} \times \sum_{i\in I} \mathfrak{b}_i = \sum_{i\in I} \mathfrak{a} \times \mathfrak{b}_i,$$

$$\mathfrak{a}^{\sum_{i\in I} \mathfrak{b}_i} = \prod_{i\in I} \mathfrak{a}^{\mathfrak{b}_i},$$

$$\left(\prod_{i\in I} \mathfrak{a}_i\right)^{\mathfrak{b}} = \prod_{i\in I} \mathfrak{a}_i^{\mathfrak{b}},$$

Dokažte je jako cvičení.

Analogií komutativního a asociativního zákona je, že se v definici neuplatňuje žádné uspořádání indexové množiny.

Cvičení. Ukažte, že

$$\sum_{n\in\mathbb{N}} 1 = \sum_{n\in\mathbb{N}} 2 = \cdots = \sum_{n\in\mathbb{N}} \aleph_0 = \aleph_0$$

a obecně

$$\sum_{n\in\mathbb{N}} \mathfrak{m} = \aleph_0 \times \mathfrak{m}.$$

4.2. Uspořádání mohutností

Řekneme, že mohutnost $\mathfrak{a}$ je menší nebo rovna mohutnosti $\mathfrak{b}$, a zapisujeme $\mathfrak{a} \le \mathfrak{b}$, jestliže existuje injektivní zobrazení $A \to B$ takové, že $\mathfrak{a} = \#A$ a $\mathfrak{b} = \#B$. Injektivní zobrazení existuje nebo neexistuje nezávisle na volbě reprezentantů A, B. S trochou velkorysosti dostáváme relaci $\le$ mezi kardinálními čísly (odhlédneme-li od toho, že zatím neumíme definovat třídu kardinálních čísel).

Relace $\le$ je zřejmě reflexivní (skrze identické zobrazení) a tranzitivní (skrze skládání injektivních zobrazení). Cantor–Bernsteinova věta praví, že relace $\le$ je i antisymetrická. Jde o netriviální tvrzení.

Pokud jste zapomněli, co je antisymetrie, odskočte níže na definici 5.1 a zase se vraťte.

4.9. Cantor–Bernsteinova věta. *Jestliže* $\mathfrak{a} \le \mathfrak{b}$ *a zároveň* $\mathfrak{b} \le \mathfrak{a}$*, pak* $\mathfrak{a} = \mathfrak{b}$.

Důkaz. Nechť $\mathfrak{a} = \#A$ a $\mathfrak{b} = \#B$. Podle předpokladu existují injektivní zobrazení $f : A \to B$ a $g : B \to A$. Konstruujme bijektivní zobrazení $A \to B$. Označme

$$\begin{aligned} &A_0 = A, && B_0 = B,\\ &A_1 = gB_0, && B_1 = fA_0,\\ &A_2 = gB_1, && B_2 = fA_1,\\ &A_3 = gB_2, && B_3 = fA_2,\\ &A_4 = gB_3, && B_4 = fA_3,\\ &\quad\vdots \end{aligned}$$

a obecně $A_{i+1} = gB_i$, $B_{i+1} = fA_i$ pro každé přirozené číslo i. Přitom

$$\begin{aligned} &A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots,\\ &B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots, \end{aligned}$$

Dále g dává bijekci $B_i \to A_{i+1}$ a f dává bijekci $A_i \to B_{i+1}$. Tudíž, $g|_{B_{i-1}\setminus B_i}$ je bijekce

$$B_{i-1} \setminus B_i \to A_i \setminus A_{i+1}$$

a podobně $f|_{A_{i-1}\setminus A_i}$ je bijekce

$$A_{i-1} \setminus A_i \to B_i \setminus B_{i+1}.$$

Složením dostáváme bijekce

$$A_0 \setminus A_1 \to B_1 \setminus B_2 \to A_2 \setminus A_3 \to B_3 \setminus B_4 \to \cdots$$

zprostředkované zobrazením f a bijekce

$$B_0 \setminus B_1 \to A_1 \setminus A_2 \to B_2 \setminus B_3 \to A_3 \setminus A_4 \to \cdots$$

zprostředkované zobrazením g. Z nich je možné sestavit bijekce mezi sjednoceními

$$\bigcup_{i\in\mathbb{N}} A_{2i} \setminus A_{2i+1} \longleftrightarrow \bigcup_{i\in\mathbb{N}} B_{2i+1} \setminus B_{2i+2}$$

a rovněž mezi sjednoceními

$$\bigcup_{i\in\mathbb{N}} B_{2i} \setminus B_{2i+1} \longleftrightarrow \bigcup_{i\in\mathbb{N}} A_{2i+1} \setminus A_{2i+2}.$$

Celkově je tím nalezena bijekce mezi podmnožinami

$$\bigcup_{i\in\mathbb{N}} B_i \setminus B_{i+1} \longleftrightarrow \bigcup_{i\in\mathbb{N}} A_i \setminus A_{i+1}.$$

Podmnožina $\bigcup_{i\in\mathbb{N}} B_i \setminus B_{i+1}$ resp. $\bigcup_{i\in\mathbb{N}} A_i \setminus A_{i+1}$ ovšem není rovna celému A resp. B. Nicméně,

$$\bigcup_{i\in\mathbb{N}} A_i \setminus A_{i+1} = A \setminus \bigcap_{i\in\mathbb{N}} A_i, \qquad \bigcup_{i\in\mathbb{N}} B_i \setminus B_{i+1} = B \setminus \bigcap_{i\in\mathbb{N}} B_i.$$

Inkluze $\subseteq$ plyne z inkluzí $A_i \setminus A_{i+1} \subseteq A \setminus \bigcap_{i\in\mathbb{N}} A_i$ pro každé i; podobně pro B. Opačnou inkluzi $\supseteq$ dokážeme úvahou, že pro libovolný prvek $a \in A \setminus \bigcap_{i\in\mathbb{N}} A_i$ existuje nejmenší i takové, že $a \notin A_{i+1}$, načež $a \in A_i \setminus A_{i+1}$.

Tudíž, zatím jsme našli bijekci

$$A \setminus \bigcap_{i\in\mathbb{N}} A_i \longleftrightarrow B \setminus \bigcap_{i\in\mathbb{N}} B_i$$

a ještě zbývá zkonstruovat bijekci mezi průniky $\bigcap_{i\in\mathbb{N}} A_i$ a $\bigcap_{i\in\mathbb{N}} B_i$. To lze provést například následujícím způsobem:

$$\begin{aligned}\bigcap_{i\in\mathbb{N}} A_i = \bigcap_{i\in\mathbb{N}} A_{2i} = \bigcap_{i\in\mathbb{N}} (g\circ f)^i A \xleftrightarrow{f} \bigcap_{i\in\mathbb{N}} f(g\circ f)^i A \\ = \bigcap_{i\in\mathbb{N}} (f\circ g)^i fA = \bigcap_{i\in\mathbb{N}} B_{2i+1} = \bigcap_{i\in\mathbb{N}} B_i.\end{aligned}$$

Důkaz je hotov.

Cantor–Bernsteinova věta je velmi užitečná při výpočtech mohutností. Dokázat dvě nerovnosti (najít dvě injektivní zobrazení) bývá velmi často mnohem snazší než najít bijekci. Příklady najdete v pojednání o mohutnosti kontinua níže.

Hodí se i následující tvrzení o nerovnostech mezi mohutnostmi.

4.10. Tvrzení. *Nechť* $\mathfrak{a}, \mathfrak{a}', \mathfrak{b}, \mathfrak{b}'$ *jsou mohutnosti takové, že* $\mathfrak{a} \le \mathfrak{a}'$*,* $\mathfrak{b} \le \mathfrak{b}'$*. Pak*

1° $\quad \mathfrak{a} + \mathfrak{b} \le \mathfrak{a}' + \mathfrak{b}'$,

2° $\quad \mathfrak{a} \times \mathfrak{b} \le \mathfrak{a}' \times \mathfrak{b}'$,

3° $\quad \mathfrak{a}^{\mathfrak{b}} \le \mathfrak{a}'^{\mathfrak{b}'}$.

Důkaz. Nechť $\mathfrak{a} = \#A$, $\mathfrak{a}' = \#A'$, $\mathfrak{b} = \#B$, $\mathfrak{b}' = \#B'$. Podle předpokladu existují injektivní zobrazení $f : A \longrightarrow A'$, $g : B \longrightarrow B'$. Snadno se ukáže, že zobrazení $f \sqcup g$ a $f \times g$ zkonstruovaná v částech 1° a 2° důkazu tvrzení 4.4 jsou injektivní (proveďte podrobně sami).

V případě 3° je potřeba zkonstruovat injektivní zobrazení $A^B \longrightarrow A'^{B'}$. Buď $h : B \longrightarrow A$ libovolné zobrazení. Z injektivity zobrazení $g : B \longrightarrow B'$ plyne, že existuje zobrazení $\bar{h} : B' \longrightarrow A$ takové, že $\bar{h} \circ g = h$ (proč?). Pak je kompozice $h' = f \circ \bar{h}$ hledané zobrazení $B' \longrightarrow A'$.

Dokažme injektivitu přiřazení $h \mapsto h'$. Nechť jsou dvěma zobrazením $h_1, h_2 : B \longrightarrow A$ přiřazena stejná zobrazení $h_1' = h_2' : B' \longrightarrow A'$. Pak $f \circ h_1' \circ g = f \circ h_2' \circ g$, čili $f \circ h_1 = f \circ h_2$. Jelikož je f injektivní, smíme jím krátit zleva, načež $h_1 = h_2$ a důkaz je hotov.

Cvičení. Proč se v případě 3° nedá použít konstrukce z důkazu tvrzení 4.4?

Klasický Dirichletův princip praví, že pro žádné přirozené číslo n neexistuje injektivní zobrazení $n + 1 \longrightarrow n$. Dokážeme jej jako součást obecnějšího tvrzení.

4.11. Dirichletův princip. *Platí*

$$0 < 1 < 2 < 3 < \cdots < \aleph_0.$$

Důkaz. Připomeňme, že $n + 1 = \{0, 1, 2, \ldots, n\}$.

Neostré nerovnosti $\leq$ plynou z existence injektivních vložení

$$\emptyset \to \{0\} \to \{0,1\} \to \{0,1,2\} \to \cdots \to \mathbb{N}.$$

Nerovnosti $n+1 \neq n$ bezprostředně vyplývají z klasického Dirichletova principu. Důkaz Dirichletova principu povedeme indukcí. Označme D_n tvrzení: "Pro $n \in \mathbb{N}$ neexistuje injektivní zobrazení $n+1 \to n$." Tvrzení D_0 zřejmě platí (proč?). Nechť D_n platí pro pro některé n, dokažme platnost D_{n+1}. Důkaz povedeme sporem. Připusťme tedy, že existuje injektivní zobrazení $f : n+2 \to n+1$. Připomeňme, že $n+2 = \{0,1,2,\ldots,n+1\}$. Prvek $f(n+1) \in n+1$ není obrazem žádného jiného prvku z $n+2$, jak plyne z injektivity. Pak je dobře definována restrikce $f|_{n+1} : n+1 \to n+1 \setminus \{f(n+1)\}$ a je rovněž injektivní. Avšak $n+1 \setminus \{f(n+1)\} \sim n$ (zkonstruujte bijekci), takže jsme obdrželi injektivní zobrazení $n+1 \to n$, což je ve sporu s D_n.

Zbývá dokázat nerovnost $n < \aleph_0$ pro všechna $n \in \mathbb{N}$. Označme D_n tvrzení: "Pro přirozené číslo n neexistuje injektivní zobrazení $\mathbb{N} \to n$." Důkaz indukcí proveďte jako cvičení (princip je podobný, opět je nutno z injektivního zobrazení $\mathbb{N} \to n+1$ vyčlenit injektivní zobrazení $\mathbb{N} \to n$).

4.12. Tvrzení. *Jestliže $\mathfrak{a} < \mathfrak{b} < \mathfrak{c}$, pak $\mathfrak{a} < \mathfrak{c}$.*

Důkaz. Nechť $\mathfrak{a} < \mathfrak{b} < \mathfrak{c}$. Zřejmě $\mathfrak{a} \leq \mathfrak{c}$ (složení injektivních zobrazení je injektivní). Připusťme, že $\mathfrak{a} = \mathfrak{c}$. Pak $\mathfrak{a} < \mathfrak{b} < \mathfrak{a}$ a z Cantor–Bernsteinovy věty plyne, že $\mathfrak{a} = \mathfrak{b}$, spor.

4.13. Cantorova věta. *Pro každou mohutnost $\mathfrak{a}$ platí $\mathfrak{a} < 2^{\mathfrak{a}}$.*

Důkaz. Nechť $\mathfrak{a} = \#A$. Injektivní zobrazení $A \to \wp A$ je například $a \mapsto \{a\}$. Odtud $A \preceq \wp A$, a tedy $\mathfrak{a} \leq 2^{\mathfrak{a}}$.

Připusťme, že $A \sim \wp A$. Nechť $F : A \to \wp A$ je bijektivní zobrazení. Označme

$$X = \{a \in A \mid a \notin F(a)\}.$$

Jelikož je F surjektivní, existuje $x \in A$ takové, že $F(x) = X$. Pak nastane právě jedna ze dvou možností.

1) $x \in X$, čili $x \in F(x)$, načež $x \notin X$ podle definice množiny X, spor;

2) $x \notin X$, čili $x \notin F(x)$, načež $x \in X$ podle definice množiny X, spor.

Tudíž, $A \not\sim \wp A$, a proto $\mathfrak{a} \neq 2^{\mathfrak{a}}$.

4.14. Důsledek. *Ke každému kardinálnímu číslu existuje větší kardinální číslo.*

Poznamenejme, že zatím neumíme odpovědět na otázku, zda existují nesrovnatelné mohutnosti, tj. mohutnosti $\mathfrak{a}, \mathfrak{b}$, pro něž nenastává žádná z možností $\mathfrak{a} < \mathfrak{b}$, $\mathfrak{a} = \mathfrak{b}$, $\mathfrak{a} > \mathfrak{b}$. Odpověď je záporná (neexistují), ale vyžaduje větší úsilí. Odložíme ji do jedné z dalších kapitol spolu s tzv. pohlcovacími zákony, které umožňují stanovovat součty a součiny libovolných mohutností bez zdlouhavého počítání. Mezitím se budeme věnovat dalším mohutnostem, které mají uplatnění v matematické analýze.

4.3. Mohutnost kontinua

Mohutnost $2^{\aleph_0}$, o níž zatím víme jen tolik, že je nespočetná (ostře větší než $\aleph_0$, podle Cantorovy věty), se nazývá *mohutnost kontinua.* Značí se $\mathfrak{c}$. Pojmenování pochází z názvu "kontinuum" pro množinu reálných čísel.

4.15. Tvrzení. *Platí $\mathfrak{c} = \#\mathbb{R}$.*

Důkaz. 1) Nerovnost $\mathfrak{c} \leq \#\mathbb{R}$ dokážeme konstrukcí injektivního zobrazení $2^{\mathbb{N}} \longrightarrow \mathbb{R}$. Zobrazení $\mathbb{N} \longrightarrow 2$ je totéž, co posloupnost $[a_n]_{n\in\mathbb{N}}$ nul a jedniček, $a_n \in \{0,1\}$. Takové posloupnosti můžeme přiřadit třeba reálné číslo s desetinným rozvojem

$$\sum_{n\in\mathbb{N}} a_n 10^n = 0, a_0a_1a_2\dots$$

Přiřazení je injektivní, protože různým posloupnostem odpovídají různá reálná čísla (problematická splynutí jako např. $1 = 0,999\dots$ se nevyskytnou díky tomu, že jsme zvolili číselnou soustavu se základem $10 \neq 2$).

2) Nerovnost $\#\mathbb{R} \leq \mathfrak{c}$ dokážeme konstrukcí injektivního zobrazení $\mathbb{R} \longrightarrow 2^{\mathbb{Q}}$ (racionálních čísel je též spočetně mnoho). Přiřazení budiž

$$r \longmapsto \mathbb{Q}_{<r} = \{q \in \mathbb{Q} \mid q < r\}.$$

Důkaz injektivity: Nechť jsou $r_1 < r_2$ různá reálná čísla. Pak $\mathbb{Q}_{<r_1} \neq \mathbb{Q}_{<r_2}$, protože existuje racionální číslo $r_1 < q < r_2$ a toto číslo q náleží $\mathbb{Q}_{<r_2}$ a nenáleží $\mathbb{Q}_{<r_1}$.

Důkaz je hotov.

Stejně tak mají mohutnost kontinua intervaly $\mathrm{I}(a,b)$, $\mathrm{I}(a,b]$, $\mathrm{I}[a,b)$, $\mathrm{I}[a,b]$, kde $a < b$ jsou reálná čísla (pro jednoznačnost používáme značení obvyklé v analýze, ale s předsunutým písmenem I). Stačí si všimnout, že pro ně prochází již provedený důkaz rovnosti $\mathfrak{c} = \#\mathbb{R}$ jen s malou modifikací nahrazující injektivní zobrazení $2^{\mathbb{N}} \longrightarrow \mathbb{R}$ injektivním zobrazením $2^{\mathbb{N}} \longrightarrow \mathrm{I}(a,b)$ (jakým?). Potažmo i do zbývajících intervalů $\mathrm{I}(a,b]$, $\mathrm{I}[a,b)$, $\mathrm{I}[a,b]$.

Z Cantor–Bernstainovy věty vyplývá, že existují bijekce mezi množinami $2^{\mathbb{N}}$, $\mathbb{R}$, $\mathrm{I}(a,b)$, $\mathrm{I}(a,b]$, $\mathrm{I}[a,b)$, $\mathrm{I}[a,b]$. Z důkazu Cantor–Bernstainovy věty pak také vyplývá návod, jak by bylo možné ony bijekce sestavit, ale je zřejmé, že konstrukce by byly značně komplikované. V sadě následujících cvičení ukážeme, jak takové bijekce sestrojit snáze.

Cvičení. Najděte bijekci mezi $\mathrm{I}(0,1)$ a $\mathbb{R}$.

Návod: kompozice tg a lineární funkce.

Cvičení. Najděte bijekci mezi $\mathrm{I}(0,1)$ a $\mathrm{I}(0,1]$.

Návod: Oba intervaly rozložte na sjednocení spočetně mnoha jednobodových množin a spočetně mnoha otevřených intervalů, např.

$$\begin{aligned}
\mathrm{I}(0,1) &= \bigcup_{i\in\mathbb{N}\setminus\{0\}} \left\{\frac{1}{2^n}\right\} \quad \cup \quad \bigcup_{i\in\mathbb{N}} \mathrm{I}\left(\frac{1}{2^{n+1}}, \frac{1}{2^n}\right),\\
\mathrm{I}(0,1] &= \bigcup_{i\in\mathbb{N}} \left\{\frac{1}{2^n}\right\} \quad \cup \quad \bigcup_{i\in\mathbb{N}} \mathrm{I}\left(\frac{1}{2^{n+1}}, \frac{1}{2^n}\right).
\end{aligned}$$

Cvičení. Najděte bijekci mezi $\mathrm{I}(0,1]$ a $\mathrm{I}[0,1]$.

Návod: Upravte kontrukci z předchozího cvičení.

Cvičení. Ukažte, že

$$\begin{aligned}
&\mathfrak{c} = \mathfrak{c} + 1 = \mathfrak{c} + 2 = \dots = \mathfrak{c} + \aleph_0 = \mathfrak{c} + \mathfrak{c} = \mathfrak{c} + \mathfrak{c} + \mathfrak{c} = \dots = \aleph_0 \times \mathfrak{c}\\
&\quad = \mathfrak{c} \times \mathfrak{c} = \mathfrak{c} \times \mathfrak{c} \times \mathfrak{c} = \dots = \mathfrak{c}^{\aleph_0}.
\end{aligned}$$

Cvičení. Ukažte, že $\#\mathbb{C} = \mathfrak{c}$.

Cvičení. Ukažte, že množina všech spojitých funkcí $\mathbb{R} \to \mathbb{R}$ má mohutnost kontinua.
Návod: Spojitá funkce je určena svými hodnotami na racionálních číslech.

Příklad. **Cantorovo diskontinuum** V první části důkazu věty 4.15 jsme sestrojili injektivní zobrazení $2^{\mathbb{N}} \to \mathbb{R}$. Posloupnosti $[a_n]_{n\in\mathbb{N}}$ nul a jedniček jsme přiřadili reálné číslo s desetinným rozvojem

$$\sum_{n\in\mathbb{N}} a_n 10^n = 0, a_0 a_1 a_2 \ldots$$

Obrazem tohoto zobrazení je podmnožina v $\mathbb{R}$, která se nazývá Cantorovo diskontinuum. Můžeme ji popsat jako množinu všech reálných čísel z intervalu $\mathrm{I}[0,1]$, jejichž desetinný rozvoj obsahuje jen nuly a jedničky (včetně rozvojů s nekonečně mnoha po sobě jdoucími jedničkami). Stejnou množinu dostaneme tak, že z intervalu $\mathrm{I}[0,1]$ vyloučíme otevřený interval $\mathrm{I}(\frac{1}{10}, \frac{9}{10})$, tedy prostředních osm desetin, což opakujeme do nekonečna. Jak se dá ukázat, z jednotkového intervalu takto vyloučíme intervaly v celkové délce 1. Přesto má Cantorovo diskontinuum mohutnost kontinua.

Cvičení. Dokažte tvrzení uvedená v předchozím příkladu.

4.4. Cantorův důkaz existence transcendentních čísel

V Cantorově době byla známa jen jednotlivá transcendentní čísla, přičemž množina transcendentních čísel není dodnes úplně prozkoumána. Cantor překvapivě snadno dokázal, že transcendentních čísel je nekonečně mnoho.

Připomeňme definice. Algebraickým číslem se rozumí komplexní číslo, které je kořenem nenulového polynomu s racionálními koeficienty. Transcendentním číslem se rozumí komplexní číslo, které není algebraické.

4.16. Tvrzení. *Mohutnost množiny algebraickcýh čísel je $\aleph_0$.*

Důkaz. Nechť $\mathfrak{A}$ je množina všech algebraických čísel.
1) $\aleph_0 \le \#\mathfrak{A}$, protože každé racionální číslo je algebraické (proč?).
2) Ukažme, že $\#\mathfrak{A} \le \aleph_0$. Množinu algebraických čísel vyjádříme jako sjednocení

$$\mathfrak{A} = \bigcup_{n\in\mathbb{N}} \mathfrak{A}_n,$$

kde n je stupeň příslušného minimálního polynomu (minimální polynom algebraického čísla a je polynom minimálního stupně mezi polynomy s racionálními koeficienty a kořenem a). Mohutnost množiny $\mathfrak{A}_n$ je $n \times \#\mathbb{Q}^n = n \times {\aleph_0}^n = \aleph_0$ (proč?). Dostáváme tedy

$$\#\mathfrak{A} \le \# \bigcup_{n\in\mathbb{N}} \mathfrak{A}_n \le \sum_{n\in\mathbb{N}} \#\mathfrak{A}_n = \sum_{n\in\mathbb{N}} \aleph_0 = \aleph_0 \times \aleph_0 = \aleph_0.$$

Důkaz je hotov.

4.17. Důsledek. *Mohutnost množiny transcendentních čísel je $\mathfrak{c}$.*

4.5. Další mohutnosti matematické analýzy

Již jsme se zmínili, že existuje nekonečně mnoho (dokonce vlastní třída) nekonečných mohutností. Kromě alefů $\aleph$, které patří k poměrně obtížným pojmům, existuje nekonečná řada mohutností $\beth$ (beth, druhé písmeno hebrejské abecedy), které jsou mohutnostmi množin hojných v analýze.

Pro přirozená čísla $n \in \mathbb{N}$ definujme $\beth_n$ rekurzivním předpisem

$$\beth_0 = \aleph_0, \quad \beth_{n+1} = 2^{\beth_n}.$$

Podle Cantorovy věty zřejmě $\beth_0 < \beth_1 < \beth_2 < \cdots$. Máme

$$\beth_1 = 2^{\aleph_0} = \mathfrak{c}, \quad \beth_2 = 2^{\beth_1} = 2^{\mathfrak{c}}, \quad \beth_3 = 2^{\beth_2} = 2^{2^{\mathfrak{c}}}, \quad \ldots$$

a také

$$\beth_0 = \#\mathbb{N}, \quad \beth_1 = \#\wp\mathbb{N}, \quad \beth_2 = \#\wp\wp\mathbb{N}, \quad \beth_3 = \#\wp\wp\wp\mathbb{N}, \quad \ldots$$

Cvičení. Ukažte, že mohutnost $\beth_2$ mají množiny
1) $\wp\mathbb{R}$ všech podmnožin množiny reálných čísel;
2) $\mathbb{R}^{\mathbb{R}}$ všech reálných funkcí jedné reálné proměnné;
3) $\sum_{n\in N} \mathbb{R}^{\mathbb{R}^n}$ všech reálných funkcí konečně mnoha reálných proměnných.

4.18. Poznámka. Čím se aritmetika kardinálních čísel liší od aritmetiky přirozených čísel? Především nelze krátit ani v součtech ani v součinech. Například $1 + \aleph_0 = 0 + \aleph_0$, ačkoliv $1 \neq 0$. Podobně $1 \times \aleph_0 = 2 \times \aleph_0$, ačkoliv $1 \neq 2$. Nelze pak zavést ani rozumné odečítání a dělení.

Společné zase mají to, že ani v oboru kardinálních čísel neexistují dělitelé nuly. Když $\mathfrak{a} \times \mathfrak{b} = 0$, pak $\mathfrak{a} = 0$ nebo $\mathfrak{b} = 0$, protože kartézský součin neprázdných množin je neprázdný. Žádné důsledky pro krácení to ovšem nemá, protože není k dospozici odečítání.

5. Dobře uspořádané množiny a ordinální čísla

Na předchozích stránkách jsme došli k jisté představě o kardinálních číslech (mohutnostech množin), které je ovšem prozatím značně děravá. O nekonečných mohutnostech hodnověrně víme jen tolik, že existuje vzrůstající řada nekonečných mohutností, ale nevíme skoro nic o ostatních mohutnostech.

Nejlepší znalosti máme o spočetných množinách, kde funguje metoda matematická indukce. Metodu lze snadno zobecnit na obecnější dobře uspořádané množiny. Zobecnění se nazývá transfinitní indukce.

Zatímco kardinální čísla zobecňují přirozená čísla ve smyslu množství, ordinální čísla zobecňují přirozená čísla ve smyslu seřazení. Pokračování za konečná čísla je ovšem rozdílné. Na jedno nekonečné kardinální číslo připadá nekonečně mnoho ordinálních čísel. Například, zatímco existuje jen jedna spočetná mohutnost $\aleph_0$, spočetných ordinálních čísel je nekonečně mnoho a dokonce nespočetně mnoho (přesně $\aleph_1$). A že paradoxů není nikdy dost, uvidíme, že mezi kardinálními čísly a ordinálními čísly existuje bijekce.

5.1. Uspořádání

Nejdříve připomeneme pojmy týkající se obecných relací uspořádání.

5.1. Definice. Řekneme, že relace $\leq$ na třídě A je *antisymetrická*, jestliže platí implikace $(a \leq b \wedge b \leq a) \Rightarrow a = b$ pro všechna $a, b \in A$.

Reflexivní, antisymetrická a tranzitivní relace se nazývá *uspořádání*.

Je-li $\leq$ uspořádání na třídě A, pak $\geq$ definovaná předpisem $a \geq b \Leftrightarrow b \leq a$ je rovněž uspořádání na třídě A.

Je-li $\leq$ uspořádání na třídě A, pak relace $<$ definovaná předpisem $a < b \Leftrightarrow (a \leq b \wedge a \neq b)$ se nazývá *ostré uspořádání*. Podobně $>$.

Třída spolu se zadaným uspořádáním se nazývá *uspořádaná třída*. Množina spolu se zadaným uspořádáním se nazývá *uspořádaná množina*.

Každá podtřída $B \subseteq A$ uspořádané třídy A je uspořádaná třída, definujeme-li indukované uspořádání na B formulí $\leq_B \, = \, \leq_A \cap (B \times B)$, to jest, klademe-li $a \leq_B b \Leftrightarrow a \leq_A b$ pro $a, b \in B$. Podobně pro ostré uspořádání.

Příklad. Inkluze $\subseteq$ je uspořádání na univerzální třídě $\mathcal{U}$ a každé její podtřídě. Ostrá inkluze $\subset$ je ostré uspořádání na univerzální třídě $\mathcal{U}$ a každé její podtřídě.

Příklad. Množiny $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ jsou uspořádány obvyklým způsobem "podle velikosti."

Příklad. Prázdná relace $\emptyset \times \emptyset$ na prázdné množině je ostré i neostré uspořádání.

5.2. Definice. Buď A uspořádaná třída. Prvek $m \in A$ se nazývá *největší prvek* resp. *nejmenší prvek*, jestliže

$$(\forall a \in A)\, a \leq m \quad \text{resp.} \quad (\forall a \in A)\, m \leq a.$$

Prvek $m \in A$ se nazývá *maximální prvek* resp. *minimální prvek*, jestliže

$$(\forall a \in A)\, (m \leq a \Rightarrow m = a) \quad \text{resp.} \quad (\forall a \in A)\, (a \leq m \Rightarrow m = a).$$

Příklad. Univerzální třída $\mathcal{U}$ má nejmenší prvek $\emptyset$ a nemá žádný největší prvek.

Cvičení. Uspořádaná třída má nejvýše jeden největší a nejvýše jeden nejmenší prvek.

Cvičení. Největší prvek uspořádané třídy je jediným maximálním prvkem této třídy. Nejmenší prvek uspořádané třídy je jediným minimálním prvkem této třídy.

Cvičení. Uveďte příklad uspořádané množiny, která má jediný maximální prvek a žádný největší prvek.

Návod. Množina je nutně nekonečná.

5.3. Definice. Buď X uspořádaná třída, $A \subseteq X$ její podtřída. Prvek $m \in X$ se nazývá *horní závora* resp. *dolní závora* podtřídy A, jestliže

$$(\forall a \in A)\, a \leq m \quad \text{resp.} \quad (\forall a \in A)\, m \leq a.$$

Existuje-li nejmenší horní závora, nazývá se *supremum* a značí se $\sup A$. Existuje-li největší dolní závora, nazývá se *infimum* a značí se $\inf A$.

Cvičení. Každá množina $A \subseteq \mathcal{U}$ (tj. množina množin) má supremum i infimum vzhledem k uspořádání inkluzí a platí $\sup A = \bigcup A$ a $\inf A = \bigcap A$.

5.2. Řetězce

5.4. Definice. Prvky a, b uspořádané množiny se nazývají *srovnatelné*, jestliže platí

$$(a \leq b) \vee (b \leq a).$$

Uspořádání $\leq$ na třídě A je *úplné*, jestliže jsou každé dva prvky třídy A srovnatelné. Třída spolu s úplným uspořádáním se nazývá *úplně uspořádaná třída*.

Úplně uspořádaná množina se nazývá *řetězec*.

Příklad. Množina reálných čísel s obvyklým upořádáním je řetězec.

Podmnožina řetězce s indukovaným uspořádáním je opět řetězec (protože nemá nesrovnatelné prvky) a nazývá se *podřetězec*.

Příklad. Intervaly $\mathrm{I}(a,b)$, $\mathrm{I}(a,b]$, $\mathrm{I}[a,b)$, $\mathrm{I}[a,b]$ jakož i množiny $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ tvoří podřetězce v řetězci reálných čísel.

Příklad. Uspořádání třídy $\mathcal{U}$ inkluzí není úplné. Množiny $\{a\}$ a $\{b\}$, kde $a \neq b$, jsou nesrovnatelné.

Buď M řetězec, buďte $m, n \in M$ dva prvky takové, že $m < n$ a neexistuje $p \in M$ takové, že $m < p < n$. Pak řekneme, že prvek n je *následovník* prvku m, resp., že prvek m je *předchůdce* prvku n a zapisujeme $m <\circ\, n$ nebo $n \circ\!> m$.

Cvičení. Ukažte, že každý prvek $a \in M$ má nejvýše jednoho předchůdce a nejvýše jednoho následovníka .

5.3. Dobré uspořádání

5.5. Definice. Řekneme, že uspořádaná třída T je *dobře uspořádaná*, jestliže každá neprázdná podtřída $A \subset T$ obsahuje nejmenší prvek.

5.6. Tvrzení. *Každá dobře uspořádaná třída je úplně uspořádaná.*

Důkaz. Připusťme, že existují nesrovnatelné prvky a, b. Pak množina $\{a, b\}$ nemá nejmenší prvek.

Příklad. Každý konečný řetězec je dobře uspořádaný.

Příklady. 1. Množiny $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nejsou dobře uspořádané, neboť neobsahují nejmenší prvek.
2. Polouzavřený interval $\mathrm{I}[0,1)$ není dobře uspořádaná množina, protože jeho podmnožina $\mathrm{I}(0,1)$ neobsahuje nejmenší prvek.

5.7. Tvrzení. *Množina přirozených čísel je dobře uspořádaná.*

Důkaz. Buď $A \subseteq \mathbb{N}$ neprázdná podmnožina, buď $a \in A$ libovolný prvek. Prvky větší než a nemají vliv na existenci nejmenšího prvku, prvky menší nebo rovné a zase tvoří neprázdný konečný řetězec, který má nejmenší prvek.

Připomeňme, že prvek b uspořádané množiny je *následovníkem* prvku a, jestliže $a < b$ a neexistuje c takové, že $a < c < b$.

5.8. Tvrzení. *Každý prvek dobře uspořádané třídy, s výjimkou největšího, má následovníka.*

Důkaz. Buď X dobře uspořádaná třída, buď $a \in X$ libovolný prvek, který není největším prvkem v X. Nechť $B = \{x \in X \mid a < x\}$. Kdyby byla třída B prázdná, bylo by $x \geq a$ pro všechny prvky $x \in X$ (protože X je úplně uspořádaná) a a by byl největším prvkem v X, což podle předpokladu není. Tudíž, B je naprázdná a podle předpokladu má nejmenší prvek. Označme jej b. Evidentně $a < b$. Ukažme, že b je následovník prvku a. Připusťme opak, tedy že existuje prvek c takový, že $a < c < b$. Pak $c \in B$, a tedy nutně $b \leq c$, což je spor.

Dobře uspořádanou množinu můžeme znázornit diagramem, v němž jsou prvky seřazeny zleva doprava od menších k větším a každý prvek je spojen úsečkou se svým následovníkem.

Příklady. Pětiprvkový řetězec má diagram

$$\circ\!\!-\!\!\circ\!\!-\!\!\circ\!\!-\!\!\circ\!\!-\!\!\circ.$$

Množina přirozených čísel má diagram

$$\circ\!\!-\!\!\circ\!\!-\!\!\circ\!\!-\!\!\circ\!\!-\cdots,$$

kde tři tečky znamenají spočetné opakování vzoru $\circ\!\!-$.

Cvičení. Ukažte, že v dobře uspořádané množině nemůže existovat nekonečná ostře klesající posloupnost prvků $\cdots < a_2 < a_1 < a_0$.

5.4. Transfinitní indukce

Princip transfinitní indukce umožňuje dokazovat tvrzení tvaru

$$(\forall x \in X)\, \phi(x),$$

kde X je dobře uspořádaná třída. Indukční krok spočívá v důkazu, že z pravdivosti $\phi(x)$ pro všechna $x < a$ plyne pravdivost $\phi(a)$.

5.9. Tvrzení. *Buď $\phi(x)$ formule, buď X dobře uspořádaná třída. Nechť pro všechna $a \in X$ podmínka $(\forall x < a)\, \phi(x)$ implikuje $\phi(a)$. Pak je $\phi(x)$ pravdivá pro všechna $x \in X$.*

Důkaz. Buď $A \subseteq X$ podtřída, tvořená prvky x, pro něž $\phi(x)$ neplatí. Připusťme, že $A \neq \emptyset$. Pak existuje nejmenší prvek $a \in A$, což je nejmenší prvek, pro něž ϕ neplatí. Pro všechny prvky $x < a$ (pokud existují) potom $\phi(x)$ platí, takže, podle předpokladu, platí i $\phi(a)$, což je ve sporu s $a \in A$. Tudíž, $A = \emptyset$, a tedy $\phi(x)$ platí pro všechna $x \in X$.

Může se zdát, že $\phi(x)$ nemusí platit pro nejmenší prvek a třídy X. Opak je pravdou, neboť třída $\{x \in X \mid x < a\}$ je v tomto případě prázdná, a proto je podmínka $(\forall x < a)\, \phi(x)$ splněna.

Princip transfinitní indukce také umožňuje konstruovat množiny F_x závislé na prvku dobře uspořádané třídy X. K tomu stačí dokazovat formule tvaru

$$(\forall x \in X)(\exists F_x \in \mathcal{U})\, \phi(x, F_x).$$

V tom případě hovoříme o transfinitně rekurzívní konstrukci tříd F_x.

5.5. Izotonní zobrazení a izomorfismy

5.10. Definice. Zobrazení $f : X \to Y$ mezi uspořádanými třídami se nazývá *izotonní*, jestliže platí implikace $a \le b \Rightarrow f(a) \le f(b)$ pro libovolná $a, b \in X$.

Zobrazení $f : X \to Y$ mezi uspořádanými třídami se nazývá *ostře izotonní*, jestliže platí implikace $a < b \Rightarrow f(a) < f(b)$ pro libovolná $a, b \in X$.

Příklad. Identické zobrazení $\mathrm{id}_X : X \to X$ je izotonní i ostře izotonní při jakémkoliv uspořádání na X. Konstantní zobrazení $X \to 1$ (všichni na jednoho) je izotonní, ale nikoliv ostře izotonní, má-li X více než jeden prvek.

Cvičení. Nechť je injektivní zobrazení izotonní. Ukažte, že je potom ostře izotonní.

Je-li bijektivní zobrazení izotonní, neznamená to ještě, že i inverzní zobrazení je izotonní. Nejjednodušším protipříkladem je zobrazení dvouprvkové množiny sestáváající ze dvou nesrovnatelných prvků na dvouprvkový řetězec.

5.11. Definice. Bijektivní zobrazení $f : X \to Y$ mezi uspořádanými třídami se nazývá *izomorfismus*, jsou-li f i f^{-1} izotonní. Říkáme, že uspořádané třídy X, Y jsou *izomorfní*, pokud mezi nimi existuje izomorfismus. Zapisujeme $X \cong Y$.

Cvičení. Každý izomorfismus $X \to Y$ je ostře izotonní zobrazení.

5.12. Tvrzení. *Každé bijektivní izotonní zobrazení $X \to Y$, kde třída X je řetězec, je izomorfismus.*

Důkaz. Nechť $f(a) < f(b)$. Protože X je úplně uspořádaná, platí $a < b$ nebo $a = b$ nebo $b < a$. Druhá možnost odporuje injektivitě, třetí odporuje izotónnosti a zbývá jen první, tedy $a < b$.

6. Ordinální čísla

O izomorfních uspořádaných množinách říkáme, že mají stejný *ordinální typ*. Ordinální čísla můžeme definovat jako ordinální typy dobře uspořádaných množin. Znamená to, že dvě ordinální čísla jsou si rovna, právě když jsou ordinálními typy izomorfních dobře uspořádaných množin. Pro ordinální typy zavedeme zvláštní symboly. Podobným způsobem jsme zavedli kardinální čísla, jen místo bijekcí mezi množinami rozhodují izomorfismy dobře uspořádaných množin.

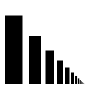
Izomorfismus uspořádaných množin je bijekce, a proto mají izomorfní uspořádané množiny stejnou mohutnost. Odtud plyne, že každé ordinální číslo má určitou mohutnost, přičemž může existovat více různých ordinálních čísel stejné mohutnosti.

Podobně jako u mohutností taková definice neumožňuje utvořit třídu ordinálních čísel. To nám dovolí až von Neumannova definice ordinálních čísel čili ordinálů, kterou uvedeme později. Není tak názorná jako definice pomocí ordinálních typů.

Příklady. 1. Každé přirozené číslo n označuje rovněž ordinální typ řetězce o n prvcích (již víme, že je dobře uspořádaný). Jeho diagram sestává z n bodů spojených úsečkami, např. $1, 2, 3$ mají po řadě diagramy

$$\circ, \quad \circ\!\!-\!\!\circ, \quad \circ\!\!-\!\!\circ\!\!-\!\!\circ.$$

2. Symbolem ω se označuje ordinální typ množiny všech přirozených čísel uspořádaných podle velikosti (rovněž dobře uspořádaná množina). Výše jsme uvedli její diagram $\circ\!\!-\!\!\circ\!\!-\!\!\circ\!\!-\!\!\circ\!\!-\cdots$. Jinou názornou ilustrací čísla ω je nekonečné sloupořadí



(nekonečná řada skoupů táhnoucích se k obzoru).

6.1. Aritmetika ordinálních čísel

Podobně jako kardinální čísla, lze i ordinální čísla sečítat, násobit a umocňovat. Operace sčítání a násobení definujeme podobně jako stejnojmenné operace s kardinálními čísly, pouze je potřeba zařídit, aby disjunktní sjednocení a součiny dobře uspořádaných množin byly dobře uspořádané množiny. (Podobný postup není možný v případě umocňování.)

Upozorněme též, že operace s ordinálními čísly nejsou komutativní.

6.2. Sčítání ordinálních čísel

6.1. Definice. Buďte A, B dvě dobře uspořádané množiny. Množina $(\{0\} \times A) \cup (\{1\} \times B)$ s uspořádáním daným formulí

$$(i, a) \leq (j, b) \quad \Leftrightarrow \quad i < j \vee (i = j \wedge a \leq b)$$

se nazývá *disjunktní sjednocení dobře uspořádaných množin* nebo také *součet dobře uspořádaných množin* A, B a značí se $A \sqcup B$ nebo $A + B$.

Slovy: Prvky disjunktního sjednocení uspořádáme

1. podle prvních složek, přičemž $0 < 1$;
2. v případě rovnosti podle druhých složek, přičemž použijeme uspořádání z té množiny, kde se oba prvky nacházejí.

Nebo jinak: Prvky původem z A předcházejí všechny prvky původem z B, kdežto dvojice prvků původem z jedné a téže množiny jsou uspořádány stejně jako ve "své" množině.

Schematicky

$$\boxed{\mathrm{A}}\!-\!\boxed{\mathrm{B}}.$$

6.2. Definice. Buďte α, β po řadě ordinální typy dobře uspořádaných množin A, B. Součet $\alpha + \beta$ definujeme jako ordinální typ disjunktního sjednocení $A \sqcup B$.

Definice je korektní, protože jsou-li $A \cong A'$, $B \cong B'$ izomorfní dobře uspořádané množiny, pak jsou i $A \sqcup B$, $A' \sqcup B'$ izomorfní dobře uspořádané množiny. Ohledně izomorfismu se důkaz vede podobně jako ohledně ekvivakence množin (jsou-li f, g izomorfismy, je i $f \sqcup g$ izomorfismus). Ohledně dobrého uspořádání je důkaz proveden níže v zobecnění na systémy.

Příklad. Kolik je $1 + 2$? Máme

$$\circ \sqcup \circ\!-\!\circ = \boxed{\circ}\!-\!\boxed{\circ\!-\!\circ} = \circ\!-\!\circ\!-\!\circ,$$

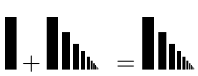
a tedy $1 + 2 = 3$.

Poznámka. Ordinální čísla jsou spíš obdobou řadových číslovek než číslovek základních, přesto si dovolíme se na ně ptát otázkou "kolik?" spíše než otázkou "kolikátý?".

Příklad. Kolik je $1 + \omega$? Máme

$$\circ \sqcup \circ\!-\!\circ\!-\cdots = \boxed{\circ}\!-\!\boxed{\circ\!-\!\circ\!-\cdots} = \circ\!-\!\circ\!-\cdots = \omega$$

neboli

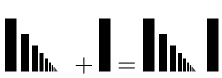


(sloup a sloupořadí = sloupořadí). Tudíž, $1 + \omega = \omega$. Podobně $2 + \omega = \omega$, atd.

Příklad. Kolik je $\omega + 1$? Máme

$$\circ\!-\!\circ\!-\cdots \sqcup \circ = \boxed{\circ\!-\!\circ\!-\cdots}\!-\!\boxed{\circ} = \circ\!-\!\circ\!-\cdots\circ.$$

neboli

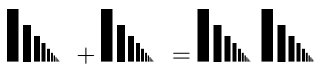


Vidíme, že $\omega + 1 \neq \omega$. Vskutku, v ω je jediný prvek, 0, který nemá přechůdce, kdežto v $\omega + 1$ jsou takové prvky dva. Podobně $\omega + 2 \neq \omega + 1$ (proč?), atd.

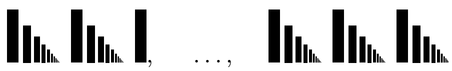
Příklad. Kolik je $\omega + \omega$? Máme

$$
\begin{aligned}
&\circ\!-\!\!\circ\!-\cdots \sqcup \circ\!-\!\!\circ\!-\cdots \\
&\quad = \boxed{\circ\!-\!\!\circ\!-\cdots}-\boxed{\circ\!-\!\!\circ\!-\cdots} \\
&\quad = \circ\!-\!\!\circ\!-\cdots\circ\!-\!\!\circ\!-\cdots
\end{aligned}
$$

neboli



(dvě nekonečná sloupořadí za sebou). Vidíme, že $\omega+\omega$ je další ordinální číslo, různé od již sestrojených. Podobně $\omega + \omega + 1, \ldots, \omega + \omega + \omega$ jsou po řadě



další nová ordinální čísla.

Shora uvedené příklady ukazují, že na rozdíl od sčítání kardinálních čísel není sčítání ordinálních čísel komutativní. Například $1 + \omega = \omega \neq \omega + 1$. Nicméně, sčítání ordinálních čísel je asociativní (ověřte jako cvičení).

Vyplatí se rovnou zavést i zobecnění na systémy. Dobře uspořádaný systém dobře uspořádaných množin je systém $\{A_i\}_{i\in I}$, kde jednotliví sčítanci A_i i indexová množina I jsou dobře uspořádáni. Disjunktní sjednocení

$$\bigsqcup_{i\in I} A_i = \bigcup_{i\in I}(\{i\} \times A_i)$$

uspořádáme podle předpisu

$$(i, a_i) \leq (j, a_j) \quad \Leftrightarrow \quad i < j \vee (i = j \wedge a_i \leq a_j)$$

(zde $a_i \in A_i$ a $a_j \in A_j$).

Opět platí, že prvky disjunktního sjednocení uspořádáváme

1. podle prvních složek, přičemž přebíráme uspořádání z I;
2. v případě rovnosti podle druhých složek, přičemž použijeme uspořádání z té množiny, kde se oba prvky nacházejí.

Schematicky

$$\boxed{A_{i_1}}-\boxed{A_{i_2}}-\boxed{A_{i_3}}-,$$

přičemž jednotlivé "bloky" jsou uspořádány stejně jako jejich indexy v množině I.

Je zřejmé, že dříve zavedené disjunktní sjednocení dvou množin je speciální případ, kdy indexovou množinou je řetězec 0—1. Zobecnění na n-prvkový řetězec je zřejmé — obdržíme součet n množin.

6.3. Tvrzení. *Disjunktní sjednocení dobře uspořádaného systému dobře uspořádaných množin je dobře uspořádaná množina.*

Důkaz. Buď B neprázdná podmnožina v disjunktním sjednocení $\bigsqcup_{i\in I} A_i$. Nechť I_B je množina všech indexů i takových, že $B \cap A_i \neq \emptyset$. Zřejmě je $I_B \neq \emptyset$ neprázdná (proč?) podmnožina v dobře uspořádané množině I, takže má nejmenší prvek, což je podle definice nejmenší index i takový, že $B \cap A_i \neq \emptyset$. Pak je ovšem $B \cap A_i$ neprázdná podmnožina dobře uspořádané množiny A_i, takže má nejmenší prvek, který je současně nejmenším prvkem podmnožiny B (proč?).

6.4. Definice. Buďte α_i ordinální typy dobře uspořádaných množin A_i, $i \in I$, kde I je dobře uspořádaná. Součet $\sum_{i\in I} \alpha_i$ definujeme jako ordinální typ disjunktního sjednocení $\bigsqcup_{i\in I} A_i$.

Příklad. Máme

$$\sum_{i\in\omega} i = \omega,$$

jak je snadno vidět z diagramu

$$\boxed{\circ}\!-\!\boxed{\circ\!-\!\circ}\!-\!\boxed{\circ\!-\!\circ\!-\!\circ}\!-\!\cdots$$

6.3. Násobení ordinálních čísel

Jako další operaci zavedeme násobení, přičemž se ukáže, že v případě dvou operandů jde o speciální případ sčítání systému ordinálních čísel.

6.5. Definice. Buďte A, B dvě dobře uspořádané množiny. Množina $A \times B$ s uspořádáním daným formulí

$$(a, b) \le (a', b') \quad\Leftrightarrow\quad a < a' \vee (a = a' \wedge b \le b')$$

se nazývá *lexikografický součin dobře uspořádaných množin* nebo jen *součin dobře uspořádaných množin* A, B a značí se $A \times B$.

Slovy: Prvky součinu uspořádáme
1. podle prvních složek,
2. v případě rovnosti podle druhých složek.

Původ přívlastku "lexikografický" nalezneme ve slovníkovém uspořádání dvoupísmenných slov. Je to dobře patrné v níže uvedených příkladech.

Jinak: A krát B znamená, že prvky množiny A nahradíme kopiemi mnžiny B; v rámci jedné a téže kopie přebíráme uspořádání z B, zatímco mezi různými kopiemi přebíráme uspořádání z A. Schematicky

$$\underbrace{\boxed{B}\!-\!\boxed{B}\!-\!\boxed{B}\!-\!\cdots}_{A}$$

Z definic je patrné, že součin $A \times B$ není nic jiného, než disjunktní součet

$$A \times B = \bigsqcup_{A} B$$

systému sestávajícího z kopií množiny B, po jedné pro každý prvek z A, a proto je dobře uspořádaný.

Příklad. Počítejme 3×3. Máme

$$3 \times 3 = \left\{\begin{matrix} [0,0] & [0,1] & [0,2] \\ [1,0] & [1,1] & [1,2] \\ [2,0] & [2,1] & [2,2] \end{matrix}\right\}$$

s lexikografickým uspořádáním

$$[0,0] < [0,1] < [0,2] < [1,0] < [1,1] < [1,2] < [2,0] < [2,1] < [2,2].$$

Vidíme, že zároveň jde o disjunktní sjednocení

$$\boxed{[0,0]\!-\![0,1]\!-\![0,2]}\!-\!\boxed{[1,0]\!-\![1,1]\!-\![1,2]}\!-\!\boxed{[2,0]\!-\![2,1]\!-\![2,2]}.$$

Jelikož součin dvou dobře uspořádaných množin je speciálním případem součtu systému množin, je dobře uspořádán. Můžeme pak pro ordinální čísla α, β, která jsou po řadě ordinálními typy množin A, B, definovat součin $\alpha\beta = \alpha \times \beta$ jako ordinální typ množiny $A \times B$. Čislo α se nazývá *násobitel* (multiplicator), čislo β *násobenec* (multiplicandus). Jelikož násobení není obecně komutativní, na pořadí záleží.

Pro zapamatování: Při zápisu “$\times$” násobíme v pořádí “kolikrát co,” to jest, $\alpha \times \beta$ má význam “αkrát β.”

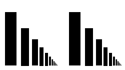
Poznámka. Obvyklý je i zápis součinu v převráceném pořadí jako $\beta \cdot \alpha = \alpha \times \beta$, což znamená, že násobíme v pořádí “co kolikrát,” to jest, $\alpha \cdot \beta$ má význam “α βkrát.” Důvody pro převrácený zápis uvedeme v souvislosti s umocňováním níže.

Pro zachování historické pravdy uveďme, že G. Cantor původně zavedl součin ekvivalentní součinu “$\times$” [v práci Ueber unendliche, lineare Punktmannichfaltigkeiten, *Mathematische Annalen* 21 (1883) 545–591 na str. 551], ale později přešel k převrácenému součinu.

Příklad. Kolik je $2 \times \omega = \bigsqcup_2 \omega$? Dostáváme

$$\boxed{\circ - \circ - \cdots} - \boxed{\circ - \circ - \cdots}$$

což je $\omega + \omega$ neboli



(dvě nekonečná sloupořadí za sebou).

Pro srovnání, $\omega \times 2 = \bigsqcup_\omega 2$ je

$$\boxed{\circ - \circ} - \boxed{\circ - \circ} - \boxed{\circ - \circ} - \cdots$$

čili

$$\circ - \circ - \circ - \circ - \cdots,$$

což je ω. Vidíme, že $2 \times \omega \neq \omega = \omega \times 2$.

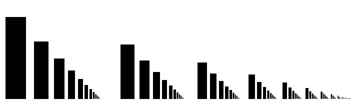
Příklad. Kolik je $\omega \times \omega = \bigsqcup_\omega \omega$? Dostáváme

$$\boxed{\circ - \circ - \cdots} - \boxed{\circ - \circ - \cdots} - \boxed{\circ - \circ - \cdots} - \cdots$$

čili

$$\circ - \circ - \cdots \; \circ - \circ - \cdots \; \circ - \circ - \cdots \;\; \cdots$$

nebo názorněji



(dvojitě nekonečné sloupořadí).

Může se psát i jako mocnina ω^2.

Stejný výsledek dostaneme, když v  nahradíme každý sloup celým sloupořadím.

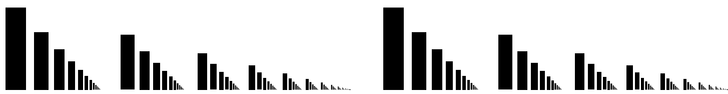
Všimněte si, že ω prvků nemá předchůdce.

Cvičení. Kolik je $1 + \omega^2$? Kolik je $\omega + \omega^2$?

Cvičení. Ukažte, že každý prvek z ω^2 je tvaru $a_1\omega + a_0$, kde a_1, a_0 jsou přirozená čísla.

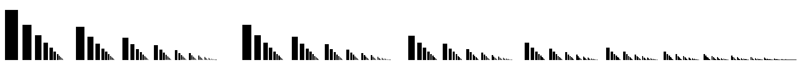
Návod: Viz předchozí obrázek.

Příklad. Dvojnásobek ordinálního čísla ω^2 je $2\omega^2 = 2 \times \omega^2$, což je



(dvě nekonečné řady nekonečných sloupořadí). Všimněte si, že 2ω prvků nemá předchůdce. Podobně trojnásobek atd.

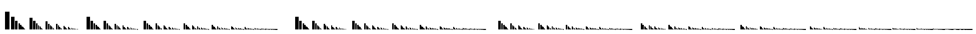
Příklad. Co je ω^3? Definujeme jej jako ω-násobek ordinálního čísla ω^2. Znázornit jej můžeme diagram



(trojitě nekonečné sloupořadí). Stejný výsledek dostaneme, když v ω^2 nahradíme každý sloup sloupořadím, čili jako ω^2-násobek ordinálního čísla ω. Všimněte si, že ω^2 prvků nemá předchůdce.

Cvičení. Ukažte, že každý prvek z ω^3 je tvaru $a_2\omega^2 + a_1\omega + a_0$, kde a_2, a_1, a_0 jsou přirozená čísla.

Příklad. Analogicky ω^4 je



(čtyřnásobně nekonečné sloupořadí). Stejný výsledek dostaneme, když v ω^3 nahradíme každý sloup sloupořadím, čili jako ω^3-násobek ordinálního čísla ω. V tomto případě ω^3 prvků nemá předchůdce.

Cvičení. Zobrazte tento PDF soubor na monitoru a pozorujte obrázky při zvětšujícím se rozlišení.

Cvičení. Ukažte, že každý prvek z ω^4 je tvaru $a_3\omega^3 + a_2\omega^2 + a_1\omega + a_0$, kde a_2, a_1, a_0 jsou přirozená čísla.

Příklad. Libovolnému polynomu $p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{N}[x]$ jedné neurčité x s koeficienty z $\mathbb{N}$ odpovídá ordinální číslo $p(\omega) = a_n\omega^n + a_{n-1}\omega^{n-1} + \cdots + a_1\omega + a_0$, přičemž pro různé polynomy p, q jsou čísla $p(\omega)$ a $q(\omega)$ různá. Připomeňme však, že je nutno dodržet pořadí sčítanců (proč?).

Čísla $p(\omega)$ vyčerpávají ordinální čísla, která lze vyjádřit pomocí konečných součtů a součinů přirozených čísel a čísla ω.

Na rozdíl od nekonečných součtů, nekonečné součiny ani nekonečné mocniny nenesou přirozené dobré uspořádání. Například $2^{\aleph_0}$, množina spočetných posloupností čísel $0, 1$, sice připouští lexikografické uspořádání, ale snadno najdeme nekonečnou klesající posloupnost

$$[1,0,0,0,0,\dots] \quad > \quad [0,1,0,0,0,\dots] \quad > \quad [0,0,1,0,0,\dots], \quad \dots$$

Nekonečné součiny a mocniny je nutno konstruovat jiným způsobem.

6.6. Definice. Nechť α, β jsou ordinální čísla. Položme

$$\alpha^\beta = \bigcup_{k \in \beta} \alpha^k.$$

Vysvětlení: Jde o ordinální typ prostého, nikoliv disjunktního, sjednocení množin α^k. Konečné mocniny α^k jsou stejně jako předtím konečné součiny

$$\underbrace{\alpha \times \cdots \times \alpha}_{k}$$

a jsou vloženy jeden do druhého, $\alpha^k \subseteq \alpha^{k+1}$, prostřednictvím zobrazení $[a_1, a_2, \ldots, a_k] \mapsto [0, a_1, a_2, \ldots, a_k]$, takže prvky z α^k předcházejí ostatním v α^{k+1} (tvoří tam počátek; obecně počátky zavedeme v příštím oddílu). Potom $\alpha^k \subseteq \alpha^{k+2}$ prostřednictvím zobrazení $[a_1, a_2, \ldots, a_k] \mapsto [0, 0, a_1, a_2, \ldots, a_k]$, atd.

Příklad. Počítejme

$$2^\omega = \bigcup_{k \in \omega} 2^k$$

Zde 2^0 je jednoprvková množina $1 = \{0\}$, vložená do $2^1 = \{0, 1\}$ jako prvek $[0, 1]$. Přitom $2^1 = \{0, 1\}$ je vložená do 2^2 jako prvky $[0, 0]$, $[0, 1]$, zatímco 2^2 je vložená do 2^3 jako prvky $[0, 0, 0]$, $[0, 0, 1]$, $[0, 1, 0]$, $[0, 1, 1]$, atd. Vidíme, že sjednocení $\bigcup_{k \in \omega} 2^k$ lze ztotožnit s množinou všech posloupností $\ldots, a_2, a_2, a_0$ nekonečných směrem doleva, kde a_1 je 0 nebo 1, ale jen konečně mnoho prvků a_i je nenulových. Uspořádání zůstává lexikografické, čili rozhodujs se podle nejlevějšího nenulového a_i. Dostáváme

$$(\ldots, 0, 0, 0) < (\ldots, 0, 0, 1) < (\ldots, 0, 1, 0) < (\ldots, 0, 1, 1) < \cdots,$$

což je izomorfní řetězci ω, čili

$$2^\omega = \omega.$$

Poznámka. Všimněte si, že oproti kardinálnímu číslu $2^{\aleph_0}$ je ordinální číslo 2^ω *spočetné.*

Příklad. Počítejme $1^\omega = \bigcup_{k \in \omega} 1^k$. Jelikož $1 \subset 2$, můžeme použít postup z předchozího příkladu, kde se omezíme jen na posloupnosti sestavené z prvků z 1. Tam je ovšem jediný prvek 0 a proto 1^ω obsahuje jediný prvek, a sice nulovou posloupnost $\ldots, 0, 0, 0$. Tudíž,

$$1^\omega = 1.$$

Příklad. Počítejme ω^ω. Opět můžeme použít postup z předchozího příkladu, ale tentokrát budou posloupnosti $\ldots, a_2, a_2, a_0$ sestaveny ze všech přirozených čísel, přičemž vše ostatní zůstane stejné, včetně uspořádání. Dostáváme

$$\begin{aligned}
&(\ldots, 0, 0, 0, 0) < (\ldots, 0, 0, 0, 1) < (\ldots, 0, 0, 0, 2) < \cdots \\
&< (\ldots, 0, 0, 1, 0) < (\ldots, 0, 0, 1, 1) < (\ldots, 0, 0, 1, 2) < \cdots \\
&< (\ldots, 0, 0, 2, 0) < (\ldots, 0, 0, 2, 1) < (\ldots, 0, 0, 2, 2) < \cdots \\
&< \cdots \\
&< (\ldots, 0, 1, 2, 0) < (\ldots, 0, 1, 2, 1) < (\ldots, 0, 1, 2, 2) < \cdots,
\end{aligned}$$

což není žádné z dosud zkonstruovaných ordinálních čísel, protože všechna doposud zkonstruovaná ordinální čísla jsou tvaru $p(\omega) = c_n\omega^n + c_{n-1}\omega^{n-1} + \cdots + c_1\omega + c_0$ a odpovídají posloupnostem $a_n, \ldots, a_2, a_2, a_0$ konečné délky. Vidíme, že ω^ω je zcela nové ordinální číslo.

Diagram množiny ω^ω obdržíme, když v množině ω nahradíme každý sloup množinou ω (vznikne ω^2), poté opět nahradíme každý sloup množinou ω (vznikne ω^3), a tak dále do nekonečna. Vznikne tak sobě podobná množina, jejíž každá část je podobná celku, čili fraktál.

Příklad. Podle podobného návodu se sestrojí číslo ω^{ω^ω}, jen použité posloupnosti budou indexovány prvky z ω^ω. Analogicky $\omega^{\omega^{\omega^\omega}}$, atd.

Poznámka. Ordinální čísla ω^ω, ω^{ω^ω}, $\omega^{\omega^{\omega^\omega}}, \ldots,$ jsou opět *spočetná.*

Zde naši exkurzi do zoo ordinálních čísel ukončíme. Vidíme, že svět ordinálních čísel je mnohem rozmanitější než svět kardinálních čísel. Zdůrazněme, že všechna zatím zkonstruovaná ordinální čísla mají spočetnou mohutnost.

Z obvyklých zákonů aritmetiky platí pro operace s ordinálními čísly jen některé. Již jsme viděli, že obecně naplatí komutativní zákon ani pro sčítání, ani pro násobení.

6.7. Tvrzení. *Buďte α, β, γ libovolná ordinální čísla. Pak*

$$\begin{aligned}
&0 + \alpha = \alpha = \alpha + 0,\\
&(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma),\\
&1 \times \alpha = \alpha = \alpha \times 1,\\
&(\alpha \times \beta) \times \gamma = \alpha \times (\beta \times \gamma),\\
&(\alpha + \beta) \times \gamma = \alpha \times \gamma + \alpha \times \gamma,\\
&0 \times \alpha = 0 = \alpha \times 0,\\
&\alpha^0 = 1,\\
&\alpha^1 = \alpha.\\
&\alpha^{\beta+\gamma} = \alpha^\gamma \times \alpha^\beta,\\
&(\alpha^\beta)^\gamma = \alpha^{\gamma \times \beta}.
\end{aligned}$$

Všimněte si změny pořadí β a γ v posledních dvou identitách.

Poznámka. Použijeme-li převrácený zápis součinu, který jsem označili "$\cdot$", nenastane změna pořadí exponentů v posledních dvou identitách,

$$\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma, \quad (\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma},$$

zato bude platit jiný distributivní zákon, a sice

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma.$$

Cvičení. Ukažte, že $\alpha \times (\beta + \gamma)$ nemusí být rovno $\alpha \times \beta + \alpha \times \gamma$. Z distributivních zákonů mezi násobením a sčítáním tak platí jen jeden.

Návod: Volte $\alpha = 2$, $\beta = \omega$, $\gamma = 1$.

Cvičení. Ukažte, že $(\alpha \times \beta)^\gamma$ nemusí být rovno ani $\alpha^\gamma \times \beta^\gamma$, ani $\beta^\gamma \times \alpha^\gamma$.

Návod: Volte $\alpha = \omega$, $\beta = \gamma = 2$.

6.4. Uspořádání ordinálních čísel

6.8. Definice. Nechť A je řetězec. Podmnožina $I \subseteq A$ se nazývá *počátek* v A, jestliže s každým prvkem $a \in I$ obsahuje i všechny prvky $b \in A$ takové, že $b \leq a$.

Počátek I se nazývá *vlastní*, když $I \neq A$.

Příklad. Prázdná množina je vlastním počátkem libovolného řetězce. Každý řetězec je svým vlastním počátkem.

Příklad. Otevřené a uzavřené intervaly Prázdná množina je vlastním počátkem libovolného řetězce. Každý řetězec je svým vlastním počátkem.

Cvičení. Počátek $K \subseteq J$ počátku $J \subseteq I$ je počátek $K \subseteq I$. Dokažte.

Cvičení. Jsou-li I, I' dva počátky v řetězci A, pak buď $I \subseteq I'$ nebo $I' \subseteq I$. Dokažte.
Návod: Připusťme naopak, že $I \setminus I'$ a $I' \setminus I$ jsou neprázdné a obsahují po řadě prvky i a i'. Jelikož A je řetězec, jsou i a i' srovnatelné...

Cvičení. 1. Je-li $\{I_j\}_{j \in J}$ systém počátků v řetězci A, pak je sjednocení $\bigcup_{j \in J} I_j$ také počátek v A. Dokažte.
2. Je-li $\{I_j\}_{j \in J}$ neprázdný systém počátků v řetězci A, pak je průnik $\bigcap_{j \in J} I_j$ také počátek v A. Dokažte.

Nadále bude A dobře uspořádaná množina. Pro libovolný prvek $a \in A$ zaveďme

$$A_a = \{x \in A \mid x < a\}.$$

Množina A_a je zřejmě vlastní počátek v A.

Příklad. Vlastní počátky v ω jsou právě všechna konečná ordinální čísla.

6.9. Tvrzení. *Buďte $I \subset A$ vlastní počátek. Pak existuje prvek $a \in A$ takový, že*

$$I = A_a.$$

Důkaz. Jestliže I je vlastní počátek, pak je rozdíl $A \setminus I$ neprázdný a obsahuje nejmenší prvek. Označme jej a. Pak $I = A_a$.

6.10. Tvrzení. *Buďte A, B dobře uspořádané množiny. Pak nastane právě jedna ze tří možností:*
1. *A je izomorfní s B;*
2. *A je izomorfní s některým vlastním počátkem v B;*
3. *některý vlastní počátek v A je izomorfní s B.*

Naivní důkaz by mohl spočívat v konstrukci izomorfizmu ϕ po jednotlivých krocích, kdy v každém kroku přiřadíme nejmenšímu prvku, který ještě nemá obraz, nejmenší prvek, který ještě nemá vzor. Výsledkem bude jeden z případů věty v závislosti na tom, zda se vyčerpají obě množiny současně nebo jedna z nich dříve. Nemáme však žádné axiomy, které by nám dovolily provádět konstrukce v nekonečně mnoha krocích.

Důkaz. Uvažujme o množině M všech trojic (I, J, ϕ), kde I je počátek v A a J je počátek v B a $\phi : I \longrightarrow J$ je izomorfismus, který splňuje

$$\phi A_a = B_{\phi(a)}.$$

Prvky $a \in A$, které leží v některém z počátků I, tj. $a \in \bigcup I$, jakož i prvky $b \in B$, které leží v některém z počátků J, tj. $b \in \bigcup J$, nazveme *vypořádané*. Je zřejmé, že vypořádané prvky z A tvoří počátek v A a vypořádané prvky z B tvoří počátek v B (je-li a vypořádaný a $a' \leq a$, je a' vypořádaný ohraničením izomorfizmu na prvky $\leq a'$).

Jeden a týž prvek a může ležet ve vícero počátcích I, ale vždy s touž přiřazenou hodnotou $\phi(a)$, nazávislou na I, jak plyne transfinitní indukcí s použitím podmínky $\phi A_a = B_{\phi(a)}$ (ověřte).

Jsou-li všechny prvky z A nebo z B vypořádané, pak jsme hotovi a nastane jeden z případů věty v závislosti na tom, zda vypořádané prvky vyčerpají obě množiny nebo jen jednu z nich. Jinak označíme a nejmenší nevypořádaný prvek z A a b nejmenší nevypořádaný prvek z B. To znamená, že prvky z A_a i z B_b jsou vypořádané. a existuje $\phi : A_a \to B_b$, ležící v M. Definujme $\bar{A} = \{a\} \cup A_a$, $\bar{B} = \{b\} \cup B_b$ a $\bar{\phi} : \bar{A} \to \bar{B}$ předpisem $\bar{\phi}|_{A_a} = \phi$ a $\bar{\phi}(a) = b$. Zjišťujeme, že $(\bar{A}, \bar{B}, \bar{\phi}) \in M$ a a, b jsou rovněž vypořádané, což je spor.

6.11. Definice. Buďte α, β ordinální čísla, která jsou po řadě ordinálními typy dobře uspořádaných množin A, B. Definujme uspořádání mezi α, β tak, že možnosti

$$\alpha = \beta, \quad \alpha < \beta, \quad \alpha > \beta$$

nastávají po řadě v případech
1. A je izomorfní s B;
2. A je izomorfní s některým vlastním počátkem v B;
3. některý vlastní počátek v A je izomorfní s B.

z předchozí věty,

Ukažme, že definice skutečně zavádí uspořádáním které je navíc úplné. Reflexivita a tranzitivita jsou zřejmé, z věty plyne úplnost (že vždy nastane alespoň jedna z možností $\alpha = \beta$, $\alpha < \beta$, $\alpha > \beta$), ale antisymetrie pak plyne z toho, že nemohou současně nastat dvě různé možnosti.

7. Zermelova věta a její důsledky

Zermelova věta praví, že každou množinu lze dobře uspořádat. Jde o velmi důležitou větu, jejímž důsledkem je, že na každé množině lze uplatnit transfinitní indukci a s její pomiocí dokazovat významná tvrzení.

7.1. Zermelova věta. *Na každé množině existuje dobré uspořádání.*

Ernst Zermelo (1871–1953) dokázal tuto větu jako první v práci E. Zermelo, Beweis, daß jede Menge wohlgeordnet werden kann, *Math. Annalen* 59 (1904) 514–516.

Je známo několik důkazů, které všechny používají axiom výběru. Nevyhnutelnost jeho použití plyne z toho, že axiom výběru je sám důsledkem Zermelovy věty. Dobré uspořádání totiž umožňuje zkonstruovat výběrové zobrazení tak, že se z každé podmnožiny vybere nejmenší prvek.

O důkazech. Buď A libovolná množina. Původní Zermelův důkaz spočívá v tom, že se aplikací axiomu výběru z každé neprízdné podmnožiny $B \in 2^A \setminus \{\emptyset\}$ vybere po jednom prvku. Poté se indukcí konstruuje uspořádání na A, přičemž indukční krok spočívá v tom, že se k množině P všech již vyřízených prvků připojí prvek vybraný z doplňku $A \setminus P$ a prohlásí za větší než všechny prvky z P. Přitom je však nutno zařídit, že indukční krok probíhal na nějaké dobře uspořádané množině, což je hlavní komplikace důkazu.

Jednodušší jsou důkazy používající ordinály (viz níže), protože třída všech ordinálů $\mathcal{O}$ je dobře uspořádaná i bez axiomu výběru a transfinitní rekurzí lze konstruovat injektivní zobrazení z libovolné množiny do $\mathcal{O}$. Ačkoliv ordinály umožňují významná zjednodušení důkazů, v tomto textu je odsuneme až na samotný konec výkladu. Upřednostníme některé důsledky Zermelovy věty, které jsou významné i pro aplikovatelnou matematiku a nejen pro řešení vnitřních problémů teorie množin.

Cvičení. Najděte dobré uspořádání množiny $\mathbb{Z}$ celých čísel.
Nápověda: Ordinální typ $\omega + \omega$.

Cvičení. Najděte dobré uspořádání množiny $\mathbb{Q}$ racionálních čísel.
Nápověda: Ordinální typ $\omega \times \omega$.

7.2. Poznámka. Přestože podle Zermelovy věty existuje dobré uspořádání množiny reálných čísel, není známa žádná formule, která by takové uspořádání zadávala.

Důvod je patrný i z torza důkazu Zermelovy věty, které jsme uvedli. Není totiž známa ani žádná formule, která by zadávala výběrové zobrazení $\wp\mathbb{R} \setminus \{\emptyset\} \longrightarrow \mathbb{R}$, tj. umožňovala vybrat po jednom prvku z každé neprázdné množiny reálných čísel.

7.1. Hausdorffův princip maximality

V následujících odstavcích popíšeme některé další důsledky axiomu výběru, které se často používají v různých oblastech matematiky mimo teorii množin.

7.3. Haussdorfův princip. *Každý řetězec v uspořádané množině lze rozšířit na maximální řetězec.*

Maximálním řetězcem se rozumí řetězec, ke kterému nelze přidat žádný další prvek (to jest, po přidání libovolného prvku přestane být řetězcem). Při důkazu použijeme Zermelovu větu.

Důkaz. Buď $(A, \leq)$ libovolná uspořádaná množina, B její podřetězec. Princip důkazu spočívá v tom, že k řetězci přidáváme další prvky takové, že výsledek zůstává řetězcem, přičemž uplatníme transfinitní rekurzi. Podle Zermelovy věty na množině A existuje i dobré uspořádání, které označíme $\preceq$. Transfinitní rekurzí nad dobrým uspořádáním $\preceq$ definujeme zobrazení $\phi : A \longrightarrow \wp A$ tak, aby

$$\phi(a) = \begin{cases} \{a\}, & \text{když } B \cup \{a\} \cup \bigcup_{b \prec a} \phi(b) \text{ je řetězec vzhledem k } \leq, \\ \emptyset & \text{jinak.} \end{cases}$$

Pak

$$B \cup \bigcup_{a \in A} \phi(b)$$

je je maximální řetězec, protože kdyby bylo možné k němu přidat další prvek, během transfinitní rekuze by k tomu došlo.

7.2. Zornovo lemma

V různých partiích matematiky se běžně provádějí konstrukce maximálních prvků pomocí Zornova lemmatu. Jde o obvyklý název výsledku, který v roce 1935 publikoval německý matematik Max Zorn a v nepříliš odlišné podobě v roce 1922 polský matematik Kazimierz Kuratowski. Proto se někdy nazývá Kuratowského–Zornovo lemma.

7.4. Zornovo lemma. *Nechť A je uspořádaná množina taková, že každý řetězec v A má horní závoru. Pak ke každému prvku $a \in A$ existuje prvek $b \in A$, který je maximálním prvkem v A a $a \leq b$.*

Zornovo lemma je snadným důsledkem Hausdorffova principu.

Důkaz. Podle Hausdorffova principu lze jednoprvkový řetězec $\{a\}$ rozšířit na maximálmní řetězec I, který jej obsahuje. Podle předpokladu má I horní závoru b. Prvek b je hledaným prvkem. Zaprvé platí $a \leq b$, protože $a \in I$ a b je horní závora řetězce I. Zadruhé je b maximální prvek v A, protože kdyby nebyl, existoval by v A prvek $c > b$. Prvek c by byl ostře větší než všechny prvky z I, načež by $I \cup \{c\}$ byl řetězec v A obsahující I, v rozporu s maximalitou I.

Zornovo lemma se obvykle aplikuje v situacích, kdy A je systém nějakých množin (např. algebraických struktur), pro něž platí, že sjednocení řetězce do sebe vložených struktur je opět prvkem systému (a v této podobě lemma dokázal K. Kuratowski v r. 1922). Dá se tak například ukázat, že každou vlastní podalgebru lze vložit do maximální vlastní podalgebry. Analogické tvrzení se dokazuje pro vlastní ideály okruhů apod.

7.3. Srovnatelnost kardinálních čísel

Z Zermelovy věty snadno plyne, že libovolná dvě kardinální čísla $\mathfrak{a}, \mathfrak{b}$ jsou srovnatelná. Množiny A, B, které mají po řadě mohutnosti $\mathfrak{a}, \mathfrak{b}$, můžeme podle Zermelovy věty dobře uspořádat, a potom podle věty 6.10 existuje injektivní zobrazení $A \to B$ nebo $B \to A$.

8. Ordinály

V předchozích odstavcích jsme se seznámili s ordinálními čísly v podobě tříd izomorfních dobře uspořádaných množin, což odpovídá původnímu Cantorovu pohledu, ale nelze pak zavést třídu všech ordinálních čísel. Tento nedostatek lze odstranit zavedením ordinálů, speciálních dobře uspořádaných množin takových, že každá dobře uspořádaná množina je izomorfní s právě jedním ordinálem. Existuje vícero možností a verzí. Společnou vlastností je, že ordinály jsou (podobně jako von Neumannova přirozená čísla) dobře uspořádané množiny všech menších ordinálů.

Pro každé ordinální číslo σ totiž platí, že je izomorfní se systémem všech vlastních počátků σ_a, $a \in \sigma$, uspořádaným inkluzí, protože

$$a \leq b \quad \Leftrightarrow \quad \sigma_a \subseteq \sigma_b.$$

Definici ordinálu obdržíme, pokud v předchozím tvrzení “izomorfní” zaměníme za “identický”.

8.1. Definice (E. Zermelo, J. von Neumann). Dobře uspořádaná množina σ se nazývá *ordinál*, je-li každý prvek $z \in \sigma$ identický s počátkem σ_z tj.

$$z = \sigma_z = \{\zeta \in \sigma \mid \zeta < z\}. \tag{1}$$

Třídu všech ordinálů označíme $\mathcal{O}$.

Příklad. $0 = \emptyset$ je ordinál, protože nemá žádné prvky.

Příklad. $1 = \{0\}$ je ordinál, protože jediným prvkem je 0 a pro něj platí $1_0 = \emptyset = 0$.

Příklad. $2 = \{0, 1\}$ s uspořádáním $0 < 1$ je ordinál, protože $2_0 = \emptyset = 0$ a $2_1 = \{0\} = 1$.

Příklad. Dobře uspořádaná množina ω je ordinál, neboť pro každé von Neumannovo přirozené číslo n platí $\omega_n = \{0, 1, 2, \ldots, n-1\} = n$.

8.2. Tvrzení. *Každý prvek ordinálu je zase ordinál.*

Důkaz. Nechť je σ je ordinál a $\tau \in \sigma$. Pak $\tau = \sigma_\tau$ je počátek v σ, čili τ je dobře uspořádaná množina. Současně je každý prvek $\zeta \in \tau$ roven počátku $\sigma_\zeta = \tau_\zeta$ (protože $\zeta < \tau$). Tudíž, τ je ordinál.

Ordinály lze snadno uspořádat.

8.3. Definice. Řekneme, že ordinál σ je ostře menší než ordinál τ a zapoisujeme $\sigma < \tau$, jestliže σ je počátkem v τ.

Všechna následující tvrzení uvedeme bez důkazu. Není to tím, že by důkazy byly dlouhé, ale semestr je krátký.

8.4. Tvrzení. *Pro každé dva ordinály platí buď $\sigma < \tau$ nebo $\sigma = \tau$ nebo $\sigma > \tau$.*

8.5. Tvrzení. *Třída $\mathcal{O}$ všech ordinálů je vlastní třída.*

Důkaz tvrzení je znám jako Burali-Fortiho paradox. Burali-Forti (1861–1931) jej v dobách naivní teorie množin odvodil z předpokladu, že ordinální čísla tvoří množinu.

8.6. Tvrzení. *Třída $\mathcal{O}$ všech ordinálů je dobře uspořádaná.*

Uvedené tvrzení nám umožňuje provádět transfinitní indukci na ordinálech.

8.7. Důsledek. *Každá množina ordinálů je dobře uspořádaná.*

8.8. Tvrzení. *Každá dobře uspořádaná množina je izomorfní s právě jedním ordinálem.*

8.9. Tvrzení. *Je-li σ ordinál, pak i $\sigma + \{\sigma\}$ je ordinál a jeho ordinální typ je $\sigma + 1$.*

8.10. Důsledek. *Všechna von Neumannova přirozená čísla jsou ordinály.*

8.11. Tvrzení. *Je-li $\{\sigma_i\}_{\imath \in I}$ systém ordinálů, pak $\bigcup_{\imath \in I} \sigma_i$ je také ordinál.*

Příklad. Podle posledního tvrzení je $\omega = \bigcup_{n \in \mathbb{N}} n$ ordinál.

9. Třída všech kardinálních čísel

Výše jsme zavedli kardinální čísla prostřednictvím tříd ekvivalence. Třídy ekvivalence (kromě jednoprvkové třídy $[\emptyset]_\sim$) se ovšem ukázaly být vlastními třídami, a proto z nich není možné sestavit třídu kardinálních čísel. Nyní ukážeme, jak v každé třídě vybrat po jednom reprezentantu tak, aby zmíněné potíže odpadly.

Podle Zermelovy věty lze každou množinu dobře uspořádat a podle tvrzení 8.8 potom existuje bijekce na některý ordinál. Tudíž, každá množina je v bijekci s některým ordinálem.

9.1. Definice. *Mohutnost* množiny X je nejmenší ordinál ξ takový, že existuje bijekce mezi X a ξ. Zapisujeme $\xi = \#X$.

Ordinál ξ se nazývá *kardinální číslo*, jestliže je nejmenším prvkem množiny ordinálů jedné a téže mohutnosti.

Příklad. $\aleph_0 = \omega$.

9.2. Důsledek. *Každá dvě kardinální čísla jsou srovnatelná. Třída všech kardinálních čísel je dobře uspořádaná.*

Podle Cantorovy věty ke každému kardinálnímu číslu existuje větší. Protože je třída kardinálních čísel dobře uspořádaná, má každé kardinální číslo svého následovníka.

Pro každý ordinál $\sigma \in \mathcal{O}$ definujeme transfinitní rekurzí nekonečné kardinální číslo $\aleph_\sigma$ následujícím způsobem.

9.3. Definice. Jsou-li pro všechny ordinály $\tau < \sigma$ definována kardinální čísla $\aleph_\tau$, definujeme $\aleph_\sigma$ jako nejmenší kardinální číslo větší než všechna $\aleph_\tau$.

Příklad. Nejmenší kardinální číslo větší než $\aleph_0$ je $\aleph_1$. Nejmenší kardinální číslo větší než $\aleph_1$ je $\aleph_2$. Nejmenší kardinální číslo větší než všechna $\aleph_n$, $n \in \mathbb{N}$, je $\aleph_\omega$.

9.4. Tvrzení. *Každé nekonečné kardinální číslo je rovno $\aleph_\sigma$ pro nějaký ordinál σ.*

9.5. Poznámka. Otázka, kterému alefu je rovno $\mathfrak{c}$, však nemá jednoznačnou odpověď. Evidentně, $\mathfrak{c} > \aleph_0$, ale odnikud neplyne rovnost $\mathfrak{c} = \aleph_1$ ani žádná jiná rovnost $\mathfrak{c} = \aleph_\sigma$ pro konkrétní $\sigma > 0$ lze pouze některé možnosti vyloučit, například je známo, že $\mathfrak{c} \neq \aleph_\omega$.

Hypotéza kontinua je předpoklad, že $\aleph_1 = 2^{\aleph_0} = \mathfrak{c}$. *Zobecněná hypotéza kontinua* je předpoklad, že $\aleph_{\sigma+1} = 2^{\aleph_\sigma}$. Je dokázáno, že hypotéza kontinua je tvrzení nezávislé na dosud uvedených axiomech.

9.1. Pohlcovací zákony

Dále lze dokázat tak zvané *pohlcovací zákony* aritmetiky kardinálních čísel. Platí pro všechna kardinální čísla $\mathfrak{a}, \mathfrak{b}$, z nichž alespoň jedno je nekonečné a znějí

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{a} \times \mathfrak{b} = \max(\mathfrak{a}, \mathfrak{b}).$$

Dokazuje se pro všechny alefy (kardinální čísla tvaru $\aleph_\alpha$) v podobě

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha \times \aleph_\beta = \max(\aleph_\alpha, \aleph_\beta),$$

načež se využije toho, že každá nekonečná mohutnost je některým alefem.