2-UMA-115 Teória množín

Martin Sleziak

4. novembra 2010

Obsah

Kapitola 1

Úvod

Verzia: 4. novembra 2010

1.1 Predhovor

Zjednodušene sa dá povedať, že teória množín je vlastne disciplína, ktorá sa zaoberá prácou s nekonečnými množinami. Jej vznik si vyžiadal istý filozofický posun v chápaní nekonečna. V matematike sa dosť dlho pracovalo s nekonečne malými a nekonečne veľkými veličinami tak, že vlastne išlo o limitné procesy, v ktorých sa tieto veličiny postupne mohli dostatočne zmenšovať či rásť. Pohľad teórie množín je v ostrom kontraste s týmto prístupom, keďže v nej sa pracuje s nekonečnými množinami ako už s hotovými objektmi, ktorých proces vytvárania už je ukončený.

Za počiatky teórie množín môžeme pokladať práce nemeckého matematika Georga Cantora. Okolo roku 1870 pracoval na problémoch súvisiacich s teóriou trigonometrických radov a v súvislosti s nimi použil pojem derivácie množiny A' (=množina hromadných bodov množiny A). Pracoval tu s iteráciami tohoto pojmu – $A', A'', \dots, A^{(n)}$ (prvá, druhá, n-tá derivácia). Keď sa mu podarilo nájsť množinu, pre ktorú sa všetky konečné iterácie $A^{(n)}$ líšili, bolo prirodzené definovať ďalšiu iteráciu $A^{(\infty)}$ a potom pokračovať s ďalšími iteráciami ako $A^{(\infty+1)}$. Tieto úvahy boli jedným zo zdrojov, ktoré ho viedli k zavedeniu *transfinitných čísel,* ktoré dnes poznáme ako ordinálne a kardinálne čísla.

Už fakt, že pri zrode teórie množín stáli Cantorove výskumy v matematickej analýze naznačuje, že táto oblasť má veľký význam pre ostatné matematické disciplíny. Potvrdzuje sa to dodnes, postupne matematici našli mnohé aplikácie výsledkov a techník z teórie množín v takmer všetkých matematických disciplínach.

Dôležitosť teórie množín je aj v tom, že poskytuje rôznym matematickým disciplínam spoločný jazyk – (takmer) celá dnešná matematika je sformulovateľná v jazyku teórie množín.

Tento text je zamýšľaný ako učebný text k predmetu Teória množín pre učiteľské zamerania na FMFI. Obsahuje určite aj časti, ktoré na prednáške nestihneme prebrať, môžu byť však pre vás zaujímavé (prípadne niektoré z týchto rozširujúcich častí by mohli byť zaujímavé aj pre študentov odboru matematika či iných odborov). Rozširujúce časti sú vyznačené menším fontom alebo hviezdičkou pri názve príslušnej časti. Text prednášky budem priebežne dopĺňať a opravovať, aktuálna verzia bude dostupná na `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

V texte nájdete množstvo vyriešených úloh. Určite nezaškodí, ak sa ich pokúsite riešiť samostatne – len samostatným uvažovaním si môžete skutočne dôkladne osvojiť niektorú matematickú disciplínu. Som presvedčený o tom, že v rámci tejto prednášky sa nájde veľa zaujímavých poznatkov. Ako ste však isto spoznali aj z iných predmetov, matematika môže byť zaujímavá a zábavná, vyžaduje si to však najprv nemalé úsilie na strane študenta.

1.2 Sylaby a literatúra

1.2.1 Literatúra

Pri príprave týchto poznámok som čerpal najmä z kníh [BŠ, D, ŠS]. V častiach o histórii teórie množín som čerpal hlavne z [BŠ, GG, Z]. Samozrejme, pomohli mi aj rôzne internetové zdroje ako napríklad [WIK], blogy rôznych matematikov, s niektorým úlohami, ktoré uvádzam ako cvičenia, som sa stretol na rôznych matematických diskusných fórach. Mnohé cvičenia som prebral z [Li, ŠS].

Kniha [ŠS] je veľmi zrozumiteľne písaná a je určená pre študentov učiteľských odborov. Kniha [BŠ] je náročnejšia a obsahuje aj veľmi pokročilé časti, ktoré výrazne presahujú obsah tohoto kurzu. Prvé dve jej kapitoly zhruba zodpovedajú tomu, čo budeme preberať.[1] Z ďalších textov dostupných v slovenčine alebo češtine spomeňme ešte [B3]. Pokiaľ ste schopní čítať text v angličtine, ľahko nájdete veľké množstvo ďalších výborných textov o teórii množín.

1.2.2 Sylaby predmetu

Zermelov-Fraenkelov axiomatický system teórie množín. Kardinálne čísla a kardinálna aritmetika. Konečné a nekonečné množiny. Množina prirodzených čísel a matematická indukcia. Spočítateľné a nespočítateľné množiny. Mohutnosť kontinua a kardinalita množín vyskytujúcich sa v školskej matematike.

1.2.3 Štátnicové otázky

Štátnicové otázky z predmetu matematika, ktoré by ste sa mali naučiť na tomto predmet sú:

1. Axiomatická metóda v teórii množín, Zermelov-Fraenkelov axiomatický systém teórie množín.
2. Konečné a nekonečné množiny, vlastnosti konečných množín.
3. Spočítateľné množiny, vlastnosti spočítateľných množín, existencia nespočítateľnej množiny.
4. Model Peanovej aritmetiky celých nezáporných čísel v teórii množín.
5. Kardinálne čísla. Súčet a súčin kardinálnych čísel, vlastnosti súčtu a súčinu kardinálnych čísel.

Krátky komentár si zaslúži štvrtá otázka týkajúca sa konštrukcie prirodzených čísel v rámci axiomatickej teórii množín. Prístup, ktorý som zvolil v tomto texte, je taký, že najprv zadefinujeme ordinálne čísla a prirodzené čísla potom chápeme ako konečné ordinálne čísla. Urobil som tak z toho dôvodu, že ordinálne čísla sú zaujímavé a užitočné a mnohé z prostriedkov potrebných na formálnu definíciu prirodzených čísel sa dajú využiť aj pri definícii ordinálnych čísel. Napríklad v texte [Č2] môžete nájsť priamočiarejší prístup, pri ktorom sa priamo konštruujú prirodzené čísla, pričom o ordináloch tam nepadne ani zmienka.

V časti 6.4.4 sa dotkneme aj otázky: „Konštrukcia oboru (usporiadaného okruhu) celých čísel z oboru celých nezáporných čísel a oboru (usporiadaného pola) racionálnych čísel z oboru celých čísel.“ Nebudeme sa však ňou zaoberať podrobne.

[1] Jeden exemplár [BŠ] sa kedysi nachádzal aj v knižnici na átriových domkoch – ak tá knižnica ešte funguje, možno ju tam zoženiete. Obe knihy by však mali byť u nás pomerne dostupné. Ak by ste však mali záujem prečítať si akúkoľvek literatúru, ktorú v tomto texte citujem a nepodarilo by sa vám ju zohnať, pokojne sa obráťte na mňa.

1.3 Niečo z histórie

No one shall expel us from the Paradise that Cantor has created.
(*Nikto nás nevyženie z raja stvoreného Cantorom.*)
David Hilbert

V tejto prednáške sa budeme zaoberať axiomatickou teóriou množín. Na úvod by bolo azda vhodné povedať aspoň stručne niečo o tom ako a prečo vznikla. Pokiaľ sa chcete dozvedieť viac, ako veľmi pekný (a súčasne stručný) text o histórii modernej teórie množín by som vám odporučil [BŠ, s.11-s.25]. (Túto úvodnú kapitolu nazvali autori spomínanej knihy „Romance matematické analýzy a teorie množin".)

Za zakladateľa teórie množín je všeobecne považovaný *Georg Cantor* (hoci niektoré idey možno nájsť napríklad aj v dielach *Bernarda Bolzana*). Za základnú tézu teórie množín môžeme prehlásiť možnosť uchopiť viacero objektov ako jediný objekt (ich množinu).[2] Matematikov na celom svete veľmi prekvapil Cantorov dôkaz, že existuje nekonečne veľa transcendentných reálnych čísel, uverejnený v roku 1874. Originálna bola najmä metóda dôkazu – Cantor dokázal tento výsledok bez toho, aby nejaké takéto číslo skonštruoval. Tento dôkaz si v rámci tejto prednášky aj ukážeme. Sami budete mať možnosť vidieť, že po vybudovaní potrebného aparátu je už tento dôkaz veľmi jednoduchý – na rozdiel od konštruktívneho dôkazu existencie transcendentných čísel pochádzajúceho od Josepha Liouvillea.

Teória množín sa u mnohých matematikov stretla s výrazným odporom. Dôvody boli rôzne, jedným z nich bol aj nekonštruktívny charakter viacerých dôkazov – ako napríklad v prípade existencie transcendentných čísel. Tento odpor ešte zosilnel po objavení viacerých paradoxov (sporov) v teórii množín, o ktorých budeme hovoriť o chvíľu.

V Cantorových prácach sa objavilo mnoho dôležitých výsledkov z teórie množín – dá sa povedať, že väčšina z tých, s ktorými sa v rámci tejto prednášky stretneme. Stále však nešlo o axiomatickú teóriu množín. Cantorov prístup, pri ktorom bol pojem množiny chápaný intuitívne a pomerne voľne, sa zvykne nazývať *naivná teória množín.* Na mnohé účely je tento prístup úplne postačujúci, v podstate je to presne ten prístup, ktorý ste používali na prednáškach z matematiky, ktoré ste doteraz absolvovali. Začiatkom 20-teho storočia sa však zistilo, že naivný prístup k množinám môže viesť k viacerým paradoxom.

Ako ilustráciu stručne popíšme *Russellov paradox.* (Neskôr sa budeme paradoxami teórie množín zaoberať o niečo podrobnejšie.) Povedali sme si, že základná ide teórie množín je chápať viac objektov ako prvky jedného celku – jednej množiny. Takto môžeme zaviesť množinu všetkých množín, ktorú označíme **Set**. Z tejto množiny môžeme vymedzovať podmnožiny pomocou rôznych vlastností prvkov. Uvažujme vlastnosť $x \notin x$, t.j. množina nie je prvkom samej seba. Táto vlastnosť určí podmnožinu $A = \{x \in \mathbf{Set}; x \notin x\}$. Má aj množina A takúto vlastnosť?

Ak ju má, čiže ak $A \notin A$, tak podľa definície množiny A má platiť $A \in A$, čo je spor.

Obrátene, ak túto vlastnosť nemá, tak $A \in A$. Ale do množiny A patria len množiny s uvedenou vlastnosťou. To znamená, že $A \notin A$ a opäť dostávame spor.

Pokiaľ nechceme teóriu množín zavrhnúť úplne, mali by sme sa pokúsiť nejako takýmto problémom predísť. Významný pokus týmto smerom urobili Alfred North Whitehead a Bertrand Russell vo svojom diele Principia Mathematica. Paradoxom sa snažili predísť tým, že vybudovali rozsiahlu teóriu typov. Množiny istého typu mohli byť len prvkami množín vyššieho typu, čím sa predišlo možným cyklom a tak aj Russelovmu paradoxu. Nevýhodou systému typov bola veľká zložitosť – do istej miery je tento fakt ilustrovaný tým, že výsledok

[2] Takto napísané to znie asi pomerne naivne – ale asi nie je reálne očakávať, že sa podarí vystihnúť podstatu celej teórie v jedinej vete. Treba dúfať, že jej podstatu pochopíte po tomto jednosemestrovom kurze.

$1 + 1 = 2$ sa nachádza na strane 379 [WR, p.379,*54.43].[3]

Oveľa viac sa presadil axiomatický prístup, pri ktorom sa teória množín buduje z dvoch primitívnych (=nedefinovaných) pojmov *množina* a *byť prvkom množiny* pomocou axióm, ktoré popisujú správanie týchto prvkov. Takýto axiomatický systém začal budovať nemecký matematik Ernst Zermelo, po ňom je pomenovaný v súčasnosti najrozšírenejší Zermelov-Fraenkelov axiomatický systém (označovaný ako ZF resp. ZFC – po pridaní axiómy výberu).

S použitím axiomatického systému sa podarilo odstrániť všetky dovtedy známe paradoxy. Samozrejme, stále vo vzduchu visela otázka, či sa neobjavia nejaké nové spory v rámci axiomatickej teórie množín. Táto otázka bola jednou z pohnútok, ktoré viedli k tzv. *Hilbertovmu programu.* Jeho ciele boli veľmi ambiciózne, tu spomeňme len dva z nich: Jedným z cieľov bolo sformalizovať celú matematiku v rámci teórie množín. Druhým cieľom bolo ukázať bezospornosť teórie množín, a tým pádom vlastne aj celej matematiky (alebo aspoň tej časti, ktorú budeme schopní v rámci teórie množín sformulovať). Viac o Hilbertovom programe sa môžete dozvedieť napríklad v [Z, Kapitola 10].

Dnes už vieme, že Hilbertov program sa nedá naplniť v pôvodnom rozsahu. Z výsledkov rakúskeho matematika Kurta Gödla vyplýva, že bezospornosť systému ZFC sa nedá dokázať v tomto systéme. Hilbertov program i tak výrazne ovplyvnil podobu súčasnej matematiky, ktorá je skutočne vybudovaná na teórii množín. Možno nie je až také neopodstatnené očakávať, že za približne storočie intenzívnej práce v tomto axiomatickom systéme (ak teda prijmeme tézu, že drvivá väčšina súčasnej matematiky je sformalizovateľná v ZFC) sa spor v základoch matematiky neobjavil, takže tam snáď žiadny spor nebude. Úplnú istotu však mať nemôžeme.

Viac o Gödelových vetách (ako aj o niektorých filozofických otázkach súvisiacich s teóriou množín) sa môžete dozvedieť v [Z]. Tento text je pomerne náročný, rozhodne je vhodné mať zvládnuté základy teórie množín prv, než ho začnete čítať.

Poznamenajme, že smery načrtnuté v práve uvedenom stručnom historickom prehľade do istej miery aj naznačujú akým smerom sa bude uberať náš kurz o základoch teórie množín. Na jednej strane zavedieme axiómy systému ZFC a ukážeme si, ako v ňom možno vybudovať napríklad obor prirodzených čísel (a naznačíme konštrukciu ďalších číselných oborov). Ako sme už však spomenuli, na mnohé účely stačí „naivný“, t.j. neaxiomatický prístup k teórii množín. Ani my zväčša nebudeme dôkazy rozpitvávať až po najnižšiu logickú úroveň, t.j. až z axióm, čo znamená, že mnohé časti uvedené v tomto texte by sa dali zvládnuť aj bez znalosti axiomatického systému, len s použitím naivnej téorie množín.

1.4 Základné označenia

Budeme používať štandardné označenia:
$\mathbb{N} = \{0, 1, 2, \dots\}$ je množina prirodzených čísel (čiže na tejto prednáške považujeme aj nulu za prirodzené číslo)
$\mathbb{Z}$ = celé čísla
$\mathbb{Q}$ = racionálne čísla
$\mathbb{R}$ = reálne čísla
$\mathbb{C}$ = komplexné čísla

Poznámka 1.4.1. V rôznych aplikáciách a príkladoch (kontrapríkladoch) budeme bežne pracovať s množinou prirodzených čísel $\mathbb{N}$, množinou reálnych čísel $\mathbb{R}$ a ďalšími spoemnutými {prelim:POZNMNOZN}

[3]Ako však budeme vidieť, aj vybudovanie prirodzených čísel v teórii ZFC bude pomerne zdĺhavé a náročné, takže tento fakt nie je spôsobený len zložitosťou zvoleného systému, ale aj tým, že sa snažíme prirodzené čísla vybudovať z veľmi obmedzeného systému základných pojmov a axióm.

číselnými obormi, ktoré poznáte z nižších ročníkov. Až neskôr si ukážeme, že všetky tieto číselné obory možno vybudovať v rámci teórie množín – takže ich skutočne môžeme považovať za množiny v systéme ZFC.

Kapitola 2

Axiomatický prístup k teórii množín

2.1 Logika prvého rádu

Ešte predtým, než sa začneme zaoberať množinami ako takými, povieme si niečo o logike prvého rádu, ktorá sa zaoberá výrokmi vytvorenými pomocou logických spojok a kvantifikátorov.

Logikou prvého rádu sa nebudeme zaoberať detailne, zjednodušene povedané, je to súhrn pravidiel pre prácu s výrokmi, ktoré sú v súlade s tým ako obvykle uvažujeme. Ak by ste sa chceli o prvorádovej logike dozvedieť viac, môžete si o nej prečítať v knihách a textoch venovaných čisto tejto problematike, ako napríklad [B1, E, So, Š].

2.1.1 Výroková logika

Pripomenieme si niektoré pravidlá na overovanie pravdivosti výrokov, ktoré už poznáte z nižších ročníkov. Za výrok môžeme považovať akékoľvek tvrdenie, ktoré môže byť pravdivé alebo nepravdivé. (Presná definícia výroku pre nás nie je až taká dôležitá – v skutočnosti jediné výroky, s ktorými budeme na tejto prednáške pracovať, sú formuly jazyka teórie množín, ktoré zadefinujeme v podkapitole 2.3.1.)

Definícia 2.1.1. *Negáciou* výroku p rozumieme výrok „neplatí p“. Označujeme ju $\neg p$.
Pre dva výroky p a q nazývame ich *konjunkciou* výrok „p a q“, označujeme $p \wedge q$.
Disjunkcia je výrok „p alebo q“, označujeme $p \vee q$.
Pod *implikáciou* rozumieme výrok „ak platí p, tak platí q“, označujeme $p \Rightarrow q$.
Ekvivalencia výrokov p a q je výrok „p platí práve vtedy, keď platí q“, označujeme $p \Leftrightarrow q$.

Tieto definície logických spojok sú zhrnuté v nasledujúcich pravdivostných tabuľkách.[1]

p	$\neg p$
1	0
0	1

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

p	q	$p \Rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

p	q	$p \Leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

[1] Na označovanie pravdivosti a nepravdivosti budeme v tabuľke používať symboly 1 a 0. Niekedy sa zvyknú používať aj T a F, ako skratky pre anglické true a false.

Definícia 2.1.2. *Tautológiou* nazývame taký výrok, zložený z výrokových premenných a logických spojok, ktorý je vždy pravdivý, bez ohľadu na pravdivosť výrokových premenných, ktoré v ňom vystupujú.

Tautológie môžeme overovať jednoducho tabuľkovou metódou, ktorú poznáte z nižších ročníkov a pravdepodobne i zo strednej školy.

Príklad 2.1.3. Overme napríklad tautológiu $p \vee (\neg p)$ (princíp vylúčenia tretieho).

p	$\neg p$	$p \vee \neg p$
1	0	1
0	1	1

Ako ďalší príklad si ukážeme overenie jedného z de Morganových pravidiel.

{logika:PRDEMORGAN}

Príklad 2.1.4. *De Morganove pravidlá* sú pravidlá ako negovať konjunkciu a disjunkciu.

$$\begin{aligned} \neg(p \wedge q) &\quad\Leftrightarrow\quad \neg p \vee \neg q \\ \neg(p \vee q) &\quad\Leftrightarrow\quad \neg p \wedge \neg q \end{aligned}$$

Samozrejme, pretože teraz vo výroku vystupuje viacero premenných, budeme potrebovať viac riadkov tabuľky na to, aby sme vyčerpali všetky možnosti.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$	$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$
1	1	1	0	0	1
1	0	1	0	0	1
0	1	1	0	0	1
0	0	0	1	1	1

Niekedy si môžeme pri overovaní platnosti tautológie použiť aj jednoduchší postup. V predchádzajúcom príklade sme napríklad mohli na základe symetrie overovať o jeden riadok menej. Inú možnosť zjednodušenia ilustruje nasledujúci príklad.

{logika:PRTAUTNEPR}

Príklad 2.1.5. Dokážeme tautológiu $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$. (Táto tautológia súvisí s princípom nepriameho dôkazu. Implikácia $\neg q \Rightarrow \neg p$ sa zvykne nazývať *obmena implikácie* $p \Rightarrow q$.)

Aby sme dokázali ekvivalenciu dvoch výrokov, stačí ukázať, že výrok na ľavej strane je nepravdivý práve v tých prípadoch, kedy je nepravdivý výrok na pravej strane.

Implikácia je nepravdivá jedine v prípade, že ľavý výrok je pravdivý a pravý je nepravdivý (prípad $1 \Rightarrow 0$). Teda výrok $p \Rightarrow q$ je nepravdivý práve vtedy, keď $p = 1$ a $q = 0$. Podobne, aby bol výrok $\neg q \Rightarrow \neg p$ nepravdivý, musí byť $\neg q = 1$ a $\neg p = 0$, čo je presne ten istý prípad $p = 1$ a $q = 0$. Vidíme, že obe strany ekvivalencie majú vždy tú istú pravdivostnú hodnotu.

(Tento spôsob overenia tautológie sa až tak veľmi nelíši od tabuľkovej metódy – vlastne sme si len rozmysleli, v ktorých riadkoch tabuľky sa na oboch stranách uvedenej ekvivalencie vyskytne 0 – zdá sa mi byť bližší ku spôsobu, ako prirodzene uvažujeme o výrokoch.)

V cvičení 2.1.1 nájdete viacero tautológií. Je dobré si uvedomiť ako súvisia tautológie s niektorými typmi dôkazov. Tautológia z príkladu 2.1.5 je presne princíp nepriameho dôkazu, ktorý sme už spomínali. Tautológia z cvičenia 2.1.1b) sa tiež často používa pri dokazovaní – namiesto výroku tvaru $p \Leftrightarrow q$ dokážeme zvlášť jednotlivé implikácie $p \Rightarrow q$ a $q \Rightarrow p$.

Disjunkívna normálne forma

Logické spojky môžeme chápať ako binárne operácie na množine $\{0,1\}$, čiže funkcie z $\{0,1\} \times \{0,1\}$ do $\{0,1\}$. Existuje teda celkovo 16 možných logických spojok. (Inak: $2^4 = 16$ spôsobov ako vyplniť tabuľku so 4 riadkami.) Okrem spojok $\wedge$, $\vee$, $\Leftrightarrow$, $\Rightarrow$, ktoré sme zvyknutí používať, dostaneme aj niektoré menej obvyklé; napríklad spojku, ktorá bez ohľadu na hodnoty p a q má vždy hodnotu 1.

Všetky možné logické spojky môžeme dostať pomocou $\neg$, $\wedge$ a $\vee$. Ak napríklad chceme dostať spojku s tabuľkou

p	q	$p * q$
1	1	1
1	0	0
0	1	1
0	0	1

tak to môžeme dosiahnuť takto: $(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$. Inak povedané, použili sme disjunkciu formúl z ktorých každá je pravdivá pre jediný riadok v tabuľke; a pridali sme tie formuly v ktorých chceme, aby v tabuľke bola jednotka. Rovnaký postup by sme vedeli použiť aj keby sme mali viac premenných. (Jediný prípad, kedy to nefunguje, je spojka, ktorá je vždy rovná 0 – museli by sme použiť disjunkciu 0 formúl. Tú ale vieme dostať napríklad ako $p \wedge \neg p$.)

Zápis v takomto tvare sa zvykne nazývať *disjunktívna normálna forma*.

2.1.2 Výroky s kvantifikátormi

Okrem logických spojok, ďalším nástrojom pomocou ktorého môžeme vytvárať zložitejšie tvrdenia z jednoduchších, sú *kvantifikátory.* V nasledujúcej definícii $P(x)$ označuje *výrokovú funkciu,* čím rozumieme to, že po dosadení akéhokoľvek objektu za x dostaneme výrok.

Definícia 2.1.6. Výrok $(\forall x)P(x)$ znamená, že pre každý objekt x platí výrok $P(x)$. Symbol $\forall$ nazývame *všeobecný kvantifikátor.*

Výrok $(\exists x)P(x)$ znamená, že existuje taký objekt x, pre ktorý platí výrok $P(x)$. Symbol $\exists$ nazývame *existenčný kvantifikátor.*

Opäť, podobne ako pri výroku, je táto definícia pomerne nepresná – nie je jasné, čo sa skrýva za slovom „objekt". Túto nepresnosť odstránime v časti 2.3.1. Zatiaľ si môžete predstaviť, že hovoríme o objektoch z akéhosi vopred daného systému (univerza), čiže výrok $(\forall x)P(x)$ znamená, že $P(x)$ platí pre každé x z tohoto univerza. (Univerzom pre nás neskôr bude systém všetkých množín – k axiomatickej definícii množín sa dostaneme až neskôr.)

V praxi obvykle i tak budeme chcieť hovoriť nie o všetkých objektoch, ale objektoch z nejakej konkrétnej množiny A. Budeme preto používať nasledujúce zápisy[2]

$$(\forall x \in A)P(x) \overset{\text{def}}{\Leftrightarrow} (\forall x)(x \in A \Rightarrow P(x))$$
$$(\exists x \in A)P(x) \overset{\text{def}}{\Leftrightarrow} (\exists x)(x \in A \wedge P(x))$$

Čiže $(\exists x \in A)P(x)$ je len skrátený zápis toho, že existuje x, ktoré súčasne patrí do množiny A a spĺňa výrok $P(x)$.

Na overovanie platnosti tvrdení s kvantifikátormi už nemáme k dispozícii jednoduchú metódu, podobnú vyplneniu tabuľky pravdivostných hodnôt. Je možné zaviesť niekoľko pravidiel (axióm), z ktorých sa dajú ostatné tvrdenia odvodzovať. Napríklad pomerne prirodzené sa zdajú byť tieto pravidlá:
Ak platí výrok $(\forall x)P(x)$, tak platí aj výrok $P(a)$ pre daný konkrétny objekt a. (Symbol $P(a)$ označuje výrok, ktorý dostaneme dosadením a namiesto x. Presnejšie povedané, namiesto

[2]Tu používame symbol $\in$, pričom $x \in A$ označuje, že x je prvkom množiny A. Významom tohoto symbolu sa budeme zaoberať neskôr, zatiaľ si jednoducho môžete predstaviť, že naše univerzum je v tomto prípade A.

každého voľného výskytu x – o voľných a viazaných premenných vo výrokoch s kvantifikátormi budeme hovoriť o chvíľu.)
Ak platí $(\exists x)P(x)$ a súčasne platí $P(a) \Rightarrow Q$ (kde a označuje nejaký konkrétny objekt a Q je nejaký výrok), tak platí aj Q.

V tejto prednáške nebudeme vymenovávať všetky používané pravidlá a ukazovať si dôkazy tvrdení pomocou týchto pravidiel – ak by vás táto problematika zaujala, opäť sa môžete obrátiť na prednášky a texty venované špeciálne logike. Pokiaľ budeme chcieť overiť a pravdivosť nejakého výroku s kvantifikátormi, budeme sa držať zdravého rozumu – budeme postupovať tak, ako by sme o týchto výrokoch uvažovali v obvyklom jazyku a v každodenných situáciach. (Je pravda, že v každodenných situáciach neuvažujeme o množinách, pokojne si však môžeme pomôcť tým, že pod výrokom $(\forall x)P(x)$ si namiesto „každá množina má vlastnosť $P(x)$“ na chvíľu predstavíme napríklad výrok „každá gulôčka v tomto vrecku je modrá“, podobne pod $(\exists x)P(x)$ si môžeme predstaviť výrok „niektorá gulôčka v tomto vrecku je modrá“.)

{logika:PRNEGFORALL}

Príklad 2.1.7 (Negácia výrokov s kvantifikátormi)**.** Zdôvodníme platnosť výroku

$$\neg[(\forall x)P(x)] \Leftrightarrow (\exists x)\neg P(x).$$

Ľavá strana uvedenej ekvivalencie znamená, že nie všetky objekty, s ktorými pracujeme majú vlastnosť $P(x)$. To je ale presne to isté, že medzi nimi existuje aspoň jeden objekt, ktorý túto vlastnosť nemá, a teda spĺňa $\neg P(x)$. (Ak nie je pravda, že všetky gulôčky v našom vrecku sú modré, musí byť medzi nimi aspoň jedna inej farby.)

Podobným spôsobom si môžeme ozrejmiť, že platí ekvivalencia

$$\neg[(\exists x)P(x)] \Leftrightarrow (\forall x)\neg P(x).$$

(Túto ekvivalenciu môžeme odvodiť z predchádzajúcej aj jednoducho znegovaním oboch strán v predchádzajúcej ekvivalencii – pozri úlohu 2.1.1e).)

Obidve tieto ekvivalencie často používame, ak potrebujeme znegovať výrok obsahujúci kvantifikátor. Stručne sa dajú zhrnúť tak, že zmeníme kvantifikátor a výrok pod ním znegujeme.

Príklad 2.1.8. Pokúsme sa znegovať výrok

$$R(x) := (\forall x)[P(x) \Rightarrow (\exists y)Q(x,y)].$$

Postupne dostaneme

$$\begin{aligned}\neg R(x) \Leftrightarrow &(\exists x)\neg[P(x) \Rightarrow (\exists y)Q(x,y)] \Leftrightarrow\\ &(\exists x)[P(x) \wedge \neg(\exists y)Q(x,y)] \Leftrightarrow\\ &(\exists x)[P(x) \wedge (\forall y)\neg Q(x,y)]\end{aligned}$$

Okrem pravidiel na negovanie výrokov s kvantifikátormi sme použili negáciu implikácie – pozri príklad 2.1.1f).

Príklad 2.1.9. Skúsme nejaký praktickejší príklad. Najprv sa pokúsme pomocou kvantifikátorov zapísať, že postupnosť reálnych čísel $(x_n)_{n=0}^{\infty}$ konverguje. To znamená, že existuje reálne číslo, ktoré je limitou tejto postupnosti:

$$(\exists L \in \mathbb{R})(\forall \varepsilon > 0)(\exists n_0 \in \mathbb{N})(\forall n \in \mathbb{N})[n > n_0 \Rightarrow |x_n - L| < \varepsilon].$$

Podľa pravidiel, ktoré sme uviedli, je negácia tohoto výroku

$$(\forall L \in \mathbb{R})(\exists \varepsilon > 0)(\forall n_0 \in \mathbb{N})(\exists n \in \mathbb{N})[n > n_0 \wedge |x_n - L| \geq \varepsilon].$$

V matematickej analýze ste možno niekedy použili overenie tohoto výroku na dôkaz toho, že postupnosť nekonverguje.

V skutočnosti sme tak trochu podvádzali – namiesto $(\exists L \in \mathbb{R})(\forall \varepsilon)\dots$ by sme mali podľa našej dohody písať $(\exists L)[L \in \mathbb{R} \wedge \{(\forall \varepsilon)\dots\}]$. (Podobne ako sme to urobili v poslednej časti tvrdenia, ktorú sme mohli zapísať v tvare $(\forall n > n_0)|x_n - L| < \varepsilon$.) Môžete si skúsiť rozmyslieť, že aj keby sme uvedené výroky podrobnejšie rozpísali takýmto spôsobom, ako negáciu by sme dostali to isté. Čiže pravidlá na negovanie výrokov s kvantifikátormi fungujú aj ak premenné vyberáme len z určitej množiny.

Po odbočke venovanej negáciam výrokov s kvantifikátormi sa ešte na chvíľu vráťme k overovaniu pravdivosti takýchto výrokov. V príklade 2.1.7 sme pre daný výrok overili, že je pravdivý. Ukážme si aspoň jeden príklad, kde zdôvodníme, že nejaký výrok obsahujúci kvantifikátory nepravdivý. (V cvičeniach k tejto podkapitole nájdete ďalšie výroky, o ktorých máte rozhodnúť, či sú pravdivé alebo nie a svoje tvrdenie zdôvodniť.)

Príklad 2.1.10. Chceme overiť, či výrok

$$[(\forall x)P(x) \Rightarrow (\forall x)Q(x)] \Rightarrow [(\forall x)(P(x) \Rightarrow Q(x))]$$

je pravdivý alebo nie. Po chvíli uvažovania prídeme na to, že tento výrok asi neplatí. Radi by sme to zdôvodnili tak, že nájdeme konkrétny príklad výrokov, $P(x)$ a $Q(x)$ pre ktoré to neplatí.

Skúsme uvažovať napríklad výroky o reálnych číslach:
$P(x) := (x > 2)$
$Q(x) := (x > 3)$.
(Pokiaľ chceme zdôrazniť, že ide o reálne čísla, môžeme písať $P(x) := (x \in \mathbb{R}) \wedge (x > 2)$ a $Q(x) := (x \in \mathbb{R}) \wedge (x > 3)$. Už sme však uviedli, že sa zaoberáme reálnymi číslami, takže aj keď to explicitne nenapíšeme, všetky výskyty kvantifikátorov chápeme tak, že sa vzťahujú na reálne čísla.)

Pozrime sa najprv na ľavú stranu implikácie, ktorej neplatnosť chceme ukázať, t.j. na výrok $(\forall x)P(x) \Rightarrow (\forall x)Q(x)$. Tento výrok platí, lebo ľavá strana implikácie, t.j. $(\forall x)(x > 2)$, je nepravdivá. (Tvrdenie $x > 2$ neplatí pre všetky reálne čísla.)

Teraz sa pozrime na výrok $(\forall x)(P(x) \Rightarrow Q(x))$, t.j. $(\forall x)(x > 2 \Rightarrow x > 3)$. Tento výrok je nepravdivý. Implikácia $(x > 2 \Rightarrow x > 3)$ neplatí napríklad pre $x = \frac{5}{2}$.

Čiže výrok, o ktorého pravdivosti chceme rozhodnúť, je ekvivalentný si implikáciou $1 \Rightarrow 0$, a teda je nepravdivý.

Viazaný a voľný výskyt premennej O *viazanom výskyte* premennej vo výroku hovoríme v prípade, že sa vyskytuje v kvantifikátore, výskyt bez kvantifikátora nazývame *voľný*. Ukážme si to na jednoduchých príkladoch:
$(\forall x \in \mathbb{R})x^2 \geq 0$ – v tomto výroku je x viazaná premenná,
$x^2 \geq 0$ – tu je x voľnou premennou,
$x = 2 \wedge (\forall x \in \mathbb{R})x^2 \geq 0$ – v tomto výroku sa premenná x vyskytuje dvakrát, prvý výskyt je voľný a druhý viazaný. Znamená to, že prvé x „nie je to isté“ x ako druhé. Preto je výhodnejšie (zrozumiteľnejšie) tento výrok nahradiť ekvivalentným výrokom $x = 2 \wedge (\forall y \in \mathbb{R})y^2 \geq 0$.

Cvičenia

{logika:CVTAU

Úloha 2.1.1. Dokážte, že nasledujúce výroky sú tautológie:
a) $(\neg p \vee q) \Leftrightarrow (p \Rightarrow q)$
b) $(p \Leftrightarrow q) \Leftrightarrow [(p \Rightarrow q) \wedge (q \Rightarrow p)]$
c) $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$
d) $((p \wedge q) \Rightarrow r) \Leftrightarrow (p \Rightarrow (q \Rightarrow r))$
e) $(p \Leftrightarrow q) \Leftrightarrow (\neg p \Leftrightarrow \neg q)$
f) $\neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg q)$
g) $(p \Rightarrow \neg q) \Rightarrow \neg p$
h) $((p \Rightarrow \neg p) \Rightarrow p) \Rightarrow ((p \Rightarrow \neg p) \Rightarrow \neg p)$
i) $[p \Leftrightarrow (q \Leftrightarrow r)] \Leftrightarrow [p \Leftrightarrow (q \Leftrightarrow r)]$ j) $[p \Rightarrow (q \Rightarrow r)] \Leftrightarrow [p \Rightarrow (q \Rightarrow r)]$

{logika:CVTAUT2}

Úloha 2.1.2. Dokážte, že nasledujúce výroky sú tautológie:
a) $(p \vee q) \Leftrightarrow (q \vee p)$;
b) $(p \wedge q) \Leftrightarrow (q \wedge p)$;
c) $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$;
d) $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$;
e) $(p \vee p) \Leftrightarrow p$;
f) $(p \wedge p) \Leftrightarrow p$;
g) $[p \vee (q \wedge r)] \Leftrightarrow [(p \vee q) \wedge (p \vee r)]$;
h) $[p \wedge (q \vee r)] \Leftrightarrow [(p \wedge q) \vee (p \wedge r)]$;
i) $[p \vee (p \wedge q)] \Leftrightarrow p$;
j) $[p \wedge (p \vee q)] \Leftrightarrow p$.

Úloha 2.1.3. Zistite, či uvedené výroky sú tautológie. Svoje tvrdenie zdôvodnite (ak ide o tautológiu, tak to dokážte; ak nie, uveďte kontrapríklad).
a) $p \Leftrightarrow \neg\neg p$;
b) $\neg p \Leftrightarrow (p \Rightarrow \neg p)$;
c) $(p \wedge q) \Rightarrow p$;
d) $p \Rightarrow \neg p$;
e) $(p \vee q) \Rightarrow p$;
f) $(p \Rightarrow q) \Rightarrow (p \Rightarrow (q \wedge r))$;
g) $(p \Rightarrow (q \wedge r)) \Rightarrow (p \Rightarrow q)$;
h) $\neg p \wedge (p \vee q) \Rightarrow q$;
i) $[p \Rightarrow (r \vee \neg q)] \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)]$
j) $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow q)$

{logika:CVREDUND}

Úloha 2.1.4. Ukážte, že operácie $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ môžeme definovať pomocou:
a) negácie a konjunkcie,
b) negácie a disjunkcie,
c) negácie a implikácie,
d) logickej spojky NAND definovanej ako $P \,\mathrm{NAND}\, Q \Leftrightarrow \neg(P \wedge Q)$,
e) logickej spojky NOR definovanej ako $P \,\mathrm{NAND}\, Q \Leftrightarrow \neg(P \vee Q)$.

Úloha 2.1.5*. Nech $*$ je logická spojka (=binárna boolovská operácia). Dokážte, že pomocou $*$ môžeme dostať všetkých 16 možných logických spojok **práve vtedy, keď** $*$ je niektorá zo spojok NAND a NOR.

Úloha 2.1.6. Rozhodnite, či sú uvedené výroky pravdivé. Svoje tvrdenie zdôvodnite.
a) $[(\forall x)P(x) \Rightarrow (\forall x)Q(x)] \Rightarrow (\forall x)(P(x) \Rightarrow Q(x))$
b) $(\exists x)(P(x) \wedge Q(x)) \Leftrightarrow [(\exists x)P(x) \wedge (\exists x)Q(x)]$

c) $(\exists x)(P(x) \vee Q(x)) \Leftrightarrow [(\exists x)P(x) \vee (\exists x)Q(x)]$
d) $(\forall x)(P(x) \wedge Q(x)) \Leftrightarrow [(\forall x)P(x) \wedge (\forall x)Q(x)]$
e) $(\forall x)(P(x) \vee Q(x)) \Leftrightarrow [(\forall x)P(x) \vee (\forall x)Q(x)]$
f) $(\forall x)(P(x) \Rightarrow Q(x)) \Leftrightarrow [(\exists x P(x)) \Rightarrow (\exists x)Q(x)]$
g) $[(\forall x)(\forall y)(R(x,y) \Rightarrow \neg R(y,x))] \Rightarrow (\forall x)\neg R(x,x)$

Úloha 2.1.7. Pre výrokovú funkciu $P(x,y)$ uvažujme výroky $P_1(x,y) = (\forall x)(\forall y)P(x,y)$, $P_2 = (\forall x)(\exists y)P(x,y)$, $P_3 = (\exists x)(\forall y)P(x,y)$, $P_4 = (\exists x)(\exists y)P(x,y)$, $P_5 = (\forall y)(\forall x)P(x,y)$, $P_5 = (\forall y)(\exists x)P(x,y)$, $P_6 = (\forall y)(\exists x)P(x,y)$, $P_7 = (\exists y)(\forall x)P(x,y)$, $P_8 = (\exists y)(\exists x)P(x,y)$.
a) Ukážte, že pre tieto výroky platí: $P_1 \Leftrightarrow P_5$, $P_4 \Leftrightarrow P_8$ a

$$\begin{tikzcd}
 & P_3 \arrow[r, Rightarrow] & P_6 \arrow[dr, Rightarrow] & \\
P_1 \arrow[ur, Rightarrow] \arrow[dr, Rightarrow] & & & P_4 \\
 & P_7 \arrow[r, Rightarrow] & P_2 \arrow[ur, Rightarrow] &
\end{tikzcd}$$

b) Ukážte na príklade, že implikácie v predchádzajúcom diagrame nemožno nahradiť ekvivalenciami.
c) Ukážte na príklade, že nemusia platiť ekvialencie $P_3 \Rightarrow P_2$ a $P_7 \Rightarrow P_6$.
Toto cvičenia sa dá stručne zhrnúť tak, že všetky vzťahy medzi výrokmi $P_2, \ldots, P_7$ sú tie, ktoré sú naznačené v uvedenom diagrame.

{logikacvic:ULODISTRIB}

Úloha 2.1.8. Nech p je výrok a $Q(x)$ je výroková funkcia. Overte, či platia ekvivalencie:
a) $p \wedge (\exists x)Q(x) \Leftrightarrow (\exists x)(p \wedge Q(x))$;
b) $p \vee (\exists x)Q(x) \Leftrightarrow (\exists x)(p \vee Q(x))$;
c) $p \wedge (\forall x)Q(x) \Leftrightarrow (\forall x)(p \wedge Q(x))$;
d) $p \vee (\forall x)Q(x) \Leftrightarrow (\forall x)(p \vee Q(x))$.

Úloha 2.1.9. Znegujte nasledujúce výroky. Sú tieto výroky (alebo ich negácie) pravdivé, ak výrokové premenné berieme z $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (s obvyklým sčitovaním, násobením, usporiadaním)?
a) $(\forall x,y)(x^2 = y^2 \Rightarrow x = y)$;
b) $(\forall x)(\exists y)(x^2 = y)$;
c) $(\forall x)(\exists y)(x^3 = y)$;
d) $(\forall x,y)(\exists z)(x + y = z)$;
e) $(\exists x)x^2 \neq 0$;
f) $(\forall x)x^2 < 0$;
g) $(\forall x)x^2 \leq x$.

2.2 Naivná teória množín a jej paradoxy

{paradox:SECTNAIV}

Základom pôvodného Cantorovho prístupu k teórii množín je nasledujúca definícia množiny: „Množina je akýkoľvek systém objektov, jednoznačne vymedzený nejakou vlastnosťou.“ Inak povedané, množinu si môžeme predstaviť ako nový názov pre nejaký systém objektov, čo nám umožní stručnejšie a jednoduchšie vyjadrovanie.[3]

Súčasne s množinami môžeme robiť rôzne operácie, utvárať nové množiny pomocou niektorých vlastností. Napríklad prienik množín A a B je taká množina, do ktorej patria práve prvky spĺňajúce podmienku $(x \in A) \wedge (x \in B)$, čiže opäť je to systém objektov určený nejakou podmienkou. Stručne to môžeme zapísať

$$A \cap B = \{x; (x \in A) \wedge (x \in B)\}.$$

Potom namiesto „všetky racionálne čísla ležiace v intervale $\langle 0,1\rangle$“ môžeme použiť stručnejší množinový zápis $\mathbb{Q} \cap \langle 0,1\rangle$.

Russellov[4] paradox. Vidíme teda, že každej podmienke zodpovedá nejaká množina prvkov spĺňajúcich túto podmienku. Špeciálne, pokiaľ nepoužijeme žiadnu podmienku (inak povedané, použijeme prázdnu podmienku) dostaneme množinu všetkých množín (všetkých objektov). Mohli by sme ju definovať napríklad ako

$$\mathbf{Set} = \{x; x = x\},$$

keďže podmienku $x = x$ spĺňa každý objekt.

Uvažujme teraz podmienku $x \notin x$. Pomocou nej dostaneme množinu

$$A = \{x; x \notin x\}$$

takých množín, ktoré nie sú svojimi vlastnými prvkami. Položme si otázku, či do tejto množiny patrí aj množina **Set** všetkých množín. Na jednej strane vieme, že množina **Set** obsahuje všetky množiny, teda aj samu seba. To znamená, že $\mathbf{Set} \in \mathbf{Set}$, a teda $\mathbf{Set} \in A$. Súčasne si však všimnime, že podmienka $\mathbf{Set} \in \mathbf{Set}$ je presne negáciou podmienky určujúcej množinu A, čo znamená, že $\mathbf{Set} \notin A$. Dostali sme teda dva navzájom si odporujúce výroky $\mathbf{Set} \in A$ a $\mathbf{Set} \notin A$, čo je spor.

Zdá sa, že tento paradox bol spôsobený tým, že **Set** je akási neobvyklá, príliš veľká množina. Čiže by možno pomohlo, keby sme sa nejakým spôsobom vedeli vyhýbať „príliš veľkým množinám“. Toto však nie je jediný typ paradoxov, aké v naivnej teórii množín vznikali.

Berryho paradox Zadefinujeme takúto podmnožinu prirodzených čísel

$$B = \{n; n \text{ je prirodzené číslo, ktoré sa dá definovať najviac 20 slovami slovenského jazyka}\}.$$

Napriek tomu, že slovenský jazyk je veľmi bohatý, obsahuje len konečne veľa slov, nech ich je povedzme N. Kombináciou 20 slov dostaneme teda najviac N^{20} slov, čo je stále konečný počet. Existuje teda nekonečne veľa prirodzených čísel, ktoré nepatria do množiny B. Označme najmenšie z nich ako n. Zrejme $n \notin B$, čo znamená, že

n je najmenšie prirodzené číslo, ktoré sa nedá popísať najviac 20 slovami slovenského jazyka.

Práve sme však číslo n popísali menej ako 20 slovami slovenského jazyka, a teda $n \in B$. Opäť dostávame spor.

Zdá sa, že takýmto problémom by sa dalo vyhnúť, keby sme upresnili, čo rozumieme pod pojmom „vlastnosť“, keď hovoríme o tom, že množina je súbor prvkov určených nejakou vlastnosťou.

[3] Samozrejme, teória množín nám poskytuje omnoho viac, než len jednoduchší spôsob vyjadrovania. V tejto časti však chceme hlavne ilustrovať problémy, ktoré vznikajú v naivnej teórii množín, aby sme si hneď potom mohli ukázať, ako ich možno axiomatickým prístupom odstrániť. Skutočne zaujímavé výsledky a aplikácie teórie množín stretneme až v ďalších kapitolách.

[4] Bertrand Russell (1872–1970), britský matematik a filozof

2.3 Zermelov-Fraenkelov axiomatický systém

{zfc:SECTZFC}

V časti 2.2 sme videli, že potrebujeme spresniť pravidlá, pomocou ktorých môžeme vytvárať množiny, ak chceme dostať teóriu v ktorej sa nebudú dať odvodiť sporné tvrdenia. Práve to je účelom axiomatizácie teórie množín, ktorú si predstavíme v tejto podkapitole.

Teória množín je založená na dvoch *primitívnych pojmoch* – tak nazývame pojmy, ktoré nedefinujeme.[5] Sú to pojmy *množina* a *patrí* (označujeme $\in$).

Jediné objekty, o ktorých budeme v rámci teórie množín hovoriť, budú množiny. Stručne povedané: „Všetko je množina.“. Jedna množina môže patriť do inej množiny. Tento fakt označíme $a \in b$, jeho negáciu budeme zapisovať $a \notin b$.

Poznámka 2.3.1. Na základe predchádzajúcich riadkov by sa mohlo zdať, že napriek tomu, že názov prednášky je teória množín, sa na nej nedozviete, čo je to vlastne množina je. Nie je to celkom tak – pretože o chvíľu uvedieme viacero axióm popisujúcich, ako sa množiny správajú. Tieto axiómy nám teda hovoria, aké sú vlastnosti množiny, čo je vlastne to najdôležitejšie, čo potrebujeme o množinách vedieť.

S podobnou situáciou ste sa už viackrát stretli na iných matematických predmetoch. Napríklad pri skúmaní grúp nezáležalo na tom, aké majú prvky – grupy, ktoré boli izomorfné (=mali rovnaké grupové vlastnosti) sme považovali z hľadiska teórie grúp za rovnaké. Izomorfizmus medzi dvoma grupami znamená vlastne, že ich nemožno rozlíšiť grupovo-teoretickými prostriedkami. Podobne to bolo i v prípade vektorových priestorov v prvom ročníku na lineárnej algebre.

2.3.1 Jazyk teórie množín

{zfc:SSECTJAZYK}

V predchádzajúcej podkapitole sme hovorili o tom, že množina je súbor prvkov určených nejakou vlastnosťou. Berryho paradox nás presvedčil o tom, že nemôžeme používať úplne ľubovoľné vlastnosti, iba dostatočne „rozumné“. V tejto časti sa s použitím logiky prvého rádu pokúsime formálne zadefinovať, akými vlastnosťami množín sa budeme zaoberať.

Teória množín bude obsahovať viacero axióm o množinách, z ktorých budeme o množinách môcť odvodiť rôzne tvrdenia. Tieto tvrdenia a axiómy budú mať podobu formúl teórie množín.

Všetky formuly budú zostavené z premenných označujúcich množiny (budeme používať písmená $a, b, c, \dots, z, A, B, \dots, Z$, prípadne $a_1, a_2, \dots$), symbolov $=$ (označuje rovnosť množín), $\in$, $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\exists$, $\forall$ a pomocných symbolov (,), [,], {, } podľa pravidiel popísaných v nasledujúcej definícií:

Definícia 2.3.2.

1. Ak x, y sú množinové premenné, tak $(x = y)$ a $(x \in y)$ sú formuly teórie množín. (Tieto dva typy formúl nazývame *atomické formuly*.)
2. Ak φ, ψ sú formuly teórie množín, tak aj zápisy $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \Rightarrow \psi$ a $\varphi \Leftrightarrow \psi$ sú formuly teórie množín.
3. Ak x je množinová premenná a φ je formula teórie množín, tak $((\exists x)\varphi)$ a $((\forall x)\varphi)$ sú tiež formuly teórie množín.

Za *formuly teórie množín* považujeme len atomické formuly a formuly, ktoré z nich vieme získať použitím konečného počtu uvedených pravidiel.

[5] Primitívnym pojmom sa nedá vyhnúť. Ak by sme každý pojem chceli definovať pomocou ešte jednoduchších pojmov, dostali by sme tak nekonečnú reťaz definícií, ktoré závisia jedna od druhej.

2.3.2 Axiómy systému ZFC

Teraz uvedieme jednotlivé axiómy teórie množín a pri niektorých stručne spomenieme aj motiváciu pre ich zavedenie a ich najzákladnejšie dôsledky. Axiomatizácia, ktorú tu uvedieme, nie je jediná používaná, je však najrozšírenejšia. Nazýva sa Zermelov-Fraenkelov systém. (Odtiaľ pochádzajú písmená ZF, písmeno C zastupuje axiómu výberu – Axiom of Choice. Pokiaľ vynecháme axiómu výberu, dostaneme systém ZF.) Kvôli jednotnosti budeme používať rovnaké číslovanie axióm ako v [ŠS], hoci sme zvolili o čosi iné poradie. Spolu s axiómami spomenieme aj niektoré jednoduché tvrdenia, ktoré z nich vyplývajú.

Axióma I (Axióma extenzionality)**.**

$$(\forall x)(\forall y)[(x = y) \Leftrightarrow (\forall z)(z \in x \Leftrightarrow z \in y)]$$

Dve množiny sa rovnajú práve vtedy, keď obsahujú rovnaké prvky.

Táto axióma vlastne popisuje základnú vlastnosť množín – množina je jednoznačne určená prvkami, ktoré obsahuje.

Viacero ďalších axióm sa zaoberá tým, existenciou niektorých množín a vytváraním nových množín z už existujúcich množín. Napríklad je pomerne prirodzené požadovať existenciu aspoň jednej množiny, aby náš axiomatický systém nebol úplne bezobsažný. Túto vlastnosť môžeme formálne zapísať napríklad takto.

Axióma IV (Axióma existencie)**.**

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

Existuje aspoň jedna množina.

Pre každú množinu platí $x = x$ vďaka vlastnostiam vzťahu rovnosti.

Nasledujú 2 axiómy popisujúce vytváranie množín z iných množín.

Axióma II (Axióma zjednotenia množín)**.**

$$(\forall A)(\exists U)(\forall z)(z \in U \Leftrightarrow (\exists a \in A)(z \in a))$$

Pre ľubovoľnú množinu A existuje taká množina U, ktorá obsahuje práve tie prvky, ktoré patria do niektorej z množín patriacich do A.

Definícia 2.3.3. Množinu U z predchádzajúcej axiómy nazývame *zjednotenie systému* A a označujeme $\bigcup A$.

Z axiómy extenzionality je zrejmé, že množina $\bigcup A$ je určená jednoznačne.

Axióma III (Axióma dvojice)**.**

$$(\forall A)(\forall B)(\exists C)(\forall z)[z \in C \Leftrightarrow (z = B) \vee (z = C)]$$

Ak a, b sú množiny, tak existuje množina ktorá obsahuje práve prvky a, b a žiadne iné. Túto množinu označíme $\{a, b\}$.

{zfc:TVRZJEDPAIR}

Tvrdenie 2.3.4. *Pre ľubovoľné množiny A, B existuje taká množina C, do ktorej patria práve prvky patriace do množiny A alebo do množiny B. Túto množinu označujeme $A \cup B$ a nazývame* zjednotenie množín A a B.

Dôkaz. Ak A, B sú množiny, tak podľa axiómy dvojice existuje množina $\{A, B\}$ a podľa axiómy zjednotenia existuje množina C, ktorá obsahuje práve prvky patriace do niektorej z množín A, B. □

Ďalšou aplikáciou axiómy dvojice je nasledujúce jednoduché tvrdenie:

TVRSINGLETON}

Tvrdenie 2.3.5. *Pre každú množinu a existuje jediná množina A, ktorá obsahuje a ako jediný svoj prvok, t.j.*

$$z \in A \Leftrightarrow z = a.$$

Túto množinu označujeme $\{a\}$.

Dôkaz. Na dôkaz existencie stačí použiť axiómu dvojice pre dvojicu množín a, a. Jednoznačnosť vyplýva z axiómy extenzionality. □

Nasledujúca axióma vlastne zahŕňa nekonečne veľa axióm – jednu pre každú formulu teórie množín. Preto hovoríme o schéme axióm.

Axióma V (Schéma axióm vymedzenia)**.** Nech $\varphi(x)$ je formula teórie množín, ktorá neobsahuje B ako voľnú premennú. Potom platí

$$(\forall A)(\exists B)(\forall z)(z \in B \Leftrightarrow z \in A \wedge \varphi(z))$$

Pre každú množinu A existuje množina B obsahujúca práve tie prvky z A, pre ktoré je pravdivý výrok $\varphi(z)$, ktorý dostaneme nahradením všetkých voľných výskytov premennej x premennou z. Túto množinu budeme označovať

$$B := \{x \in A; \varphi(x)\}.$$

Všimnime si, že s podobným spôsobom tvorby množín sme sa už stretli v časti 2.2. Nastala však jedna drobná zmena – do novovytvorenej množiny patria len prvky z nejakej vopred danej množiny s danou vlastnosťou. Teda pomocou tejto axiómy nemôžeme zopakovať postup, ktorý sme urobili pri odvodení Russellovho paradoxu.

Túto schému axióm budeme veľmi často využívať, ako ukážku si môžeme ukázať existenciu prázdnej množiny.

Tvrdenie 2.3.6. *Existuje (práve jedna) množina $\emptyset$ s vlastnosťou*

$$(\forall z)(z \notin \emptyset).$$

Túto množinu nazývame prázdna množina.

Dôkaz. Jednoznačnosť ľahko vyplýva z axiómy extenzionality. Ukážeme existenciu.

Podľa axiómy existencie existuje aspoň jedna množina x. Definujme teraz množinu

$$\emptyset := \{z \in x; z \neq z\}.$$

□

Môžeme poznamenať, že v niektorých textoch sa namiesto axiómy existencie uvádza ako axióma existencia prázdnej množiny. Z predchádzajúceho tvrdenia je zrejmé, že takto dostaneme ekvivalentný systém axióm – pomocou ostatných axióm vieme z axiómy existencie dokázať existenciu prázdnej množiny a obrátene.

Schému axióm vymedzenia použijeme napríklad aj v nasledujúcej podkapitole, keď budeme definovať viaceré množinové operácie. Na tomto mieste ešte zadefinujeme prienik dvojice množín.

Tvrdenie 2.3.7. *Pre ľubovoľné dve množiny A, B existuje práve jedna množina C, ktorá obsahuje práve tie prvky, ktoré patria súčasne do A aj do B. Túto množinu nazývame* prienik *množín A a B a označujeme ju $A \cap B$.*

Dôkaz. Množina
$$A \cap B = \{x \in A; x \in B\}$$
existuje podľa schémy axióm vymedzenia použitej pre množinu A a formulu $x \in B$.

Jednoznačnosť vyplýva z axiómy extenzionality. $\square$

Definícia 2.3.8. Množiny A a B sa nazývajú *disjunktné,* ak $A \cap B = \emptyset$, t.j. ak majú prázdny prienik.

Pred uvedením ďalšej axiómy budeme potrebovať ešte jednu definíciu, ktorá nám umožní túto axiómu stručnejšie zapísať.

Definícia 2.3.9. Ak A, B sú množiny, tak hovoríme, že A je *podmnožinou* B, ak každý prvok množiny A je prvkom množiny B. Tento fakt označíme $A \subseteq B$.

$$A \subseteq B \overset{\text{def}}{\Leftrightarrow} (\forall z)(z \in A \Rightarrow z \in B)$$

Vidíme teda, že $A \subseteq B$ je tiež formula teórie množín. Budeme ju často používať ako stručnejší zápis namiesto dlhšej formuly na pravej strane predchádzajúcej ekvivalencie.

Axióma VI (Axióma potenčnej množiny)**.**

$$(\forall A)(\exists P)(\forall z)(z \in P \Leftrightarrow z \subseteq A)$$

Pre každú množinu A existuje množina P pozostávajúca práve z podmnožín množiny A.

Definícia 2.3.10. Množinu všetkých podmnožín množiny A nazývame *potenčná množina* množiny A a označujeme $\mathcal{P}(A)$.

$$\mathcal{P}(A) = \{B; B \subseteq A\}$$

Axióma VI teda vlastne zaručuje existenciu potenčnej množiny pre každú množinu.

Kvôli zostručneniu nasledujúcej axiómy zaveďme ešte jeden symbol.

Definícia 2.3.11. Symbolom $(\exists! x)P(x)$ označujeme fakt, že existuje jediná množina x s vlastnosťou $P(x)$.

Všimnime si, že sme tým nepridali nič nové k jazyku logiky prvého rádu, keďže ten výrok vieme ekvivalentne prepísať napríklad takýmto spôsobom

$$(\exists! x)P(x) \Leftrightarrow (\exists x)(P(x) \wedge (\forall y)(P(y) \Rightarrow y = x)).$$

Zápis $(\exists! x)P(x)$ môžeme teda chápať ako skratku zápisu na pravej strane. V prípade, že $P(x)$ je formula teórie množín, predstavuje aj tento zápis formulu teórie množín.

Pre úplnosť uveďme aj ostatné axiómy, hoci ich významom sa budeme podrobnejšie zaoberať neskôr.

Axióma VIII (Schéma axióm substitúcie)**.** Nech $\varphi(x, y)$ je formula teórie množín, ktorá neobsahuje B ako voľnú premennú. Potom platí

$$(\forall A)[(\forall x \in A)(\exists! y)\varphi(x, y) \Rightarrow (\exists B)(\forall z)(z \in B \Leftrightarrow (\exists x \in A)\varphi(x, z))].$$

Význam tejto axiómy by mohol bude jasnejší po zavedení pojmu funkcie – pozri poznámku 3.2.10. Poznamenajme tiež, že zo schémy axióm substitúcie vyplýva schéma axióm vymedzenia. Obe axiómy sa však zvyknú uvádzať, do istej miery snáď z historických dôvodov (schéma axióm substitúcie bola do axiomatického systému teórie množín zahrnutá neskôr) a azda aj preto, že schéme axióm vymedzenia je podstatne jednoduchšia a názornejšia.

Axióma (Axióma regularity).

$$(\forall A)[(\exists B)(B \in A) \Rightarrow (\exists B \in A)\neg[(\exists c)(c \in A \wedge c \in B)]]$$

Každá neprázdna množina obsahuje množinu, ktorá je s ňou disjunktná.

Z axiómy regularity sa dá pomerne ľahko odvodiť, že pre každú množinu platí $x \notin x$, preto by sa mohlo zdať, že jej zavedenie bolo do istej miery motivované Russellovým paradoxom. V skutočnosti dôvody na zavedenie tejto boli iné, my sa nimi nebudeme detailne zaoberať.

Tvrdenie 2.3.12. *Pre ľubovoľnú množinu platí $x \notin x$.*

Dôkaz. Ak x je množina, tak podľa tvrdenia 2.3.5 existuje množina $A := \{x\}$. Podľa axiómy regularity existuje $B \in A$ také, že $B \cap A = \emptyset$. Lenže ak $B \in A$, tak $B = x$ (keďže množina A je jednoprvková) a dostávame $x \cap \{x\} = \emptyset$, čo znamená, že $x \notin x$. □

Na prvý pohľad by sa mohlo zdať, že axiómu regularity

Axióma X (Axióma nekonečnej množiny).

$$(\exists A)[\emptyset \in A \wedge (x \in A \Rightarrow x \cup \{x\} \in A)]$$

Keďže sme už ukázali, že pre ľubovoľné x platí $x \notin x$, znamená to, že $x \cup \{x\} \neq x$ a spôsobom popísaným v tejto axióme pre každý prvok x pridávame nejaký nový prvok. Keď začneme z prázdnej množiny, každá nová množina, ktorú takto vytvoríme, je vlastnou nadmnožinou tej predchádzajúcej. Teda potom množina A skutočne má nekonečne veľa prvkov.

Doteraz uvedené axiómy sa zvyknú označovať ako axiomatický systém ZF. Po pridaní nasledujúcej axiómy už dostaneme celý systém ZFC.

Axióma VIII (Axióma výberu).

$$(\forall \mathcal{S})[(\forall A \in \mathcal{S})(A \neq \emptyset) \wedge (\forall A \in \mathcal{S})(\forall B \in \mathcal{S})(A \neq B \Rightarrow A \cap B = \emptyset) \Rightarrow (\exists V)(\forall A \in \mathcal{S})(\exists x)(V \cap A = \{x\})]$$

Ak $\mathcal{S}$ je systém neprázdnych disjunktných množín, tak existuje množina B, ktorá má s každou z týchto množín jednoprvkový prienik.

Axióma výberu je veľmi dôležitá axióma. Neskôr si uvedieme zrozumiteľnejšiu ekvivalentnú formuláciu tejto axiómy. Axiómou výberu sa budeme podrobne zaoberať v kapitole 5. Z formulácie, ktorú sme uviedli, by však mohlo byť jasné, prečo sa nazýva axióma výberu – množina B z každej množiny patriacej do $\mathcal{S}$ „vyberá“ práve jeden prvok.

Veľmi dobre napísané poznámky o motivácii a význame jednotlivých axióm si môžete prečítať napríklad v [Z, s.79–83][6]. (Môžete si tam prečítať aj o axiómach, ktorými sa v tomto texte podrobne nezaoberáme, ako je axióma regularity.)

[6] Táto kniha je voľne dostupná na internete

2.4 Operácie s množinami

V tejto časti sa budeme venovať niektorým operáciam s množinami a ukážeme si tvrdenia, ktoré o nich platia. Tieto výsledky majú veľmi jednoduché a názorné dôkazy, preto sa od vás očakáva, že takéto tvrdenia budete schopní samostatne dokazovať a ba dokonca aj na ne prísť, keď ich budete potrebovať použiť.

V predchádzajúcej kapitole sme definovali vzťah „byť podmnožinou“, ktorý sa zvykne nazývať aj *inklúziou*.

$$A \subseteq B \overset{\text{def}}{\Leftrightarrow} (\forall z)(z \in A \Rightarrow z \in B)$$

Nasledujúce tvrdenie zhŕňa základné vlastnosti inklúzie.

{oper:TVRSUBSET}
{oper:itSUB1} **Tvrdenie 2.4.1.** *Nech A, B, C sú ľubovoľné množiny. Potom platí:*
{oper:itSUB2} (i) *Pre každú množinu platí $A \subseteq A$.*
{oper:itSUB3} (ii) *$A = B$ práve vtedy, keď $A \subseteq B \wedge B \subseteq A$.*
(iii) *Ak platí $A \subseteq B$ a $B \subseteq C$, tak $A \subseteq C$.*

Dôkaz. (i) Uvedené tvrdenie je ekvivalentné s platnosťou implikácie $x \in A \Rightarrow x \in A$ pre ľubovoľné x. Pravdivosť tejto implikácie vyplýva z tautológie $r \Rightarrow r$ ak v nej za výrok r dosadíme $x \in A$.

(ii) Vyplýva priamo z definície podmnožiny (s použitím axiómy extenzionality a tautológie z úlohy 2.1.1b)).

(iii) Stačí použiť tautológiu $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$. □

Tvrdenie 2.4.1(ii) niekedy budeme používať na dôkaz rovnosti množín – môžeme dokazovať to, že množiny A a B sa rovnajú tak, že zvlášť dokážeme inklúzie $A \subseteq B$ a $B \subseteq A$.

Definícia 2.4.2. Ak A je podmnožina B a súčasne $A \neq B$, tak hovoríme, že A je *vlastná podmnožina* množiny B. Označenie $A \subsetneq B$.

$$A \subsetneq B \Leftrightarrow (A \subseteq B) \wedge (A \neq B)$$

Poznámka 2.4.3. V tomto texte používam $\subseteq$ na označenie podmnožiny a $\subsetneq$ na označenie vlastnej podmnožiny. Toto označenie som zvolil z toho dôvodu, že som sa chcel vyhnúť možným nedorozumeniam. Dosť často sa na označenie inklúzie používa $\subset$, nájdu sa však aj texty (hoci zriedkavejšie), v ktorých $\subseteq$ je symbolom pre podmnožinu, zatiaľčo $\subset$ označuje vlastnú podmnožinu.

Budeme teraz pokračovať tým, že pripomenieme niektoré operácie, ktoré sme definovali v predchádzajúcej podkapitole a zadefinujeme niekoľko nových.

Pre dvojicu množín sme zatiaľ zadefinovali zjednotenie a prienik množín.

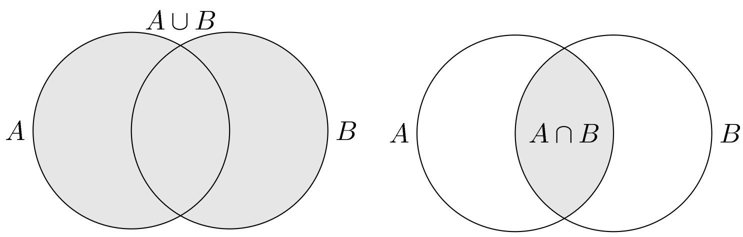
$$A \cup B = \{x; x \in A \vee x \in B\}$$
$$A \cap B = \{x \in A; x \in B\}$$

Tieto operácie sú znázornené na obrázku 2.1 pomocou Vennových diagramov. (Vennovým diagramom sa ešte budeme podrobnejšie venovať v časti 2.4.)

Na tomto mieste si môžeme pripomenúť, že pre konečné množiny ste sa na diskrétnej matematiky naučili vypočítať počet prvkov zjednotenia dvoch množín:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

(Podobné vzťahy pre viac ako dve množiny viete takisto odvodiť použitím princípu zapojenia a vypojenia.)



:FIGZJEDPRIE} Obr. 2.1: Zjednotenie a prienik dvoch množín

Na príklade týchto dvoch operácií si ukážeme, ako môžeme dokazovať rôzne množinové identity. (Keďže však ide o jednoduché dôkazy, ktoré sa dajú ľahko previesť na overovanie tautológií, väčšinu z nich ponecháme ako cvičenie.)

TVRZJEDPRIEN}

Tvrdenie 2.4.4. *Nech A, B, C sú množiny. Potom platí:*

{oper:it1ZJEDPRIEN}

(i) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ (*asociatívnosť operácií* $\cup$ *a* $\cap$);
(ii) $A \cup B = B \cup A$, $A \cap B = B \cap A$ (*komutatívnosť operácií* $\cup$ *a* $\cap$);
(iii) $\emptyset \cup A = A$, $\emptyset \cap A = \emptyset$; {oper:itDISTRIB}
(iv) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (*distributívnosť*); {oper:itIDEMP}
(v) $A \cap A = A$, $A \cup A = A$ (*idempotentosť operácií* $\cup$ *a* $\cap$) {oper:it6ZJEDPRIEN}
(vi) $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$ (*zákony absorpcie*).

Dôkaz. (i) Na základe axiómy extenzionality sa dve množiny rovnajú práve vtedy, keď obsahujú rovnaké prvky. Teda nám stačí ukázať, že platí

$$x \in A \cup (B \cup C) \qquad \Leftrightarrow \qquad x \in (A \cup B) \cup C.$$

Priamo na základe definície zjednotenia môžeme výrok $x \in A \cup (B \cup C)$ prepísať ako $(x \in A) \vee [(x \in B) \vee (x \in C)]$. Podobne výrok na pravej strane ekvivalencie je ekvivalentný s výrokom $[(x \in A) \vee (x \in B)] \vee (x \in C)$. Ak si teda označíme $p := (x \in A)$, $q := (x \in B)$ a $r := (x \in C)$, tak vlastne máme dokázať

$$p \vee (q \vee r) \qquad \Leftrightarrow \qquad (p \vee q) \vee r,$$

čo je presne tautológia z úlohy 2.1.2a).

Veľmi podobným spôsobom sa dá druhá časť tohoto tvrdenia previesť na tautológiu 2.1.2b). □

V predchádzajúcom dôkaze sme videli jeden možný spôsob dôkazu množinových identít – založený na tom, že dokazovanú identitu prevedieme na tautológiu, ktorú potom overujeme. Inou možnosťou je dôkaz spočívajúci v algebraickej manipulácii – pokiaľ máme už dokázaný dostatočne veľa identít, môžeme ich použiť na dôkaz nových identít; takýto postup si ukážeme napríklad v príklade 2.4.8. V závere tejto podkapitoly sa budeme ešte venovať metóde dôkazu množinových identít pomocou Vennových diagramov.

Niekedy budeme potrebovať urobiť prienik nie len jednej množiny, ale celého systému množín.

Ak $\mathcal{S}$ je množina, tak podľa axiómy zjednotenia existuje jej zjednotenie, ktoré budeme označovať $\bigcup \mathcal{S}$. Dosť často hovoríme v takomto prípade o *zjednotení systému množín,* pretože jednotlivé prvky množiny $\mathcal{S}$ chápeme ako množiny.

Budeme často používať aj dve ďalšie označenia pre zjednotenie systému množín, konkrétne $\bigcup\limits_{A\in\mathcal{S}} A$ a v prípade, že $\mathcal{S}=\{A_i; i\in I\}$, tak zjednotenie tohoto systému označíme $\bigcup\limits_{i\in I} A_i$.

Poznamenajme, že zápisom $\mathcal{S}=\{A_i; i\in I\}$ rozumieme to, že pre každý prvok množiny $i\in I$ je jednoznačne určená množina A_i. Potom podľa schémy axióm substitúcie existuje aj množina $\{A_i; i\in I\}$ a podľa axiómy zjednotenia existuje zjednotenie tejto množiny.

Budeme používať aj prienik systému množín – pre *neprázdny* systém $\mathcal{S}=\{A_i; i\in I\}$ zavedieme označenia:

$$\bigcap\mathcal{S}=\bigcap_{A\in\mathcal{S}} A := \{z; (\forall A\in\mathcal{S}) z\in A\}$$

$$\bigcap_{i\in I} A_i := \{z; (\forall i\in I) z\in A_i\}$$

Existenciu prieniku $\mathcal{S}$ môžeme zdôvodniť pomocou schémy axióm vymedzenia – túto množinu totiž môžeme ekvivalentne zapísať ako $\{z\in\bigcup\mathcal{S}; (\forall A\in\mathcal{S})z\in A\}$. (Ak $\mathcal{S}\neq\emptyset$, tak z vlastnosti $(\forall A\in\mathcal{S})z\in A$, ktorou definujeme prienik systému $\mathcal{S}$, vyplýva $(\exists A\in\mathcal{S})z\in A$, a teda $z\in\bigcup\mathcal{S}$. Pre $\mathcal{S}=\emptyset$ by takéto zdôvodnenie nefungovalo a keby sme rovnakým spôsobom chceli definovať prienik prázdneho systému, dostali by sme množinu všetkých množín – tá však neexistuje; pozri vetu 2.5.7.)

Na dôkaz rôznych identít platných pre prienik a zjednotenie systému množín môžeme použiť podobný prístup ako pre prienik a zjednotenie dvoch množín, ibaže namiesto tautológií v tomto prípade dostaneme výroky s kvantifikátormi, ktorých platnosť bude treba overiť.

Nasledujúce tvrdenie hovorí, že distributívnosť platí aj pre prienik a zjednotenie systému množín:

{oper:TVRDISTRIBSYSTEM}

Tvrdenie 2.4.5. *Nech $\mathcal{S}$ a B sú ľubovoľné množiny. Potom platí:*
(i) $B\cap\bigcup_{A\in\mathcal{S}} A=\bigcup_{A\in\mathcal{S}}(B\cap A)$;
(ii) $B\cup\bigcap_{A\in\mathcal{S}} A=\bigcap_{A\in\mathcal{S}}(B\cup A)$.

Dôkaz. Opäť ukážeme iba prvú časť tvrdenia, druhú identitu ponechávame ako cvičenie.

Pokúsme sa (podľa definície) prepísať, čo to znamená, že prvok x patrí do množiny uvedenej na ľavej strane dokazovanej rovnosti. Použitíme definície prieniku dvoch množín a prieniku systému množín dostaneme, že

$$x\in B\cap\bigcup_{A\in\mathcal{S}} A \Leftrightarrow (x\in B)\wedge(\forall A\in\mathcal{S})x\in A.$$

Pre množinu na pravej strane rovnosti dostávame

$$x\in\bigcup_{A\in\mathcal{S}}(B\cap A)\Leftrightarrow(\forall A\in\mathcal{S})(x\in B\wedge x\in A).$$

Ak označíme $p:=(x\in B)$ a $Q(A):=x\in A$, tak vlastne máme overiť ekvivalenciu

$$p\wedge(\forall A\in\mathcal{S})Q(A)\Leftrightarrow(\forall A\in\mathcal{S})p\wedge Q(A).$$

To je presne ekvivalencia z úlohy 2.1.8c). □

Dokážeme aj niektoré vzťahy medzi množinovými operáciami a reláciou inklúzie.

{oper:TVRSUBEKV}
{oper:it1SUBEKV}

Tvrdenie 2.4.6. *Nech A a B sú množiny. Nasledujúce podmienky sú ekvivalentné:*
(i) $A\subseteq B$;

er:it2SUBEKV}
er:it3SUBEKV} (ii) $A = A \cap B$;
(iii) $B = A \cup B$.

Dôkaz. (i) $\Rightarrow$ (ii): Podmienka $A \subseteq B$ znamená platnosť implikácie $(x \in A) \Rightarrow (x \in B)$ pre ľubovoľné x.

Ak $x \in A$, tak na základe tejto implikácie platí aj $x \in B$, čiže platí $(x \in A) \wedge (x \in B)$, t.j. $x \in A \cap B$. Tým je dokázaná inklúzia $A \subseteq A \cap B$.

Obrátene, z $x \in A \cap B$, t.j. $(x \in A) \wedge (x \in B)$ vyplýva $x \in A$. (Tu dokonca nepotrebujeme podmienku $A \subseteq B$. Používame vlastne tautológiu $p \Rightarrow (p \wedge q)$.) Teda platí aj inklúzia $A \cap B \subseteq A$.

Spojením týchto dvoch inklúzií dostávame rovnosť $A = A \cap B$.

Dôkaz implikácie (i) $\Rightarrow$ (iii) je veľmi podobný ako dôkaz predchádzajúcej časti, ponechávame ho ako cvičenie.

(ii) $\Rightarrow$ (i): Predpokladajme, že platí $A = A \cap B$. Ak $x \in A$, tak potom $x \in A \cap B$, čo znamená, že $(x \in A) \wedge (x \in B)$. Teda x patrí aj do množiny B. Tým je ukázaná inklúzia $A \subseteq B$.

Dôkaz implikácie (iii) $\Rightarrow$ (i) opäť prenecháme čitateľovi. □

{oper:TVRSUB}

Tvrdenie 2.4.7. *Nech A, B, C sú množiny. Potom platí:*

(i) $\emptyset \subseteq A$; {oper:it1SUB}
(ii) $A \cap B \subseteq A \subseteq A \cup B$; {oper:it2SUB}
(iii) *Ak $A \subseteq B$, tak $A \cap C \subseteq B \cap C$ a $A \cup C \subseteq B \cup C$.* {oper:it3SUB}

Dôkaz. (i): Množina $\emptyset$ neobsahuje žiadny prvok, teda každý prvok z $\emptyset$ patrí aj do A.

(ii): Platí $x \in A \cap B \Leftrightarrow [(x \in A) \wedge (x \in B)] \Rightarrow x \in A$. Tým je dokázaná inklúzia $A \cap B \subseteq A$.

Podobne z $x \in A$ vyplýva $(x \in A) \vee (x \in B) \Leftrightarrow x \in A \cup B$, a teda platí $A \subseteq A \cup B$.

(iii): Predpokladáme, že $A \subseteq B$, čiže platí implikácia $(x \in A) \Rightarrow (x \in C)$. Potom platí aj $[(x \in A) \wedge (x \in B)] \Rightarrow [(x \in A) \wedge (x \in C)]$ (na základe tautológie $(p \Rightarrow q) \Rightarrow [(p \wedge r) \Rightarrow (q \wedge r)]$); čo je len inak zapísaná implikácia $x \in A \cap B \Rightarrow x \in A \cap C$. Dôkaz druhej časti sa dá urobiť úplne analogicky.

Skúsme ešte urobiť dôkaz druhej časti pomocou tvrdenia 2.4.6. (Touto metódou by sa samozrejme dala dokazovať aj prvá časť tvrdenia.) Vieme teda, že platí $B = A \cup B$ a radi by sme pomocou toho dokázali $(A \cup C) \cup (B \cup C) = B \cup C$. Z tvrdenia 2.4.4 vieme, že operácia $\cup$ je asociatívna (výrazy obsahujúce len túto operáciu môžeme ľubovoľne prezátvorkovať), komutatívna (množiny môžeme vymieňať) a idempotentná. Pomocou týchto vlastností skutočne dostaneme

$$(A \cup B) \cup (B \cup C) = [A \cup (B \cup C)] \cup C = (A \cup B) \cup C = B \cup C.$$

□

Ako príklad použitia predchádzajúcich tvrdení uvedieme iný dôkaz tvrdenia 2.4.4(vi).

{oper:PRABSORP}

Príklad 2.4.8. $A \cap (A \cup B) \overset{(1)}{=} (A \cap A) \cup (A \cap B) \overset{(2)}{=} A \cup (A \cap B) \overset{(3)}{=} A$, pričom v jednotlivých rovnostiach sme použili:
(1) distributívnosť – tvrdenie 2.4.4(iv)
(2) idempotentnosť – tvrdenie 2.4.4(v)
(3) fakt, že $A \cap B \subseteq A$ – tvrdenie 2.4.7(ii) – a tvrdenie 2.4.6 pre množiny $A \cap B$ a A.

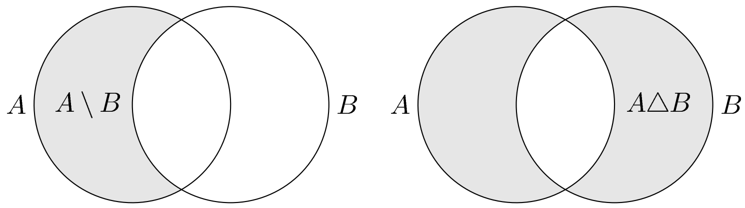
Ďalšie operácie, ktoré budeme niekedy používať sú rozdiel a symetrická diferencia (symetrický rozdiel) dvoch množín.

Definícia 2.4.9. *Rozdiel množín* A a B je množina

$$A \smallsetminus B := \{x \in A; x \notin B\}.$$

Symetrická diferencia množín A a B je množina

$$A \triangle B = (A \smallsetminus B) \cup (B \smallsetminus A)$$



{oper:FIGROZD} Obr. 2.2: Vennove diagramy pre $A \smallsetminus B$ a $A \triangle B$

Symetrický rozdiel je teda množina tých prvkov, ktoré patria práve do jednej z množín A, B. Zodpovedá logickej spojke XOR.

{oper:TVRSETMINUS}

Tvrdenie 2.4.10. *Nech A, B, C sú množiny. Potom platí:*

{oper:itDEMORGAN}

(i) $A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C)$, $A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C)$;
(ii) $A \smallsetminus (B \cup C) = (A \smallsetminus B) \smallsetminus C$;
(iii) $A \smallsetminus (B \smallsetminus C) = (A \smallsetminus B) \cup (A \cap C)$;
(iv) $(A \cup B) \smallsetminus C = (A \smallsetminus C) \cup (B \smallsetminus C)$, $(A \cap B) \smallsetminus C = (A \smallsetminus C) \cap (B \smallsetminus C)$;
(v) $A \smallsetminus B = A \smallsetminus (A \cap B)$;
(vi) $(A \smallsetminus B) \cap C = (A \cap C) \smallsetminus B = A \cap (C \smallsetminus B)$;
(vii) $(A \smallsetminus B) \cup C = (A \cup C) \smallsetminus (B \smallsetminus C)$;
(viii) $A \cup B = (A \smallsetminus B) \cup (B \smallsetminus A) \cup (A \cap B)$;
{oper:itDEMORGANSYS} (ix) $A \subseteq B \Leftrightarrow A \smallsetminus B = \emptyset$.
(x) *Ak pre každé $i \in I$ je B_i množina, tak platí $A \smallsetminus \bigcap_{i\in I} B_i = \bigcup_{i\in I}(A \smallsetminus B_i)$ a $A \smallsetminus \bigcup_{i\in I} B_i = \bigcap_{i\in I}(A \smallsetminus B_i)$.*
{oper:itSMSUBSET}
(xi) *Ak $B \subseteq C$, tak $A \smallsetminus C \subseteq A \smallsetminus B$.*
(xii) *Ak $B \subseteq C$, tak $B \smallsetminus A \subseteq C \smallsetminus A$.*

Časti (i) a (x) sa zvyknú nazývať *de Morganove zákony.*

{oper:TVRSYMDIF}

Tvrdenie 2.4.11. *Nech A, B, C sú množiny. Potom platí:*

{oper:itASOCSYMDIF}

(i) $A \triangle B = B \triangle A$;
(ii) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;
(iii) $A \triangle A = \emptyset$, $A \triangle \emptyset = A$;
(iv) $A \cup B = A \triangle B \triangle (A \cap B)$;
(v) $A \smallsetminus B = A \triangle (A \cap B)$.

Dôkaz. (ii) Štandardným spôsobom prevedieme uvedené tvrdenie na dôkaz tautológie $(p \,\mathrm{XOR}\, q) \,\mathrm{XOR}\, r \Leftrightarrow p \,\mathrm{XOR} (q \,\mathrm{XOR}\, r)$, pričom logická spojka XOR je určená tabuľkou

p	q	$p\,\mathrm{XOR}\,q$
1	1	0
1	0	1
0	1	1
0	0	0

Pri dokazovaní našej tautológie potom dostávame nasledujúcu tabuľku:

p	q	r	$p\,\mathrm{XOR}\,q$	$a := (p\,\mathrm{XOR}\,q)\,\mathrm{XOR}\,r$	$q\,\mathrm{XOR}\,r$	$b := p\,\mathrm{XOR}(q\,\mathrm{XOR}\,r)$	$a \Leftrightarrow b$
1	1	1	0	1	0	1	1
1	1	0	0	0	1	0	1
1	0	1	1	0	1	0	1
1	0	0	1	1	0	1	1
0	1	1	1	0	0	0	1
0	1	0	1	1	1	1	1
0	0	1	0	1	1	1	1
0	0	0	0	0	0	0	0

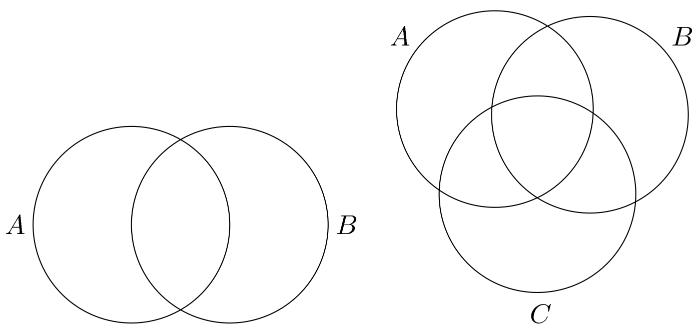
□

Vennove diagramy

{oper:SSSECTVENN}

Pri dôkazoch množinových identít môžeme použiť aj *Vennove diagramy.* Pri nich znázorníme množiny ako rovinné útvary, pričom dbáme na to, aby množiny boli v tzv. *generickej polohe,* t.j. aby sa tam vyskytli „všetky možné“ oblasti. (Napríklad oblasť predstavujúca prvky patriace do A aj B a nepatriace do C, ak kreslíme Vennov diagram pre 3 množiny.)

Na obrázku 2.3 sú znázornené 2 resp. 3 množiny v generickej polohe. (Môžete sa pokúsiť vymyslieť, ako by ste kreslili Vennove diagramy pre viac množín.)



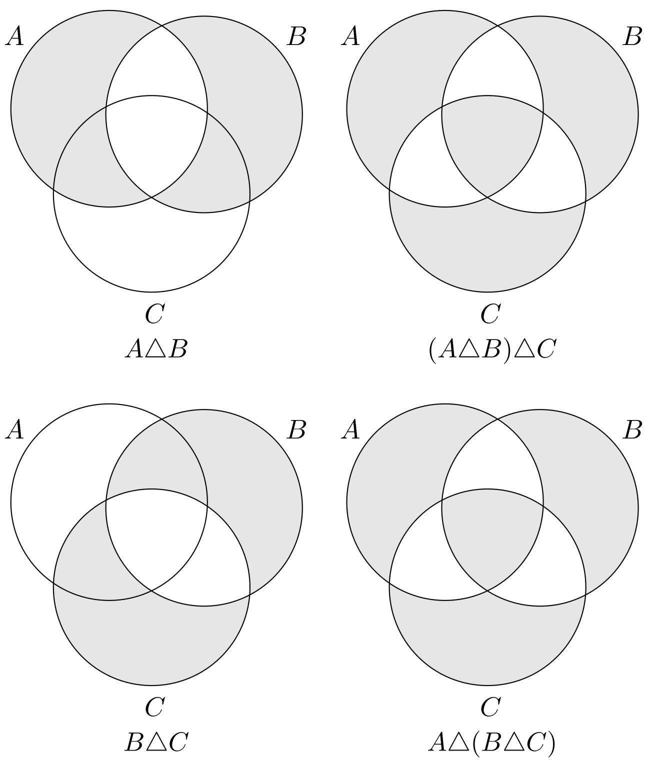
Obr. 2.3: Generická poloha

{oper:FIGGENER}

Pri dôkaze postupujeme tak, že vo Vennovom diagrame nakreslíme postupne, ako vyzerajú množiny na ľavej a pravej strane rovnosti a tieto obrázky porovnáme.

Príklad 2.4.12. Ako príklad si ukážeme dôkaz asociatívnosti pre operáciu $\triangle$ (tvrdenie 2.4.11(ii)). Dôkaz toho istého tvrdenia overením príslušnej tautológie tabuľkovou metódou sme už videli.

Na obrázku 2.4 vidíme, ako môžeme postupovať. Najprv (ako pomôcku) sme si nakreslili oblasť zodpovedajúcu množine $A\triangle B$ a potom, pomocou nej, sme dostali množinu $(A\triangle B)\triangle C$ vystupujúcu na ľavej strane rovnosti.



Obr. 2.4: Asociatívnosť operácie $\triangle$ {oper:FIGSYMD

Analogicky postupujeme pre množinu $A\triangle(B\triangle C)$ na pravej strane rovnosti. Vidíme, že sme dostali presne rovnaké obrázky, čiže rovnosť $(A\triangle B)\triangle C = A\triangle(B\triangle C)$ platí.

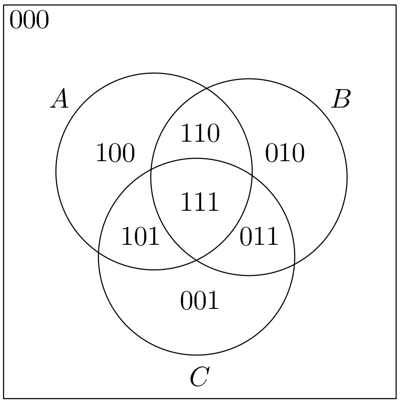
Môžete sa pýtať, do akej miery je dôkaz pomocou Vennových diagramov korektný. (Od prvého ročníka na vysokej škole ste už určite veľakrát počuli, že „obrázok nie je dôkaz".) Odpoveď je, že tento dôkaz je úplne rovnocenný s overením príslušnej tautológie tabuľkovou metódou. Robíme tam totiž presne to isté, čo pri tabuľkovej metóde, len namiesto symbolov 0 a 1 používame farebné zvýraznenie niektorej oblasti – pozri obrázok 2.5. Môžete si teda vybrať ktorúkoľvek z týchto dvoch metód a používať tú, ktorá vám väčšmi vyhovuje a pri ktorej máte menšiu obavu z toho, že by ste spravili chybu.

Cvičenia

Úloha 2.4.1. Dokážte tvrdenia 2.4.4, 2.4.6, 2.4.7, 2.4.5, 2.4.10, 2.4.11; resp. tie časti uvedených tvrdení, ktoré sme nedokázali v predchádzajúcom texte. (Vyskúšajte si aspoň na niektorom príklade tabuľkovú metódu aj Vennove diagramy; v prípade tvrdení týkajúcich sa inklúzie si môžete vyskúšať dôkaz priamo z definície ako aj použitie tvrdenia 2.4.6.)

Úloha 2.4.2. Pokúste sa vymyslieť nejaké možné nakreslenia Vennovho diagramu pre 4 (prípadne aj viac) množín.

Úloha 2.4.3. Zistite, či sú uvedené tvrdenia pravdivé (pre ľubovoľný výrok $P(x)$). V prípade nepravdivých tvrdení rozhodnite, či aspoň jedna z implikácií je pravdivá. Svoje tvrdenie



:FIGVENN3TAB} Obr. 2.5: Vzťah medzi Vennovým diagramom a tabuľkou

zdôvodnite!
a) $[(\exists x \in A)P(x) \vee (\exists x \in B)P(x)] \Leftrightarrow (\exists x \in A \cup B)P(x)$
b) $[(\forall x \in A)P(x) \vee (\forall x \in B)P(x)] \Leftrightarrow (\forall x \in A \cup B)P(x)$
c) $[(\forall x \in A)P(x) \wedge (\forall x \in B)P(x)] \Leftrightarrow (\forall x \in A \cup B)P(x)$
e) $[(\exists x \in A)P(x) \wedge (\exists x \in B)P(x)] \Leftrightarrow (\exists x \in A \cap B)P(x)$
f) $[(\forall x \in A)P(x) \vee (\forall x \in B)P(x)] \Leftrightarrow (\forall x \in A \cap B)P(x)$
g) $[(\forall x \in A)P(x) \wedge (\forall x \in B)P(x)] \Leftrightarrow (\forall x \in A \cap B)P(x)$.

2.5 Usporiadané dvojice a karteziánsky súčin

{kartez:SECTKARTEZ}

Posledný typ operácie definovanej na množinách, ktorým sa budeme zaoberať, je karteziánsky súčin. Tu ho zadefinujeme pre dve množiny, resp. pre konečný počet množín, neskôr (v časti 3.2.1) ho zadefinujeme aj karteziánsky súčin ľubovoľného systému množín. Na to, aby sme mohli zadefinovať karteziánsky súčin dvoch množín, však najprv potrebujeme definovať pojem usporiadanej dvojice.

Definícia 2.5.1. Nech a, b sú množiny. Potom množinu

$$(a,b) := \{\{a\},\{a,b\}\}$$

nazývame *usporiadanou dvojicou* množín a a b.

Táto definícia sa môže na prvý pohľad zdať neobvyklá. Treba si uvedomiť, že pracujeme iba s množinami a každý objekt chceme definovať ako nejakú množinu. Ľahko si môžete všimnúť, že množina uvedená v definícii skutočne existuje – stačí viackrát použiť axiómu dvojice. Menej zrejmé je, prečo by práve takáto množina mala byť vhodnou definíciou usporiadanej množiny. Odpoveď je, že spĺňa základnú vlastnosť, ktorú od usporiadaných množín vyžadujeme – sformulovanú v nasledujúcom tvrdení. (Pokojne by sme mohli použiť aj akúkoľvek inú definíciu usporiadanej dvojice, ktorá by vyhovovala tejto požiadavke.)

{kartez:TVRUSPDVOJ}

Tvrdenie 2.5.2. *Nech a, b, c, d sú množiny. Potom*

$$(a,b) = (c,d) \qquad \Leftrightarrow \qquad a = c \wedge b = d.$$

Dôkaz. Platnosť implikácie $\Leftarrow$ je jasná.

$\boxed{\Rightarrow}$ Predpokladáme, že platí $(a,b)=(c,d)$, t.j. $\{\{a\},\{a,b\}\}=\{\{c\},\{c,d\}\}$. Potom $\{a\}\in\{\{c\},\{c,d\}\}$, čo znamená, že buď $\{a\}=\{c\}$ (a teda $a=c$) alebo $\{a\}=\{c,d\}$.

V prvom z uvedených prípadov dostaneme $\{\{a\},\{a,b\}\}=\{\{a\},\{a,d\}\}$. Ak $b=a$, tak túto rovnosť môžeme prepísať ako $\{\{a\}\}=\{\{a\},\{a,d\}\}$, čo ale znamená, že $\{a\}=\{a,d\}$, a teda $a=d$.

Ak $b\neq a$, tak $\{a,b\}\neq\{a\}$, a preto musí platiť $\{a,b\}=\{a,d\}$ a $b=d$.

Zostáva nám rozmyslieť si druhú možnosť, keď $\{a\}=\{c,d\}$. Táto rovnosť ale znamená, že $a=c=d$. Potom pôvodnú rovnosť môžeme prepísať ako $\{\{a\},\{a,b\}\}=\{a\}$ a zopakovaním rovnakej úvahy, ako sme použili pred chvíľou, dostaneme $a=b=c=d$. □

Teraz už môžeme zadefinovať karteziánsky súčin dvoch množín.

Definícia 2.5.3. Karteziánsky súčin množín A a B je množina, ktorej prvkami sú práve také usporiadané dvojice, kde prvý prvok patrí do množiny a a druhý prvok patrí do množiny b. Túto množinu označujeme

$$A\times B:=\{(a,b);a\in A,b\in B\}.$$

Ešte overíme na základe axióm existenciu množiny $A\times B$. Všimnime si, že $\{a\}\subseteq A\cup B$ aj $\{a,b\}\subseteq A\cup B$ pre ľubovoľné prvky $a\in A$, $b\in B$. Teda $\{a\},\{a,b\}\in\mathcal{P}(\{\}A\cup B\}$ a $(a,b)=\{\{a\},\{a,b\}\}\in\mathcal{P}(\mathcal{P}(A\cup B))$. Vďaka tomu môžeme karteziánsky súčin prepísať ako

$$A\times B=\{x\in\mathcal{P}(\mathcal{P}(A\cup B));(\exists a\in A)(\exists b\in B)x=(a,b)\}.$$

Existencia takejto množiny je zaručená schémou axióm vymedzenia.[7]

Je zrejmé, že uvedená definícia sa dá veľmi ľahko rozšíriť pre konečný počet množín.

Uvedieme niektoré základné vlastnosti karteziánskeho súčinu. Opäť, ako obvykle, dôkazy viacerých z nich ponecháme ako cvičenie.

{kartez:TVROPER}

Tvrdenie 2.5.4. *Nech A, B, C, D sú množiny. Potom platí*

(i) $A\times\emptyset=\emptyset\times A=\emptyset$;
(ii) $A\times(B\cup C)=(A\times B)\cup(A\times C)$;
(iii) $A\times(B\cap C)=(A\times B)\cap(A\times C)$;
(iv) $A\times(B\smallsetminus C)=(A\times B)\smallsetminus(A\times C)$.
(v) *Ak navyše predpokladáme, že A, B, C, D sú neprázdne, tak $A\times B=C\times D$ platí práve vtedy, keď $A=C$ a $B=D$.*

Dôkaz. Ukážeme druhú a piatu časť tvrdenia – ostatné zostanú ako cvičenie pre čitateľa.

(ii): Prvok x patrí do množiny $A\times(B\cup C)$ práve vtedy, keď $x=(a,d)$ pre nejaké $a\in A$ a $d\in B\cup C$. To znamená, že $d\in B$ alebo $d\in C$. Teda dostávame, že $x\in A\times(B\cup C)$ práve vtedy, keď $x=(a,d)$ pre nejaké $a\in A$ a $d\in B$ alebo $x=(a,d)$ pre nejaké $a\in A$ a $d\in C$. Posledná časť je ale len iný zápis toho, že $x\in(A\times B)\cup(A\times C)$.

(v): Predpokladajme, že $A\neq\emptyset$. Teda existuje nejaký prvok $a\in A$. Potom pre každý prvok $b\in B$ platí $(a,b)\in A\times B=C\times D$. Z toho, že $(a,b)\in C\times D$ už vyplýva, že $b\in D$. Dokázali sme teda inklúziu $B\subseteq D$.

Inklúzia $D\subseteq B$ sa dokáže podobne, s využitím toho, že $C\neq\emptyset$. Tým je dokázané $B=D$.

Rovnosť $A=C$ možno zdôvodniť analogicky. □

[7] V ďalších kapitolách už nebudeme väčšinou posupovať úplne podrobne až k axiómam vo všetkých dôkazoch. Každopádne na základe ukážok, ktoré ste videli doteraz, by mohlo byť pre vás aj pri ďalších dôkazoch predstaviteľné, že sa dajú prepísať až na postupnosť logických krokov, ktoré využívajú iba axiómy systému ZFC.

Ukážeme si na konkrétnych príkladoch, že karteziánsky súčin nie je vo všeobecnosti komutatívny ani asociatívny.

Príklad 2.5.5. Nájdite príklad množín A, B takých, že $A \times B \neq B \times A$!

Stačí zobrať ľubovoľné dve jednoprvkové množiny $A = \{a\}$, $B = \{b\}$ také, že $a \neq b$. (Napríklad $a = \emptyset$, $B = \{\emptyset\}$.)

Potom aj množiny $A \times B = \{(a, b)\}$ a $B \times A = \{(b, a)\}$ sú jednoprvkové. Ak by sa rovnali, znamenalo by to, že $(a, b) = (b, a)$ a podľa tvrdenia 2.5.2 $a = b$, čo je spor.

Príklad 2.5.6. Nájdite príklad množín A, B, C takých, že $A \times (B \times C) \neq A \times (B \times C)$!

Opäť vystačíme s jednoprvkovými množinami. Vyskúšajme $A = B = C = \{\emptyset\}$. Potom dostaneme

$$A \times (B \times C) = \{\emptyset\} \times \{(\emptyset, \emptyset)\} = \{(\emptyset, (\emptyset, \emptyset))\}$$
$$(A \times B) \times C = \{(\emptyset, \emptyset)\} \times \{\emptyset\} = \{((\emptyset, \emptyset), \emptyset)\}$$

Ak by sa tieto dve množiny rovnali, tak by platilo $(\emptyset, (\emptyset, \emptyset)) = ((\emptyset, \emptyset), \emptyset)$ a podľa tvrdenia 2.5.2 aj $\emptyset = (\emptyset, \emptyset)$. Podľa definície usporiadanej dvojice ale $(\emptyset, \emptyset) = \{\{\emptyset\}\}$, čo nie je prázdna množina.

Cvičenia

Úloha 2.5.1. Dokážte ostatné časti tvrdenia 2.5.4.

Úloha 2.5.2. Dokážte, že z rovnosti $X \times X = Y \times Y$ vyplýva $X = Y$.

Úloha 2.5.3. Dokážte (priamo, nie s použitím tvrdenia 2.5.4):
a) Pre $A, B \neq \emptyset$ platí $A \times B = B \times A \Rightarrow A = B$;
b) $A \times B = \emptyset \Leftrightarrow A = \emptyset \vee B = \emptyset$.

Úloha 2.5.4. Dokážte, že pre $A \neq \emptyset$ platí $A \times B \subseteq A \times C \Leftrightarrow B \subseteq C$. Platí toto tvrdenie bez predpokladu $A \neq \emptyset$? {kartezcvic:ULOKARTSUB}

Úloha 2.5.5. Dokážte, alebo nájdite kontrapríklad:
a) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$;
b) $(A \times B) \cup (C \times D) \supseteq (A \cup C) \times (B \cup D)$;
c) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$;
d) $(A \times B) \cap (C \times D) \subseteq (A \cap C) \times (B \cap D)$;
e) $(A \times B) \cap (C \times D) \supseteq (A \cap C) \times (B \cap D)$;
f) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Úloha 2.5.6. Dokážte, že pre ľubovoľné množiny A, B, C platí $A \times (B \triangle C) = (A \times B) \triangle (A \times C)$.

Úloha 2.5.7. Ukážte, že ak $A \times C \subseteq B \times D$ a $A \times C \neq \emptyset$, tak $A \subseteq B$ a $C \subseteq D$. Ukážte na príklade, že bez predpokladu $A \times C \neq \emptyset$ už toto tvrdenie neplatí.

2.5.1 Triedy* {triedy:SSECTTRIEDY}

Niekedy je v teórii množín vhodné používať okrem pojmu množina aj pojem triedy. Pod triedou rozumieme súhrn všetkých množín spĺňajúcich nejakú danú formulu teórie množín $\varphi(x)$. Pokiaľ by sme sa obmedzili iba na x z nejakej vopred danej množiny A, na základe schémy axióm vymedzenia dostaneme takto opäť množinu. Pokiaľ však chceme hovoriť o všetkých množinách spĺňajúcich $\varphi(x)$, už nemáme zaručené, že to bude množina. Napriek tomu sa niekedy hodí používať množinové zápisy aj pre triedy, treba mať však vždy na pamäti, že nepracujeme s množinami (hoci používame podobné zápisy).

Triedu budeme teda chápať jednoducho ako alternatívny zápis nejakej formuly teórii množín, resp. označenie pre systém množín, ktoré tejto formule vyhovujú (pričom máme na pamäti, že tento systém nemusí byť množinou). S triedami sa dajú robiť niektoré operácie, ako napríklad prienik alebo zjednotenie dvojice tried, dajú sa zaviesť triedové relácie a funkcie. Napríklad inklúziu možno chápať ako reláciu na triede **Set** všetkých množín. (O reláciach a funkciách budeme hovoriť v nasledujúcej kapitole, niečo o nich však už viete z nižších ročníkov.) Podrobnejšie si o triedach môžete prečítať napríklad v [BŠ, §I.3].

V prípade, že trieda nie je množinou, hovoríme o *vlastnej triede.*

Postup, ktorý sme použili pri Russellovom paradoxe v ZFC môžeme použiť na zdôvodnenie toho, že neexistuje množina všetkých množín, čo vlastne znamená, že systém všetkých množín tvorí vlastnú triedu.

iedy:VTSETISPROPERCLASS}

Veta 2.5.7. *Trieda všetkých množín*

$$\mathbf{Set} = \{x; x = x\}$$

je vlastnou triedou. (*Inak povedané, neexistuje množina všetkých množín.*)

Dôkaz. Označme $\mathbf{Set} = \{x; x = x\}$ triedu všetkých množín. (Keďže sem patria všetky množín spĺňajúce formulu $x \in x$, ide skutočne o triedu.)

Nech by **Set** bola množina. Potom (podľa schémy axióm vymedzenia) aj

$$A = \{x \in \mathbf{Set}; x \notin x\}$$

by bola množina.

Pre množinu A by potom nastala jedna z možností $A \in A$ alebo $A \notin A$.

Ak platí $A \in A$ tak (podľa definície množiny A) musí platiť $A \notin A$, čo je spor.

Podobne z predpokladu $A \notin A$ dostávame, že $A \in A$, čo je tiež spor.

Predpoklad, že **Set** je množina vedie k sporu – takáto množina preto existovať nemôže (a je to teda skutočne vlastná trieda.) □

Kapitola 3

Relácie a funkcie

V tejto kapitole sa budeme zaoberať základnými vlastnosťami relácií a funkcií, podrobnejšie sa budeme zaoberať niektorými špeciálnymi typmi relácií, konkrétne čiastočnými usporiadaniami a dobrými usporiadaniami.

3.1 Relácie

Definícia 3.1.1. *Relácia* R medzi množinami A a B je ľubovoľná podmnožina množiny $A \times B$. Pokiaľ $A = B$, hovoríme o relácii na množine A.

Obvykle namiesto $(a, b) \in R$ používame zápis aRb.

Množinu $D(R) = \{a \in A; (\exists b \in B)aRb\}$ nazývame *definičný obor* relácie R a množinu $H(R) = \{b \in B; (\exists a \in A)aRb\}$ obor hodnôt relácie R.

Príklad 3.1.2. Ak A je ľubovoľná množina, tak

$$id_A = \{(a, a); a \in A\}$$

je relácia na množine A.

{rel:PRIKLKRUZNICA}

Príklad 3.1.3. Na množine $I = \langle -1, 1\rangle$ môžeme zadefinovať reláciu

$$R = \{(x, y) \in I \times I; x^2 + y^2 = 1\}.$$

Grafom tejto relácie je kružnica.

{rel:USPN}

Príklad 3.1.4. Na množine prirodzených čísel $\mathbb{N}$ máme definovanú reláciu

$$\{(a, b) \in \mathbb{N} \times \mathbb{N}; a \leq b\}.$$

To znamená, že a a b sú v relácii práve vtedy, keď a je menšie alebo rovné b. Je prirodzené označiť túto reláciu $\leq$ a fakt, že prvky a, b sú v relácii zapisovať $a \leq b$.

Predchádzajúci príklad presne ilustruje to, ako budeme používať relácie – relácia nám hovorí o vzťahoch medzi prvkami množiny, konkrétne ak máme danú reláciu na množine A, môžeme ju chápať tak, že popisuje, ktoré prvky množiny A sú v určitom vzťahu.

Samozrejme, zaujímavé budú pre nás hlavne relácie, ktoré majú niektoré užitočné vlastnosti.

{rel:DEFTRANZ}

Definícia 3.1.5. Nech A je množina a R je relácia na množine A. Hovoríme, že relácia R je:

(i) *reflexívna,* ak pre každé $a \in A$ platí aRa,
(ii) *ireflexívna* alebo tiež *antireflexívna,* ak pre žiadne $a \in A$ neplatí aRa,
(iii) *symetrická,* ak pre ľubovoľné $a, b \in A$ platí $aRb \Rightarrow bRa$,
(iv) *antisymetrická,* ak pre ľubovoľné $a, b \in A$ platí $aRb \wedge bRa \Rightarrow a = b$,
(v) *asymetrická,* ak pre ľubovoľné $a, b \in A$ platí $aRb \Rightarrow \neg(bRa)$,
(vi) *tranzitívna,* ak pre ľubovoľné $a, b, c \in A$ platí $aRb \wedge bRc \Rightarrow aRc$,
(vii) *trichotomická,* ak pre ľubovoľné $a, b \in A$ platí práve jedna z možností aRb, bRa, $a = b$.

Tá istá množina môže predstavovať reláciu na rôznych množinách, napríklad množinu $R = \{(x, y) \in I \times I; x^2 + y^2 = 1\}$ z príkladu 3.1.3 môžeme chápať ako reláciu na množine $I = \langle 0, 1\rangle$ aj na množine $\mathbb{R}$. V každej časti predošlej definície sa vyskytuje vlastnosť, ktorá má platiť pre všetky prvky z danej množiny. Z toho je jasné, že ak hovoríme o týchto vlastnostiach, musíme uviesť aj množinu, na ktorej danú reláciu uvažujeme.

S jedným špeciálnym typom relácie – s reláciami ekvivalencie – ste sa už pravdepodobne stretli a mali by ste vedieť o vzťahu medzi reláciami ekvivalencie a rozkladmi množín, pozri napríklad [KGGS, časť 1.4], [OŠ], [ŠS, podkapitola 4.3]. (Asi ste o nich hovorili na predmete Algebra v súvislosti s faktorovými grupami a pravdepodobne ste sa o nich učili aj na diskrétnej matematike.)

Definícia 3.1.6. Relácia R na množine A sa nazýva *relácia ekvivalencie* ak je reflexívna, symetrická a tranzitívna.

V tejto prednáške sa budeme často zaoberať čiastočnými usporiadaniami.

Definícia 3.1.7. Relácia R na množine A sa nazýva *čiastočné usporiadanie* na množine A, ak relácia R je reflexívna, tranzitívna a antisymetrická.

Hovoríme tiež, že dvojica (A, R) je *čiastočne usporiadaná množina* alebo že množina A je čiastočne usporiadaná reláciou R.

Ak sú navyše ľubovoľné dva rôzne prvky množiny A *porovnateľné* reláciou R, t.j. platí

$$(\forall a, b \in A) a \neq b \Rightarrow aRb \vee bRa,$$

nazývame ju *lineárnym usporiadaním.*

V niektorých textoch sa namiesto názvu lineárne usporiadanie používa termín úplné usporiadanie.

Príkladom čiastočného usporiadania je relácia $\leq$ na množine $\mathbb{N}$ (príklad 3.1.4). Táto relácia je dokonca lineárnym usporiadaním.

Čiastočnými usporiadaniami sa budeme podrobne zaoberať v časti 3.3. Teraz sa ešte pozrieme na to, ako môžeme relácie skladať.

Definícia 3.1.8. Nech R je relácia medzi množinami A, B a S je relácia medzi množinami B, C. Potom reláciu

$$S \circ R = \{(a, c) \in A \times C; (\exists b \in B) aRb \wedge bSc\}$$

nazývame *zložením relácií A a B.*

Reláciu

$$R^{-1} = \{(b, a) \in B \times A; (a, b) \in R\}$$

medzi množinami B a A nazývame *inverznou reláciou* k relácii R.

{rel:TVRINVINV}

Tvrdenie 3.1.9. *Ak R je ľubovoľná relácia medzi množinami A, B, tak platí*

$$(R^{-1})^{-1} = R.$$

Jednoduchý dôkaz ponechávame ako cvičenie.

{rel:DEFID}

Definícia 3.1.10. Nech A je množina. Potom reláciu

$$id_A = \{(a,a); a \in A\}$$

na množine A nazývame *identita* na množine A.

Tvrdenie 3.1.11. *Nech A, B sú množiny R je relácia medzi množinami A, B a S je relácia medzi množinami B, A. Potom platí*

$$R \circ id_A = R$$
$$id_A \circ S = S.$$

Dôkaz. Označme $T := R \circ id_A$.

Ak $(a,b) \in T$, tak existuje $x \in A$ také, že $(a,x) \in id_A$ a $(x,b) \in R$. Lenže podmienka $(a,x) \in id_A$ znamená, že $a = x$. Preto $(a,b) \in R$. Tým sme ukázali, že $T \subseteq R$

Obrátene, ak $(a,b) \in R$, tak pre $x = a$ máme $(a,x) \in id_A$ a $(x,b) \in R$, čo podľa definície skladania relácií znamená $R \subseteq T$.

Celkovo teda dostávame $T = R \circ id_A = R$. Dôkaz druhej časti tvrdenia je podobný. □

{rel:TVRINVZLOZ}

Tvrdenie 3.1.12. *Nech R je relácia medzi množinami A a B, S je relácia medzi množinami B a C. Potom platí:*

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}.$$

Dôkaz. Označme ľavú a pravú stranu rovnosti $L = (S \circ R)^{-1}$ a $P = R^{-1} \circ S^{-1}$.

Nech $c \in C$, $a \in A$. Dvojica (c,a) patrí do L práve vtedy, keď $(a,c) \in S \circ R$. To je ekvivalentné s tým, že existuje $b \in B$ také, že $(a,b) \in R$ a $(b,c) \in S$. Na základe definície inverzného zobrazenia môžeme túto podmienku ekvivalentne zapísať tak, že existuje $b \in B$ s vlastnosťami $(c,b) \in S^{-1}$ $(b,a) \in R^{-1}$. To je ale ekvivalentné s podmienkou $(c,a) \in R^{-1} \circ S^{-1} = P$.

Tým je dokázaná rovnosť $L = P$. □

{rel:TVRTRANZSKLAD}

Tvrdenie 3.1.13. *Nech R je relácia na množine A. Potom platí:*

(i) *relácia R je reflexívna práve vtedy, keď $id_A \subseteq R$;*
(ii) *relácia R je symetrická práve vtedy, keď $R^{-1} = R$;*
(iii) *relácia R je antisymetrická práve vtedy, keď $R \cap R^{-1} = id_A$;*
(iv) *relácia R je tranzitívna práve vtedy, keď $R \circ R \subseteq R$;* {rel:itTRANZSKLAD}
(v) *ľubovoľné dva rôzne prvky A sú porovnateľné v relácii R práve vtedy, keď $R \cup R^{-1} \supseteq A \times A \setminus id_A$.*

Dôkaz. Dokážeme iba časť (iv) ostatné ponecháme ako cvičenie, keďže sú pomerne jednoduché.

(iv) $\boxed{\Rightarrow}$ Nech R je tranzitívna relácia. Ak $(x,z) \in R \circ R$, tak existuje $y \in R$ také, že xRy a yRz. Z tranzitívnosti ale potom vyplýva, že $(x,z) \in R$. Ukázali sme, že $R \circ R \subseteq R$.

$\boxed{\Leftarrow}$ Nech platí $R \circ R \subseteq R$. Nech ďalej xRy a yRz. Podľa definície skladania relácií máme potom $(x,z) \in R \circ R \subseteq R$, teda aj xRz a R je tranzitívna. □

Pomocou tohoto tvrdenia môžeme pomerne ľahko ukázať, že ak R je čiastočné (lineárne) usporiadanie na množine A, tak to isté platí aj o relácii R^{-1}. Môžete si vyskúšať dokázať toto tvrdenie priamo z definície.

Tvrdenie 3.1.14. *Ak R je čiastočné usporiadanie na množine A, tak aj R^{-1} je čiastočné usporiadanie na A.*

Ak navyše R je lineárne, tak to isté platí aj o usporiadaní R^{-1}.

Dôkaz. Predpokladáme, že R je reflexívna, antisymetrická a a tranzitívna relácia.

Z reflexívnosti máme $id_A \subseteq R$, z čoho vyplýva $id_A = id_A^{-1} \subseteq R^{-1}$ (pozri úlohu 3.1.11). Táto inklúzia znamená, že R^{-1} je reflexívna.

Antisymetria implikuje, že $R \cap R^{-1} = id_A$, čo je súčasne antisymetria pre reláciu R^{-1}, keďže $(R^{-1})^{-1} = R$.

Tranzitívnosť znamená, že $R \circ R \subseteq R$, a teda $R^{-1} \circ R^{-1} = (R \circ R)^{-1} \subseteq R^{-1}$. (Využili sme tvrdenie 3.1.12 a úlohu 3.1.11.)

Ak navyše predpokladáme, že ľubovoľné dva rôzne prvky množiny A sú v tejto relácii porovnateľné, znamená to, že $R \cup R^{-1} \supseteq A \times A \setminus id_A$. Ak je táto podmienka splnená pre R, tak je splnená aj pre R^{-1}. □

Tranzitívny uzáver V niektorých aplikáciách býva užitočný pojem tranzitívneho uzáveru, čo je vlastne relácia vytvorená z danej relácie R tak, aby sa od R priveľmi nelíšila a súčasne bola tranzitívna. Nasledujúca definícia spresňuje, čo rozumieme pod pojmom „priveľmi nelíšila“. Neskôr, keď sa budeme zaoberať pojmom najmenšieho prvku v čiastočne usporiadanej množine, by malo byť jasnejšie, prečo sme použili práve takúto definíciu.

Definícia 3.1.15. Nech $P(x)$ je ľubovoľná formula teórie množín s voľnou premennou x. Potom hovoríme, že A je *najmenšia množina* s vlastnosťou $P(x)$ *vzhľadom na inklúziu,* ak pre každú množinu B s vlastnosťou $P(x)$ platí $A \subseteq B$.

$$(\forall B)(P(B) \Rightarrow A \subseteq B)$$

Matematickou indukciou[1] zavedieme nasledujúce označenie pre ľubovoľnú reláciu R na množine A:
$R^0 = id_A$;
$R^1 = R$;
$R^{n+1} = R^n \circ R$ pre ľubovoľné prirodzené číslo $n \in \mathbb{N}$.

Tvrdenie 3.1.16. *Nech R je relácia na množine A. Označme $T := \bigcup_{n=1}^{\infty} R^n$. Potom relácia T je najmenšia (vzhľadom na inklúziu) relácia, ktorá je tranzitívna a obsahuje reláciu R ako svoju podmnožinu. Túto reláciu nazývame* tranzitívny uzáver *relácie R.*

Dôkaz. TODO □

V skutočnosti existenciu tranzitívneho uzáveru by sme mohli ukázať aj trochu iným (snáď jednoduchším) spôsobom, použitím faktu, že prienik tranzitívnych relácií je opäť tranzitívna relácia – úloha 3.1.16. Dôkaz, ktorý sme tu uviedli, má však tú výhodu, že od istej miery aj popisuje, ako tranzitívny uzáver danej relácie vyzerá.

Cvičenia

Úloha 3.1.1. Dokážte tvrdenie 3.1.9 a tvrdenie 3.1.13.

Úloha 3.1.2. Nech R je relácia medzi množinami A a B a nech $D(R) = A$. Zistite, či platia nasledujúce tvrdenia. Svoje tvrdenie vždy zdôvodnite (dokážte alebo nájdite kontrapríklad):
a) $R^{-1} \circ R = id_A$;
b) $R^{-1} \circ R \subseteq id_A$;
c) $R^{-1} \circ R \supseteq id_A$.

Úloha 3.1.3. Nech R, S sú relácie na množine A. Pre ktoré z vlastností uvedených v definícii 3.1.5 platí:
a) Ak má danú vlastnosť relácia R, tak ju má aj R^{-1}.
b) Ak majú danú vlastnosť relácie R a S, tak ju má aj $S \circ R$.

[1] Matematickou indukciou sa budeme podrobnejšie zaoberať neskôr, budeme ju však bežne používať už teraz – poznáte ju z nižších ročníkov – hoci jej správnosť sme ešte nezdôvodnili. (Zatiaľ sme dokonca v teórii množín nedefinovali ani množinu prirodzených čísel, pozri poznámku 1.4.1.)

Úloha 3.1.4. Nech R, S sú relácie ekvivalencie na množine A. Dokážte alebo nájdite kontrapríklad:
a) relácia R^{-1} je relácia ekvivalencie na A;
b) relácia $R \circ S$ je relácia ekvivalencie na A;
c) relácia $R \cap S$ je relácia ekvivalencie na A.

Úloha 3.1.5. Nech R, S sú čiastočné usporiadania na množine A. Dokážte alebo nájdite kontrapríklad:
a) relácia R^{-1} je čiastočné usporiadanie na A;
b) relácia $R \circ S$ je čiastočné usporiadanie na A;
c) relácia $R \cap S$ je čiastočné usporiadanie na A.

Úloha 3.1.6. Ukážte, že skladanie relácií je asociatívne, t.j. pre relácie R medzi A a B, S medzi B a C, a T medzi C a D platí $T \circ (S \circ R) = (T \circ S) \circ R$.

Úloha 3.1.7. Graficky znázornite dané relácie R, S na množine A; pokúste sa popísať a znázorniť aj relácie R^{-1}, S^{-1}, $S \circ R$, $R \circ S$, $R \circ R$, $S \circ S$. Ktoré z vlastností uvedených v definícii 3.1.5 majú tieto relácie?
a) $A = \langle -1, 1 \rangle$, $R = \{(x, y) \in A \times A; x^2 + y^2 = 1\}$, $S = \{(x, y) \in A \times A; x^2 + y^2 \leq 1\}$;
b) $A = \mathbb{R}$; $R = \{(x, y) \in A \times A; |x| \geq |y|\}$, $S = \{(x, y) \in A \times A; |y| \geq |x|\}$;
c) $A = \mathbb{R}$; $R = \{(x, y) \in A \times A; |x - y| < a\}$, $S = \{(x, y) \in A \times A; |x - y| < b\}$, kde a, b sú nejaké (pevne zvolené) reálne čísla;

Úloha 3.1.8. Nech A je konečná množina, ktorá má n prvkov. Koľko relácií, reflexívnych relácií, symetrických relácií existuje na množine A?

Úloha 3.1.9. Dokážte, že ak R je relácia na množine A, ktorá je reflexívna a tranzitívna, tak $R \circ R = R$. Platí aj obrátená implikácia?

Úloha 3.1.10. Nech R, S sú relácie medzi množinami A, B. Dokážte, že $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ a $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$.

{relcvic:ULOSKLADSUB}

Úloha 3.1.11. Dokážte nasledujúce tvrdenia. (V každom z nich implicitne predpokladáme, že ide o relácie medzi takými množinami, aby ich bolo možné skladať.)
a) Ak R, $S_{1,2}$ sú relácie a $S_1 \subseteq S_2$, tak $S_1 \circ R \subseteq S_2 \circ R$. Platí aj obrátená implikácia?
b) Ak $R_{1,2}$, S sú relácie $R_1 \subseteq R_2$, tak $S \circ R_1 \subseteq S \circ R_2$. Platí aj obrátená implikácia?
c) Nech $R_{1,2}$ sú relácie na množine A a $R_1 \subseteq R_2$. Potom $R_1^{-1} \subseteq R_2^{-1}$.
d) Nech R je relácia na množine A taká, že $D(R) = A$. Ak $R \subseteq R^{-1}$, tak $id_A \subseteq R \circ R$. Platí aj obrátená implikácia?

Úloha 3.1.12. Nech $A \neq \emptyset$. Je relácia $\emptyset$ na množine A reflexívna, symetrická, tranzitívna? Ktoré z týchto vlastností platia pre reláciu id_A?

Úloha 3.1.13. Pre reláciu R medzi množinami $\{1, 2, \ldots, m\}$ a $\{1, 2, \ldots, n\}$ definujme *maticu relácie* (označme ju A_R) tak, že $a_{ij} = 1$ ak iRj a v opačnom prípade $a_{ij} = 0$. Nech R je relácia medzi množinami $\{1, 2, \ldots, m\}$ a $\{1, 2, \ldots, n\}$ a S je relácia medzi množinami $\{1, 2, \ldots, n\}$ a $\{1, 2, \ldots, k\}$. Viete nájsť nejaký vzťah medzi maticou $A_{S \circ R}$ a súčinom matíc $A_R.A_S$? (Pozor na výmenu poradia!)

Úloha 3.1.14. Jednotlivé podmienky z definície 3.1.5 prepíšte pomocou kvantifikátorov a znegujte ich.

Úloha 3.1.15. Nájdite príklady čiastočných usporiadaní $\leq$ na množine $\mathbb{N}$ takých, že:
a) Každý prvok $\mathbb{N}$ je minimálnym prvkom $\leq$.
b) $(\mathbb{N}, \leq)$ má najväčší prvok a nemá najmenší prvok.
c) $(\mathbb{N}, \leq)$ nemá najmenší ani najväčší prvok.

{relcvic:ULOTR

Úloha 3.1.16. Nech A je množina.

Ukážte, že prienik ľubovoľného systému tranzitívnych relácií na množine A je opäť tranzitívna relácia na množine A.

Pomocou tohoto výsledku ukážte, že pre danú reláciu R na A je relácia $T := \bigcap\{S \subseteq A \times A; S \supseteq A, S$ je tranzitívna$\}$ najmenšou (vzhľadom na inklúziu) reláciou, ktorá obsahuje A a je tranzitívna. (Čiže T je tranzitívny uzáver relácie R.)

Úloha 3.1.17. Nech R je relácia na množine A. Dokážte, že:
a) Najmenšia (vzhľadom na inklúziu) reflexívna relácia obsahujúca R ako svoju podmnožinu je $R \cup id_A$. (Táto relácia sa zvykne nazývať *reflexívny uzáver* relácie R.)
b) Najmenšia (vzhľadom na inklúziu) symetrická relácia obsahujúca R ako svoju podmnožinu je $R \cup R^{-1}$. (Táto relácia sa zvykne nazývať *symetrický uzáver* relácie R.)

3.2 Funkcie

Veľmi dôležitú úlohu v niektorých úvahách v ďalších častiach tejto prednášky budú hrať funkcie (alebo tiež zobrazenia, obidva názvy budeme používať ako ekvivalentné).

Definícia 3.2.1. *Zobrazenie* (*funkcia*) z množiny A do B je relácia medzi množinami A a B taká, že pre každé $a \in A$ existuje práve jedno $b \in B$ s vlastnosťou $(a, b) \in f$.

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

Zobrazenie f z A do B budeme označovať $f\colon A \to B$. Množinu A nazývame *definičný obor* a B *obor hodnôt* zobrazenia f.

Poznámka 3.2.2. Namiesto zápisu $(a, b) \in f$ budeme používať zápis $f(a) = b$, tak ako ste boli zvyknutí aj doteraz. Definícia zobrazenia zaručuje, že tento zápis je zmysluplný, že ide o rovnosť nejakých dvoch objektov, keďže $f(a)$ predstavuje práve jeden prvok z množiny B (ten, ktorý je v relácii s prvkom a).

Niekedy budeme používať aj zápis $f\colon a \mapsto b$.

Príklad 3.2.3. Jednoduchým príkladom zobrazenia je zobrazenie $id_A\colon A \to A$ (pozri definíciu 3.1.10). Pre každé $a \in A$ platí $id_A(a) = a$. Toto zobrazenie zvykneme nazývať *identické zobrazenie*.

Definícia 3.2.4. Ak $f\colon A \to B$ je zobrazenie a $C \subseteq A$, tak zobrazenie $f|_C\colon C \to B$, definované predpisom

$$f|_C(x) = f(x)$$

pre všetky $x \in C$, nazývame *zúženie zobrazenia* f na množinu C.

Množinovo môžeme definíciu zúženia zobrazenia zapísať ako

$$f|_C = f \cap (C \times B).$$

Skladanie zobrazení je vlastne špeciálnym prípadom skladania relácií. Môžeme si všimnúť, že na základe definície zobrazenia môžeme vlastne zloženie zobrazení $f\colon A \to B$ a $g\colon B \to C$ ekvivalentne definovať ako

$$g \circ f(a) = g(f(a)) \text{ pre každé } a \in A.$$

Vyplýva to z toho, že ku každému a existuje práve jeden prvok, s ktorým je a v relácii f a je to prvok $f(a)$, to isté platí aj pre $f(a)$ a $g(f(a))$.

Keďže skladanie zobrazení sme definovali ako špeciálny prípad skladania relácií, zatiaľ vieme, že pre zobrazenia $f\colon A \to B$, $g\colon B \to C$ je $g \circ f$ relácia. Overme, že táto relácia je zobrazením.

Tvrdenie 3.2.5. *Nech $f\colon A \to B$, $g\colon B \to C$ sú zobrazenia. Potom aj $g \circ f$ je zobrazenie*

Dôkaz. Nech $a \in A$. Platí $(a,c) \in g \circ f$ práve vtedy, keď existuje $b \in B$ také, že $(a,b) \in f$ a $(b,c) \in g$. Pretože f je zobrazenie, ku každému $a \in A$ existuje práve jedno b s vlastnosťou $(a,b) \in f$. Ďalej, keďže g je zobrazenie, k tomuto a existuje jediné $c \in C$ také, že $(b,c) \in g$. Z toho celkovo dostávame, že (k danému $a \in A$) existuje práve jedno $c \in C$ také, že $(a,c) \in g \circ f$. Teda $g \circ f$ je skutočne zobrazenie. $\square$

Takisto inverznú reláciu k zobrazeniu f budeme nazývať *inverzným zobrazením,* ale len v prípade, že f^{-1} je tiež zobrazenie. Ak f^{-1} je zobrazenie, hovoríme tiež, že k f existuje inverzné zobrazenie.

Pripomeňme si najprv potrebné pojmy, ktoré poznáte už z nižších ročníkov:

Definícia 3.2.6. Nech $f\colon X \to Y$ je zobrazenie. Hovoríme, že f je *injektívne* (*prosté*) *zobrazenie* (alebo tiež injekcia), ak pre všetky $x, y \in X$ také, že $x \neq y$ platí $f(x) \neq f(y)$.

Hovoríme, že f je *surjekcia* (*surjektívne zobrazenie, zobrazenie na*), ak pre každé $y \in Y$ existuje také, $x \in X$, že $f(x) = y$.

Hovoríme, že f je *bijekcia* (*bijektívne zobrazenie*), ak f je súčasne injekcia aj surjekcia.

Definíciu injekcie môžeme ekvivalentne prepísať ako $f(x) = f(y) \Rightarrow x = y$. Teda zobrazenie je injektívne práve vtedy, keď sa na žiadny prvok oboru hodnôt nezobrazí viac ako jeden prvok definičného oboru. Zobrazenie je surjektívne, ak každý prvok oboru hodnôt má nejaký vzor – prvok, ktorý sa naň zobrazí.

Niektoré základné vlastnosti injekcií, surjekcií a bijekcií sú zhrnuté v cvičeniach za touto podkapitolou. (Mnohé z nich by ste mali ovládať z prvého ročníka, prinajmenšom celkom určite tie, ktoré sú uvedené v úlohe 3.2.1.)

Ukážeme si, že inverzné zobrazenie k f existuje práve vtedy, keď f je bijekcia.

Tvrdenie 3.2.7. *Nech $f\colon A \to B$ je zobrazenie. Potom f^{-1} je zobrazenie z B do A práve vtedy, keď f je bijekcia.* {fun:TVRINVBIJEK}

Dôkaz. $\boxed{\Rightarrow}$ Predpokladajme, že inverzná relácia k f je zobrazenie, t.j. $f^{-1} = \{(b,a) \in B \times A; b = f(a)\}$ spĺňa vlastnosť z definície zobrazenia. To znamená, že ku každému $b \in B$ existuje práve jedno $a \in A$ také, že $f(a) = b$.

Fakt, že ku každému $b \in B$ existuje $a \in A$ s vlastnosťou $f(a) = b$ je presne surjektívnosť zobrazenia f. Z toho, že také a existuje jediné dostávame injektívnosť. (Ak $f(a_1) = f(a_2) =: b$, tak $a_1 = a_2$ na základe jednoznačnosti.)

$\boxed{\Leftarrow}$ V podstate môžeme zopakovať úvahu z prvej časti dôkazu len v obrátenom poradí. Nech f je bijekcia. Zo surjektívnosti f máme, že ku každému $b \in B$ existuje $a \in A$ také, že $(b,a) \in f^{-1}$. Z injektívnosti f máme jednoznačnosť takéhoto a. Čiže obe podmienky z definície zobrazenia sú pre f^{-1} splnené. $\square$

Z predchádzajúceho dôkazu vidíme, že definíciu inverzného zobrazenie môžeme ekvivalentne preformulovať tak, že je to zobrazenie, pre ktoré platí

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

Teraz sa presvedčíme, že definícia inverzného zobrazenia, ktorú sme tu uviedli, je ekvivalentná s definíciou, ktorú poznáte z prvého ročníka.

Tvrdenie 3.2.8. *Nech $f\colon A \to B$, $g\colon B \to A$ sú zobrazenia. Nasledujúce podmienky sú ekvivalentné:*
(i) $g = f^{-1}$ *(t.j. g je inverzné zobrazenie k f);*
(ii) *platí $g \circ f = id_A$ a $f \circ g = id_B$.*

Dôkaz. (i)⇒ (ii): Ak $g = f^{-1}$ je zobrazenie, tak podľa tvrdenia 3.2.7 je f bijekciou. Chceme ukázať dve rovnosti množín, ukážeme ich postupne ako jednotlivé inklúzie.

Ak $(a, x) \in g \circ f$, tak existuje $b \in B$ tak, že $f(a) = b$ a $g(b) = x$. Predpoklad, že $g(b) = x$ znamená, že $f(x) = b$. Z injektívnosti f potom dostávame, že $x = a$. Ukázali sme teda $g \circ f \subseteq id_A$.

Súčasne pre každé $a \in A$ platí $(a, f(a)) \in f$ a $(f(a), a) \in g$, teda $(a, a) \in g\circ f$ a dostávame, že $id_A \subseteq g\circ f$. Zo súčasnej platnosti týchto dvoch inklúzií dostávame prvú rovnosť $g\circ f = id_A$.

Ak $(b, x) \in f \circ g$, tak existuje $a \in A$ také, že $a = g(b)$ a $x = f(a)$. Rovnosť $a = g(b)$ znamená (na základe definície inverzného zobrazenie), že $b = f(a)$, z čoho máme $x = b$. Dokázali sme $f \circ g \subseteq id_B$.

Nech teraz $b \in B$. Potom platí $(g(b), b) \in f$ (podľa definície inverznej relácie), a teda $(b, b) \in f \circ g$. Teda máme aj platnosť inklúzie $id_B \subseteq f \circ g$ a celkovo dostávame rovnosť $id_B = f \circ g$.

(ii)⇒ (i): Predpokladajme, že g je zobrazenie spĺňajúce rovnosti $g\circ f = id_A$ a $f\circ g = id_B$.

Nech $(a, b) \in f$, t.j. $b = f(a)$. Potom $g(b) = g(f(a)) = a$, teda $(b, a) \in g$. Ukázali sme, že $f^{-1} \subseteq g$.

Podobne ak $(b, a) \in g$, t.j. $a = g(b)$, tak $f(a) = f(g(b)) = b$, teda $(a, b) \in f$ a $(b, a) \in f^{-1}$. Tým je dokázané $g \subseteq f^{-1}$. □

Poznámka 3.2.9. V predchádzajúcich dôkazoch sme so zobrazeniami pracovali ako s reláciami, preto sme ešte pomerne často používali zápis $(x, y) \in f$.

V budúcnosti už budeme väčšinou s funkciami pracovať tak, ako ste zvyknutí, t.j. budeme používať zápis $f(x) = y$ alebo tiež rovnosť zobrazení $f = g$ budeme dokazovať tak, že pre každé x z definičného oboru ukážeme platnosť rovnosti $f(x) = g(x)$.

{fun:POZNAXSUBST}

Poznámka 3.2.10. Po zavedení pojmu funkcie vidno, že schéma axióm substitúcie vlastne hovorí to, že pre každú funkciu f definovanú na množine A existuje množina $f[A] = \{f(x); x \in A\}$. [2]

{fun:POZNACFUN}

Poznámka 3.2.11. Axiómu výberu môžeme preformulovať tak, že pre každý systém $\mathcal{S}$ disjunktných neprázdnych množín existuje funkcia $f\colon \mathcal{S} \to \bigcup\mathcal{S}$, ktorá každej množine $A \in \mathcal{S}$ priradí nejaký prvok tejto množiny.

Detailnejšie zdôvodnenie, že ide skutočne o ekvivalentnú formuláciu je v tvrdení 5.1.2.

Definícia 3.2.12. Nech $f\colon X \to Y$ je zobrazenie, $A \subseteq X$, $B \subseteq Y$.

Potom množinu
$$f[A] := \{f(a); a \in A\}$$
nazývame *obraz množiny A* v zobrazení f a množinu
$$f^{-1}[B] = \{a; f(a) \in B\}$$
nazývame *vzor množiny B* v zobrazení f.

V prípade, že $B = \{b\}$ je jednoprvková množina, niekedy namiesto zápisu $f^{-1}[\{b\}]$ použijeme zápis $f^{-1}(b)$. (Z kontextu by malo byť zrejmé, či hovoríme o inverznej funkcii k f, alebo zápis $f^{-1}(b)$ znamená vzor jednoprvkovej množiny.)

[2] Toto preformulovanie nie je úplne presné – pri definícii zobrazenia sme požadovali, aby bol určený obor hodnôt, nič také v schéme axióm substitúcie nie je. Keby sme však hovorili o triedových funkciách, už by sme takto dostali presne schému axióm substitúcie.

To znamená, že vzor a obraz množiny sú charakterizované týmito podmienkami:

$$x \in f[A] \Leftrightarrow (\exists a \in A) x = f(a)$$
$$x \in f^{-1}[B] \Leftrightarrow f(x) \in B$$

Uvedieme základné vlastnosti vzoru a obrazu množín, niektoré z nich dokážeme, väčšinu ale ponecháme ako cvičenie.

{fun:TVROBRAZVZOR}

Tvrdenie 3.2.13. *Nech $f\colon X \to Y$, $g\colon Y \to Z$ sú zobrazenia, $A, B \subseteq X$, $C, D \subseteq Y$, $E \subseteq Z$, $A_i \subseteq X$ a $B_i \subseteq Y$ pre každé $i \in I$. Potom platí*

(i) $g \circ f[A] = g[f[A]]$;
(ii) $(g \circ f)^{-1}[A] = g^{-1}[f^{-1}[A]]$;
(iii) $A \subseteq f^{-1}[f[A]]$ *a ak f je injektívne, tak* $A = f^{-1}[f[A]]$;
(iv) $f[f^{-1}[C]] \subseteq C$ *a ak f je surjektívne, tak* $f[f^{-1}[C]] = C$;
(v) $f[A \cap B] \subseteq f[A] \cap f[B]$ *a ak f je injektívne, tak* $f[A \cap B] = f[A] \cap f[B]$; {fun:itOBRCAP}
(vi) $f[\bigcap_{i\in I} A_i] \subseteq \bigcap_{i\in I} f[A_i]$ *a ak f je injektívne, tak* $f[\bigcap_{i\in I} A_i] = \bigcap_{i\in I} f[A_i]$; {fun:itOBRBIGCAP}
(vii) $f[A \cup B] = f[A] \cup f[B]$;
(viii) $f[\bigcup_{i\in I} A_i] = \bigcup_{i\in I} f[A_i]$; {fun:itOBRBIGCUP}
(ix) $f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$;
(x) $f^{-1}[\bigcap_{i\in I} A_i] = \bigcap_{i\in I} f^{-1}[A_i]$; {fun:itOBRCAPSYST}
(xi) $f^{-1}[C \cup D] = f^{-1}[C] \cup f^{-1}[D]$;
(xii) $f^{-1}[\bigcup_{i\in I} B_i] = \bigcup_{i\in I} f^{-1}[B_i]$;
(xiii) $A \subseteq B \Rightarrow f[A] \subseteq f[B]$ *a ak f je injekcia, tak platí aj opačná implikácia;*
(xiv) $C \subseteq D \Rightarrow f^{-1}[C] \subseteq f^{-1}[D]$ *a ak f je surjekcia, tak platí aj opačná implikácia;*
(xv) $f[A] \subseteq C \Leftrightarrow A \subseteq f^{-1}[C]$. {fun:itFAC}

Dôkaz. (v) Ak $x \in f[A \cap B]$, znamená to, že $x = f(c)$ pre nejaké $c \in A \cap B$. Potom ale $c \in A$ a súčasne aj $c \in B$. Z toho vyplýva, že $x = f(c)$ súčasne patrí do $f[A]$ aj $f[B]$, čiže patrí aj do prieniku $f[A] \cap f[B]$, čím je dokázaná inklúzia $f[A \cap B] \subseteq f[A] \cap f[B]$.

Predpokladajme navyše, že f je injekcia a pokúsme sa za tohoto predpokladu dokázať aj opačnú inklúziu. Ak $x \in f[A] \cap f[B]$, tak $x = f(a)$ pre nejaké $a \in A$ a súčasne $x = f(b)$ pre nejaké $b \in B$. Z rovnosti $x = f(a) = f(b)$ dostaneme, na základe injektívnosti f, že platí $a = b$. Teda prvok a patrí do $A \cap B$ a $x = f(a)$ je prvkom množiny $f[A \cap B]$. Tým sme dokázali inklúziu $f[A] \cap f[B] \subseteq f[A \cap B]$. Spolu s prvou časťou dôkazu máme už dokázané obe inklúzie medzi týmito množinami, a teda platí rovnosť.

(x) Nech $x \in f^{-1}[\bigcap_{i\in I} A_i]$, čiže $f(x) \in \bigcap_{i\in I} A_i$. To je ekvivalentné s podmienkou, že $(\forall i \in I) f(x) \in A_i$. Túto podmienku môžeme ďalej ekvivalentne prepísať ako $(\forall i \in I) x \in f^{-1}[A_i]$ a tiež $x \in \bigcap_{i\in I} f^{-1}[A_i]$. Teda podmienky $x \in f^{-1}[\bigcap_{i\in I} A_i]$ a $x \in \bigcap_{i\in I} f^{-1}[A_i]$ sú skutočne ekvivalentné.

(xv) $f[A] \subseteq C \Leftrightarrow (\forall a \in A) f(a) \in C \Leftrightarrow (\forall a \in A) a \in f^{-1}[C] \Leftrightarrow A \subseteq f^{-1}[C]$. □

Nasledujúce tvrdenie už možno poznáte z nižších ročníkov, pozri napríklad [Sl, cvičenia v časti 2.2] alebo [KGGS, Vety 1.3.3,1.3.4]. (Je treba dať pozor na to, že skladanie zobrazení je v [KGGS] definované opačne ako v tejto prednáške, a preto je aj toto tvrdenie sformulované inak.)

Tu ho uvádzame preto, aby sme zdôraznili použitie axiómy výberu v jednej časti dôkazu tohoto tvrdenia. (V časti 5.1.2 ukážeme, že táto časť tvrdenia je dokonca ekvivalentná s axiómou výberu v systéme ZF.)

{fun:TVRSURJINV}

Tvrdenie 3.2.14. *Nech $f\colon A \to B$ je zobrazenie. Potom platí:* {fun:itSURJ}

(i) *f je surjekcia práve vtedy, keď existuje zobrazenie $g\colon B \to A$ také, že $f \circ g = id_B$.*

{fun:itINJ}

(ii) *Nech navyše $A \neq \emptyset$. Potom f je injekcia práve vtedy, keď existuje zobrazenie $g\colon B \to A$ také, že $g \circ f = id_A$.*

Dôkaz. (i) $\boxed{\Rightarrow}$ (Toto je vlastne jediná náročnejšia časť dôkazu celého tvrdenia, je to práve tá časť, ktorá využíva axiómu výberu. Ostatné časti by ste mali byť schopní zvládnuť samostatne.)

Ak f je surjekcia, tak $\{f^{-1}(x); x \in B\}$ je systém neprázdnych disjunktných podmnožín A. Neprázdnosť každej množiny $f^{-1}(x)$ vyplýva zo surjektívnosti (každé $x \in B$ má aspoň jeden vzor). Disjunktnosť vyplýva z toho, že f je zobrazenie, čiže žiadne $a \in A$ nemôže patriť do $f^{-1}(x)$ aj do $f^{-1}(y)$, ak $x = y$. (Žiadne $a \in A$ sa nemôže zobraziť na dva rôzne prvky b.)

Potom podľa axiómy výberu (tak ako sme ju preformulovali v poznámke 3.2.11) existuje funkcia $g\colon B \to A$ taká, že $g(b) \in f^{-1}(b)$ pre každé $b \in B$. (Ak chceme byť úplne presní, tak axióma výberu hovorí o zobrazení z množiny $\{f^{-1}(x); x \in B\}$, s použitím bijekcie $x \mapsto f^{-1}(x)$ medzi B a touto množinou už vieme dostať skutočne zobrazenie z B do A.)

Podmienka $g(b) \in f^{-1}(b)$ vlastne znamená, že $f(g(b)) = b$. Platnosť tejto podmienky pre každé $b \in B$ znamená, že $f \circ g = id_B$.

(i) $\boxed{\Leftarrow}$ Chceme ukázať, že pre každé $b \in B$ existuje v zobrazení f vzor. Rovnosť $f(g(b)) = b$ implikuje, že $g(b)$ je vzorom pre b.

(ii) $\boxed{\Rightarrow}$ Keďže $A \neq \emptyset$, existuje nejaký prvok $a \in A$; zvoľme si jeden taký prvok a označme ho a_0. Zobrazenie g definujeme nasledovne:
$$g(b) = \begin{cases} a, & \text{ak existuje } a \text{ také, že } f(a) = b,\\ a_0, & \text{inak.}\end{cases}.$$
Z injektívnosti f vyplýva, že takýmto spôsobom skutočne dostaneme zobrazenie. Rovnosť $g(f(a)) = a$ (pre každé $a \in A$) je zrejmá z definície zobrazenia g.

(ii) $\boxed{\Leftarrow}$ Ak $f(x) = f(y)$, tak platí aj $g(f(x)) = g(f(y))$, čiže $x = y$. □

{fun:DOSINJSUR}

Dôsledok 3.2.15. *Ak $A \neq \emptyset$ a existuje injekcia $f\colon A \to B$, tak existuje surjekcia $f\colon B \to A$.*

Dôkaz. Ak f je injekcia, tak podľa druhej časti tvrdenia 3.2.14 existuje $g\colon B \to A$ také, že $g \circ f = id_A$. Potom ale z prvej časti toho istého tvrdenia dostávame, že g je surjekcia. □

3.2.1 Karteziánsky súčin systému množín

{fun:SSECTKARTEZ}

V časti 2.5 sme definovali karteziánsky súčin dvojice množín. V tejto časti by sme chceli zaviesť do istej miery analogický pojem pre ľubovoľný (nielen konečný) systém množín. Ešte predtým však zadefinujeme projekciu, čo je zobrazenie úzko súvisiace s karteziánskym súčinom množín.

Projekcie, ktoré budeme definovať, sú zobrazenia definované na karteziánskom súčine dvoch množín. Ak zobrazujeme usporiadané dvojice, často budeme namiesto $f((a, b))$ používať stručnejší zápis $f(a, b)$. (Z kontextu by malo byť vždy jasné, že máme na mysli usporiadané dvojice.)

Definícia 3.2.16. Ak A, B sú ľubovoľné množiny, tak zobrazenia $p_1\colon A \times B \to A$ a $p_2\colon A \times B \to B$, dané predpismi

$$p_1(a, b) = a$$
$$p_2(a, b) = b$$

pre $(a, b) \in A \times B$, budeme nazývať *projekcie* z karteziánskeho súčinu $A \times B$ na množiny A a B.

Niekedy budeme používať aj označenie p_A, p_B, t.j. vlastne nie je vyznačené, či ide o projekciu na prvú a druhú množinu, ale či ide o projekciu na množinu A alebo množinu B.

Môžeme si všimnúť, že usporiadaná dvojica je jednoznačne určená hodnotami zobrazení $p_{1,2}$. (To je vlastne len inak preformulované tvrdenie 2.5.2).

Teraz by sme chceli zadefinovať karteziánsky súčin systému množín $\{A_i, i \in I\}$, ktorý by mal podobné vlastnosti, t.j. ak pre každé $i \in I$ zvolíme nejaký prvok z A_i, mal by tým byť jednoznačne určený prvok súčin. Túto požiadavku spĺňa nasledujúca definícia.

Definícia 3.2.17. Nech I je množina a pre každé $i \in I$ je A_i množina. Potom *karteziánsky súčin* systému množín A_i, $i \in I$ definujeme ako množinu všetkých zobrazení z I do $\bigcup\limits_{i\in I} A_i$ takých, že obraz prvku i patrí do A_i. Označujeme ho $\prod\limits_{i\in I} A_i$.

$$\prod_{i\in I} A_i = \{f : I \to \bigcup_{i\in I} A_i; f(i) \in A_i\}$$

Pre každé $i \in I$ definujeme zobrazenie $p_i \colon \prod\limits_{i\in I} A_i \to A_i$

$$p_i(f) = f(i),$$

ktoré nazývame *i-ta projekcia.*

Vidíme, že ide skutočne o pojem analogický ku karteziánskemu súčinu dvoch množín. Zatiaľčo pri karteziánskom súčine dvoch množín bol každý jeho prvok jednoznačne určený dvomi súradnicami, tu máme súradnice indexované prvkami z I.

3.2.2 Karteziánsky súčin funkcií

Ďalší pojem, ktorý bude pre nás neskôr užitočný, je karteziánsky súčin funkcií. Podobne ako pri karteziánskom súčine množín, budeme ho definovať zvlášť pre súčin dvoch množín a zvlášť pre súčin systému množín.

Definícia 3.2.18. Nech $f \colon A \to C$, $g \colon B \to D$ sú zobrazenia. Potom ich *karteziánsky súčin* je zobrazenie $f \times g \colon A \times B \to C \times D$ určené predpisom

$$f \times g(a, b) = (f(a), g(b)).$$

Ak pre každé $i \in I$ je $f_i \colon A_i \to B_i$ zobrazenie, tak karteziánsky súčin týchto zobrazení je $g = \prod\limits_{i\in I} f_i \colon \prod\limits_{i\in I} A_i \to \prod\limits_{i\in I} B_i$, kde $g(f)$ pre $f \in \prod\limits_{i\in I} A_i$ je určená ako

$$g(f)(i) = f_i(f(i)).$$

Keď nad týmito definíciami trochu porozmýšľame, opäť by malo byť vidno, že ide o analogické pojmy. Zobrazenie $f \times g$ je vlastne zobrazenie, ktoré sa na prvej súradnici správa rovnako ako f a na druhej súradnici ako g. Zobrazenie $\prod\limits_{i\in I} f_i$ je skonštruované pomocou systému zobrazení indexovaného množinou I a je to zobrazenie, ktoré sa na i-tej súradnici správa rovnako ako f_i.

{fun:TVRSUCBIJ}

Tvrdenie 3.2.19. *Nech $f \colon A \to C$, $g \colon B \to D$ sú zobrazenia.*

(i) *Ak f aj g sú injekcie, tak $f \times g$ je injekcia.*
(ii) *Ak f aj g sú surjekcie, tak $f \times g$ je surjekcia.*
(iii) *Ak f aj g sú bijekcie, tak $f \times g$ je bijekcia.*

Dôkaz. (i) Nech f a g sú injekcie. Ak platí $f \times g(a,b) = f \times g(a',b')$, znamená to, že $(f(a),g(b)) = (f(a'),g(b'))$, čiže $f(a) = f(a')$, $g(b) = g(b')$. Z injektívnosti zobrazení f, g potom máme $a = a'$, $b = b'$ a $(a,a') = (b,b')$.

(ii) Nech f, g sú surjekcie a $(c,d) \in C \times D$. Potom existujú $a \in A$ a $b \in B$ tak, že $f(a) = c$, $g(b) = c$. Z toho máme, že $f \times g(a,b) = (c,d)$. Ukázali sme, že pre ľubovoľné (c,d) existuje vzor, a teda zobrazenie $f \times g$ je surjektívne.

(iii) Vyplýva z častí (i) a (ii). □

V dôkaze analogického tvrdenia pre súčin systému množín budeme potrebovať na jednom mieste využiť axiómu výberu; odvoláme sa na jej ekvivalentnú formuláciu, ktorú dokážeme neskôr v kapitole 5.

Tvrdenie 3.2.20. *Nech $f_i\colon A_i \to B_i$ je zobrazenie pre každé $i \in I$.*
(i) *Ak f_i je injekcia pre každé $i \in I$, tak $\prod\limits_{i\in I} f_i$ je injekcia.*
(ii) *Ak f_i je surjekcia pre každé $i \in I$, tak $\prod\limits_{i\in I} f_i$ je surjekcia.*
(iii) *Ak f_i je bijekcia pre každé $i \in I$, tak $\prod\limits_{i\in I} f_i$ je bijekcia.*

Dôkaz. Označme $g := \prod\limits_{i\in I} f_i$.

(i) Predpokladajme, že všetky f_i sú injekcie. Nech $f, f' \in \prod\limits_{i\in I} A_i$ a nech $g(f) = g(f')$. To znamená, že pre každé $i \in I$ platí $g(f)(i) = g(f')(i)$. Podľa definície zobrazenia g potom dostaneme pre každé $i \in I$ rovnosť $f_i(f(i)) = f_i(f'(i))$ a z injektívnosti zobrazenia f_i vyplýva $f(i) = f'(i)$. Teda zobrazenia f a f' sa rovnajú a g je skutočne injektívne.

(ii) Nech každé f_i je surjektívne a nech $f \in \prod\limits_{i\in I} B_i$. Potom pre každé $i \in I$ existuje $a_i \in A_i$ také, že $f_i(a_i) = f(i)$. Inak povedané, $\{a \in A_i; f_i(a) = f(i)\}$ je systém neprázdnych množín. Z ekvivalentnej formulácie axiómy výberu (tvrdenie 5.1.2(iii)) vyplýva existencia zobrazenia h definovaného na I takého, že $h(i) \in \{a \in A_i; f_i(a) = f(i)\}$, čiže $h(i) \in A_i$ a $f_i(h(i)) = f(i)$ pre každé $i \in I$. Posledná rovnosť hovorí presne to, že $g(h) = f$. Ukázali sme, že pre každé $f \in \prod\limits_{i\in I} B_i$ existuje vzor, čiže g je surjektívne zobrazenie.

(iii) Ľahko vyplýva z predchádzajúcich dvoch častí. □

{funcvic:ULOSKLAD}

Cvičenia

Úloha 3.2.1. Dokážte, že:
a) Zloženie dvoch injekcií je injekcia.
b) Zloženie dvoch surjekcií je surjekcia.
c) Zloženie dvoch bijekcií je bijekcia.

Úloha 3.2.2. Nech $f\colon X \to Y$, $g, h\colon Y \to Z$ sú zobrazenia. Dokážte, že:
a) Ak f je surjekcia, tak platí $g \circ f = h \circ f \Rightarrow g = h$.
b) Ak $Z \neq \emptyset$ a platí (pre ľubovoľné $g, h\colon Y \to Z$) implikácia $g \circ f = h \circ f \Rightarrow g = h$, tak f je surjekcia.

Úloha 3.2.3. Nech $g, h\colon X \to Y$, $f\colon Y \to Z$ sú zobrazenia. Dokážte, že:
a) Ak f je injekcia a platí $f \circ g = f \circ h$, tak $g = h$.

b) Ak $X \neq \emptyset$ a pre ľubovoľné $g, h\colon X \to Y$ platí implikácia $f \circ g = f \circ h \Rightarrow g = h$, tak f je injekcia.

{funcvic:ULOINVSURINJ}

Úloha 3.2.4. Ak $f\colon X \to Y$ a $g\colon Y \to X$ sú zobrazenia také, že $g \circ f = id_X$, tak g je surjekcia a f je injekcia. Ukážte na príklade, že g nemusí byť injekcia a f nemusí byť surjekcia.

Zdôvodnite pomocou tohoto výsledku a tvrdenia 3.2.14, že ak pre množiny X, Y existuje injekcia $f\colon X \to Y$ práve vtedy, keď existuje surjekcia $g\colon Y \to X$.

Úloha 3.2.5. Dokážte tvrdenie 3.2.13. Pre časti tvrdenia, ktoré obsahujú inklúziu a nie rovnosť, nájdite príklady ukazujúce, že nerovnosť môže byť ostrá (rovnosť nemusí vždy platiť).

{funcvic:NEGKVANTINJ}

Úloha 3.2.6. Predpokladajme, že $f\colon X \to Y$ je zobrazenie. Zapíšte pomocou kvantifikátorov výroky „f je injekcia“ a „f je surjekcia“ a znegujte tieto výroky.

3.3 Čiastočne usporiadané množiny

{cum:SECTCUM}

Pripomeňme najprv definíciu čiastočného usporiadania. Čiastočné usporiadanie množiny A je taká relácia $\leq$ na množine A, ktorá je reflexívna, antisymetrická a tranzitívna, t.j.:

$$(\forall a \in A) a \leq a \tag{R}$$
$$(\forall a, b \in A) a \leq b \wedge b \leq a \Rightarrow a = b \tag{A}$$
$$(\forall a, b, c \in A) a \leq b \wedge b \leq c \Rightarrow a \leq c \tag{T}$$

Keďže definícia čiastočného usporiadania je do istej miery motivovaná obvyklým usporiadaním reálnych a prirodzených čísel, budeme dosť často pre čiastočné usporiadanie používať symbol $\leq$. Niekedy budeme používať aj symbol $<$, ktorým budeme označovať to, že $a \leq b$ a prvky a a b sa nerovnajú.

$$a < b \qquad \Leftrightarrow \qquad (a \leq b) \wedge a \neq b$$

O lineárnom usporiadaní hovoríme, ak sú ľubovoľné 2 prvky množiny A porovnateľné, teda ak

$$(\forall a, b \in A) a \neq b \Rightarrow a \leq b \vee b \leq a.$$

V prípade, že budete študovať aj inú literatúru, je treba dať pozor na to, že niektorí autori definujú čiastočné usporiadanie inak. Súvis týchto dvoch definícií je podrobne vysvetlený na konci tejto podkapitoly.

Začnime tým, že uvedieme niekoľko príkladov čiastočných usporiadaní.

Príklad 3.3.1. Jednoduchými príkladmi čiastočne usporiadaných množín sú $(\mathbb{R}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{N}, \leq)$ s obvyklým usporiadaním. Vo všetkých spomenutých prípadoch ide o lineárne usporiadanie.

{cum:PRPOMDNCUM}

Príklad 3.3.2. Môžeme si všimnúť, že ak $(A, \leq)$ je čiastočne usporiadaná množina a $B \subseteq A$, tak $(B, \leq \cap (B \times B))$ je tiež čiastočne usporiadaná množina. Inak povedané, podmnožina čiastočne usporiadanej množiny s tým istým usporiadaním (zúženým na túto podmnožinu) tvorí opäť čiastočne usporiadanú množinu.

Ilustráciou sú napríklad podmnožiny $\mathbb{R}$ uvedené v predchádzajúcom príklade.

Vyplýva to z toho, že všetky požiadavky v definícii čiastočne usporiadanej množiny sú tvaru $(\forall a, b, c \in A) P(a, b, c)$, kde $P(a, b, c)$ predstavuje nejakú vlastnosť relácie. Je zrejmé, že ak nejaká vlastnosť platí pre ľubovoľné prvky danej množiny, tak platí aj pre prvky každej jej podmnožiny.

Príklad 3.3.3. Ak A je ľubovoľná množina, tak $(\mathcal{P}(A), \subseteq)$ je čiastočne usporiadaná množina. Všetky vlastnosti z definície čiastočne usporiadanej množiny sme overili v tvrdení 2.4.1.

Podľa príkladu 3.3.2 dostaneme čiastočne usporiadanú množinu aj pre ľubovoľnú podmnožinu množiny $\mathcal{P}(A)$.

Príklad 3.3.4. Ďalším príkladom je relácia „delí“ na množine prirodzených čísel definovaná tak, že

$$a \mid b \qquad \Leftrightarrow \qquad (\exists c \in \mathbb{N}) b = a.c.$$

Túto reláciu dôverne poznáte z predmetu Elementárna teória čísel [Č1] a nemalo by vám robiť problém, že ide skutočne o čiastočne usporiadanú množinu.

Môžeme si tiež všimnúť, že $(\mathbb{Z}, |)$ nie je čiastočne usporiadanou množinou, keďže nespĺňa požiadavku antisymetrie. Platí napríklad $1 \mid -1$ aj $-1 \mid 1$.

Hasseho diagram. V prípade čiastočného usporiadania na konečných množinách môžeme znázorniť reláciu usporiadania pomocou *Hasseho diagramu.*

Definícia 3.3.5. Nech $(A, \leq)$ je čiastočne usporiadaná množina. Prvok a nazývame *predchodcom* prvku b, ak $a \leq b$ a súčasne platí

$$a \leq c \leq b \qquad \Rightarrow \qquad c = a \vee c = b.$$

Prvok b sa nazýva *nasledovník* prvku a.

Predchádzajúca definícia vlastne hovorí, že a je predchodcom b, ak $a \leq b$ a medzi nimi už nie je žiadny iný prvok.

Reláciu čiastočného usporiadania môžeme znázorniť, ak znázorníme dvojice prvok a jeho predchodca. Takýmto spôsobom síce nedostaneme všetky dvojice, ktoré sú v relácii, no keď doplníme ďalšie dvojice, ktoré do nej musia patriť na základe tranzitívnosti a reflexívnosti, dostaneme už celú reláciu. (Inak povedané, pridáme všetky dvojice tvaru (a, a) a urobíme tranzitívny uzáver.)

Často sa zvykne kresliť Hasseho diagram tak, že vždy nakreslíme šípku z prvku do jeho nasledovníka. My budeme kresliť Hasseho diagramy bez šípok, ak budú dva prvky spojené hranou, tak nasledovník je ten z nich, ktorý je na obrázku nakreslený vyššie.

Na obrázku 3.1 sú nakreslené Hasseho diagramy pre čiastočne usporiadanú množinu $(\mathcal{P}(X), \subseteq)$ v prípade, že množina X je 2-,3- alebo 4-prvková. Môžeme si všimnúť, že tento diagram pre 2-prvkovú množinu má tvar štvorca a pre 3-prvkovú množinu tvar kocky. Je preto prirodzené považovať diagram pre n-prvkovú množinu za znázornenie vrcholov a hrán n-rozmernej (hyper)kocky. Napríklad na obrázku 3.2 je 5-rozmerná hyperkocka.

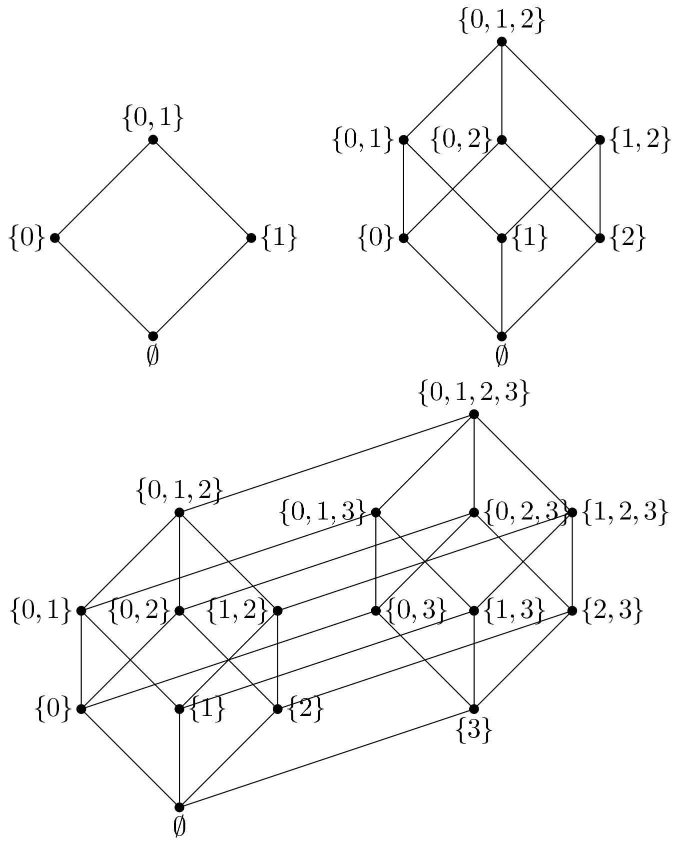
Môžeme si tiež všimnúť, že ak nakreslíme Hasseho diagram pre čiastočne usporiadanú množinu $(\{0, 1, 2, 3, 5, 6, 10, 15\}, |)$, tak dostaneme (pri vhodnom umiestnení vrcholov), presne ten istý obrázok ako pre $(\mathcal{P}(\{0, 1, 2\}), \subseteq)$. Vidíme, že tieto dve čiastočne usporiadané množiny sú v istom zmysle rovnaké. Toto pozorovanie nás vedie k definícii izomorfizmu čiastočne usporiadaných množín. Táto definícia je podobná s definíciou izomorfizmu pre iné typy štruktúr.

Definícia 3.3.6. Nech $(X, \leq)$ a $(Y, \preceq)$ sú čiastočne usporiadané množiny a $f\colon X \to Y$ je zobrazenie. Hovoríme, že zobrazenie f je *monotónne,* ak platí

$$(\forall x_1, x_2 \in X) x_1 \leq x_2 \Rightarrow f(x_1) \preceq f(x_2).$$

Niekedy používame aj zápis $f\colon (X, \leq) \to (Y, \preceq)$.

Ak je zobrazenie f navyše bijektívne a f^{-1} je tiež monotónne, tak f nazývame *izomorfizmus.* Ak existuje izomorfizmus medzi čiastočne usporiadanými množinami $(X, \leq)$ a $(Y, \preceq)$, tak hovoríme, že $(X, \leq)$ a $(Y, \preceq)$ sú *izomorfné,* označujeme $(X, \leq) \cong (Y, \preceq)$.



m:FIGHASSEPX} Obr. 3.1: Hasseho diagram $(\mathcal{P}(X), \subseteq)$ pre 2-,3- a 4-prvkovú množinu

Vidíme, že f je izomorfizmus, práve vtedy, keď je to bijekcia a platí

$$(\forall x_1, x_2 \in X) x_1 \leq x_2 \Leftrightarrow f(x_1) \preceq f(x_2).$$

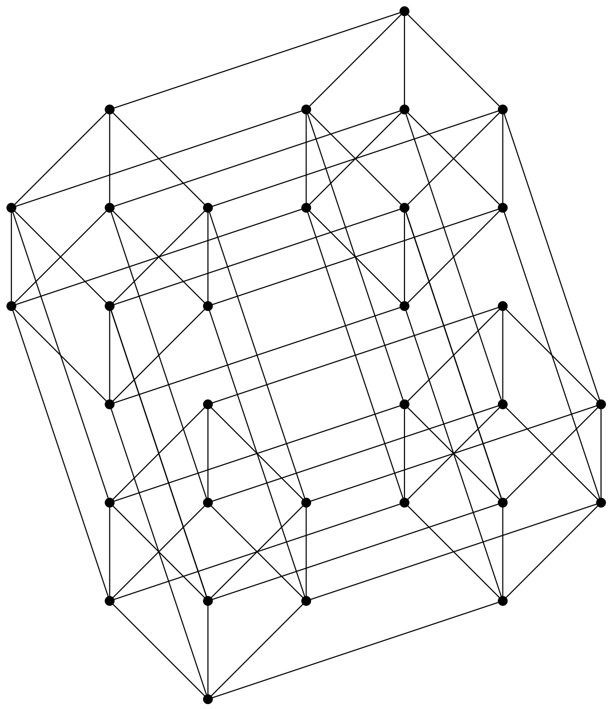
Podobne, ako to bolo v prípade grúp či vektorových priestorov, existencia izomorfizmu vlastne znamená, že ide o rovnaké čiastočne usporiadané množiny, ktoré sa líšia len pomenovaním prvkov.

Definícia 3.3.7. Nech $(A, \leq)$ je čiastočne usporiadaná množina a $a \in A$. Hovoríme, že a je
(i) *najmenší prvok* množiny A, ak pre každý prvok $b \in A$ platí $a \leq b$;
(ii) *najväčší prvok* množiny A, ak pre každý prvok $b \in A$ platí $b \leq a$;
(iii) *minimálny prvok* množiny A, ak pre každé $b \in A$ platí $b \leq a \Rightarrow b = a$;
(iv) *maximálny prvok* množiny A, ak pre každé $b \in A$ platí $a \leq b \Rightarrow a = b$.

Definíciu minimálneho prvku môžeme voľne preformulovať tak, že neexistuje prvok, ktorý by bol od neho menší. Podobne, prvok a je maximálny, ak neexistuje prvok, ktorý je od neho (ostro) väčší.

Ľahko sa dá vidieť, že najmenší prvok je súčasne aj minimálnym prvkom; najväčší prvok je súčasne aj maximálnym prvkom.

V prípade, že ide lineárne usporiadanie, tak minimálny prvok je najmenší prvok, maximálny prvok je najväčší prvok. Vo všeobecnosti to však neplatí. Dá sa nájsť veľa jednoduchých



{cum:FIGCUBE5} Obr. 3.2: 5-rozmerná hyperkocka – Hasseho diagram pre $\mathcal{P}(X)$, kde X je 5-prvková množina

príkladov (môžete si rozmyslieť, ako je to s čiastočne usporiadanými množinami znázornenými na obrázku 3.4); my si ukážeme jeden z nich. Ak uvažujeme ľubovoľnú množinu A, ktorá má aspoň dva prvky, tak relácia id_A je čiastočné usporiadanie na množine A. Pri tomto usporiadaní je každý prvok množiny A minimálny (a súčasne aj maximálny), ale množina A nemá najmenší ani najväčší prvok.

Predchádzajúci príklad súčasne ukazuje, že maximálnych (minimálnych) prvkov môže mať čiastočne usporiadaná množina viacero. Ak však čiastočne usporiadaná množina má najväčší (najmenší) prvok, tak tento prvok je jednoznačne určený.

Ostré čiastočné usporiadanie V definícii čiastočného usporiadania sme sa vlastne snažili nájsť spoločné vlastnosti relácií ako sú $\leq$, $\subseteq$. V niektorých textoch nájdete inú definíciu čiastočného usporiadania, ktorú spĺňajú napríklad relácie $<$, $\subsetneqq$. (Napríklad v [ŠS], pozri [ŠS, s.52,Poznámka 4.4.1].) My takúto reláciu budeme nazývať ostré čiastočné usporiadanie.

V nasledujúcom tvrdení ukážeme, aký je vzťah medzi týmito dvoma definíciami. V podstate zistíme to, že ku každému čiastočnému usporiadaniu existuje zodpovedajúce ostré čiastočné usporiadanie a obrátene.

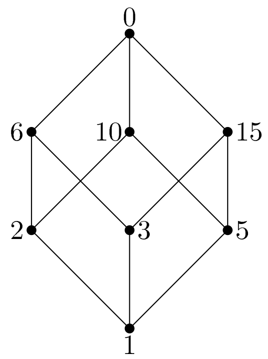
Definícia 3.3.8. Reláciu $<$ na množine A nazývame *ostré čiastočné usporiadanie,* ak je antireflexívna, asymetrická a tranzitívna; t.j. pre ľubovoľné $a, b, c \in A$ platí

$$a \not< a;$$
$$a < b \Rightarrow b \not< a;$$
$$a < b \wedge b < c \Rightarrow a < c.$$

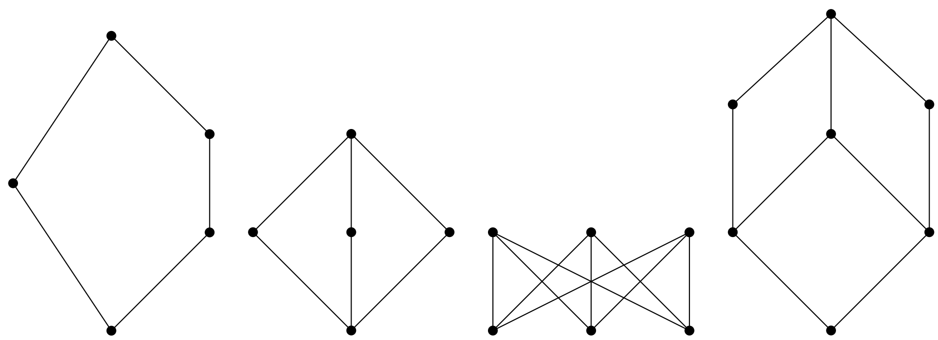
Ak sú navyše ľubovoľné dva rôzne prvky porovnateľné, tak hovoríme o *ostrom lineárnom usporiadaní.*

$$a \neq b \Rightarrow a < b \vee b < a$$

Najprv dokážeme dve pomerne jednoduché lemy.



{cum:FIGMID} Obr. 3.3: Hasseho diagram pre čiastočné usporiadanie $|$ na množine $\{0, 1, 2, 3, 5, 6, 10, 15\}$



FIGMOREHASSE} Obr. 3.4: Ďalšie príklady Hasseho diagramov

Lema 3.3.9. *Nech R je relácia na množine A a $S = R \cup id_A$. Potom:*
(i) *relácia S je reflexívna;*
(ii) *ak R je asymetrická, tak S je antisymetrická;*
(iii) *ak R je tranzitívna, tak aj S je tranzitívna.*

Dôkaz. (i) Priamo z definície relácie S vidíme, že $id_A \subseteq S$, čo je podľa tvrdenia 3.1.13 ekvivalentné s podmienkou, že S je reflexívna.

(ii) Nech aSb a bSa. Z definície S vidíme, že to môže nastať jedine v prípade, že $a = b$ alebo súčasne platí aRb aj bRa. Druhá možnosť však nenastane nikdy, lebo R je asymetrická. Tým sme dokázali, že $aSb \wedge bSa \Rightarrow a = b$, čo znamená, že S je antisymetrická.

(iii) Nech aSb a bSc. Rozoberme jednotlivé možnosti:
a) $a = b$ a $b = c$. Potom $a = c$, a teda aSc.
b) $a = b$ a bRc. Potom aRc, a teda aSc.
c) aRb a $b = c$. Potom aRc, a teda aSc.
d) aRb a bRc. Potom aRc, a teda aSc.
Ukázali sme, že v každom prípade, ktorý môže nastať, platí aSc, čiže relácia S je tranzitívna. □

Lema 3.3.10. *Nech R je relácia na množine A a $S = R \setminus id_A$. Potom:*
(i) *relácia S je antireflexívna;*
(ii) *ak R je antisymetrická, tak S je asymetrická;*
(iii) *ak R je tranzitívna a antireflexívna, tak aj S je tranzitívna.*

Dôkaz. (i) Zrejmé.

(ii) Sporom. Nech by platilo aSb aj bSa. To by znamenalo, že $a \neq b$ a súčasne platí aRb i bRa. Dostali sme spor s predpokladom, že R je antisymetrická.

(iii) Nech aSb, bSc. To znamená, že $a \neq b$, $b \neq c$, aRb a bRc. Z tranzitívnosti relácie R dostávame, že aRc. Pretože R je antireflexívna, $a \neq c$ a aSc. □

Na základe predchádzajúcich liem už dostávame platnosť korešpondencie medzi čiastočnými usporiadaniami a ostrými čiastočnými usporiadaniami, ktorú sme chceli dokázať.:

Dôsledok 3.3.11. *Nech R je relácia na množine A.*

Ak R je čiastočné usporiadanie, tak $R \setminus id_A$ je ostré čiastočné usporiadanie, pričom ak R je lineárne, tak aj $R \setminus id_A$ je lineárne.

Ak S je ostré čiastočné usporiadanie, tak $S \cup id_A$ je čiastočné usporiadanie, pričom ak S je lineárne tak aj $S \cup id_A$ je lineárne.

Navyše, priradenia $R \mapsto R \setminus id_A$ a $S \mapsto S \cup id_A$ sú navzájom inverzné priradenia medzi množinou všetkých čiastočných usporiadaní množiny A a množinou všetkých ostrých čiastočných usporiadaní množiny A (a teda tieto priradenia sú bijektívne).

{cum:POZNTRICHOT}

Poznámka 3.3.12. Z antireflexívnosti a asymetrie ostrého čiastočného usporiadania vidíme, že ak $<$ je ostré čiastočné usporiadanie na množine A, tak pre každé $a, b \in A$ platí **práve jedna** z množností

$$a = b \qquad a < b \qquad b < a.$$

Čiže ostré čiastočné usporiadanie je trichotomická relácia.

Cvičenia

{cumcvic:ULOJEDNNAJV}

Úloha 3.3.1. Ukážte, že ak $(A, \leq)$ je čiastočne usporiadaná množina, tak A má nanajvýš jeden najväčší prvok a nanajvýš jeden najmenší prvok.

Úloha 3.3.2. Ukážte, že pre zobrazenia medzi čiastočne usporiadanými množinami platí:
a) zloženie dvoch monotónnych zobrazení je monotónne zobrazenie;
b) zloženie dvoch izomorfizmov je izomorfizmus.

Úloha 3.3.3. Nech A je množina a $R_{1,2}$ sú čiastočné usporiadania na A. Dokážte, alebo vyvráťte:
a) Relácia $R_1 \cap R_2$ je čiastočné usporiadanie na A.
b) Relácia $R_1 \cup R_2$ je čiastočné usporiadanie na A.
c) Ak $R_1 \cup R_2$ je čiastočné usporiadanie na A, tak $R_1 \subseteq R_2$ alebo $R_2 \subseteq R_1$.

Úloha 3.3.4. Nájdite pre každý z Hasseho diagramov na obrázku 3.4 podmnožinu $A \subseteq \mathbb{N}$ takú, že čiastočne usporiadaná množina $(A, |)$ má daný Hasseho diagram.

Úloha 3.3.5. Nájdite pre každý z Hasseho diagramov na obrázku 3.4 množinu $A \subseteq \mathcal{P}(\mathbb{N})$ takú, že čiastočne usporiadaná množina $(A, \subseteq)$ má daný Hasseho diagram.

{cumcvic:ULOPRAZDCUM}

Úloha 3.3.6. Nech A je ľubovoľná množina. Sú relácie $A \times A$, id_A a $\emptyset$ čiastočnými usporiadaniami na množine A?

Úloha 3.3.7. Môže byť čiastočné usporiadanie na množine A zobrazením z A do A?

Úloha 3.3.8. Pre aké množiny A je $(\mathcal{P}(A), \subseteq)$ lineárne usporiadaná množina?

Úloha 3.3.9. Nech $f\colon A \to B$ je ľubovoľné zobrazenie a $(B, \leq)$ je čiastočne usporiadaná množina. Dokážte potom, že relácia $\preceq$ definovaná ako $a \preceq a' \Leftrightarrow f(a) \leq f(a')$ je čiastočným usporiadaním na množina A. Bude $\preceq$ lineárne usporiadanie, ak $\leq$ je lineárne usporidanie?

3.4 Dobre usporiadané množiny

Definícia 3.4.1. Nech $(A, \leq)$ je čiastočne usporiadaná množina. Hovoríme, že $(A, \leq)$ je *dobre usporiadaná množina*, resp. že $\leq$ je *dobré usporiadanie* na množine A, ak každá neprázdna podmnožina množiny A má minimálny prvok v usporiadaní $\leq$.

Ľahko vidno, že dobre usporiadaná množina musí byť lineárne usporiadaná, a teda minimálny prvok neprázdnej podmnožiny, o ktorom je reč v definícii, je súčasne jej najmenším prvkom. (Stačí si všimnúť, že ak minimálny prvok množiny $\{a, b\}$ je prvok a, tak platí $a \leq b$, ak je to prvok b, tak platí $b \leq a$.)

Tiež je ľahké ukázať, že podmnožina dobre usporiadanej množiny je tiež dobre usporiadaná (úloha 3.4.1).

Skôr než uvedieme aspoň jeden príklad dobre usporiadanej množiny, sformulujeme a dokážeme vetu naznačujúcu, prečo by mohli byť dobre usporiadané množiny užitočné.

Definícia 3.4.2. Ak $(A, \leq)$ je lineárne usporiadaná množina, tak symbolom A_a budeme označovať množinu všetkých prvkov menších než A.

$$A_a = \{x \in A; x < a\}$$

{dum:VTIND}

Veta 3.4.3 (Indukcia v dobre usporiadanej množine)**.** *Nech $(A, \leq)$ je dobre usporiadaná množina. Nech podmnožina $B \subseteq A$ má nasledujúcu vlastnosť:*

$$(\forall a \in A) A_a \subseteq B \Rightarrow a \in B.$$

Potom $B = A$.

Skôr než pristúpime k dôkazu, vysvetlime si, o čom vlastne hovorí táto veta. Nech B je množina prvkov z A určených nejakou vlastnosťou. Potom podmienka z vety vlastne hovorí: „Ak túto vlastnosť majú všetky prvky menšie ako a, tak ju má aj a.“ A veta 3.4.3 hovorí, že v taktomto prípade uvedenú vlastnosť majú všetky prvky z A.

Toto pozorovanie vysvetľuje pomenovanie vety – ide skutočne presne o postup, ktorý využívame pri dôkaze matematickou indukciou: Ukážeme, že ak vlastnosť platí pre všetky prvky menšie ako a, tak platí aj pre a.

Dôkaz. Sporom. Nech by B bola vlastná podmnožina A, čiže $A \setminus B \neq \emptyset$. Keďže $A \setminus B$ je neprázdna podmnožina dobre usporiadanej množiny A, existuje jej najmenší prvok a.

Platí $A_a \subseteq B$, inak by totiž do B patril niektorí prvok menší než a. Potom ale $a \in B$, čo je spor. $\square$

Už sme viackrát spomínali, že prirodzené čísla neskôr zavedieme v rámci ZFC. Predchádzajúce poznámky o súvise dobrého usporiadania a indukcie naznačujú, že ich zavedieme ako nejakú dobre usporiadanú množinu. Potom budeme mať vďaka vete 3.4.3 automaticky k dispozícii aj matematickú indukciu na množine prirodzených čísel.

Zatiaľ, kým ich nemáme vybudované v ZFC, teda prirodzené čísla využívame iba v príkladoch, ľahko však nahliadneme, že matematickou indukciou by sme boli schopní ukázať, množina prirodzených čísel a aj všetky jej podmnožiny (teda aj všetky konečné lineárne usporiadané množiny) sú dobre usporiadané.

Príklad 3.4.4. Každá konečná lineárne usporiadaná množina je dobre usporiadaná.

Množina prirodzených čísel $\mathbb{N}$ s obvyklým usporiadaním je dobre usporiadaná.

Zaujímavé sú hlavne príklady nekonečných dobre usporiadaných množín. Pre nekonečného množiny samozrejme nemôžeme nakresliť Hasseho diagram (musel by obsahovať nekonečne veľa vrcholov), často ho však môžeme aspoň naznačiť. Nasledujúce pozorovanie ukazuje, že je splnená základná podmienka pre kreslenie Hasseho diagramov – každý prvok má nasledovníka.

Lema 3.4.5. *Ak $(A, \leq)$ je dobre usporiadaná množina a prvok $a \in A$ nie je maximálny, tak existuje nasledovník prvku a.*

Dôkaz. Nasledovník prvku a je najmenší prvok množiny $\{b \in A; b > a\}$. Táto množina je neprázdna ak a nie je najväčší prvok množiny A. □

Ukážeme si aj niekoľko spôsobov, ako z už vytvorených dobre usporiadaných množín môžeme dostať nové.[3] Takto môžeme získať veľké množstvo ďalších príkladov.

Definícia 3.4.6. Nech $(A, \leq_A)$, $(B, \leq_B)$ sú čiastočne usporiadané množiny. Potom reláciu $\leq$ na množine $A \times B$ definovanú ako

$$(a, b) \leq (a', b') \quad \overset{\text{def}}{\Leftrightarrow} \quad (a <_A a') \vee [(a = a') \wedge (b \leq_B b')]$$

nazývame *lexikografické usporiadanie.* Tiež hovoríme, že $(A \times B, \leq)$ je *lexikografický súčin* čiastočne usporiadaných množín $(A, \leq_A)$ a $(B, \leq_B)$.

Antilexikografické usporiadanie na $A \times B$ definujeme ako

$$(a, b) \leq (a', b') \quad \overset{\text{def}}{\Leftrightarrow} \quad (b <_B b') \vee [(b = b') \wedge (a \leq_B a')].$$

Lexikografické usporiadanie je podobné abecednému usporiadaniu slov v slovníku alebo mien v telefónnom zozname. Pozrieme sa na prvé písmeno (prvú súradnicu) oboch slov. Ak sú prvé písmená rozličné, tak už podľa nich vieme rozhodnúť, ktoré zo slov patrí na prvé miesto. Ak nie porovnávame ďalšie súradnice.

Z uvedenej definície by malo byť zrejmé, že by sa veľmi ľahko dala podobným spôsobom rozšíriť na viac ako dve súradnice.

Antilexikografické usporiadanie je veľmi podobné, len ako najdôležitejšiu sme zobrali druhú (poslednú) pozíciu namiesto prvej. Tvrdenia, ktoré tu uvedieme, budeme dokazovať len pre lexikografické usporiadanie; dôkazy pre antilexikografické usporiadanie by boli takmer totožné (pozri aj poznámku 3.4.8).

V nasledujúcom tvrdení (kvôli jednoduchosti zápisu) používame ten istý symbol pre usporiadanie na A, B aj $A \times B$, z kontextu by malo byť jasné, ktorú z týchto troch relácií máme na mysli.

{dum:TVRLEXI}

Tvrdenie 3.4.7. *Nech $(A, \leq)$, $(B, \leq)$ sú čiastočne usporiadané množiny a $(A \times B, \leq)$ je ich (anti)lexikografický súčin. Potom*

(i) *$(A \times B, \leq)$ je čiastočne usporiadaná množina;*

(ii) *ak $(A, \leq)$ a $(B, \leq)$ sú lineárne usporiadané, tak aj $(A \times B, \leq)$ je lineárne usporiadaná množina;*

(iii) *ak $(A, \leq)$ a $(B, \leq)$ sú dobre usporiadané, tak aj $(A \times B, \leq)$ je dobre usporiadaná množina.*

[3] Síce tieto operácie budeme definovať pre ľubovoľné čiastočne usporiadané množiny, využívať ich budeme hlavne pre dobre usporiadané množiny.

Dôkaz. (i): *Reflexívnosť* je zrejmá z definície lexikografického usporiadania.

Antisymetria. Nech platí $(a,b) \le (a',b')$ aj $(a',b') \le (a,b)$.

Ak by platilo $a < a'$, tak $(a,b) < (a',b')$, čo znamená, že by neplatilo $(a',b') \le (a,b)$. Teda musí platiť $a \le a'$. Analogickou úvahou zistíme, že $a' \le a$, a teda $a = a'$.

Ak $a = a'$, tak z platnosti $(a,b) \le (a',b')$ a $(a',b') \le (a,b)$ dostaneme $b \le b'$ a $b' \le b$. To ale znamená, že $b = b'$.

Ukázali sme, že $a = a'$, $b = b'$, z čoho vyplýva $(a,b) = (a',b')$.

Tranzitívnosť. Nech $(a,b) \le (a',b')$ a súčasne $(a',b') \le (a'',b'')$. Ukážeme, že potom aj $(a,b) \le (a'',b'')$.

Uvažujme najprv prípad, že $a < a'$ alebo $a' < a''$. V ktoromkoľvek z týchto dvoch prípadov dostávame, že $a < a''$, a teda $(a,b) \le (a'',b'')$.

Ako druhá možnosť nám zostáva $a = a' = a''$. Potom ale platí $b \le b'$ a $b' \le b''$, z čoho vyplýva $b \le b''$ a $(a,b) \le (a'',b'')$.

(ii): Teraz budeme predpokladať, že $(A,\le)$ aj $(B,\le)$ sú lineárne usporiadané. Nech $(a,b),(a',b') \in A \times B$. Potom platí niektorá z možností $a \le a'$ alebo $a' \le a$. Bez ujmy na všeobecnosti, nech $a \le a'$ (dôkaz v druhom možnom prípade by bol presne symetrický).

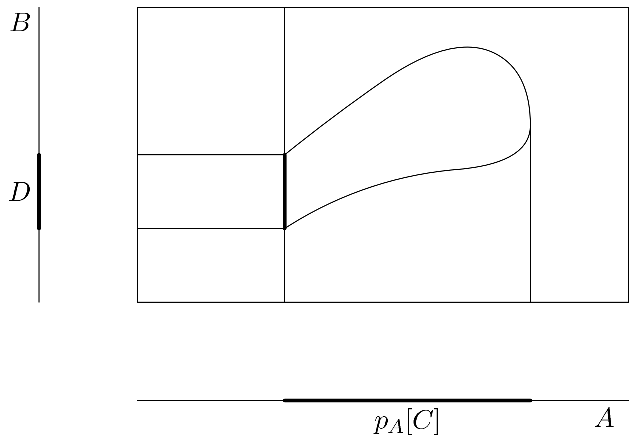
Ak $a < a'$, tak z definície lexikografického usporiadania máme $(a,b) \le (a',b')$.

Ak $a = a'$, tak pre prvky b a b' máme opäť dve možnosti. Buď $b \le b'$, vtedy platí $(a,b) \le (a',b')$; alebo $b' \le b$ a v tomto prípade $(a',b') \le (a,b)$.

Zistili sme, že dvojice (a,b), (a',b') sú vždy porovnateľné.

(iii): Teraz budeme navyše predpokladať, že $(A,\le)$ a $(B,\le)$ sú dobre usporiadané. Pripomeňme, že projekcia $p_A\colon A \times B \to A$ je zobrazenie $p_A(a,b) = a$.

Ak C je neprázdna podmnožina množiny $A \times B$, tak $p_A[C]$ je neprázdna podmnožina A. Keďže $(A,\le)$ je dobre usporiadaná, existuje najmenší prvok a_0 množiny $p_A[C]$.

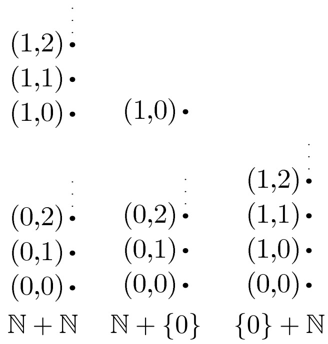


Obr. 3.5: Ilustrácia k dôkazu tvrdenia 3.4.7 {dum:FIGLEXI}

Označme $D := \{b \in B; (a_0,b) \in C\}$. Množina D je neprázdna, keďže $a_0 \in p_A[C]$, t.j. existuje aspoň jedna dvojica $(a,b) \in C$, kde prvá súradnica je $a = a_0$. Pretože $(B,\le)$ je dobre usporiadaná množina, existuje najmenší prvok množiny D, označme ho b_0.

Ukážeme, že (a_0,b_0) je najmenší prvok množiny C. Nech $(a,b) \in C$.

Z toho, že $a \in p_A[C]$, máme $a_0 \le a$. Ak $a = a_0$, znamená to, že $b \in D$, preto $b_0 \le b$ a $(a_0,b_0) \le (a,b)$. Ak $a < a_0$, tak tiež (na základe definície lexikografického usporiadania) platí $(a_0,b_0) \le (a,b)$. □



{dum:FIGSUCET} Obr. 3.6: Príklady na súčet dobre usporiadaných množín

{dum:POZNIZOM

Poznámka 3.4.8. Nech $\leq$ označuje lexikografické a $\leq'$ antilexikografické usporiadanie na množine $A \times B$. Ľahko sa možno presvedčiť, že $f(a,b) = (b,a)$ je izomorfizmus medzi $(A \times B, \leq)$ a $(A \times B, \leq')$. Keďže ide o izomorfné čiastočne usporiadané množiny, čokoľvek dokážeme o lexikografickom usporiadaní, platí aj pre antilexikografické usporiadanie. (Čiže v dôkaze tvrdenia 3.4.7 skutočne stačilo dokázať jednotlivé časti pre jedno z týchto dvoch usporiadaní.)

Názorne si môžeme lexikografický súčin predstaviť pomerne jednoducho – vlastne stačí v Hasseoveom diagrame pre množinu A každú bodku nahradiť množinou B.

{dum:PRSUCET}

Príklad 3.4.9. Nech $(B, \leq_B)$ a $(C, \leq_C)$ sú čiastočne usporiadané množiny. Na množine $M := \{0\} \times B \cup \{1\} \times C$ zadefinujeme čiastočné usporiadanie $\leq$ takýmto spôsobom:
$(0,b) \leq (1,c)$ pre ľubovoľné $b \in B$, $c \in C$;
pre $b, b' \in B$ platí $(0,b) \leq (0,b')$ práve vtedy, keď $b \leq_B b'$;
pre $c, c' \in C$ platí $(0,c) \leq (0,c')$ práve vtedy, keď $c \leq_C c'$.

Nie je ťažké overiť, že takto skutočne dostaneme čiastočné usporiadanie. Názorne si výsledné usporiadanie môžeme predstaviť tak, že sme všetky prvky množiny C dali nad prvky množiny B.

Ak obe množiny sú lineárne (dobre) usporiadané, platí to aj o výslednej množine – overenie tohoto faktu ponecháme ako cvičenie pre čitateľa. (Zovšeobecnenie tohoto faktu môžete nájsť v úlohe 3.4.3.)

Pre potreby tohoto príkladu budeme volať takúto množinu súčtom čiastočne usporiadaných množín a označovať $(B, \leq_B) + (C, \leq_C)$ alebo stručne $B + C$. Na obrázku 3.6 môžete vidieť, čo dostaneme, ak za B resp. C zvolíme $\mathbb{N}$ (s obvyklým usporiadaním) alebo jednoprvkovú množinu. Môžete si napríklad všimnúť, že dobre usporiadaná množina $\{0\} + \mathbb{N}$ je izomorfná s dobre usporiadanou množinou $\mathbb{N}$, zatiaľčo $\mathbb{N} + \{0\}$ nie je. Neskôr uvidíme, že takto definovaný súčet a antilexikografický súčin dobre usporiadaných množín sa dajú použiť na zavedenie súčtu a súčinu ordinálnych čísel.

{dum:POZNDISJZJED}

Poznámka 3.4.10. Namiesto $B \cup C$ sme v predchádzajúcom príklade použili $\{0\} \times B \cup \{1\} \times C$ kvôli tomu, aby sme zabezpečili, že dostaneme disjunktné množiny. (Ak by množiny $\{0\} \times B$ a $\{1\} \times C$ mali spoločný prvok, znamenalo by to, že $(0,b) = (1,c)$, a teda $0 = 1$.) Namiesto 0 a 1 sme mohli použiť ľubovoľné dva rôzne prvky, napríklad $\emptyset$ a $\{\emptyset\}$. Takýto trik sa často využíva, keď z nejakého dôvodu potrebujeme dostať dve množiny, ktoré sú podobné na dané množiny ale zabezpečiť, aby boli disjunktné. (V tomto konkrétnom prípade sme chceli dostať množiny, ktoré sa podobajú na B a C z hľadiska ich usporiadania, ale sú disjunktné.) V niektorých textoch nájdete podobným spôsobom definovanú operáciu *disjunktné zjednotenie množín.*

Ešte zavedieme jeden pojem, ktorý budeme potrebovať neskôr a na precvičenie práce s ním si ukážeme jedno jednoduché tvrdenie.

Definícia 3.4.11. *Počiatočný úsek* lineárne usporiadanej množiny $(X, \leq)$ je podmnožina $U \subseteq X$ s vlastnosťou $x \in U \wedge y \leq x \Rightarrow y \in U$.

Ak $(X, \leq)$ je dobre usporiadaná množina, tak počiatočné úseky v $(X, \leq)$ sú X a množiny tvaru $X_a = \{x \in X; x < a\}$ pre $a \in X$. Ak totiž U je počiatočný úsek v X a $U \neq X$, tak $X \smallsetminus U$ je neprázdna podmnožina X. Označme a najmenší prvok množiny $U \smallsetminus X$. Keďže a je najmenší prvok doplnku U, všetky menšie prvky už musia patriť do U, a teda $U \subseteq X_a$. {dum:TVRIZOMPOCUSEK}

Tvrdenie 3.4.12. *Nech $(X, \leq)$ je lineárne usporiadaná množina a nech $X' = \{X_a; a \in X\}$ je množina všetkých vlastných počiatočných úsekov množiny X. Potom zobrazenie $f\colon X \to X'$ určené predpisom*

$$f(a) = X_a$$

je izomorfizmus medzi čiastočne usporiadanými množinami $(X, \leq)$ a $(X', \subseteq)$.

Dôkaz. Surjektívnosť zobrazenia f je zrejmá z definície množiny X'. Overme injektívnosť tohoto zobrazenia.

Nech $a, b \in X$ a $a \neq b$. Keďže X je lineárne usporiadaná množina, tieto dva prvky sú porovnateľné. Bez ujmy na všeobecnosti, nech $a < b$. Potom $a \in X_b$ ale súčasne $a \notin X_a$, čo znamená, že $X_a \neq X_b$. Ukázali sme implikáciu $a \neq b \Rightarrow f(a) \neq f(b)$, čo znamená, že f je injektívne.

Ďalej chceme overiť, že f je monotónne. Ak platí $a \leq b$, tak $f(a) = \{x \in X; x < a\} \subseteq \{x \in X; x < b\} = f(b)$. (Stačí si uvedomiť, že na základe tranzitívnosti z $x < a$ a $a \leq b$ vyplýva $x < b$.) □

Cvičenia

{dumcvic:ULOSUB}

Úloha 3.4.1. Ukážte, že každá podmnožina dobre usporiadanej množiny (so zdedeným usporiadaním) je dobre usporiadaná.

Úloha 3.4.2. Nech $(X, \leq)$ je lineárne usporiadaná množina. Ukážte, že $a \in X$ je minimálny prvok množiny X práve vtedy, keď $X_a = \emptyset$.

{dumcvic:SUMSYST}

Úloha 3.4.3. V tejto úlohe zadefinujeme isté zovšeobecnenie lexikografického súčinu. Nech $(A, \leq_A)$ je čiastočne usporiadaná množina a pre každé $a \in A$ je $(B_a, \leq_a)$ čiastočne usporiadaná množina. Na množine $\bigcup_{a\in A} \{a\} \times B_a$ definujeme reláciu $\leq$ predpisom:

$$(a, b) \leq (a', b') \qquad \Leftrightarrow \qquad (a <_A a') \vee [(a = a') \wedge (b \leq_a b')].$$

Túto množinu budeme označovať v tejto úlohe $\sum\limits_{a\in A} B_a$.

a) Overte, že takto dostaneme čiastočne usporiadanú množinu a navyše, ak všetky použité množiny sú lineárne (dobre) usporiadané, aj $\sum\limits_{a\in A} B_a$ je lineárne (dobre) usporiadaná množina.

b) Ukážte, že ak $B_a = B$ pre každé A, tak dostaneme takýmto spôsobom lexikografický súčin množín A a B.

c) Ak $A = \{0, 1\}$ (s obvyklým usporiadaním, t.j. $0 < 1$), $B_0 = B$ a $B_1 = C$, tak dostaneme čiastočne usporiadanú množinu z príkladu 3.4.9.

d) Nech $A = \mathbb{N}$, $B_n = \{0, 1, \dots, n\}$ (v oboch prípadoch s obvyklým usporiadaním prirodzených čísel). Ako vyzerá $\sum\limits_{a\in A} B_a$? (Pod otázkou „ako vyzerá“ sa tu myslí: Vedeli by ste ju graficky znázorniť? Je izomorfná s nejakou čiastočne usporiadanou množinou, ktorá sa už v niektorých príkladoch vyskytla?)

Úloha 3.4.4. Zistite, ktoré z uvedených dobre usporiadaných množín sú izomorfné. Môžete sa pokúsiť ich aj nejako graficky znázorniť.
a) $(\mathbb{N}, \leq)$
b) $(\mathbb{N}, \leq) + (\mathbb{N}, \leq)$
c) $(\mathbb{N}, \leq) + (\{0\}, \leq)$
d) $(\{0\}, \leq) + (\mathbb{N}, \leq)$
e) $(\{0,1\}, \leq) \times (\mathbb{N}, \leq)$ (lexikografický súčin)
f) $(\mathbb{N}, \leq) \times (\{0,1\}, \leq)$ (lexikografický súčin)
g) $(\mathbb{N}, \leq) \times (\mathbb{N}, \leq)$ (lexikografický súčin)
h) $\sum_{n\in\mathbb{N}}(\{1,2,\ldots,n\}, \leq)$
i) $\sum_{n\in\mathbb{N}}(\mathbb{N}, \leq)$

Úloha 3.4.5*. Dokážte, že:
a) (2 body) Každá podmnožina $\mathbb{R}$, ktorá je dobre usporiadaná (pri obvyklom usporiadaní reálnych čísel) je spočítateľná.
b) (2 body) Každá dobre usporiadaná podmnožina $\mathbb{R}$ je izomorfná s podmnožinou $\mathbb{Q}$ (s obvyklým usporiadaním racionálnych čísel).
c) (2 body) Každá spočítateľná dobre usporiadaná množina je izomorfná s podmnožinou $(\mathbb{R}, \leq)$.
(Časti a), b) a c) nemusíte nutne riešiť v uvedenom poradí, zvoľte si také, aké vám vyhovuje najviac.)

Kapitola 4

Kardinálne čísla

V tejto kapitole zavedieme pojem kardinality, čo je azda najužitočnejší a najdôležitejší pojem teórie množín. Zjednodušene povedané, ide o rozšírenie pojmu počtu prvkov množiny na nekonečné množiny.

4.1 Porovnávanie mohutností množín

Ľahko vidíme, že dve konečné množiny majú rovnaký počet prvkov práve vtedy, keď medzi nimi existuje bijekcia (vieme nájsť jednojednoznačné priradenie medzi ich prvkami). Toto pozorovanie motivuje spôsob, ktorým by sme chceli zaviesť pojem analogický k počtu prvkov aj pre nekonečné množiny.

{def:DEFKARD}

Definícia 4.1.1. Hovoríme, že množiny X a Y majú rovnakú *kardinalitu* (*mohutnosť*), ak existuje bijekcia $f\colon X \to Y$. Označujeme $|X| = |Y|$.

{def:POZNTRANZEQ}

Poznámka 4.1.2. Je užitočné si všimnúť, že ak $|X| = |Y|$ a $|Y| = |Z|$, tak aj $|X| = |Z|$. (Vyplýva to z toho, že zložením dvoch bijekcií dostaneme opäť bijekciu.)

Ďalšie očividné vlastnosti sú, že $|X| = |X|$ platí pre každú množinu X (lebo $id_X\colon X \to X$ je bijekcia) a ak $|X| = |Y|$, tak $|Y| = |X|$.

Hoci uvedená definícia nie je zložitá, predsa len si zaslúži istý komentár.

{def:POZNDEFKARD}

Poznámka 4.1.3. Znak $=$ zvykneme písať medzi nejaké dva objekty v prípade, že sú totožné. V definícii 4.1.1 sme však symbol rovnosti použili v trochu inom význame. Jedna možnosť, ako sa na to pozerať, je skutočne všetky výskyty zápisov tvaru $|X| = |Y|$ chápať ako iný zápis pre to, že existuje bijekcia medzi X a Y. Pozorovanie z poznámky 4.1.2 do istej miery oprávňuje použitie symbolu $=$, lebo ukazuje, že vzťah „mať rovnakú mohutnosť“ má skutočne podobné vlastnosti ako rovnosť. (Je to triedová relácia ekvivalencie na triede všetkých množín.)

Oveľa lepšie by bolo, keby sme skutočne boli schopní definovať nejaké objekty, ktoré by zodpovedali symbolu $|X|$. Keďže pracujeme v systéme ZFC, kde „všetko je množina“, ideálne by bolo, keby to boli množiny. Pýtame sa teda vlastne, či je možné každej množine X priradiť množinu $|X|$ takým spôsobom, že ak medzi X a Y existuje bijekcia, tak obidvom množinám priradíme tú istú množinu $|X| = |Y|$.

Odpoveď na túto otázku je, že sa to skutočne dá. Túto množinu $|X|$ budeme nazývať *kardinálne číslo* množiny X. (Kardinálne čísla budeme často označovať malými gréckymi písmenami.) Bohužiaľ zatiaľ nemáme vybudovaný aparát na to, aby sme mohli podať štandardný spôsob, ako sa to v súčasnej teórii množín robí. Čiže zatiaľ vám nezostáva iná možnosť, iba tomu uveriť a používať pojem kardinálneho čísla s prísľubom, že neskôr uvidíte, že tento pojem sa dá v ZFC zmysluplne vybudovať.

Môžete sa na kardinálne čísla zatiaľ pozerať aj takým spôsobom, že kardinálne číslo X definujeme ako *spoločnú vlastnosť všetkých množín, pre ktoré existuje bijekcia s množinou X*. Toto je vlastne pôvodná Cantorova definícia a je pre mnohé účely úplne postačujúca a dostatočne intuitívna. Jediná nevýhoda, ktorú má pre nás, je tá, že takto definované kardinálne číslo nie je množina a my chceme pracovať v systéme ZFC, čiže iba s množinami.

Na tomto mieste by som však spomenul ešte niektoré, zdanlivo vcelku prirodzené, spôsoby definície kardinálnych čísel a vysvetlil na aké problémy narážajú a aké sú dôvody, že sme sa rozhodli vydať inou cestou. (Možno niektorým z čitateľov takéto možnosti prišli na um, hoci vyžadujú trochu praxe v teórii množín. Každopádne, pokiaľ ste existencii kardinálnych čísel ochotní uveriť a netrápi vás, či by sme ich mohli definovať nejako inak, môžete zvyšok tejto poznámky úplne pokojne preskočiť.) Na pochopenie niektorých častí v tejto poznámke je užitočné mať prečítanú časť 2.5.1 o triedach.

Vidíme, že sme vlastne rozdelili všetky množiny na akési „triedy ekvivalencie“. (Nemôžeme celkom hovoriť o relácii ekvivalencie, keďže vzťah „mať rovnakú kardinalitu“ definujeme na všetkých množinách a tie netvoria množinu.) Množine X zodpovedá trieda ekvivalencie

$$\{Y; \text{existuje bijekcia medzi } X \text{ a } Y\}.$$

Nemohli by sme jednoducho priradiť množine X uvedenú triedu ekvivalencie a tú označiť ako $|X|$? Mali by sme predsa každej množine priradený jeden objekt a dosiahli by sme presne to, čo chceme. Bohužiaľ, ako ukazuje tvrdenie 4.3.6, táto „trieda ekvivalencie“ nie je množinou. (Je to tak dokonca už pre jednoprvkové množiny – tvrdenie 4.3.5.) Čiže s takto definovanými kardinálnymi číslami by sa nám dosť zle manipulovalo, napríklad by sme z nich nemohli vytvárať množiny.

Situáciu by sme vedeli zachrániť, ak by sme ak by sme mali k dispozícii axiómu výberu pre triedy. (Intuitívne by malo byť jasné, čo by taká axióma hovorila, hoci v systéme ZFC ju nie je úplne ľahké sformulovať, keďže nepoužívame pojmy trieda a triedová funkcia.) Z každej triedy ekvivalencie by sme potom mohli vybrať jedného reprezentanta, aj keď tieto triedy nie sú množinami.

Axióma výberu pre triedy sa v matematike niekedy skutočne používa, pozri napríklad [Le, Section V.4], [M, p.334,Table 10]. Často sa nazýva aj *axióma globálneho výberu* a označuje AGC, systém ZF rozšírený o túto axiómu sa označuje ZFGC. Táto axióma je silnejšia než axióma výberu. Je však známe, že ZFGC je konzervatívne rozšírenie ZFC, t.j. akékoľvek tvrdenie o množinách dokázateľné v ZFGC je dokázateľné aj v ZFC, [Le, p.180,V.4.8]. (Axióma globálneho výberu však prináša nové tvrdenia o triedach.) My sme sa však rozhodli pracovať v systéme ZFC, ktorý takúto axiómu neobsahuje, teda tento prístup nemôžeme použiť.

V skutočnosti sa výber reprezentanta dá istým spôsobom urobiť aj v ZFC. Tento spôsob, nazývaný Scottov trik, je založený na výbere prvku z triedy ekvivalencie, ktorý má minimálny rank v kumulatívnej hierarchii množín [F, Section 8.6.1]. My sa však kumulatívnou hierarchiou množín v rámci tejto prednášky nezaoberáme, takže tento spôsob definície kardinálov nemôžeme detailnejšie popísať. Navyše, hoci je takáto definícia správna a v princípe použiteľná, drvivá väčšina textov z teórie množín využíva definíciu pomocou ordinálov, ktorú uvedieme aj my (alebo už spomenutý pôvodný Cantorov prístup).

Čiže ak ešte raz zhrnieme predchádzajúcu poznámku, kardinálne číslo budeme zatiaľ chápať „naivne“, ako spoločnú vlastnosť všetkých množín rovnakej kardinality (=všetkých množín medzi ktorými existuje bijekcia). A až neskôr si ukážeme, ako sa dá pojem kardinálneho čísla zaviesť tak, aby kardinálne číslo tiež bolo množinou. Napriek tomu, že sme dôkaz toho faktu odložili na neskôr, budeme s kardinálnymi číslami bežne zaobchádzať ako s množinami, budeme napríklad pracovať s množinami kardinálnych čísel alebo s funkciami definovanými na kardinálnom čísle.

Vlastne všetko, čo zatiaľ potrebujeme vedieť o kardinálnych číslach, je toto:

{def:KARDINALAMAKARDINAL

Poznámka 4.1.4. Neskôr ukážeme, že v ZFC je možné zadefinovať kardinálne čísla (inými slovami existuje formula jazyka ZFC, ktorú spĺňajú práve kardinálne čísla) tak, že platí:

(i) Pre každú množinu A existuje kardinálne číslo a také, že A a a majú rovnakú mohutnosť (t.j. existuje medzi nimi bijekcia). Označenie: $|A| = a$.
(ii) Platí $|a| = a$.
(iii) Ak $|A| = a$, $|B| = b$ a existuje bijekcia medzi množinami A a B, tak $a = b$.

Práve poslednú vlastnosť je základnou vlastnosťou kardinálnych čísel, budeme ju často používať na dôkaz rovnosti medzi kardinálnymi číslami.

Po tejto dlhej (a pri prvom čítaní asi aj ťažko zrozumiteľnej) poznámke týkajúcej sa definície kardinálnych čísel poďme s nimi skúsiť aj niečo robiť. Ako prvú vec sa kardinálne čísla naučíme porovnávať.

Definícia 4.1.5. Hovoríme, že *kardinalita* množiny X je *menšia alebo rovná* ako kardinalita množiny Y, označujeme $|X| \leq |Y|$, ak existuje injekcia z X do Y.

Ak platí $|X| \leq |Y|$ ale X a Y nemajú rovnakú kardinalitu, tak hovoríme, že X má *menšiu kardinalitu* ako množina Y, označujeme $|X| < |Y|$.

$$|X| < |Y| \Leftrightarrow |X| \leq |Y| \wedge |X| \neq |Y|$$

Poznámka 4.1.6. Už vieme (pozri tvrdenie 3.2.14 a úlohu 3.2.4), že pre $X \neq \emptyset$ je existencia injekcie z X do Y ekvivalentná s existenciou surjekcie z Y do X. (Pričom implikácia $\Leftarrow$ vyžaduje axiómu výberu – dokonca je s ňou ekvivalentná, ako ukážeme v tvrdení 5.1.2(vi).)

Ľahko sa overí, že nerovnosť medzi kardinálnymi číslami je dobre definovaná, t.j. ak $|X| = |X'|$ a $|Y| = |Y'|$, tak platí $|X| \leq |Y| \Leftrightarrow |X'| \leq |Y'|$.

Prirodzená otázka je, či aj pre nerovnosť kardinálnych čísel platí reflexívnosť, tranzitívnosť a antisymetria. Na prvé dve časti tejto otázky vieme odpovedať okamžite, tretia bude o čosi náročnejšia, odpoveď na ňu je však tiež pozitívna.

{def:TVRCUM}

Tvrdenie 4.1.7. *Nech X, Y, Z sú ľubovoľné množiny. Potom platí:*

(i) $|X| \leq |X|$;
(ii) $|X| \leq |Y| \wedge |Y| \leq |Z| \Rightarrow |X| \leq |Z|$
(iii) $|X| = |Y| \Rightarrow |X| \leq |Y|$

Dôkaz. (i) $id_X : X \to X$ je injekcia.

(ii) Zloženie dvoch injekcií je injekcia.

(iii) Každá bijekcia je injekcia. □

Teraz dokážeme veľmi dôležitú Cantor-Bernsteinovu vetu, ktorá ukazuje platnosť antisymetrie pre porovnávanie kardinalít.

{def:VTCANTBER}

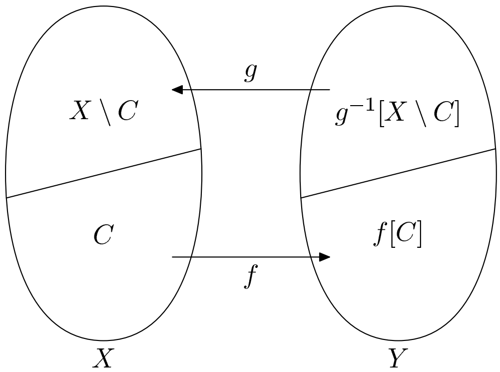
Veta 4.1.8 (Cantor-Bernstein)**.** *Nech X, Y sú množiny. Ak platí $|X| \leq |Y|$ a $|Y| \leq |X|$, tak $|X| = |Y|$.*

$$|X| \leq |Y| \wedge |Y| \leq |X| \Rightarrow |X| = |Y|$$

Inak: Ak existuje injekcia $f : X \to Y$ a injekcia $g : Y \to X$, tak existuje bijekcia $h : X \to Y$.

Túto vetu budeme veľmi často využívať, ak budeme chcieť dokázať, že dve množiny majú rovnakú kardinalitu. Mnohokrát je totiž jednoduchšie skonštruovať injekcie oboma smermi, než priamo nájsť bijekciu medzi danými množinami.

Uvedieme dva dôkazy tejto vety, základná myšlienka je v oboch veľmi podobná. Budeme sa snažiť ukázať existenciu takej podmnožiny $C \subseteq X$, pre ktorú je $f|_C$ bijekcia medzi C a $f[C]$ a $g|_{Y \setminus f[C]}$ je bijekcia medzi $X \setminus C$ a $Y \setminus f[C]$, pozri obrázok 4.1. Z týchto dvoch bijekcií už potom vieme poskladať bijekciu medzi X a Y.



{del:FIGCANTBER} Obr. 4.1: Ilustrácia k dôkazu Cantor-Bernsteinovej vety

Dôkaz. Nech $f\colon X \to Y$, $g\colon Y \to X$ sú injekcie. Definujme zobrazenie $F\colon \mathcal{P}(X) \to \mathcal{P}(X)$ predpisom
$$F(A) = X \setminus g[Y \setminus f[A]].$$

Ďalej indukciou definujeme množiny A_n, $n \in \mathbb{N}$ nasledovne:
$A_0 = \emptyset$,
$A_{n+1} = F(A)$
a položme $C := \bigcup_{n=1}^{\infty} A_n$.

Potom platí

$$F(C) = F\left(\bigcup_{n=1}^{\infty} A_n\right) = X \setminus g[Y \setminus f[\bigcup_{n=1}^{\infty} A_n]] = X \setminus g[Y \setminus \bigcup_{n=1}^{\infty} f[A_n]] = X \setminus g[\bigcap_{n=1}^{\infty} Y \setminus f[A_n]] =$$
$$= X \setminus \bigcap_{n=1}^{\infty} g[Y \setminus f[A_n]] = \bigcup_{n=1}^{\infty} (X \setminus g[Y \setminus f[A_n]]) = \bigcup_{n=1}^{\infty} F(A_n).$$

V predchádzajúcich úpravách sme použili viackrát tvrdenie 3.2.13 a fakt, že zobrazenia f a g sú injektívne a tiež de Morganove zákony z tvrdenia 2.4.10.

Ukázali sme teda, že pre množinu C platí $F(C) = C$, čo je ekvivalentné s rovnosťami $C = X \setminus g[Y \setminus f[C]]$,
$$X \setminus C = g[Y \setminus f[C]].$$

Definujme teraz zobrazenie $h\colon X \to Y$ nasledovne:

$$h(x) = \begin{cases} f(x), & \text{ak } x \in C, \\ y, & \text{kde } y \in Y \text{ je prvok s vlastnosťou } g(y) = x \text{ ak } x \notin C. \end{cases}$$

Tento predpis skutočne definuje zobrazenie: Každý prvok x množiny X buď patrí do C alebo do $X \smallsetminus C$, čiže sa použije práve jedna z uvedených dvoch vetiev. Ak $x \in X \smallsetminus C$, tak existuje $y \in Y$ s vlastnosťou $g(y) = x$, lebo $X \smallsetminus C = g[Y \smallsetminus f[C]]$. Súčasne z injektívnosti g existuje jediné také y.

Ukážeme ďalej, že toto zobrazenie je bijektívne. Overme najprv injektívnosť. Nech platí $h(x_1) = h(x_2)$. Rozlíšme tri možnosti, ktoré môžu nastať:
a) Oba prvky sú z množiny C, t.j. $x_1, x_2 \in C$. Potom ak $h(x_1) = h(x_2)$, tak $f(x_1) = f(x_2)$ a z injektívnosti f dostaneme $x_1 = x_2$.
b) Jeden z týchto prvkov je z C a druhý patrí do $X \smallsetminus C$. Nech napríklad $x_1 \in C$ a $x_2 \in X \smallsetminus C$. Ak $h(x_1) = h(x_2)$, tak máme $g(f(x_1)) = x_2$. Potom $x_2 \in g[f[C]]$ a súčasne $x_2 \in X \smallsetminus C = g[Y \smallsetminus f[C]]$, z čoho dostaneme $x_2 \in g[f[C]] \cap g[Y \smallsetminus f[C]] = g[f[C] \cap (Y \smallsetminus f[C])] = g[\emptyset] = \emptyset$, čo je samozrejme spor.
c) Oba prvky sú v $X \smallsetminus C$, t.j. $x_1, x_2 \in X \smallsetminus C$. Potom z $h(x_1) = h(x_2) = y$ vyplýva $g(y) = x_1 = x_2$.

Ešte zostáva overiť surjektívnosť. Ak $y \in Y$, tak môžu nastať dva prípady. Buď $y \in f[C]$ a potom $y = f(c)$ pre nejaké $c \in C$, čo znamená, že $y = h(c)$. Ak $y \in Y \smallsetminus f[C]$, tak $g(y) \in X \smallsetminus C = g[Y \smallsetminus f[C]]$, čo podľa definície zobrazenia h znamená, že $y = h(g(y))$. □

Uvedený dôkaz má nevýhodu, že využíva matematickú indukciu a prirodzené čísla, ktoré sme zatiaľ nedefinovali. (Preto sa ich snažíme využívať iba v príkladoch, nie však v dôležitých dôkazoch.) Nasledujúci dôkaz je len o trošičku komplikovanejší – líši sa od predchádzajúceho vlastne iba na jednom mieste, tento problém v ňom však už nie je.

Dôkaz. Opäť budeme predpokladať, že $f\colon X \to Y$ a $g\colon Y \to X$ sú injekcie a zadefinujeme zobrazenie $F\colon \mathcal{P}(X) \to \mathcal{P}(X)$ presne rovnako, ako v predchádzajúcom dôkaze, t.j.

$$F(A) = X \smallsetminus g[Y \smallsetminus f[A]].$$

Budeme sa snažiť ukázať, že existuje množina C s vlastnosťou $F(C) = C$, konštrukcia bijekcie h pomocou tejto množiny už je rovnaká ako v predchádzajúcom dôkaze.

Najprv ukážeme, že zobrazenie F je monotónne (vzhľadom na čiastočné usporiadanie $\subseteq$). Ak $A \subseteq B$, tak použitím tvrdení 2.4.10(xi) a 3.2.13 postupne dostaneme

$$\begin{aligned} f[A] &\subseteq f[B] \\ Y \smallsetminus f[A] &\supseteq Y \smallsetminus f[B] \\ g[Y \smallsetminus f[A]] &\supseteq g[Y \smallsetminus f[B]] \\ X \smallsetminus g[Y \smallsetminus f[A]] &\subseteq X \smallsetminus g[Y \smallsetminus f[B]] \\ F(A) &\subseteq F(B) \end{aligned}$$

Položme $\mathcal{S} := \{B \subseteq X; B \subseteq F(B)\}$ a $C := \bigcup \mathcal{S} = \bigcup \{B \subseteq X; B \subseteq F(B)\}$.

Ak $B \in \mathcal{S}$, tak $B \subseteq C$, a teda $F(B) \subseteq F(C)$.

Súčasne z nerovnosti $B \subseteq F(B)$ na základe monotónnosti dostaneme $F(B) \subseteq F(F(B))$, čiže aj $F(B) \in \mathcal{S}$. Teda pre každé $B \in \mathcal{S}$ platí $B \subseteq F(B) \subseteq F(C)$, z čoho vyplýva $C = \bigcup\limits_{B \in \mathcal{S}} B \subseteq F(C)$.

Zistili sme teda, že $C \subseteq F(C)$. Z monotónnosti potom vyplýva $F(C) \subseteq F(F(C))$, čo znamená, že $F(C) \in \mathcal{S}$. Teda $F(C)$ je jedna z množín, ktoré zjednocujeme, čo znamená, že $F(C) \subseteq C$.

Zistili sme, že platia obe inklúzie, čiže $C = F(C)$. □

Poznámka 4.1.9. Pre čitateľa, ktorý sa zaoberal teóriou zväzov, môže byť zaujímavé všimnúť si, že sme v dôkaze vlastne zostrojili zobrazenie $F\colon \mathcal{P}(X) \to \mathcal{P}(X)$, ktoré je monotónne. Na dôkaz Cantor-Bernsteinovej vety nám stačilo nájsť pevný bod tohoto zobrazenia. Jeho existencia vyplýva z Knaster-Tarského vety o pevnom bode, keďže $(\mathcal{P}(X), \subseteq)$ je úplný zväz. Takýmto spôsobom je dokázaná Cantor-Bernsteinova veta napríklad v [F, Theorem 3.1.9], [KLŠZ, Príklad 2.3.6]. (V podstate náš dôkaz bol do značnej miery podobný spôsobu, akým sa dokazuje Knaster-Tarského veta, resp. prvý z uvedených dôkazov sa väčšmi ponášal na dôkaz Kleeneho vety o pevnom bode.)

Doteraz dokázané výsledky o nerovnostiach medzi kardinálmi môžeme preformulovať aj nasledovným spôsobom:

Veta 4.1.10. *Nech a, b, c sú kardinálne čísla. Potom platí:*
(i) $a \leq a$;
(ii) $a \leq b \wedge b \leq a \Rightarrow a = b$;
(iii) $a \leq b \wedge b \leq c \Rightarrow a \leq c$.

{def:POZNPOROVKARD}

Poznámka 4.1.11. V tomto kontexte je ďalšou prirodzenou otázkou to, či sú ľubovoľné dve kardinálne čísla porovnateľné. Je to skutočne pravda, dôkaz využíva axiómu výberu. Tento fakt ukážeme neskôr pomocou výsledkov o dobre usporiadaných množinách v kapitole o ordinálnych číslach ako dôsledok 6.1.4.

Cvičenia

Úloha 4.1.1. Pokúste sa urobiť dôkaz vety 4.1.8 (Cantor-Bernstein) tak, že položíte $C = \bigcap\{B \subseteq X; B \supseteq F(B)\}$.

Úloha 4.1.2. Rozhodnite o platnosti nasledujúceho tvrdenia. (Svoju odpoveď zdôvodnite, t.j. dokážte toto tvrdenie alebo nájdite kontrapríklad.)
Pre množiny A, B platí $|A| < |B|$ práve vtedy, keď existuje bijekcia medzi množinou A nejakou vlastnou pomnožinou množiny B.

Úloha 4.1.3. Nech A, B sú ľubovoľné množiny. Dokážte (s použitím axiómy výberu), že $|f[A]| \leq |A|$.

4.2 Kardinálna aritmetika

{aritm:SECTKARDARITM}

Základné operácie s kardinálnymi číslami, ktoré zavedieme, sú súčet, súčin a umocňovanie kardinálnych čísel.

Definícia 4.2.1. Nech a, b sú kardinálne čísla a nech A, B sú množiny také, že $|A| = a$, $|B| = b$. Potom:

(i) Predpokladajme navyše, že množiny A a B sú disjunktné. Potom *súčet kardinálnych čísel* a a b je kardinálne číslo množiny $A \cup B$, t.j.
$$a + b = |A \cup B|.$$

(ii) *Súčin kardinálnych čísel* a a b je kardinálne číslo množiny $A \times B$, t.j.
$$a.b = |A \times B|.$$

(iii) Kardinálne číslo a *umocnené* na kardinálne číslo b je kardinalita množiny všetkých zobrazení z B do A. Túto množinu budeme označovať A^B. T.j. $a^b = |A^B|$, kde

$$A^B = \{f; f \text{ je zobrazenie z } B \text{ do } A\}.$$

Táto definícia si zaslúži niekoľko komentárov. V prvom rade sa môžeme zamyslieť nad tým, či vôbec pre ľubovoľné kardinálne číslo a existuje množina A taká, že $|A| = a$. Pokiaľ ste uverili poznámke 4.1.4, tak viete, že môžeme za A zvoliť priamo kardinál a. Tu sa však odvolávame na konštrukciu kardinálov, ktorú urobíme až v neskoršej kapitole. Ale funguje to aj pri naivnom pohľade na kardinálne čísla – za kardinálne čísla totiž považujeme iba tie „objekty“, ktoré môžeme dostať ako kardinality nejakých množín.

V prvej časti definície navyše požadujeme, aby množiny A a B boli disjunktné. Ak sme už našli množiny A, B spĺňajúce $|A| = a$ a $|B| = b$, tak namiesto nich môžeme zobrať napríklad množiny $A \times \{\emptyset\}$ a $B \times \{\{\emptyset\}\}$. Tieto množiny majú takú istú kardinalitu a určite sú disjunktné (pozri poznámku 3.4.10).

V súvislosti s poslednou časťou definície sa môžeme pýtať, či množina A^B musí existovať. Môžete sa pokúsiť ukázať z axióm systému ZFC, že pre ľubovoľné dve množiny takáto množina skutočne existuje – úloha 4.2.1.

Takisto má zmysel pýtať sa, či sú tieto operácie dobre definované. Inými slovami, či nezávisia od voľby množín A, B s uvedenými vlastnosťami. Presvedčíme sa, že je to v poriadku pri súčine kardinálov, ostatné operácie ponechávame na rozmyslenie čitateľovi.

Máme teda vlastne ukázať, že ak $|A| = |A'|$ a $|B| = |B|'$, tak aj $|A \times B| = |A' \times B'|$. Uvedené predpoklady znamenajú, že existujú bijekcie $f\colon A \to A'$ a $g\colon B \to B'$. Potom podľa tvrdenia 3.2.19 je zobrazenie $f \times g\colon A \times A' \to B \times B'$ tiež bijekcia.

Spôsob, akým sme zaviedli operácie na kardinálnych číslach je pomerne prirodzený – prinajmenšom pre konečné množiny funguje tak, ako obvyklé sčitovanie, násobenie a umocňovanie. Ľahko si uvedomíte, že ak máme m-prvkovú a n-prvkovú množinu, ktoré sú disjunktné, tak ich zjednotenie má $m + n$ prvkov. Takisto karteziánsky súčin m-prvkovej a n-prvkovej množiny má $m.n$ prvkov a zobrazení z n-prvkovej množiny do m-prvkovej je m^n (pre každý z n prvkov mám práve m možností výberu jeho obrazu).

Tu si môžeme súčasne uvedomiť, že platí $0^0 = 1$, keďže $\emptyset^\emptyset = \{\emptyset\}$. Prázdna množina $\emptyset$ je totiž jediná podmnožina $\emptyset \times \emptyset = \emptyset$, teda jediná relácia na množine $\emptyset$. Ľahko vidno, že táto relácia spĺňa definíciu zobrazenia.

O chvíľu si ukážeme niektoré vlastnosti kardinálnej aritmetiky (mnohé z nich sú do istej miery podobné na aritmetiku prirodzených čísel, ale v niektorých veciach je zasa počítanie s kardinálmi výrazne odlišné). Ešte predtým však skúsme zadefinovať niektoré konkrétne kardinálne čísla.

Definícia 4.2.2. Ľubovoľné prirodzené číslo n budeme stotožňovať s kardinálnym číslom n-prvkovej množiny. Teda napríklad $|\emptyset| = 0$, $|\{\emptyset\}| = 1$ a $|\{\emptyset, \{\emptyset\}\}| = 2$.

Kardinálne číslo množiny prirodzených čísel budeme označovať $\aleph_0$. Kardinálne čísla menšie než $\aleph_0$ voláme *konečné.* Kardinálne číslo a voláme *nekonečné,* ak $a \geq \aleph_0$.

Kardinálne číslo množiny $\mathcal{P}(\mathbb{N})$ budeme označovať $\mathfrak{c}$. (Toto kardinálne číslo sa niekedy nazýva *kardinalita kontinua.*)

Poznámka 4.2.3. Zatiaľ ešte nemáme dokázané, že pre každé kardinálne číslo platí buď $a < \aleph_0$ alebo $a \geq \aleph_0$, teda že musí byť buď konečné alebo nekonečné. Ako sme už spomenuli v poznámke 4.1.11, na to aby ľubovoľné dve kardinálne čísla boli porovnateľné potrebujeme axiómu výberu. Keďže my pracujeme v ZFC, tak uvedená definícia je ekvivalentná s takou definíciou, kde by sme nekonečné kardinály zaviedli ako tie, ktoré nie sú konečné.

V teórii množín sa skutočne pracuje s viacerými definíciami konečnosti, ktoré sú ekvivalentné v ZFC, nie všetky z nich sú však ekvivalentné v ZF; pozri napríklad [B2, Problém 1B], [H2, Section 4.1], [ŠS, Kapitoly 7.1 a 7.4]

Označenie $\mathfrak{c}$ a názov kardinalita kontinua pochádza z toho, že $\mathfrak{c}$ je kardinalita množiny $\mathbb{R}$. Tento fakt overíme neskôr. Už teraz ukážeme, že $\mathfrak{c} = 2^{\aleph_0}$.

{aritm:VTPX2NAX}

Veta 4.2.4. *Nech X je ľubovoľná množina. Potom platí*

$$|\mathcal{P}(X)| = 2^{|X|}.$$

Dôkaz. Na dôkaz nám stačí nájsť bijekciu medzi množinami $\{0,1\}^X$ a $\mathcal{P}(X)$.

Stačí si všimnúť, že zobrazenia $f\colon \mathcal{P}(X) \to \{0,1\}^X$ a $g\colon \{0,1\}^X \to \mathcal{P}(X)$ definované predpisom

$$\begin{aligned} f(A) &= \chi_A && \text{pre } A \subseteq X, \\ g(h) &= \{x \in X; h(x) = 1\} && \text{pre } h\colon X \to \{0,1\}, \end{aligned}$$

kde $\chi_A(x) = 1$ pre $x \in A$ a $\chi_A(x) = 0$ pre $x \notin A$, čiže χ_A je charakteristická funkcia množiny A. (Skutočne platí $g(f(A)) = \{x \in X; \chi_A(x) = 1\} = A$ a $f(g(h)) = \chi_{\{x\in X; h(x)=1\}} = h$ pre ľubovoľné $A \in \mathcal{P}(X)$ a $h \in \{0,1\}^X$.)

Keďže k zobrazeniu f existuje inverzné zobrazenie, je to bijekcia. $\square$

Dôsledok 4.2.5.

$$\mathfrak{c} = 2^{\aleph_0}$$

4.2.1 Vlastnosti sčitovania kardinálov

V tejto a nasledujúcich častiach budeme dokazovať niektoré rovnosti a nerovnosti, ktoré platia pre kardinálne operácie. Keďže postup pri všetkých dôkazoch je veľmi podobný, môžete si niekoľko pozrieť, aby ste videli základný princíp, ktorý sa v nich používa. Potom sa ostatné môžete pokúsiť dokázať samostatne a len ak si s nimi nebudete vedieť poradiť, pozrite sa na dôkazy, ktoré sú uvedené tu.

Veta 4.2.6. *Nech a, b, c sú kardinálne čísla, potom platí*

$$\begin{gathered} a+b = b+a \\ a+(b+c) = (a+b)+c \end{gathered}$$

Dôkaz. Najprv ukážme prvú rovnosť. Nech A, B sú disjunktné množiny také, že $|A| = a$ a $|B| = b$. Tvrdenie, že $|A|+|B| = |B|+|A|$ znamená, že existuje bijekcia medzi $A\cup B$ a $B\cup A$. To ale vyplýva z rovnosti $A\cup B = B\cup A$ a z toho, že identické zobrazenie je bijektívne.

Druhú rovnosť dostaneme podobným spôsobom z rovnosti $A\cup(B\cup C) = (A\cup B)\cup C$. $\square$

{aritm:VTNEROVSUCET}

Veta 4.2.7. *Nech a, b, c sú kardinálne čísla také, že $b \leq c$. Potom*

$$a+b \leq a+c.$$

Dôkaz. Nech A, B, C sú množiny také, že $|A| = a$, $|B| = b$, $|C| = c$ a súčasne platí $A\cap B = A\cap C = \emptyset$. Ďalej predpokladáme, že existuje injekcia $f\colon B \to C$. Chceme ukázať existenciu injekcie z $A\cup B$ do $A\cup C$.

Definujme zobrazenie $g\colon A \cup B \to A \cup C$ ako

$$g(x) = \begin{cases} x & \text{ak } x \in A, \\ f(b) & \text{ak } x \in B. \end{cases}$$

Z toho, že A a B sú disjunktné, vyplýva, že g je skutočne zobrazenie.

Takisto sa vcelku ľahko ukáže, že zobrazenie g je injektívne. Predpokladajme, že $g(x) = g(y)$. Uvažujme najprv možnosť $x \in A$, čo znamená, že $g(x) = x$. Potom $y \notin B$, lebo z $y \in B$ by vyplýva, že $g(y) \in C$ a $C \cap A = \emptyset$. Teda $y \in A$ a $g(y) = y$, čiže rovnosť $g(x) = g(y)$ znamená priamo $x = y$.

Teraz predpokladajme, že platí $g(x) = g(y)$ a $x \in B$. To znamená, že $g(x) = f(x)$. Súčasne to znamená, že $y \in B$. (Ak by platilo $y \in A$, tak $g(x) = y \in C \cap A = \emptyset$.) Potom máme $g(y) = f(y)$. Teda z $g(x) = g(y)$ vyplýva $f(x) = f(y)$ a, keďže f je injekcia, aj rovnosť $x = y$. □

Pri dôkaze tejto vety sa oplatí všimnúť si jednu všeobecnú zákonitosť. V dôkaze sme mohli použiť ľubovoľnú množinu B takú, že $|B| = b$ (a súčasne $A \cap B = \emptyset$). Takouto množinou je aj množina $f[B]$, pretože $f\colon B \to f[B]$ je bijekcia.

To znamená, že pri vhodnej voľbe množiny B môžeme priamo predpokladať $B \subseteq C$. Tým sa dôkaz značne zjednoduší – z tvrdenia 2.4.7(iii) vieme, že potom $A \cup B \subseteq A \cup C$. Z toho už je jasná existencia injekcie definovanej jednoducho ako $x \mapsto x$ pre všetky $x \in A \cup B$.

Príklad 4.2.8. Priamo, konštrukciou príslušnej bijekcie, ukážeme, že platí

$$\aleph_0 + \aleph_0 = \aleph_0.$$

Uvažujme množiny $\mathbb{N} \times \{0\}$ a $\mathbb{N} \times \{1\}$. Obidve majú kardinalitu $\aleph_0$ a navyše sú disjunktné. Stačí ukázať, že existuje bijekcie medzi $\mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\}$ a $\mathbb{N}$. Bijekciu môžeme definovať napríklad ako

$$f(n,0) = 2n,$$
$$f(n,1) = 2n+1.$$

Pre každé prirodzené číslo platí $0 \le n \le \aleph_0$ (keďže $\emptyset \subseteq \{0,1,\dots,n-1\} \subseteq \mathbb{N}$), z čoho dostávame

$$\aleph_0 = 0 + \aleph_0 \le n + \aleph_0 \le \aleph_0 + \aleph_0 = \aleph_0$$

Z Cantor-Bernsteinovej vety potom máme

$$\aleph_0 = n + \aleph_0 = \aleph_0 + \aleph_0.$$

Z toho vidíme napríklad aj to, že výsledok analogický k vete 4.2.7 neplatí pre ostrú nerovnosť.

Dôkaz nasledujúceho tvrdenia je založený na podobnej myšlienke ako predchádzajúci dôkaz.

{aritm:TVRNEKPLUSALNUL}

Tvrdenie 4.2.9. *Ak a je nekonečné kardinálne číslo, tak $\aleph_0 + a = \aleph_0$.*

Dôkaz. Máme vlastne dokázať, že ak A je taká množina, že $|A| = a \ge \aleph_0$, tak $|\mathbb{N} \times \{0\} \cup A \times \{1\}| = |A|$.

Predpoklad $|A| \ge \aleph_0$ znamená, že existuje injekcia $\mathbb{N} \to A$. Môžeme priamo predpokladať, že $\mathbb{N} \subseteq A$.

Teraz už vieme veľmi jednoducho zostrojiť bijekciu medzi $\mathbb{N} \times \{0\} \cup A \times \{1\}$ a A analogickým spôsobom ako v predchádzajúcom príklade.

$$f(n,0) = 2n, \text{pre } a \in \mathbb{N}$$
$$f(n,1) = 2n+1, \text{pre } a \in \mathbb{N}$$
$$f(a,1) = a, \text{ak } a \notin \mathbb{N}$$

□

4.2.2 Vlastnosti násobenia kardinálov

Veta 4.2.10. *Nech a, b, c sú kardinálne čísla, potom platí*

$$ab = ba$$
$$a(bc) = (ab)c$$
$$a(b+c) = ab + ac$$

Dôkaz. Nech A, B, C sú ľubovoľné množiny.

Na dôkaz prvého tvrdenia stačí ukázať existenciu bijekcie medzi $A \times B$ a $B \times A$. Zobrazenie $f\colon A \times B \to B \times A$ definovaní predpisom

$$f\colon (a,b) \mapsto (b,a)$$

pre $a \in A$, $b \in B$ je bijekcia.

Na dôkaz druhej časti stačí nájsť bijekciu $g\colon A \times (B \times C) \to (A \times B) \times C$. Takouto bijekciou je zobrazenie definované ako

$$g\colon (a,(b,c)) \mapsto ((a,b),c)$$

pre $a \in A$, $b \in B$, $c \in C$.

V tretej časti máme, za predpokladu, že B a C sú disjunktné, nájsť bijekciu medzi $A \times (B \cup C)$ a $(A \times B) \cup (A \times C)$. Z tvrdenia 2.5.4 však vieme, že platí dokonca rovnosť $A \times (B \cup C) = (A \times B) \cup (A \times C)$. □

Veta 4.2.11. *Nech a, b, c sú kardinálne čísla také, že $b \leq c$. Potom*

$$ab \leq ac.$$

Dôkaz. Nech $f\colon B \to C$ je injekcia. Potom podľa tvrdenia 3.2.19 je aj zobrazenie $id_A \times f\colon A \times B \to A \times C$ injekcia. □

Opäť platí analogická poznámka ako pri vete 4.2.7. Mohli by sme priamo predpokladať, že $B \subseteq C$ a potom si stačí všimnúť, že $A \times B \subseteq A \times C$ (pozri úlohu 2.5.4).

{aritm:PRIKLBIJEKNxN} **Príklad 4.2.12.** Ukážeme, že platí

{aritm:EQNxN}
$$\aleph_0 . \aleph_0 = \aleph_0. \qquad (4.1)$$

Z rovnosti (4.1) dostaneme, že pre každé $n \in \mathbb{N}$, $n > 0$, platí

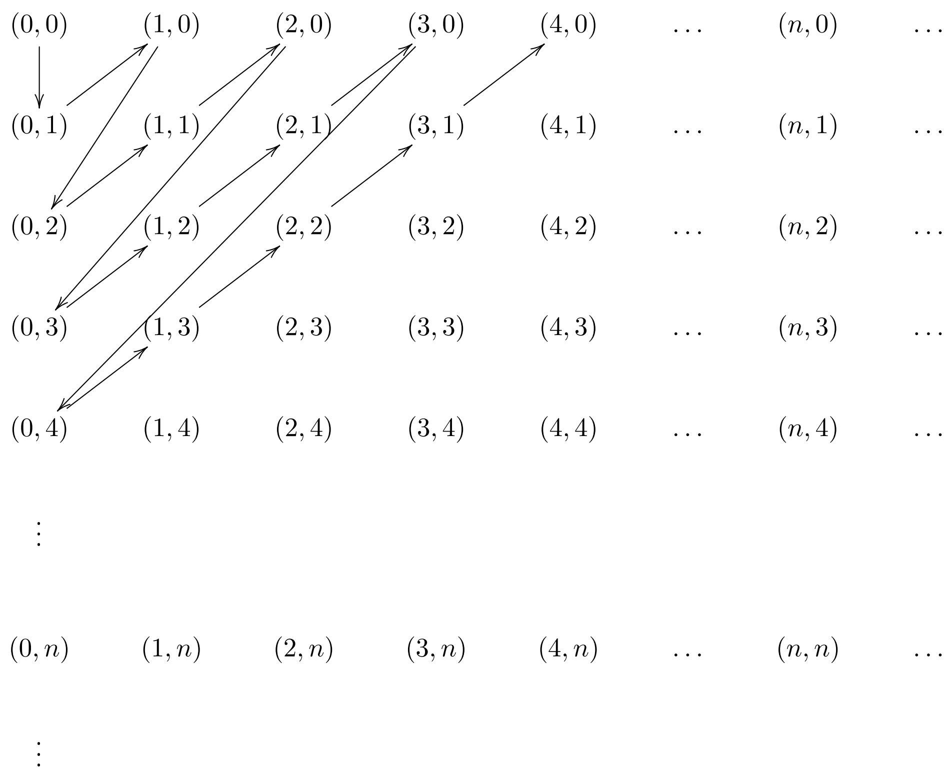
$$\aleph_0 \leq n.\aleph_0 \leq \aleph_0.\aleph_0 = \aleph_0.$$

Z Cantor-Bernsteinovej vety potom vyplýva rovnosť

$$\aleph_0 = n.\aleph_0 = \aleph_0.\aleph_0.$$

Na dôkaz rovnosti (4.1) nám stačí zostrojiť bijekciu medzi $\mathbb{N} \times \mathbb{N}$ a $\mathbb{N}$. Takýchto bijekcií sa dá nájsť veľa, ako prvú si ukážeme jednu veľmi známu pochádzajúcu už od G. Cantora.

Nasledujúci obrázok nám ukazuje, ako môžeme usporiadané dvojice prirodzených čísel usporiadať do postupnosti:



Zobrazenie $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definujeme tak, že každej dvojici priradíme pozíciu, na ktorej sa nachádza v tejto postupnosti, t.j. $(0,0) \mapsto 0$, $(0,1) \mapsto 1$, $(1,0) \mapsto 2$, $(0,2) \mapsto 3$, $(1,1) \mapsto 4$, $(2,0) \mapsto 5$ atď.

Toto zobrazenie vieme popísať aj jednoduchým predpisom. Všimnime si, že dvojice na tej istej diagonále (t.j. také dvojice (m,n), ktoré majú rovnaký súčet $m+n$) zoraďujeme podľa prvej súradnice a všetky prvky z diagonál, ktoré sú naľavo od nich. Teda ak $m+n=s$, tak $1+2+\dots+n = \frac{s(s+1)}{2}$ prirodzených čísel sme použili na predchádzajúce diagonály. Poradie na diagonále určíme podľa m, čiže dostaneme

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

(Môžete si túto formulu prekontrolovať pre niektoré konkrétne dvojice.)

O tom, že takéto zobrazenie je bijektívne, by vás snáď mohol presvedčiť obrázok, ktorým sme ho znázornili.

Pokiaľ by vám však takýto argument nestačil, je tu pre vás aj podrobnejší formálny dôkaz.

Dôkaz. Označme $\Delta_a = \sum_{k=1}^{a} k = \frac{a(a+1)}{2}$. (Čiže Δ_a je a-te trojuholníkové číslo.)

Potom funkciu f môžeme zapísať ako

$$f(m,n) = \Delta_{m+n} + m.$$

Ďalej označme $I_a = \{\Delta_a, \Delta_a + 1, \dots, \Delta_{a+1} - 1\}$ pre každé $a \in \mathbb{N}$. Systém $\{I_a, a \in \mathbb{N}\}$ tvorí rozklad množiny $\mathbb{N}$. (Tento fakt ľahko vyplýva z $\Delta_a = 0$ a $\Delta_a < \Delta_{a+1}$.)

Takisto je zrejmé, že $f(m,n) \in I_{m+n}$. Vďaka tomu z rovnosti $f(m+n) = f(m'+n')$ vyplýva $m+n = m'+n'$. Z $\Delta_{m+n} + m = \Delta_{m+n} + m'$ dostaneme $m = m'$, a teda aj $n = n'$. Tým je dokázaná injektívnosť zobrazenia f.

Overme ešte surjektívnosť. Vieme, že každé $x \in \mathbb{N}$ patrí do niektorej množiny I_a (keďže tieto množiny tvoria rozklad). Stačí teda nájsť m, n tak, že $m+n = a$ a $x = \Delta_a + m$. Z nerovnosti $\Delta_a \le x \le \Delta_{a+1} - 1$ a z toho, že $\Delta_{a+1} - \Delta_a = a + 1$ dostaneme, že pre $m = x - \Delta_a$ platí nerovnosť $0 \le m \le \Delta_{a+1} - 1 - \Delta_a = a$. Z toho vyplýva, že ak položíme $n = a - m$, tak m aj n sú prirodzené čísla a platí $f(m,n) = a$. □

Inú bijekciu $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ môžeme dostať s použitím faktu, že každé prirodzené číslo väčšie ako 0 sa dá zapísať ako súčin mocniny čísla 2 a nepárneho čísla. (Toto viete odvodiť z poznatkov o deliteľnosti prirodzených čísel, ktoré máte z prvého ročníka [Č1].) Teda zobrazenie

$$g(m,n) = 2^m.(2n+1) - 1$$

je bijekcia z $\mathbb{N} \times \mathbb{N}$ do $\mathbb{N}$.

{aritm:POZNMAX}

Poznámka 4.2.13. Neskôr ukážeme (s použitím axiómy výberu), že kardinálne sčitovanie a násobenie je jednoduché, pre ľubovoľné nekonečné kardinály a, b totiž platí

$$a + b = a.b = \max\{a, b\}.$$

(Zatiaľ dokonca nevieme ani to, či existuje maximum z kardinálnych čísel a, b; pozri poznámku 4.1.11.)

V tejto kapitole však budeme (v dôkazoch i cvičeniach) využívať iba veci, ktoré sme o kardinálnej aritmetike dokázali.

4.2.3 Vlastnosti kardinálneho umocňovania

Pri prirodzených číslach sme používali označenie a^2 ako synonymum zápisu $a.a$. (Podobne pre $a^3, a^4, \dots$) Ukážeme si, že aj pre kardinálne čísla predstavujú tieto dva zápisy to isté.

Tvrdenie 4.2.14. *Ak a je ľubovoľné kardinálne číslo, tak platí*

$$a^2 = a.a.$$

Dôkaz. Máme vlastne ukázať, že pre ľubovoľnú množinu existuje bijekcia medzi $A^{\{0,1\}}$ a $A \times A$.

Definujme $\varphi\colon A^{\{0,1\}} \to A \times A$ ako

$$\varphi(f) = (f(0), f(1)).$$

Súčasne definujme $\psi\colon A \times A \to A^{\{0,1\}}$ tak, že $\psi(a,b)$ je zobrazenie určené predpisom

$$\psi(a,b)(0) = a,$$
$$\psi(a,b)(1) = b.$$

(Namiesto zápisu $\psi((a,b))$ píšeme stručnejšie $\psi(a,b)$.) Ľahko sa overí, že φ a ψ sú navzájom inverzné zobrazenia, čiže φ aj ψ sú bijekcie. □

Takisto by bolo ľahké rozšíriť toto tvrdenie indukciou na ďalšie prirodzené čísla. (Hoci sme zatiaľ stále formálne neskonštruovali prirodzené čísla a ani neukázali, že sú dobre usporiadané a teda na nich funguje indukcia.)

Veta 4.2.15. *Ak a, b, c sú kardinálne čísla také, že $a \leq b$, tak $a^c \leq b^c$.*

Dôkaz. Nech $|A| = a$, $|B| = b$, $|C| = c$. Môžeme priamo predpokladať, $A \subseteq B$. Potom platí aj $A^C \subseteq B^C$. (Každé zobrazenie z C do A je súčasne zobrazením z B do A.) □

Napriek tomu, že máme takýto jednoduchý dôkaz, pokúsme sa ešte urobiť dôkaz priamo z existencie injekcie z A do B. (Aby sme si trochu precvičili prácu so zobrazeniami medzi množinami zobrazení – v ďalších dôkazoch budeme takéto niečo často potrebovať.)

Dôkaz. Vlastne máme dokázať: Ak existuje injekcia $f\colon A \to B$, tak existuje aj injekcia z množiny A^C do množiny B^C. Skúsme teda najprv vymyslieť, ako by sme pomocou zobrazenia f mohli definovať zobrazenie $\varphi\colon A^C \to B^C$ a pri troche šťastia sa nám ho snáď podarí vymyslieť tak, aby bolo injektívne a aj jeho injektívnosť dokázať.

Hľadáme teda zobrazenie, ktoré ľubovoľnej funkcii $g\colon C \to A$ priradí nejakú funkciu z C do B. Našu situáciu si môžeme znázorniť takto:

Hneď vidíme, že f a g určujú zobrazenie z C do B – konkrétne zobrazenie $f \circ g$. Teda asi najprirodzenejší spôsob ak definovať nejaké zobrazenie z A^C do B^C pomocou f je

$$\varphi\colon g \mapsto f \circ g$$
$$\varphi(g) = f \circ g$$

Overme ešte, že toto zobrazenie je injektívne. Pýtame sa, či platí

$$\varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$$
$$f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2$$

Táto rovnosť znamená, že pre každé $x \in C$ platí

$$f(g_1(x)) = f(g_2(x)).$$

Pretože f je injektívne, vyplýva z nej rovnosť

$$g_1(x) = g_2(x).$$

Platnosť tejto rovnosti pre každé $x \in X$ znamená rovnosť zobrazení $g_1 = g_2$; čiže presne to, čo sme chceli dokázať. □

Veta 4.2.16. *Ak a, b, c sú kardinálne čísla také, že $a \leq b$ a $c \neq 0$, tak*

$$c^a \leq c^b.$$

Dôkaz. Môžeme predpokladať, že platí $A \subseteq B$. □

Dôkaz. Nech A, B, C sú množiny také, že $|A| = a$, $|B| = b$ a $|C| = c$.

Predpoklad $c \neq 0$ nám hovorí, že $C \neq \emptyset$. Zvoľme si ľubovoľné $c_0 \in C$.

Vieme, že existuje injekcia $f\colon A \to B$. Na základe už viackrát spomenutej úvahy môžeme priamo predpokladať, že $A \subseteq B$. Definujme zobrazenie $\varphi\colon C^A \to C^B$ tak, že

$$\varphi(f)(x) = \begin{cases} f(x) & \text{pre } x \in A, \\ c_0 & \text{pre } x \notin A. \end{cases}$$

Zobrazenie φ je injekcia. Ak platí $\varphi(f) = \varphi(g)$, tak pre každé $x \in A$ platí $f(x) = \varphi(f)(x) = \varphi(g)(x) = g(x)$, a teda $f = g$. □

V tomto prípade by sa dôkaz príliš nezmenil, ak by sme priamo predpokladali, že $A \subseteq B$. Injekciu φ by sme definovali ako

$$\varphi(f)(x) = \begin{cases} x & \text{pre } x \in A, \\ c_0 & \text{pre } x \notin A, \end{cases}$$

t.j. namiesto zobrazenia f by sme použili vloženie A do B.

Ukážeme si ešte iný dôkaz. (Oproti predchádzajúcemu má však istú nevýhodu, keďže používame tvrdenie 3.2.14 a úlohu 3.2.4, a teda axiómu výberu.)

Dôkaz. Nech $f\colon A \to B$ je injekcia. Potom pre každé $g\colon B \to C$ máme zobrazenie $g \circ f$.

Definujme zobrazenie $\varphi\colon C^B \to C^A$ ako

$$\varphi(g) = g \circ f$$

pre $g\colon B \to C$.

Ukážeme, že toto zobrazenie je surjektívne. Nech $h\colon A \to C$ je ľubovoľný prvok C^A. Predpokladajme navyše, že $A \neq \emptyset$. Podľa tvrdenia 3.2.14 existuje zobrazenie $f'\colon B \to A$ také, že $f' \circ f = id_A$. Potom pre zobrazenie $h \circ f'$ platí $\varphi(h \circ f') = h \circ f' \circ f = h \circ id_A = h$. Ukázali sme, že ľubovoľné zobrazenie $h \in C^A$ má v zobrazení vzor.

Zostáva rozobrať len prípad $A = \emptyset$. Vtedy platí $C^\emptyset = \{\emptyset\}$. Súčasne, keďže $C \neq \emptyset$, takže C^B je aspoň jednoprvková. Teda aj v tomto prípade uvedená nerovnosť platí. □

Veta 4.2.17. *Pre ľubovoľné kardinálne čísla platí*

$$a^{b+c} = a^b.a^c.$$

Dôkaz. Vlastne máme dokázať, že pre ľubovoľné množiny A, B, C také, že B a C sú disjunktné, existuje bijekcia medzi $A^{B\cup C}$ a $A^B \times A^C$.

T.j. chceli by sme nájsť zobrazenie $\varphi\colon A^{B\cup C} \to A^B \times A^C$ alebo zobrazenie $\psi\colon A^B \times A^C \to A^{B\cup C}$ a ukázať o ňom, že je bijekcia. My budeme postupovať tak, že nájdeme zobrazenia oboma smermi a ak sa nám podarí ukázať, že jedno z nich je inverzné k druhému, tak z toho vieme, že ide o bijekcie.

Aby sme definovali φ, tak vlastne potrebujeme každej funkcii $f\colon B \cup C \to A$ priradiť dvojicu funkcií – prvá z nich ide z B do A a druhá z C do A. Zobrazeniu z $B \cup C$ do A však vieme priradiť zobrazenie na menšej množine veľmi prirodzeným spôsobom – pôjde o zúženie zobrazenia na túto podmnožinu. Môžeme teda definovať zobrazenie $\varphi\colon A^{B\cup C} \to A^B \times A^C$ nasledovne:

$$\varphi\colon f \mapsto (f|_B, f|_C)$$
$$\varphi(f) = (f|_B, f|_C)$$

Ak hľadáme zobrazenie $\psi\colon A^B \times A^C \to A^{B\cup C}$, tak vlastne každej dvojici zobrazení $g\colon B \to A$, $h\colon C \to A$ chceme priradiť zobrazenie z $B \cup C$ do A. Opäť, máme pomerne prirodzený spôsob, ako to môžeme spraviť, dvojici (g, h) priradíme zobrazenie definované predpisom

$$\psi(g,h)(x) = \begin{cases} g(x) & \text{ak } x \in B, \\ h(x) & \text{ak } x \in C. \end{cases}$$

Na tomto mieste využívame fakt, že B a C sú disjunktné – v opačnom prípade by predchádzajúci predpis nemusel definovať zobrazenie.

(Intuitívna predstava za predchádzajúcimi úvahami je asi takáto: Jedným smerom sme postupovali tak, že zobrazenie z $B \cup C$ do A sme rozdelili na 2 zobrazenia na 2 častiach definičného oboru. Zobrazenie ψ zase tieto 2 zobrazenia naspäť zlepí – to je zhruba aj dôvod, prečo sú tieto 2 priradenia jedno k druhému inverzné; overíme to však podrobne.)

To, že ψ je inverzné zobrazenie k φ overíme, tak, že ukážeme, že pri zložení $\varphi \circ \psi$ aj $\psi \circ \varphi$ dostaneme identické zobrazenie.

Skúsme najprv vyrátať, čomu sa rovná $\psi \circ \varphi$. Pre ľubovoľné $f\colon B \cup C \to A$ máme $\psi(\varphi(f)) = \psi(f|_B, f|_C)$ po dosadení $x \in B \cup C$ dostaneme

$$\psi(\varphi(f))(x) = \psi(f|_B, f|_C)(x) = \begin{cases} f|_B(x) = f(x) & \text{ak } x \in B, \\ f|_C(x) = f(x) & \text{ak } x \in C, \end{cases}$$

teda $\psi(\varphi(f))(x) = f(x)$ pre každé $x \in B \cup C$, čiže zobrazenia $\psi(\varphi(f))$ a f sa rovnajú. Dostali sme:

$$(\forall f \in A^{B\cup C})\ \psi(\varphi(f)) = f$$
$$\psi \circ \varphi = id_{A^{B\cup C}}$$

Zostáva nám ešte pozrieť sa na zobrazenie $\varphi\circ\psi\colon A^B \times A^C \to A^B \times A^C$. Ak máme ľubovoľnú dvojicu $g\colon B \to A$, $h\colon C \to A$, tak priamo z definície zobrazenia ψ vidno, že $\psi(g,h)|_B = g$ a $\psi(g,h)|_C = h$, a teda

$$\varphi(\psi(g,h)) = (\psi(g,h)|_B, \psi(g,h)|_C) = (g,h).$$

Teda $\varphi \circ \psi = id_{A^B\times A^C}$.

Zistili sme, že $\psi = \varphi^{-1}$, teda φ aj ψ sú bijekcie. □

{aritm:VTMOCKARTEZ}

Veta 4.2.18. *Pre ľubovoľné kardinálne čísla platí* $(a^b)^c = a^{bc}$.

Dôkaz. Pre ľubovoľné A, B, C chceme nájsť bijekciu medzi $(A^B)^C$ a $A^{B\times C}$. Opäť, pokúsime sa nájsť nejaké zobrazenia $\varphi\colon (A^B)^C \to A^{B\times C}$ a $\psi\colon A^{B\times C} \to (A^B)^C$ a ukázať, že sú navzájom inverzné.

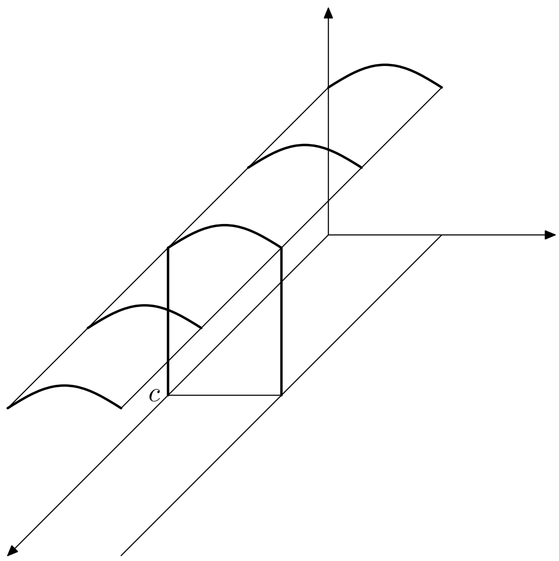
Hľadáme zobrazenie $\varphi\colon (A^B)^C \to A^{B\times C}$. T.j. ak máme dané nejaké zobrazenie $f\colon C \to A^B$, chceli by sme k nemu nájsť niečo, čo dvojiciam $(b,c) \in B \times C$ priradí prvky z A. Pre ľubovoľné $c \in C$ však máme zobrazenie $f(c)\colon B \to A$ – čiže je dosť prirodzené dvojici (b,c) priradiť $f(c)(b)$, t.j.

$$\varphi(f)\colon B \times C \to A$$
$$\varphi(f)(b,c) = f(c)(b)$$

Obrátene, každému zobrazeniu $g\colon B\times C \to A$ by sme chceli priradiť zobrazenie $\psi(g)\colon C \to A^B$, t.j. zobrazenie, ktoré každému prvku z C priradí nejaké zobrazenie z B do A. Ak máme dané zobrazenie z $B \times C$ do A, zafixujeme nejaké $c \in C$ a meníme len prvok $b \in B$ vidíme, že dostaneme zobrazenie z B do A. Presnejšie to môžeme zapísať

$$(\psi(g))(c)\colon B \to A$$
$$(\psi(g))(c)(b) = g(b,c)$$

Toto priradenie je načrtnuté na obr. 4.2, kde $A = \mathbb{R}$, $B = \langle 0,1\rangle$, $C = \langle 0,\infty)$. Rezy načrtnuté na grafe funkcie sú práve funkcie z B do A priradené jednotlivým prvkom z C.



Obr. 4.2: Obrázok ilustrujúci postup v dôkaze vety 4.2.18. (Použitá funkcia je $f(x,y) = \frac{3}{2} + \frac{1}{5}\sin \pi x$.) {aritm:FIGMOC

(Naschvál som zvolil množiny A, B a C rôzne, aby sa na obrázku dalo vidieť, ktorá množina je ktorá.)

Opäť, priamo dosadením nám vyjde, že $\varphi \circ \psi$ aj $\psi \circ \varphi$ je identita. Počítajme najprv $\varphi \circ \psi \colon A^{B\times C} \to A^{B\times C}$. Pre ľubovoľné $g\colon B\times C \to A$ chceme zistiť, čomu sa rovná zobrazenie $\varphi(\psi(g))\colon B \times C \to A$. Dostaneme (priamo použitím definície zobrazení φ a ψ)

$$\varphi(\psi(g))(b,c) = \psi(g)(c)(b) = g(b,c).$$

Vyšlo nám, že $\varphi(\psi(g)) = g$ pre každé $g \in A^{B\times C}$, a teda $\varphi \circ \psi = id_{A^{B\times C}}$.

Skúsme teraz vyrátať $\psi \circ \varphi \colon (A^B)^C \to (A^B)^C$. Ak máme zobrazenie $f\colon C \to A^B$, chceme zistiť, či platí $\psi(\varphi(f)) = f$. Použitím definície φ a ψ máme

$$\psi(\varphi(f))(c)(b) = \varphi(f)(b,c) = f(c)(b).$$

Keďže táto rovnosť platí pre všetky $b \in B$, znamená to rovnosť zobrazení

$$\psi(\varphi(f))(c) = f(c).$$

Opäť, predchádzajúca rovnosť platí pre každé $c \in C$, teda $\psi \circ \varphi(f) = f$. Posledná rovnosť (ktorá platí pre ľubovoľné $f \in (A^B)^C$) znamená rovnosť zobrazení $\psi \circ \varphi = id_{(A^B)^C}$.

Zistili sme, že $\psi = \varphi^{-1}$, preto obe zobrazenia φ aj ψ sú bijekcie. □

{aritm:VTANABPOD2NAAB}

Veta 4.2.19. *Pre ľubovoľné kardinálne čísla platí*

$$a^b \leq 2^{ab}.$$

Dôkaz. Ak množiny A, B sú také, že $|A| = a$ a $|B| = b$, tak $A^B \subseteq \mathcal{P}(B \times A)$. (Vyplýva to priamo z definície zobrazenia.)

To ale znamená, že $|A^B| \leq |\mathcal{P}(B \times A)|$ a $a^b \leq 2^{ab}$. □

LOANABEXISTS}

Cvičenia

Úloha 4.2.1. Ukážte pomocou schémy axióm vymedzenia, že pre ľubovoľné množiny A a B existuje množina všetkých zobrazení z B do A.

Úloha 4.2.2. Ukážte, že $|\mathbb{Z}| = \aleph_0$. (T.j. nájdite bijekciu medzi $\mathbb{Z}$ a $\mathbb{N}$.)

Úloha 4.2.3. Ukážte, že $\mathfrak{c}.\mathfrak{c} = \mathfrak{c}$ a $\mathfrak{c}^{\aleph_0} = \mathfrak{c}$.

Úloha 4.2.4. Ukážte, že pre ľubovoľný konečný kardinál n platí $\mathfrak{c} = n.\mathfrak{c} = \mathfrak{c}.\mathfrak{c} = \mathfrak{c}^n = \mathfrak{c}^{\aleph_0}$.

Úloha 4.2.5. Ukážte, že pre ľubovoľný konečný kardinál n platí $2^{\aleph_0} = n^{\aleph_0} = \aleph_0^{\aleph_0} = \mathfrak{c}^{\aleph_0} = \mathfrak{c}$.

Úloha 4.2.6. S využitím faktu, že pre nekonečné kardinály platí $b.b = b$ (ktorý dokážeme neskôr) ukážte, že ak $2 < a \leq b$, kde a, b sú nekonečné kardinály, tak $2^b = a^b$.

Úloha 4.2.7. Nech $S = \mathbb{Q}\times\mathbb{Q}$. Ukážte, že existujú množiny V, H také, že $S = V \cup H$, prienik V sa každou vertikálnou priamkou v rovine $\mathbb{R}^2$ je konečný a prienik H sa každou horizontálnou priamkou je konečný. (T.j. pre každé $x \in \mathbb{Q}$ sú množiny $\{y \in \mathbb{Q}; (x, y) \in V\} = \{x\} \times \mathbb{Q} \cap V$ aj $\{y \in \mathbb{Q}; (y, x) \in H\} = \mathbb{Q} \times \{x\} \cap H$ konečné.)

Úloha 4.2.8*. Aká je kardinalita množiny všetkých bijekcií z $\mathbb{N}$ do $\mathbb{N}$? (Bijekcie z $\mathbb{N}$ do $\mathbb{N}$ sa niekedy zvyknú nazývať aj permutáciami množiny $\mathbb{N}$. Na základe analógie s prirodzenými číslami by sme kardinalitu takejto množiny mohli nazvať $\aleph_0$-faktoriál.)

4.3 Cantorova veta a diagonálna metóda

{cantor:VTCANTOR}

Veta 4.3.1 (Cantor)**.** *Pre každú množinu X platí $|X| < |\mathcal{P}(X)|$.*

Cantorovu vetu môžeme ekvivalentne preformulovať tak, že pre každé kardinálne číslo a platí $a < 2^a$.

Dôkaz. Nerovnosť $|X| \leq |\mathcal{P}(X)|$ vyplýva z toho, že $x \mapsto \{x\}$ je injekcia z X do $\mathcal{P}(X)$.

Predpokladajme teraz, že by existovala bijekcia $f\colon X \to \mathcal{P}(X)$. Ďalej označme

$$A := \{x \in X; x \notin f(x)\}.$$

Pretože f je bijekcia, existuje $y \in X$ s vlastnosťou $A = f(y)$.

Sú dve možnosti. Buď platí $y \in A$, čo ale znamená, že $y \notin f(y) = A$; alebo platí $y \notin A$ a v tomto prípade $y \in f(y) = A$. Obidve možnosti vedú k sporu a teda nemôže existovať bijekcia medzi X a $\mathcal{P}(X)$. □

{cantor:PRIKLPOST01}

Príklad 4.3.2. Možno nám lepšie pomôže pochopiť tento dôkaz, ak si ho ešte raz osvetlíme na prípade $X = \mathbb{N}$. Budeme sa teda zaoberať kardinalitou množiny $\mathcal{P}(\mathbb{N})$, namiesto nej však môžeme zobrať množinu $\{0, 1\}^{\mathbb{N}}$ všetkých postupností núl a jednotiek. Vo vete 4.2.4 sme totiž skonštruovali bijekciu $A \mapsto \chi_A$ medzi týmito dvoma množinami.

Chceme ukázať, že $|\{0, 1\}^{\mathbb{N}}| \neq \aleph_0$. Postupujme sporom – predpokladajme, že by existovala bijekcia $f\colon \mathbb{N} \to \{0, 1\}^{\mathbb{N}}$. Máme teda postupnosti prirodzených čísel

$$\begin{aligned}
f(0) &= (a_0^{(0)}, a_1^{(0)}, a_2^{(0)}, \dots)\\
f(1) &= (a_0^{(1)}, a_1^{(1)}, a_2^{(1)}, \dots)\\
f(2) &= (a_0^{(2)}, a_1^{(2)}, a_2^{(2)}, \dots)\\
&\vdots
\end{aligned}$$

Ak definujeme postupnosť $b = (b_n)_{n=0}^{\infty}$ ako

$$b_n = 1 - a_n^{(n)},$$

čiže b_n je 0 ak $a^{(n)} = 1$ a obrátene, tak potom b nie je rovné žiadnej z postupností $f(n)$, $n \in \mathbb{N}$. Od postupnosti $f(n)$ sa totiž líši na n-tom mieste.

Dôkaz vety 4.3.1 je v podstate totožný s postupom z predchádzajúceho príkladu. (Jediný rozdiel je v tom, že sme nemohli prvky $f(x)$, $x \in X$, zapísať do postupnosti, keďže tam sme pracovali s ľubovoľnou množinou X a nie s množinou $\mathbb{N}$.)

{cantor:POZNDIAG}

Poznámka 4.3.3. Metóda použitá v predchádzajúcom dôkaze pochádza od Cantora a nazýva sa *diagonálna metóda.* (V predchádzajúcom príklade vidno, že sme vlastne menili diaognálne prvky.) Podobný argument je používaný často, aj v iných oblastiach matematiky. Mohli ste sa s ním stretnúť napríklad aj na predmete formálne jazyky a automaty, pri dôkaze, že existujú jazyky, ktoré nie sú rozpoznateľné žiadnym Turingovým strojom [RF, Kapitola 6], [HMU, Chapter 9] (voľne povedané, nie všetko sa dá naprogramovať).

My si ukážeme ešte jednu aplikáciu tejto metódy v príklade 4.5.3.

Môžeme si všimnúť, že na základe Cantorovej vety dostávame nekonečnú hierarchiu kardinálnych čísel. (Pre každé kardinálne číslo existuje kardinál, ktorý je od neho väčší.)

{cantor:PRALNULxC}

Príklad 4.3.4. Ukážeme, že platí

$$\aleph_0.\mathfrak{c} = \mathfrak{c}.$$

Z Cantorovej vety máme $\aleph_0 < 2^{\aleph_0} = \mathfrak{c}$. Na základe toho dostaneme nerovnosť

$$\aleph_0.\mathfrak{c} \le \mathfrak{c}.\mathfrak{c} = 2^{\aleph_0}.2^{\aleph_0} = 2^{\aleph_0+\aleph_0} = 2^{\aleph_0} = \mathfrak{c}.$$

Platí aj nerovnosť $\mathfrak{c} \le \aleph_0.\mathfrak{c}$, takže z Cantor-Bernsteinovej vety dostaneme dokazovanú rovnosť.

Kardinálne čísla tvoria vlastnú triedu

Nadviažeme na časť 2.5.1 a povieme si ešte niečo o vlastných triedach. Aby boli dôkazy výsledkov v tejto časti úplne korektné treba uveriť tomu, že kardinálne čísla sa skutočne dajú zadefinovať formulou jazyka teórie množín a majú vlastnosti, ktoré sme už uviedli (pozri poznámku 4.1.4.)

Pokiaľ chceme ukázať, že nejaký systém množín je vlastnou triedou, často môžeme postupovať sporom – pokúsiť sa ukázať pomocou axióm ZFC, že ak by tento systém bol množinou, bola by množinou aj trieda **Set**. Ukážeme si to na príklade dvoch tvrdení:

{def:TVRSINGLETONSCLASS}

Tvrdenie 4.3.5. *Systém všetkých jednoprvkových množín tvorí vlastnú triedu.*

Dôkaz. Predpokladajme, že by systém všetkých jednoprvkových množín $\{\{x\}; x \in \mathbf{Set}\}$ tvoril množinu. Potom $f\colon \{x\} \mapsto x$ je zobrazenie definované na tejto množine. Jeho obrazom je vlastná trieda **Set**. Podľa schémy axióm substitúcie by potom **Set** bola množina, čo je spor s vetou 2.5.7. ☐

Iný dôkaz. Predpokladajme, že by systém všetkých jednoprvkových množín $\{\{x\}; x \in \mathbf{Set}\}$ tvoril množinu. Podľa axiómy zjenotenia by potom aj $\bigcup\{\{x\}; x \in \mathbf{Set}\}$ bola množina. Lenže každá množina x patrí do jednoprvkovej množiny $\{x\}$, takže $\bigcup\{\{x\}; x \in \mathbf{Set}\} = \mathbf{Set}$. Dostávame, že **Set** je množina, čo vedie k tomu istému sporu ako v predošlom dôkaze. ☐

Veľmi podobným spôsobom môžeme ukázať nasledujúce tvrdenie:

{def:TVRGIVENCARDCLASS}

Tvrdenie 4.3.6. *Nech $X \neq \emptyset$ je množina. Potom systém všetkých množín rovnakej mohutnosti ako X tvorí vlastnú triedu.*

Dôkaz. Sporom. Predpokladajme, že $A = \{m; |m| = |X|\}$ je množina. Položme $B = \{m \in A; (\exists x) m = \{x\} \times X\}$. Na základe schémy axióm vymedzenia je aj B množina. Ďalej definujeme formulu $\varphi(y, x)$ ako $y = \{x\} \times X$. Táto formula má tú vlastnosť, že pre každé $y \in B$ existuje práve jedno $x$také, že platí $\varphi(y, x)$. Existencia vyplýva priamo z definície množiny B a na základe neprázdnosti X dostaneme z $y = \{x_1\} \times X = \{x_2\} \times X$ rovnosti $\{x_1\} = \{x_2\}$ a $x_1 = x_2$. (Pozri tvrdenie 2.5.4.)

Potom zo schémy axióm obrazu, že $\{x; \{x\} \times X \in A\}$ je množina. Ľahko však vidno, že pre každú množinu x existuje bijekcia medzi X a $\{x\} \times X$, čo znamená, že $\{x; \{x\} \times X \in A\} = \mathbf{Set}$. Dostávame spor. ☐

Iný dôkaz. Sporom. Predpokladajme, že $A = \{m; |m| = |X|\}$ je množina. Stačí nám, podobne ako v prípade predchádzajúceho tvrdenia, ukázať, že $\bigcup A = \mathbf{Set}$.

Ak $x \in \mathbf{Set}$ je ľubovoľná množina, tak existuje $m \in A$ také, že $x \in m$. V prípade, že $x \in X$ je to jasné. Ak $x \notin X$, tak stačí zvoliť nejaké $x_0 \in X$ (čo môžeme urobiť, lebo $X \neq \emptyset$) a položiť $m = X \setminus \{x_0\} \cup X$. Očividne $|m| = |X|$.

Ukázali sme, že každá množina patrí do nejakého prvku množiny A, čo znamená, že $\bigcup A = \mathbf{Set}$. □

{def:VTCNISPROPERCLASS}

Veta 4.3.7. *Systém všetkých kardinálnych čísel tvorí vlastnú triedu. Túto triedu budeme označovať* Cn.

Dôkaz. Sporom. Prepokladajme, že Cn je množina. Potom aj $B = \bigcup \mathrm{Cn}$ je množina, navyše pre každé kardinálne číslo platí $a \subseteq B$. Z toho vyplýva pre každé kardinálne číslo $a \leq |B|$.

Pre kardinálne číslo $2^{|B|}$ máme potom nerovnosť $|B| < 2^{|B|}$ z Cantorovej vety a súčasne $2^{|B|} \leq |B|$ z predchádzajúcej úvahy. Teda $2^{|B|} < 2^{|B|}$, čo je spor. □

Cvičenia

{cantorcvic:ULOCnaC}

Úloha 4.3.1. Ukážte, že $\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}}$.

4.4 Spočítateľné a nespočítateľné množiny

Definícia 4.4.1. Ak pre množinu A platí $|A| \leq \aleph_0$, tak hovoríme, že A je *spočítateľná.* Spočítateľná množina môže byť buď *konečná spočítateľná* množina, ak $|A| < \aleph_0$, alebo *nekonečná spočítateľná,* ak $|A| = \aleph_0$.

Ak pre množinu A platí $|A| > \aleph_0$, tak A je nespočítateľná.

Opäť platí rovnaká poznámka, ako pri konečných množinách. Ak nespočítateľné množiny definujeme takýmto spôsobom, je to síce to isté ako povedať, že sú to tie množiny, ktoré nie sú spočítateľné, tento faktu ukážeme však až neskôr, s použitím axiómy výberu (pozri poznámku 4.1.11).

Ukážeme, že spočítateľné zjednotenie spočítateľných množín je opäť spočítateľná množina. Dôkaz tohoto faktu súvisí s dôkazom existencie bijekcie medzi $\mathbb{N}\times\mathbb{N}$ a $\mathbb{N}$ (pozri príklad 4.2.12). Je rozumné zdôrazniť, že v tomto dôkaze využijeme axiómu výberu. (Bijekciu medzi $\mathbb{N}\times\mathbb{N}$ a $\mathbb{N}$ sme popísali presným predpisom, čiže tam sme axiómu výberu nepotrebovali.)

{spoc:VTSPOCZJEDSPOC}

Veta 4.4.2. *Nech I je spočítateľná množina a A_i je spočítateľná množina pre každé $i \in I$. (T.j. $\{A_i; i \in I\}$ je spočítateľný systém spočítateľných množín.) Potom aj množina $\bigcup\limits_{i\in I} A_i$ je spočítateľná.*

Dôkaz. Predpokladáme, že $|I| \leq \aleph_0$ a $|A_i| \leq \aleph_0$. Teda existuje injekcia $f\colon I \to \mathbb{N}$ a pre každé $i \in I$ môžeme vybrať nejakú injekciu $f_i\colon A_i \to \mathbb{N}$. (Na tomto mieste využívame axiómu výberu. Formálnejšie by sme jej použitie vedeli popísať použitím výberovej funkcie na systéme množín $\{B_i; i \in I\}$, kde $B_i = \{j\colon A_i \to \mathbb{N}; j \text{ je injekcia}\}$. Ide o systém neprázdnych množín, teda podľa ekvivalentnej formulácie axiómy výberu – veta 5.1.2(iii) – existuje selektor, čiže funkcia, ktorá z každej množiny B_i vyberie nejaký prvok.)

Pomocou zobrazení f a f_i, $i \in I$, zadefinujeme injekciu z $\bigcup\limits_{i\in I} A_i$ do $\mathbb{N}\times\mathbb{N}$. Nech $a \in \bigcup\limits_{i\in I} A_i$. Ako i_a označme také $i \in I$ pre ktoré je $f(i)$ minimálne. (Také i existuje, lebo $\mathbb{N}$ je dobre usporiadaná množina a $\{f(i); a \in A_i\}$ je neprázdna podmnožina $\mathbb{N}$.) Teraz definujme $g\colon \bigcup\limits_{i\in I} A_i \to \mathbb{N}\times\mathbb{N}$ ako

$$g(a) = (f(i_a), f_{i_a}(a)).$$

Toto zobrazenie je injektívne. Ak totiž $g(a) = g(b)$, tak a aj b patria do tej istej množiny A_{i_a} (lebo $f(i_a) = f(i_b)$ a f je injektívne). Potom platí $f_{i_a}(a) = f_{i_a}(b)$ a z injektívnosti zobrazenia f_{i_a} máme $a = b$.

Ukázali sme existenciu injekcie $g\colon \bigcup\limits_{i\in I} A_i \to \mathbb{N}\times\mathbb{N}$. Ak ju zložíme s ľubovoľnou bijekciou $h\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ (dve také bijekcie sme zostrojili v príklade 4.2.12), tak dostaneme injekciu z $\bigcup\limits_{i\in I} A_i$ do $\mathbb{N}$. To znamená, že $|\bigcup\limits_{i\in I} A_i| \leq \aleph_0$ a množina $\bigcup\limits_{i\in I} A_i$ je spočítateľná. □

Tvrdenie 4.4.3. *Množina $\mathbb{Q}$ všetkých racionálnych čísel je nekonečná spočítateľná, t.j.*

$$|\mathbb{Q}| = \aleph_0.$$

Dôkaz. Pretože $\mathbb{N} \subseteq \mathbb{Q}$, platí $\aleph_0 \leq |\mathbb{Q}|$.

Súčasne každé racionálne číslo vieme zapísať jednoznačne v tvare $\frac{p}{q}$, kde $p, q \in \mathbb{Z}$, $q > 0$ a čísla p, q sú nesúdeliteľné. Máme teda injekciu z $\mathbb{Q}$ do $\mathbb{N}\times\mathbb{N}$, a o tejto množine už vieme, že má kardinalitu $\aleph_0$ (príklad 4.2.12). Dostávame teda aj druhú nerovnosť $|\mathbb{Q}| \leq \aleph_0$.

Na základe Cantor-Bernsteinovej vety potom máme $|\mathbb{Q}| = \aleph_0$. □

Spočítateľnosť množiny $\mathbb{Q}$ by sme mohli dokázať aj pomocou vety 4.4.2 (rozmyslite si ako). Výhoda dôkazu, ktorý sme uviedli, je v tom, že nevyužíva axiómu výberu.

Pod intervalom v $\mathbb{R}$ budeme rozumieť akúkoľvek množinu I s vlastnosťou

$$a \in I \wedge b \in I \wedge a < x < b \qquad \Rightarrow \qquad x \in I.$$

Tejto definícii vyhovujú aj jednoprvkové množiny, ktoré sa zvyknú nazvývať *degenerované* alebo *triviálne* intervaly. Všetky netriviálne intervaly sú tvaru (a, b), $\langle a, b\rangle$, $\langle a, b)$, $(a, b\rangle$, $(=\infty, a)$, $(-\infty, a\rangle$, $\langle a, \infty)$ alebo (a, ∞) pre nejaké $a, b \in \mathbb{R}$.

Tvrdenie 4.4.4. *Ak A je množina disjunktných netriviálnych intervalov na $\mathbb{R}$, tak množina I je spočítateľná.*

Dôkaz. Každý netriviálny interval obsahuje nejaké racionálne číslo. (Medzi ľubovoľnými dvoma rôznymi reálnymi číslami sa nachádza racionálne číslo.) Ak intervalu $I \in A$ priradíme nejaké racionálne číslo $q_I \in I$, dostaneme injekciu z A do $\mathbb{Q}$. Keďže množina $\mathbb{Q}$ je spočítateľná, musí potom byť spočítateľná aj množina A. □

V predchádzajúcom dôkaze sme použili axiómu výberu na to, aby sme pre každé $I \in A$ vybrali nejaké racionálne číslo $q_I \in I \cap \mathbb{Q}$. Použitiu axiómy výberu sa dá v tomto dôkaze veľmi ľahko vyhnúť. Stačí si všimnúť, že v predchádzajúcom dôkaze sme explicitne popísali injektívne zobrazenie $i\colon \mathbb{Q} \to \mathbb{N}\times\mathbb{N}$. Na množine $\mathbb{N}\times\mathbb{N}$ máme dobré usporiadanie určené lexikografickým súčinom $(\mathbb{N}, \leq)$ a $(\mathbb{N}, \leq)$. Z toho dostávame dobré usporiadanie na podmnožine $i[\mathbb{Q}]$, ktoré cez injekciu i vieme preniesť na množinu $\mathbb{Q}$. Namiesto použitia axiómy výberu môžeme zadefinovať q_I takým spôsobom, že je to najmenší prvok množiny $I \cap \mathbb{Q}$ vzhľadom na uvedené dobré usporiadanie množiny $\mathbb{Q}$.

Cvičenia

Úloha 4.4.1. Ukážte, že ak pre kardinálne číslo a platí $a.\aleph_0 = a$, tak $2^a = {\aleph_0}^a$.

cvic:ULONESPOCMINUSSPOC}

Úloha 4.4.2. Ukážte, že ak A je spočítateľná množina, B je nespočítateľná množina a $A \subseteq B$, tak $|B \setminus A| = |A|$.

ULOKONECPODN}

Úloha 4.4.3. Ukážte, že množina všetkých konečných podmnožín $\mathbb{N}$ je spočítateľná. (Návod: Jedna z možností je ukázať, že množina n-prvkových množín je spočítateľná pre každé prirodzené číslo n a použiť vetu 4.4.2.)

LOQdoQNESPOC}

Úloha 4.4.4. Ukážte, že množina všetkých zobrazení z $\mathbb{Q}$ do $\mathbb{Q}$ nie je spočítateľná. (Môžete vyskúšať použiť diagonálnu metódu aj priamy výpočet kardinality tejto množiny.)

Úloha 4.4.5. Postupnosť (a_n) čísel sa volá *takmer stacionárna,* ak $(\exists m \in M)(\forall n \geq m) a_n = a_m$. Inými slovami, od určitého čísla m sú už všetky členy tejto postupnosti rovnaké.

Dokážte, že:
a) množina všetkých takmer stacionárnych postupností čísel 0, 1 je spočítateľná;
b) množina všetkých takmer stacionárnych postupností prirodzených čísel je spočítateľná;
c) množina všetkých takmer stacionárnych postupností reálnych čísel má kardinalitu $\mathfrak{c}$.

4.5 Mohutnosť niektorých v praxi sa vyskytujúcich množín

V predchádzajúcej podkapitole sme skúmali kardinalitu niektorých množín, väčšinou takých, že mali kardinalitu $\aleph_0$. V tejto časti sa budeme venovať ďalším množinám, ktoré sa vyskytujú v matematickej praxi. Množiny, ktoré budeme skúmať v tejto časti, budú zväčša nespočítateľné a budú mať kardinalitu $\mathfrak{c} = 2^{\aleph_0}$.

Ako prvý výsledok si ukážeme veľmi dôležitý fakt, že kardinalita množiny reálnych čísel je $\mathfrak{c} = 2^{\aleph_0}$. (Stále platí to, čo sme spomínali v poznámke 1.4.1 – reálne čísla sme zatiaľ neskonštruovali v ZFC, až neskôr si ukážeme, ako sa to dá. Budeme pracovať s vedomosťami, ktoré máte o reálnych číslach z nižších ročníkov.)

Na úvod si všimnime, že $|(0,1)| = |\langle 0,1)| = |\langle 0,1\rangle| = |\mathbb{R}|$.

Keďže $(0,1) \subseteq \langle 0,1) \subseteq \langle 0,1\rangle \subseteq \mathbb{R}$, máme nerovnosti

$$|(0,1)| \leq |\langle 0,1)| \leq |\langle 0,1\rangle| \leq |\mathbb{R}|.$$

Ak nájdeme bijekciu medzi $(0,1)$ a $\mathbb{R}$, tak túto nerovnosť môžeme rozšíriť na

$$|\mathbb{R}| = |(0,1)| \leq |\langle 0,1)| \leq |\langle 0,1\rangle| \leq |\mathbb{R}|$$

a z Cantor-Bernsteinovej vety potom dostaneme, že všetky uvedené množiny majú rovnakú kardinalitu.

Takýchto bijekcií možno nájsť veľa. Jedna z nich je $f\colon (0,1) \to \mathbb{R}$

$$f(x) = \operatorname{tg}\left(\frac{x}{\pi} + \frac{1}{2}\right).$$

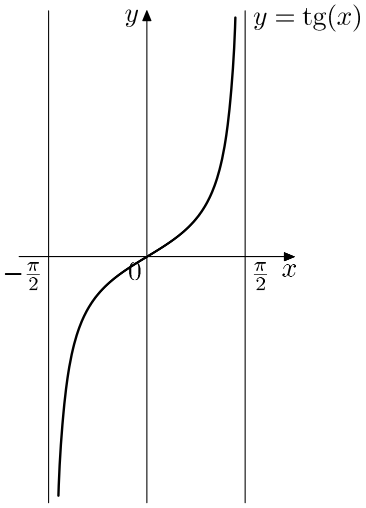
(Dostali sme ju vhodným posunutím a preškálovaním funkcie tangens – pozri obrázok 4.5). {niektore:FIGTAN}

Ak by ste chceli použiť nejakú elementárnejšiu funkciu, môžete skúsiť vhodne upraviť funkcie z obrázkov 4.4 a 4.5, ktoré sú navzájom inverzné.

Určite by ste ľahko našli bijekciu medzi $(0,1)$ a ľubovoľným otvoreným intervalom, medzi $\langle 0,1\rangle$ a ľubovoľným uzavretým intervalom.

Teda namiesto rovnosti $|\mathbb{R}| = \mathfrak{c}$ môžeme dokázať rovnakú rovnosť pre kardinalitu nejakého uzavretého, polouzavretého alebo otvoreného intervalu.

Predtým, než sa dostaneme k vlastnému dôkazu, povieme si ešte niečo o *binárnom* (*dyadickom*) zápise reálnych čísel. Je to vlastne rozšírenie zápisu v dvojkovej sústave, ktorý z predmetu Elementárna teória čísel poznáte pre prirodzené čísla. Pre reálne čísla túto konštrukciu možno poznáte z prváckej analýzy [VN, Kapitola V.8].



Obr. 4.3: Bijekcia medzi $(-\frac{\pi}{2}, \frac{\pi}{2})$ a $\mathbb{R}$

Budú nás zaujímať len reálne čísla z intervalu $\langle 0,1\rangle$, preto sa binárnemu zápisu budeme venovať iba pre tieto čísla.

Ak $(a_n)_{n=0}^{\infty}$ je ľubovoľná postupnosť núl a jednotiek, t.j. $(a_n)_{n=0}^{\infty} \in \{0,1\}^n$, tak takejto postupnosti priradíme číslo

$$r = \frac{a_0}{2} + \frac{a_1}{2^2} + \cdots = \sum_{n=0}^{\infty} \frac{a_n}{2^{n+1}}.$$

Očividne platí $0 \le r \le \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} = 1$, čiže takto dostaneme nejaké číslo z intervalu $\langle 0,1\rangle$. Čísla a_n budeme volať *cifry* binárneho zápisu reálneho čísla r.

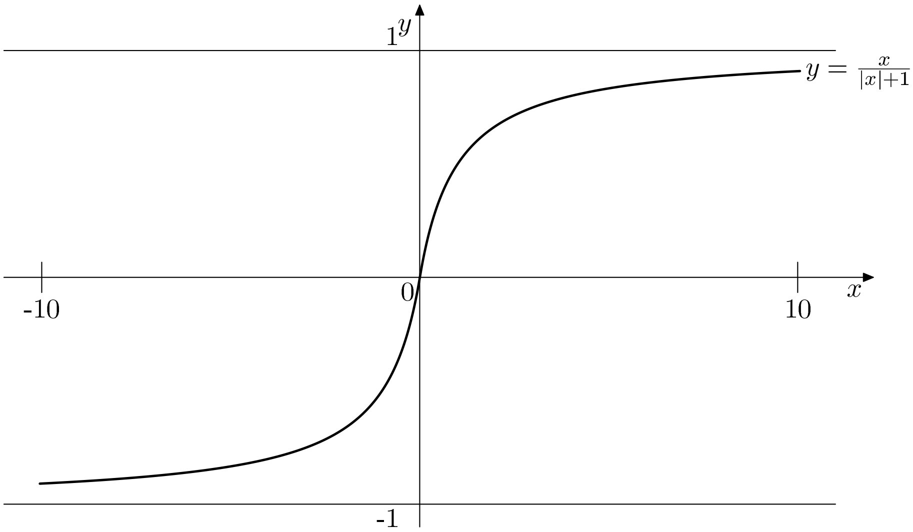
Musíme sa však ešte zamyslieť nad dvoma dôležitými otázkami: Dá sa takto zapísať každé číslo z intervalu $\langle 0,1\rangle$? Je takýto zápis reálnych čísel jednoznačný?

O tom, že takýto zápis existuje pre každé reálne číslo z intervalu $\langle 0,1)$ by nás mohla presvedčiť nasledujúca úvaha. Rozdeľme interval $\langle 0,1)$ na dve rovnaké polovice: $\langle 0,\frac{1}{2})$ a $\langle\frac{1}{2},1)$. Číslo r určite patrí do niektorého z týchto intervalov, jeho krajné body označme l_0 a r_0. Platí teda $l_0 \le r < r_0$. Pritom číslo l_0 je tvaru $\frac{a_0}{2}$, kde $a_0 \in \{0,1\}$, a platí $r_0 - l_0 = \frac{1}{2}$.

V druhom kroku rozdelíme interval $\langle l_0, r_0)$ opäť na dve rovnaké časti. Číslo r patrí do niektorého z intervalov $\langle l_0, \frac{l_0+r_0}{2})$ a $\langle \frac{l_0+r_0}{2}, r_0)$. Koncové body intervalu obsahujúceho r označíme ako l_1, r_1 a opäť si všimneme, že $l_1 = \frac{a_0}{2} + \frac{a_1}{2^2}$ pre nejaké $a_0, a_1 \in \{0,1\}$, a $r_1 - l_1 = \frac{1}{2^2}$.

Indukciou môžeme analogicky postupovať ďalej. V indukčnom kroku máme čísla l_n a r_n také, že $a \in \langle l_n, r_n)$, $l_n = \sum_{i=0}^{n} \frac{a_i}{2^{i+1}}$ pre nejaké $a_0,\dots,a_n \in \{0,1\}$ a $r_n - l_n = \frac{1}{2^{n+1}}$. Opäť platí, že r patrí do niektorého z intervalov $\langle l_n, \frac{l_n+r_n}{2})$ $\langle \frac{l_n+r_n}{2}, r_n)$ dĺžky $\frac{1}{2^{n+2}}$. Tento interval si označíme $\langle l_{n+1}, r_{n+1}\rangle$. Očividne platí $l_{n+1} = l_n$ alebo $l_{n+1} = l_n + \frac{1}{2^{n+2}}$, teda číslo l_{n+1} je tvaru $\sum_{i=0}^{n+1} \frac{a_i}{2^{i+1}}$ pre nejaké $a_0,\dots,a_{n+1} \in \{0,1\}$, pričom $a_0,\dots,a_n$ sú tie isté čísla, ktoré určovali číslo l_n.

Indukciou takto zostrojíme postupnosti $(a_n)_{n=0}^{\infty}$, $(l_n)_{n=0}^{\infty}$ a $(r_n)_{n=0}^{\infty}$ také, že pre všetky



Obr. 4.4: Bijekcia medzi $\mathbb{R}$ a $(-1, 1)$

{niektore:ROPINTA}

$n \in \mathbb{N}$ platí

$$0 \leq l_n \leq r < r_n \leq 1$$
$$r_n - l_n = \frac{1}{2^{n+1}}$$
$$l_n = \sum_{i=0}^{n} \frac{a_i}{2^{i+1}}$$
$$a_n \in \{0, 1\}$$

Z uvedených vlastností je zrejmé, že obe postupnosti l_n aj r_n konvergujú k číslu r. To znamená, že r je limita postupnosti čiastočných súčtov radu $\sum_{i=0}^{\infty} \frac{a_i}{2^{i+1}}$, čo je len iné vyjadrenie rovnosti

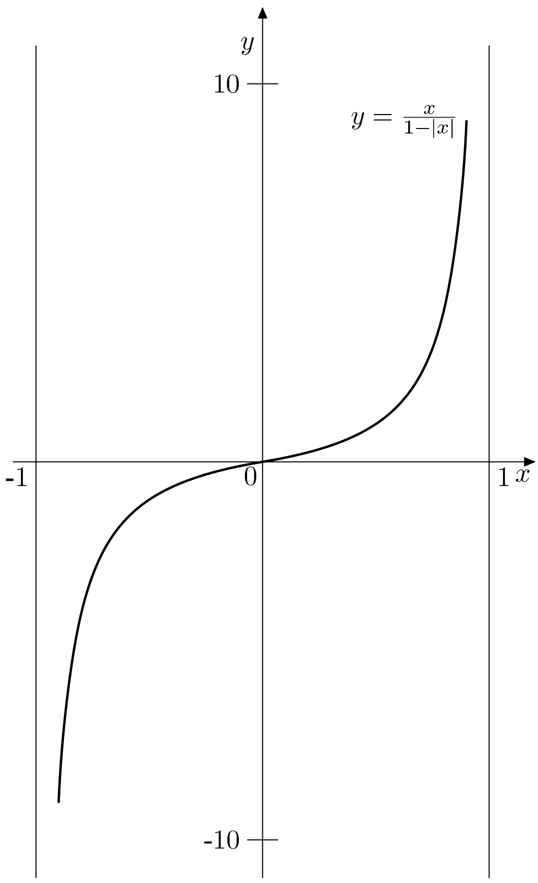
$$r = \sum_{i=0}^{\infty} \frac{a_n}{2^{i+1}}.$$

Vidíme teda, že každé číslo z intervalu $\langle 0, 1)$ má binárny rozvoj. Tento rozvoj však nemusí byť jednoznačný. Napríklad číslo

$$\frac{1}{2} = \frac{1}{2^2} + \frac{1}{2^3} + \dots$$

sa dá dostať pomocou dvoch rôznych postupností $(1, 0, 0, \dots)$ a $(0, 1, 1, \dots)$ z $\{0, 1\}^{\mathbb{N}}$. Podobným spôsobom vieme dostať dva rôzne rozvoje pre každé, ktoré sa dá binárne zapísať pomocou konečného počtu jednotiek. Stačí, keď posledné číslo tvaru $\frac{1}{2^{n+1}}$, $n \in \mathbb{N}$, ktoré sa vyskytuje v tomto zápise, nahradíme súčtom $\sum_{k=n+2}^{\infty} \frac{1}{2^k}$.

Ukážeme si, že toto je jediný prípad, kedy dochádza k nejednoznačnosti. Inými slovami, ak zakážeme konečné binárne rozvoje, tak pre každé číslo z intervalu $(0, 1)$ budeme už mať jediný rozvoj. To isté platí, ak zakážeme také rozvoje, ktoré počnúc od istého miesta už pozostávajú len zo samých jednotiek.



Obr. 4.5: Bijekcia medzi $(-1, 1)$ a $\mathbb{R}$

{niektore:ROP

Predpokladajme, že platí

$$\sum_{k=0}^{\infty} \frac{a_k}{2^{k+1}} = \sum_{k=0}^{\infty} \frac{b_k}{2^{k+1}},$$

pričom postupnosti $(a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty} \in \{0,1\}^{\mathbb{N}}$ sa nerovnajú. Nech n_0 je prvý index, na ktorom sa tieto postupnosti líšia. Bez ujmy na všeobecnosti, nech $a_{n_0} = 1$ a $b_{n_0} = 0$. Označme

$$A = \sum_{k=n_0}^{\infty} \frac{a_k}{2^{k+1}}$$

$$B = \sum_{k=n_0}^{\infty} \frac{b_k}{2^{k+1}} = \sum_{k=n_0+1}^{\infty} \frac{b_k}{2^{k+1}}$$

Vieme, že platí $A = B$. Súčasne však $B \leq \sum_{k=n_0+1}^{\infty} \frac{1}{2^{k+1}} = \frac{1}{2^{n_0+1}}$, pričom rovnosť nastane jedine v prípade, že $b_{n_0+1} = b_{n_0+2} = \cdots = 1$. Súčasne platí $A \geq \frac{1}{2^{n_0+1}}$ a rovnosť nastane jedine pre $a_{n_0} = 1$ a $a_{n_0+1} = a_{n_0+2} = \cdots = 0$. teda ide skutočne presne o taký prípad, aký sme pred chvíľou popísali.

Z toho, čo sme doteraz uviedli, je zrejmé, že existuje bijekcia medzi číslami z intervalu $(0,1\rangle$ a postupnosťami núl a jednotiek s výnimkou tých, ktoré označujú len konečne veľa jednotiek. Postupnostiam z $\{0,1\}^{\mathbb{N}}$ zasa môžeme bijektívne priradiť podmnožiny $\mathbb{N}$ (pozri dôkaz vety 4.2.4). Teda máme

$$|(0,1\rangle| = |\{B \subseteq \mathbb{N}; B \text{ nie je konečná}\}|.$$

Keďže z nespočítateľnej množiny $\mathcal{P}(\mathbb{N})$ sme vynechali množinu všetkých konečných podmnožín $\mathbb{N}$, ktorá je spočítateľná (úloha 4.4.3), dostávame podľa úlohy 4.4.2, že $|(0,1\rangle| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} = \mathfrak{c}$.

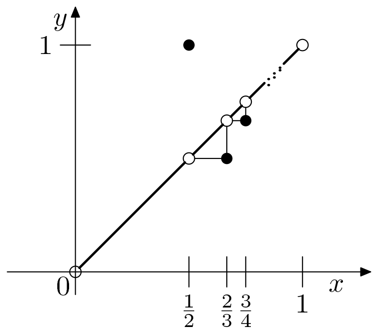
Už sme videli, že $\mathbb{R}$ má rovnakú kardinalitu ako ľubovoľný interval, dostávame teda

Tvrdenie 4.5.1.

$$|(0,1)| = |\langle 0,1\rangle| = |\mathbb{R}| = 2^{\aleph_0} = \mathfrak{c}$$

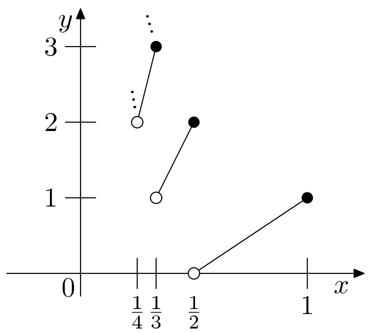
To isté platí aj pre ľubovoľné intervaly tvaru (a,b), $\langle a,b\rangle$, $(a,b\rangle$ či $\langle a,b)$.

V dôkaze sme používali Cantor-Bernsteinovu vetu, môžete sa pokúsiť nájsť priamo bijekcie medzi množinami $(0,1)$, $(0,1\rangle$, $\langle 0,1)$, $\langle 0,1\rangle$ a $\mathbb{R}$. Je veľa spôsobov, ako sa to dá urobiť, ku niektorým možnostiam by vás mohli inšpirovať obrázky 4.5 či 4.5.



Obr. 4.6: Bijekcia medzi $(0,1)$ a $(0,1\rangle$

{niektore:FIGBIJ0101}



Obr. 4.7: Bijekcia medzi $(0,1\rangle$ a $(0,1\rangle$

{niektore:FIGBIJ010INFTY

Tvrdenie 4.5.2. *Kardinalita množiny všetkých spojitých zobrazení z $\mathbb{R}$ do $\mathbb{R}$ je $\mathfrak{c}$.*

Tento fakt do istej miery kontrastuje s tým, že všetkých zobrazení z $\mathbb{R}$ do $\mathbb{R}$ je $\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}} > \mathfrak{c}$ (pozri úlohu 4.3.1). Dá sa teda povedať, že nespojitých zobrazení je oveľa viac ako spojitých.

Dôkaz. Stačí si uvedomiť, že ak vieme aké hodnoty nadobúda spojité zobrazenie $f\colon \mathbb{R} \to \mathbb{R}$ na racionálnych číslach, tak tým je už toto zobrazenie jednoznačne určené. (Racionálne čísla tvoria hustú podmnožinu reálnych čísel, pre každé reálne číslo existuje postupnosť racionálnych čísel, ktorá k nemu konverguje.) Máme teda injekciu medzi spojitými zobrazeniami z $\mathbb{R}$ do $\mathbb{R}$ a ľubovoľnými zobrazeniami z $\mathbb{Q}$ do $\mathbb{R}$ určenú predpisom $f \mapsto f|_{\mathbb{Q}}$. Kardinalita množiny zobrazení z $\mathbb{Q}$ do $\mathbb{R}$ je

$$|\mathbb{R}|^{|\mathbb{Q}|} = \mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{c}.$$

Teda spojitých zobrazení z $\mathbb{R}$ do $\mathbb{R}$ je nanajvýš $2^{\aleph_0} = \mathfrak{c}$.

Súčasne vieme ľahko nájsť pre každú podmnožinu $A \subseteq \mathbb{N}$ spojitú funkciou $f\colon \mathbb{R} \to \mathbb{R}$ takú, že $f|_{\mathbb{N}} = \chi_A$. (Jednou z možností je lomená čiara.) Z toho máme, že hľadaná kardinalita je aspoň $2^{\aleph_0} = \mathfrak{c}$. □

{niektore:PRIKLRNESPOC}

Príklad 4.5.3. Síce už vieme, že $|\mathbb{R}| = |\langle 0,1)| = \mathfrak{c}$, a teda tieto množiny sú nespočítateľné, na tomto mieste môžeme však využiť desiatkový rozvoj reálnych čísel na to, aby sme si tento fakt ukázali použitím Cantorovej diagonálnej metódy (poznámka 4.5.3). Postup je veľmi podobný ako v príklade 4.3.2.

Ukážeme, že množina $\langle 0,1)$ je nespočítateľná. Vieme, že každé číslo z tejto množiny sa dá jediným spôsobom zapísať v tvare $x = \sum_{k=0}^{\infty} \frac{a_k}{10^{k+1}}$ a navyše ak vylúčime konečné rozvoje (t.j. také, kde sú od istého miesta všetky čísla nulové), tak je tento rozvoj jednoznačný. Desiatkový zápis budeme zapisovať v tvare $0.a_0a_1a_2\dots$ (Môžete sa pokúsiť sami si overiť existenciu a jednoznačnosť takéhoto zápisu – postup je podobný ako v prípade dyadického zápisu. Všeobecnejšie tvrdenie, hovoriace o rozvoji pri ľubovoľnom základe, nájdete napríklad v [ŠHHK, kapitola 3.6].)

Predpokladajme, že interval $\langle 0,1)$ je spočítateľný. To znamená, že existuje bijekcia $f\colon \mathbb{N} \to \langle 0,1)$. Každé z čísel $f(0), f(1), f(2), \dots \in \langle 0,1)$ sa dá zapísať pomocou desiatkového zápisu

$$\begin{aligned} f(0) &= 0.a_0^{(0)}a_1^{(0)}a_2^{(0)}\dots \\ f(1) &= 0.a_0^{(1)}a_1^{(1)}a_2^{(1)}\dots \\ f(2) &= 0.a_0^{(2)}a_1^{(2)}a_2^{(2)}\dots \\ &\vdots \end{aligned}$$

Pomocou týchto desatinných zápisov zadefinujeme nové číslo

$$b = 0.b_0b_1b_2\dots$$

tak, že $b_k \neq a_k^{(k)}$ a súčasne $b_k \neq 0$. Môžeme napríklad položiť $b_k = a_k^{(k)} + 1$ ak $a_k^{(k)} < 9$ a $b_k = 8$ ak $a_k^{(k)} = 9$. Číslo, ktoré sme takto dostali má nekonečný zápis v desiatkovej sústave rôzny od všetkých čísel $f(n)$, $n \in \mathbb{N}$. (Od čísla $f(n)$ sa líši prinajmenšom na n-tom mieste zápisu, možno aj na nejakých ďalších.)

Teda $b \neq f(n)$ pre žiadne n, čo je v spore s predpokladom, že f je bijekcia.

Cvičenia

Úloha 4.5.1. Ukážte, že kardinalita množiny všetkých iracionálnych čísel je $\mathfrak{c}$.

4.6 Aplikácie kardinálnych čísel

4.6.1 Existencia transcendentných čísel

Najprv pripomeňme definíciu algebraických a transcendentných čísel.

Definícia 4.6.1. Komplexné číslo x sa nazýva *algebraické,* ak existuje polynóm $F(x) \in \mathbb{Z}[x]$ s celočíselnými koeficientami taký, že $f(x) = 0$, t.j. x je koreňom tohoto polynómu. Komplexné číslo, ktoré nie je algebraické, sa nazýva *transcendentné.*

Ukážeme, že množina algebraických čísel je spočítateľná. Z toho vyplýva, že existujú aj transcendentné čísla.

Tvrdenie 4.6.2. *Množina $\mathbb{A}$ všetkých algebraických čísel je spočítateľná.*

Dôkaz. Využijeme fakt, že každý polynóm $f \in \mathbb{C}[x]$ stupňa n má v $\mathbb{C}$ najviac n koreňov. (Presne n, ak by sme započítali aj ich násobnosť.)

Najprv vypočítajme kardinalitu množiny $\mathbb{Z}[x]$ všetkých polynómov s celočíselnými koeficientami. Každý polynóm stupňa n je jednoznačne určený postupnosťou koeficientov $a_n \in \mathbb{Z} \setminus \{0\}$, $a_{n-1}, \dots, a_0 \in \mathbb{Z}$. Kardinalita množiny P_n všetkých polynómov stupňa n s celočíselnými koeficientami je teda $\aleph_0^n = \aleph_0$.

Množinu $\mathbb{Z}[x]$ môžeme vyjadriť ako $\mathbb{Z}[x] = \bigcup_{n\in\mathbb{N}} P_n$, čiže ide o spočítateľné zjednotenie spočítateľných množín. Teda dostávame $|\mathbb{Z}[x]| = \aleph_0$.

Každé algebraické číslo je koreňom nejakého polynómu zo $\mathbb{Z}[x]$. Takýto polynóm má najviac n koreňov. Dostávame teda

$$|\mathbb{A}| \leq |\mathbb{Z}[x]|.\aleph_0 = \aleph_0.$$

Súčasne platí $|\mathbb{A}| \geq \aleph_0$, keďže každé celé číslo je algebraické. □

Z predchádzajúceho tvrdenia už dostaneme existenciu transcendentných čísel (pozri úlohu 4.6.2).

Dôsledok 4.6.3. *Kardinalita množiny $\mathbb{C} \setminus \mathbb{A}$ je $\mathfrak{c}$. Z toho dostávame, že existuje aspoň jedno transcendentné číslo.*

4.6.2 Vypočítateľné funkcie

V tejto časti si povieme – aspoň veľmi zjednodušene a neformálne – niečo o vypočítateľných funkciách.

Zjednodušene by sme mohli zaviesť pojem vypočítateľnej funkcie takto:

Definícia 4.6.4. Funkcia $f\colon \mathbb{N} \to \mathbb{N}$ sa nazýva *vypočítateľná,* ak existuje *algoritmus* ktorý pre vstup n vráti $f(n)$.

Otázka je, ako by sme mohli spresniť definíciu pojmu *algoritmus,* ktorý sa vyskytuje v predchádzajúcej definícii. Existuje viacero teoretických modelov algoritmu, snáď najrozšírenejší je Turingov stroj. Pre jednoduchosť si však môžete na tomto mieste predstaviť pod pojmom algoritmus program (procedúru) vo vašom obľúbenom programovacom jazyku.

Program nie je vlastne nič iné, než konečný reťazec znakov, ktorý navyše musí spĺňať určité pravidlá. Keďže používame iba konečne veľa znakov, všetkých možných programov je najviac toľko ako konečných postupností prvkov z danej konečnej množiny, čo je $\aleph_0$.

Súčasne vieme, že všetkých zobrazení z $\mathbb{N}$ do $\mathbb{N}$ je $\aleph_0^{\aleph_0} = \mathfrak{c} > \aleph_0$. Z toho vidíme, že existujú funkcie, ktoré nie sú vypočítateľné (nedajú sa naprogramovať). Zaujímavé je snáď aj to, že sa nám ich existenciu podarilo dokázať bez toho, aby sme nejakú konkrétnu nevypočítateľnú funkciu zostrojili.

Cvičenia

Úloha 4.6.1. Funkcia $f\colon \mathbb{R} \to \mathbb{R}$ sa nazýva funkciou *prvej Bairovej triedy,* ak existuje postupnosť spojitých funkcií $(f_n\colon \mathbb{R} \to \mathbb{R})_{n\in\mathbb{N}}$, ktorá k nej bodovo konverguje (t.j. pre každé $x \in \mathbb{R}$ číselná postupnosť $f_n(x)$ konverguje k $f(x)$). Aká je kardinalita množiny všetkých funkcií prvej Bairovej triedy? Viete na základe kardinality ukázať, že existuje funkcia, ktorá nie je prvej Bairovej triedy?

ikkardcvic:ULOTRANSKARD}

Úloha 4.6.2. Ukážte, že množina všetkých transcendentných čísel má kardinalitu $\mathfrak{c}$.

Literatúra

[B1] Lev Bukovský. Úvod do matematickej logiky. `http://ics.upjs.sk/~novotnyr/home/skola/logika_a_teoria_mnozin/ltm.pdf`.

[B2] Lev Bukovský. *Štruktúra reálnej osi.* Veda, Bratislava, 1979.

[B3] Lev Bukovský. *Množíny a všeličo okolo nich.* Alfa, Bratislava, 1985.

[BŠ] Bohuslav Balcar and Petr Štěpánek. *Teorie množin.* Academia, Praha, 2001.

[Č1] Juraj Činčura. Elementárna teória čísel. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/cvicenia/tc/`.

[Č2] Juraj Činčura. Model aritmetiky celých nezáporných čísel v teórii množín. `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/2010/temno/cisla.pdf`.

[D] Keith Devlin. *The Joy of Sets.* Springer-Verlag, New York, 1993. Undergraduate Texts in Mathematics.

[E] Herbert B. Enderton. *A Mathematcial Introduction to Logic.* Harcourt/Academic Press, San Diego, 2001.

[F] Thomas Forster. *Logic, Induction and Sets.* Cambridge University Press, Cambridge, 2003. LMS Student Texts 56.

[GG] Ivor Grattan-Guiness. *The Search for Mathematical Roots 1870–1940.* Princeton University Press, Princeton, 2000.

[H1] Horst Herrlich. Choice principles in elementary topology and analysis. *Comment. Math. Univ. Carolinae*, 38(3):545–552, 1997.

[H2] Horst Herrlich. *The Axiom of Choice.* Springer-Verlag, Berlin, 2006. Lecture Notes in Mathematics 1876.

[HMU] John E. Hopcroft, Rajeev Motwani, and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Massachusetts, 2nd edition, 2001.

[HR] Paul Howard and Jean E. Rubin. *Consequences of the axiom of choice.* Mathematical Surveys and Monographs. 59. Providence, RI: American Mathematical Society (AMS), 1998.

[J] Thomas J. Jech. *The Axiom of Choice.* North-Holland, Amsterdam, 1973.

[KGGS] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a teoretická aritmetika 1.* UK, Bratislava, 2002.

[KLŠZ] Milan Kolibiar, Anton Legéň, Tibor Šalát, and Štefan Znám. *Algebra a príbuzné disciplíny.* Alfa, Bratislava, 1992.

[Le] Azriel Levy. *Basic set theory.* Courier Dover Publications, 2002.

[Li] Seymour Lipschutz. *Schaum's Outline of Theory and Problems of Set Theory and Related Topics.* McGraw-Hill, New York, 1998.

[M] Gregory H. Moore. *Zermelo's Axiom of Choice. Its Origins, Development and Influence.* Springer-Verlag, New York, 1982.

[OŠ] Daniel Olejár and Martin Škoviera. *Úvod do teórie diskrétnych matematických štruktúr.* Univerzita Komenského, Bratislava, 2007. `http://www.dcs.fmph.uniba.sk/texty/dsmain.pdf`.

[RF] Branislav Rovan and Michal Forišek. Formálne jazyky a automaty. Poznámky k prednáške, `http://foja.dcs.fmph.uniba.sk/materialy.php`.

[Sl] Martin Sleziak. Lineárna algebra. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[So] Antonín Sochor. *Klasická matematická logika.* Karolinum, Praha, 2001.

[Š] Petr Štěpánek. Predikátová logika. `http://kti.ms.mff.cuni.cz/teaching/files/materials/StepanekPetr_PredikatovaLogika.pdf`.

[ŠHHK] T. Šalát, A. Haviar, T. Hecht, and T. Katriňák. *Algebra a teoretická aritmetika 2.* Alfa, Bratislava, 1986.

[ŠS] Tibor Šalát and Jaroslav Smítal. *Teória množín.* UK, Bratislava, 1995.

[VN] J. Vencko and T. Neubrunn. *Matematická analýza.* MFF UK, Bratislava, 1992.

[WIK] Wikipedia. `http://en.wikipedia.org`.

[WR] A. N. Whitehead and B. Russell. *Principia mathematica, vol.1.* Cambridge University Press, Cambridge, 1st edition.

[Z] Pavol Zlatoš. *Ani matematika si nemôže byť istá sama sebou.* IRIS, Bratislava, 1995. `http://thales.doa.fmph.uniba.sk/zlatos/animat/animat.pdf`.

Register

Zoznam symbolov