

2-UMA-115 Teória množín

Martin Sleziak

7. októbra 2010

Obsah

1 Úvod	4
1.1 Predhovor	4
1.2 Sylaby a literatúra	5
1.2.1 Literatúra	5
1.2.2 Sylaby predmetu	5
1.2.3 Štátnicové otázky	5
1.3 Niečo z histórie	6
1.4 Základné označenia	7
2 Axiomatický prístup k teórii množín	9
2.1 Logika prvého rádu	9
2.1.1 Výroková logika	9
2.1.2 Výroky s kvantifikátormi	11
2.2 Naivná teória množín a jej paradoxy	15
2.3 Zermelov-Fraenkelov axiomatický systém	16
2.3.1 Jazyk teórie množín	17
2.3.2 Axiómy systému ZFC	17
2.4 Operácie s množinami	21
2.5 Usporiadané dvojice a karteziánsky súčin	28
2.5.1 Triedy*	31
3 Relácie a funkcie	32
3.1 Relácie	32
3.2 Funkcie	37
3.2.1 Karteziánsky súčin systému množín	41
3.2.2 Karteziánsky súčin funkcií	42
3.3 Čiastočne usporiadané množiny	44
3.4 Dobře usporiadané množiny	49
4 Kardinálne čísla	54
4.1 Porovnávanie mohutností množín	54
4.2 Kardinálna aritmetika	59
4.3 Cantorova veta a diagonálna metóda	60
4.4 Spočítateľné a nespočítateľné množiny	60
4.5 Mohutnosť niektorých v praxi sa vyskytujúcich množín	60
4.6 Aplikácie kardinálnych čísel	61

5	Axióma výberu	64
5.1	Ekvivalentné formy axiómy výberu	64
5.2	Aplikácie axiómy výberu	70
5.2.1	Cauchyho a Heineho definícia spojitosti	70
5.2.2	Hamelova báza	70
5.2.3	Linearizácia čiastočne usporiadanej množiny	70
5.2.4	Neprijemné dôsledky axiómy výberu	71
6	Ordinálne čísla	72
6.1	Dobre usporiadané množiny II	72
6.2	Definícia ordinálnych čísel	74
6.3	Transfinitná indukcia	76
6.3.1	Definícia transfinitnou indukciou	76
6.4	Ordinálna aritmetika	76
6.4.1	Súčet ordinálnych čísel	76
6.4.2	Súčin ordinálnych čísel	76
6.4.3	Prirodzené čísla a Peanova aritmetika	76
6.4.4	Zavedenie číselných oborov	76
6.4.5	Umocňovanie ordinálnych čísel	76
6.5	Von Neumannova definícia ordinálnych čísel	76
6.6	Aplikácie kardinálnych čísel a transfinitnej indukcie	76
	Literatúra	77
	Register	79
	Zoznam symbolov	81

Kapitola 1

Úvod

Verzia: 7. októbra 2010

1.1 Predhovor

Zjednodušene sa dá povedať, že teória množín je vlastne disciplína, ktorá sa zaoberá prácou s nekonečnými množinami. Jej vznik si vyžiadala 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 pokúsíte 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 systém teórie množín. Kardinálne čísla a kardinálna aritmetika. Konečné a nekonečné množiny. Množina prirodzených čísel a matematická indukcia. Spočítateľné a nespočítateľné množiny. Mohutnosť kontinua a kardinálna množín vyskytujúcich sa v školskej matematike.

1.2.3 Štátnicové otázky

Štátnicové otázky z predmetu matematika, ktoré by ste sa mali naučiť na tomto predmete 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 teórie 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.

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.

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.

1.3 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 teórie množín“.)

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 Matematikovi 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 idea 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 Ber-

²Takto 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 jednosmernom kurze.

trand 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 $1 + 1 = 2$ 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 pohnutí, 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 teórie 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

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

\mathbb{R} = reálne čísla

\mathbb{C} = komplexné čísla

{prelim:POZNMNOZN}

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 spomenutými 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 zdefinujeme 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	$\neg p$	p	q	$p \wedge q$	p	q	$p \vee q$	p	q	$p \Rightarrow q$	p	q	$p \Leftrightarrow q$
1	0	1	1	1	1	1	1	1	1	1	1	1	1
1	0	1	0	0	1	0	1	1	0	0	1	0	0
0	1	0	1	0	0	1	1	0	1	1	0	1	0
		0	0	0	0	0	0	0	0	1	0	0	1

¹Na 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.

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

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 (prípád $1 \Rightarrow 0$). 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 vyskytnú 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 $q \Rightarrow p$.

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 zápisy²

$$\begin{aligned}(\forall x \in A)P(x) &\stackrel{\text{def}}{\Leftrightarrow} (\forall x)(x \in A \Rightarrow P(x)) \\ (\exists x \in A)P(x) &\stackrel{\text{def}}{\Leftrightarrow} (\exists x)(x \in A \wedge P(x))\end{aligned}$$

Čiže $(\exists x \in A)P(x)$ je len skrátenejší 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 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

²Tu 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 .

túto vlastnosť nemá, a teda spĺňa $\neg P(x)$. (Ak nie je pravda, že všetky guľôčky 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 negáciám 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 prideme 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:CVTAUT}

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 dokažte; ak nie, uveďte kontrapríklad).

- $p \Leftrightarrow \neg\neg p$;
- $\neg p \Leftrightarrow (p \Rightarrow \neg p)$;
- $(p \wedge q) \Rightarrow p$;
- $p \Rightarrow \neg p$;
- $(p \vee q) \Rightarrow p$;
- $(p \Rightarrow q) \Rightarrow (p \Rightarrow (q \wedge r))$;
- $(p \Rightarrow (q \wedge r)) \Rightarrow (p \Rightarrow q)$;
- $\neg p \wedge (p \vee q) \Rightarrow q$;
- $[p \Rightarrow (r \vee \neg q)] \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)]$
- $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$

{logika:CVREDUND}

Úloha 2.1.4. Ukážte, že operácie \neg , \wedge , \vee , \Rightarrow , \Leftrightarrow môžeme definovať pomocou:

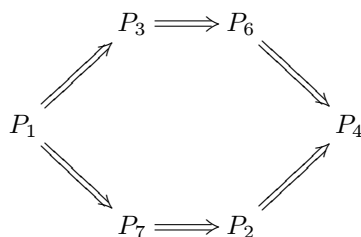
- negácie a konjunkcie,
- negácie a disjunkcie,
- negácie a implikácie,
- logickej spojky NAND definovanej ako $P \text{ NAND } Q \Leftrightarrow \neg(P \wedge Q)$,
- logickej spojky NOR definovanej ako $P \text{ NOR } Q \Leftrightarrow \neg(P \vee Q)$.

Úloha 2.1.5. Rozhodnite, či sú uvedené výroky pravdivé. Svoje tvrdenie zdôvodnite.

- $[(\forall x)P(x) \Rightarrow (\forall x)Q(x)] \Rightarrow (\forall x)(P(x) \Rightarrow Q(x))$
- $(\exists x)(P(x) \wedge Q(x)) \Leftrightarrow [(\exists x)P(x) \wedge (\exists x)Q(x)]$
- $(\exists x)(P(x) \vee Q(x)) \Leftrightarrow [(\exists x)P(x) \vee (\exists x)Q(x)]$
- $(\forall x)(P(x) \wedge Q(x)) \Leftrightarrow [(\forall x)P(x) \wedge (\forall x)Q(x)]$
- $(\forall x)(P(x) \vee Q(x)) \Leftrightarrow [(\forall x)P(x) \vee (\forall x)Q(x)]$
- $(\forall x)(P(x) \Rightarrow Q(x)) \Leftrightarrow [(\exists x)P(x) \Rightarrow (\exists x)Q(x)]$
- $[(\forall x)(\forall y)(R(x, y) \Rightarrow \neg R(y, x))] \Rightarrow (\forall x)\neg R(x, x)$

Úloha 2.1.6. Pre výrokovú funkciu $P(x, y)$ uvažujme výroky $P_1(x, y) = (\forall x)(\forall y)P(x, y)$, $P_2 = (\forall x)(\exists y)P(x, y)$, $P_3 = (\exists x)(\forall y)P(x, y)$, $P_4 = (\exists x)(\exists y)P(x, y)$, $P_5 = (\forall y)(\forall x)P(x, y)$, $P_6 = (\forall y)(\exists x)P(x, y)$, $P_7 = (\exists y)(\forall x)P(x, y)$, $P_8 = (\exists y)(\exists x)P(x, y)$.

- Ukážte, že pre tieto výroky platí: $P_1 \Leftrightarrow P_5$, $P_4 \Leftrightarrow P_8$ a



- Ukážte na príklade, že implikácie v predchádzajúcom diagrame nemožno nahradiť ekvivalenciami.

- Ukážte na príklade, že nemusia platiť ekvivalencie $P_3 \Rightarrow P_2$ a $P_7 \Rightarrow P_6$.

Toto cvičenie sa dá stručne zhrnúť tak, že všetky vzťahy medzi výroky P_2, \dots, P_7 sú tie, ktoré sú naznačené v uvedenom diagrame.

{logikacvic:ULODISTRIB}

Úloha 2.1.7. Nech p je výrok a $Q(x)$ je výroková funkcia. Overte, či platia ekvivalencie:

- $p \wedge (\exists x)Q(x) \Leftrightarrow (\exists x)(p \wedge Q(x))$;

- 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 2.1.8. 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 sčítaním, 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 $\mathbb{Q} \cap \langle 0, 1 \rangle$.

Russellov⁴ 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

³Samozrejme, 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 stretne až v ďalších kapitolách.

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

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 \mathbf{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 Zdefinujeme 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.

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 *patriť* (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.

⁵Primitívnym 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.

2.3.1 Jazyk teórie množín

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 axiém o množinách, z ktorých budeme o množinách môcť odvodiť rôzne tvrdenia. Tieto tvrdenia a axiémy 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 definícii:

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.

2.3.2 Axiómy systému ZFC

Teraz uvedieme jednotlivé axiomy 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 axiém 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 axiém 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 zjednotenie existuje množina C , ktorá obsahuje práve prvky patriace do niektorej z množín A, B . \square

Ďalšou aplikáciou axiómy dvojice je nasledujúce jednoduché tvrdenie:

{zfc: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. \square

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 axiomy 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 axiomy extenzionality. Ukážeme existenciu.

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

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

□

Môžeme poznamenať, že v niektorých textoch sa namiesto axiomy existencie uvádza ako axioma existencia prázdnej množiny. Z predchádzajúceho tvrdenia je zrejmé, že takto dostaneme ekvivalentný systém axióm – pomocou ostatných axióm vieme z axiomy 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 zdefinujeme 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 axiomy extenzionality. □

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 axiomy budeme potrebovať ešte jednu definíciu, ktorá nám umožní túto axiomu 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 $A \subseteq B$.

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

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 zavedme 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 byť 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 schéma 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 $x \notin x$. \square

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 axiomy sa zvyknú označovať ako axiomatický systém ZF. Po pridaní nasledujúcej axiomy 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 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 axiomy. 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 axiém si môžete prečítať napríklad v [Z, s.79–83]⁶. (Môžete si tam prečítať aj o axiómach, ktorými sa v tomto texte podrobne nezaobráame, ako je axióma regularity.)

2.4 Operácie s množinami

V tejto časti sa budeme venovať niektorým operáciám 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*.

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

Nasledujúce tvrdenie zhrňa základné vlastnosti inklúzie.

Tvrdenie 2.4.1. *Nech A, B, C sú ľubovoľné množiny. Potom platí:*

- (i) *Pre každú množinu platí $A \subseteq A$.*
- (ii) *$A = B$ práve vtedy, keď $A \subseteq B \wedge B \subseteq A$.*
- (iii) *Ak platí $A \subseteq B$ a $B \subseteq C$, tak $A \subseteq C$.*

{oper:TVRSUBSET}
{oper:itSUB1}
{oper:itSUB2}
{oper:itSUB3}

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 axiomy 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 $B \subseteq A$.

⁶Táto kniha je voľne dostupná na internete

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.

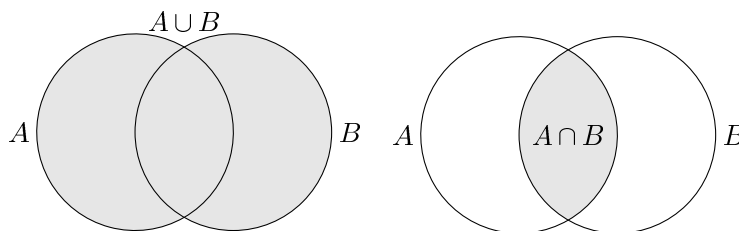
Budeme teraz pokračovať tým, že pripomenieme niektoré operácie, ktoré sme definovali v predchádzajúcej podkapitole a zadefinujeme niekoľko nových.

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.)



{oper:FIGZJEDPRIEN}

Obr. 2.1: Zjednotenie a prienik dvoch množín

Na tomto mieste si môžeme pripomenúť, že pre konečné množiny ste sa na diskkrétnej matematike 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.)

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.)

{oper: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*);

{oper:itDISTRIB} (iii) $\emptyset \cup A = A$, $\emptyset \cap A = \emptyset$;

(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

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

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

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

čo je presne tautológia z úlohy 2.1.2a).

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

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 $\bigcup \mathcal{S}$. Dost' 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 $\bigcup_{A \in \mathcal{S}} A$ a v prípade, že $\mathcal{S} = \{A_i; i \in I\}$, tak zjednotenie tohoto systému označíme $\bigcup_{i \in I} A_i$.

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:TVRDIST}

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. Použijeme 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

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

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

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

To je presne ekvivalencia z úlohy 2.1.7c). □

Dokážeme aj niektoré vzťahy medzi množinovými operáciami a reláciou inklúzie.

{oper:TVRSUBBEKV}
 {oper:it1SUBBEKV}
 {oper:it2SUBBEKV}
 {oper:it3SUBBEKV}

Tvrdenie 2.4.6. *Nech A a B sú množiny. Nasledujúce podmienky sú ekvivalentné:*

- (i) $A \subseteq B$;
- (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:*

{oper:it1SUB}
 {oper:it2SUB}
 {oper:it3SUB}

- (i) $\emptyset \subseteq A$;
- (ii) $A \cap B \subseteq A \subseteq A \cup B$;
- (iii) *Ak $A \subseteq B$, tak $A \cap C \subseteq B \cap C$ a $A \cup C \subseteq B \cup C$.*

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 $(x \in A) \Rightarrow (x \in B)$. 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 uvidíme iný dôkaz tvrdenia 2.4.4(vi).

Príklad 2.4.8. $A \cap (A \cup B) \stackrel{(1)}{=} (A \cap A) \cup (A \cap B) \stackrel{(2)}{=} A \cup (A \cap B) \stackrel{(3)}{=} A$, 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 .

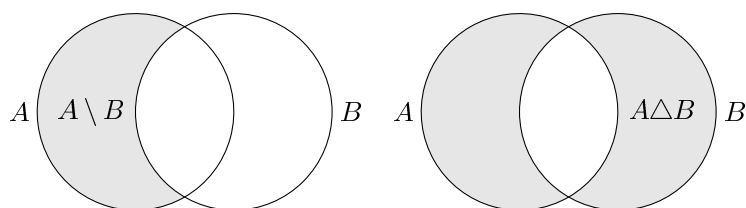
Ďalšie operácie, ktoré budeme niekedy používať sú rozdiel a symetrická diferenciacia (symetrický rozdiel) dvoch množín.

Definícia 2.4.9. Rozdiel množín A a B je množina

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

Symetrická diferenciacia množín A a B je množina

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$



Obr. 2.2: Vennove diagramy pre $A \setminus B$ a $A \Delta B$

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

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

{oper:itDEMOR

- (i) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$, $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
- (ii) $A \setminus (B \cup C) = (A \setminus B) \setminus C$;
- (iii) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$;
- (iv) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$, $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$;
- (v) $A \setminus B = A \setminus (A \cap B)$;
- (vi) $(A \setminus B) \cap C = (A \cap C) \setminus B = A \cap (C \setminus B)$;
- (vii) $(A \setminus B) \cup C = (A \cup C) \setminus (B \setminus C)$;
- (viii) $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$;

{oper:itDEMORGANSYS}

- (ix) $A \subseteq B \Leftrightarrow A \setminus B = \emptyset$.

(x) Ak pre každé $i \in I$ je B_i množina, tak platí $A \setminus \bigcap_{i \in I} B_i = \bigcup_{i \in I} (A \setminus B_i)$ a $A \setminus \bigcup_{i \in I} B_i = \bigcap_{i \in I} (A \setminus B_i)$.

{oper:itSMSUBSET}

- (xi) Ak $B \subseteq C$, tak $A \setminus C \subseteq A \setminus B$.
- (xii) Ak $B \subseteq C$, tak $B \setminus A \subseteq C \setminus A$.

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) $A \Delta B = B \Delta A$;
- (ii) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$;
- (iii) $A \Delta A = \emptyset$, $A \Delta \emptyset = A$;
- (iv) $A \cup B = A \Delta B \Delta (A \cap B)$;
- (v) $A \setminus B = A \Delta (A \cap B)$.

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

p	q	$p \text{ XOR } q$
1	1	0
1	0	1
0	1	1
0	0	0

Pri dokazovaní našej tautológie potom dostávame nasledujúcu tabuľku:

p	q	r	$p \text{ XOR } q$	$a := (p \text{ XOR } q) \text{ XOR } r$	$q \text{ XOR } r$	$b := p \text{ XOR } (q \text{ XOR } r)$	$a \Leftrightarrow b$
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

□

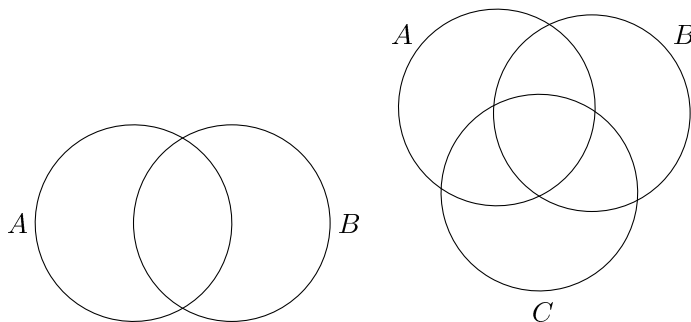
{oper:SSSECTVENN}

Vennove diagramy

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 po-*

lohe, t.j. aby sa tam vyskytli „všetky možné“ oblasti. (Například 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 Δ (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 $A\Delta B$ a potom, pomocou nej, sme dostali množinu $(A\Delta B)\Delta C$ vystupujúcu na ľavej strane rovnosti.

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

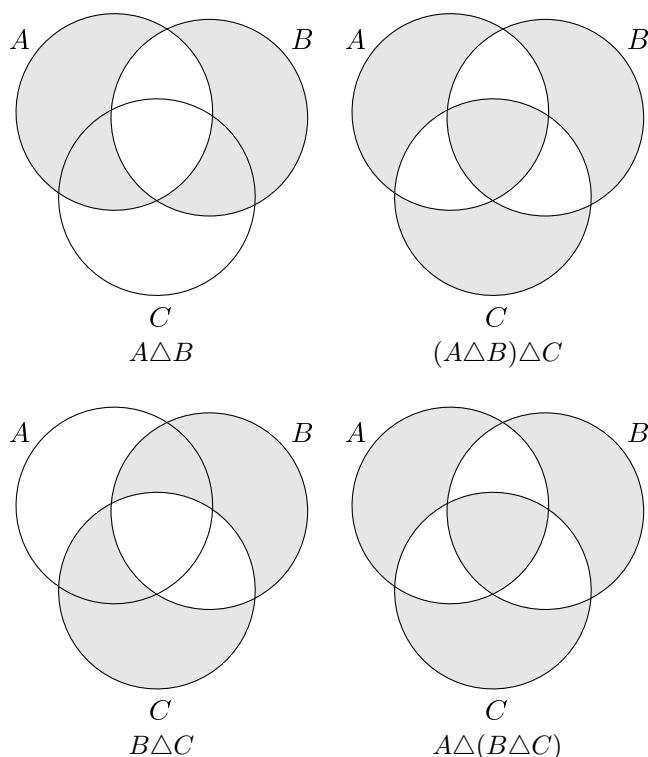
Môžete sa pýtať, do akej miery je dôkaz pomocou Vennových diagramov korektný. (Od prvého ročníka na vysokej škole ste už určite veľa krát počuli, že „obrázok nie je dôkaz“.) Odpoveď je, že tento dôkaz je úplne rovnocenný s overením príslušnej tautológie tabuľkovou metódou. Robíme tam totiž presne to 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 zdôvodnite!

Obr. 2.4: Asociativnosť operácie Δ

{oper : FIGSYMD}

- 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}

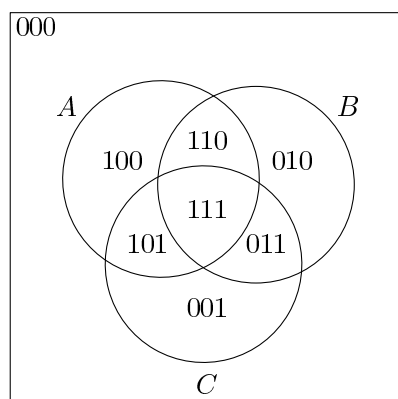
Posledný typ operácie definovanej na množinách, ktorým sa budeme zaoberať, je karteziánsky súčin. Tu ho zdefinujeme pre dve množiny, resp. pre konečný počet množín, neskôr (v časti 3.2.1) ho zdefinujeme aj karteziánsky súčin ľubovoľného systému množín. Na to, aby sme mohli zdefinovať karteziánsky súčin 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. Lahko si môžete všimnúť, že množina uvedená v definícii skutočne existuje – stačí viackrát použiť axiómu dvojice.



Obr. 2.5: Vzťah medzi Vennovým diagramom a tabuľkou

{oper:FIGVENN3TAB}

Menej zrejme 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.)

{kartz:TVRUSPDVOJ}

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

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

Dôkaz. Platnosť implikácie \Leftarrow je jasná.

\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 $a = b = c = d$. \square

Teraz už môžeme zdefinovať 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.

{kartz: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) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.
- (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. \square

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

$$\begin{aligned} A \times (B \times C) &= \{\emptyset\} \times \{(\emptyset, \emptyset)\} = \{(\emptyset, (\emptyset, \emptyset))\} \\ (A \times B) \times C &= \{(\emptyset, \emptyset)\} \times \{\emptyset\} = \{((\emptyset, \emptyset), \emptyset)\} \end{aligned}$$

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 $X = Y$.

⁷V 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 axiomy systému ZFC.

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 $A \neq \emptyset$?

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 $A \times (B \Delta C) = (A \times B) \Delta (A \times C)$.

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*

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 teórie 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 reláciách 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 parodoxe v ZFC môžeme použiť na zdôvodnenie toho, že neexistuje množina všetkých množín, čo vlastne znamená, že systém všetkých množín tvorí vlastnú triedu.

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 množiny spĺňajúce formulu $x \in x$, ide skutočne o triedu.)

Nech by \mathbf{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 \mathbf{Set} je množina vedie k sporu – takáto množina preto existovať nemôže (a je to teda skutočne vlastná trieda.) \square

{triedy:SSECTRIEDY}

{triedy:VTSETISPROPERCLA}

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:PRIKLRUZNICA}

Príklad 3.1.3. Na množine $I = \langle 0, 1 \rangle$ môžeme zdefinovať 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 diskretnej 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 *čiasťočné usporiadanie* na množine A , ak relácia R je reflexívna, tranzitívna a antisymetrická.

Hovoríme tiež, že dvojica (A, R) je *čiasťočne 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.

Čiasťočnými 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

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

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 .

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

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

{rel:TVRININV}

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. \square

{rel:TVRINVZLOZ}

Tvrdenie 3.1.12. Nech R je relácia medzi množina 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 $L = P$. \square

{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 $R \circ R \subseteq R$;
- (v) ľubovoľné dva rôzne prvky A sú porovnateľné v relácii R , ak $R \cup R^{-1} \supseteq A \times A \setminus id_A$.

{rel:itTRANZSKLAD}

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

(iv) \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 $R \circ R \subseteq R$.

\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. \square

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 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} . \square

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 indukciou¹ zavedieme nasledujúce označenie pre ľubovoľnú reláciu R na množine A :

$$R^0 = id_A;$$

$$R^1 = R;$$

$$R^{n+1} = R^n \circ R \text{ pre ľubovoľné prirodzené číslo } n \in \mathbb{N}.$$

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 \square

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 3.1.15. 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 (dokáže 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 $S \circ R$.

¹Matematickou 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:

- relácia R^{-1} je relácia ekvivalencie na A ;
- relácia $R \circ S$ je relácia ekvivalencie na A ;
- 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:

- relácia R^{-1} je čiastočné usporiadanie na A ;
- relácia $R \circ S$ je čiastočné usporiadanie na A ;
- 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?

- $A = \langle 0, 1 \rangle$, $R = \{(x, y) \in A \times A; x^2 + y^2 = 1\}$, $S = \{(x, y) \in A \times A; x^2 + y^2 \leq 1\}$;
- $A = \mathbb{R}$; $R = \{(x, y) \in A \times A; |x| \geq |y|\}$, $S = \{(x, y) \in A \times A; |y| \geq |x|\}$;
- $A = \mathbb{R}$; $R = \{(x, y) \in A \times A; |x - y| < a\}$, $S = \{(x, y) \in A \times A; |x - y| < b\}$, 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.)

- 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?
- 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?
- Nech $R_{1,2}$ sú relácie na množine A a $R_1 \subseteq R_2$. Potom $R_1^{-1} \subseteq R_2^{-1}$.
- 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 $\{1, 2, \dots, m\}$ a $\{1, 2, \dots, n\}$ 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 $\{1, 2, \dots, m\}$ a $\{1, 2, \dots, n\}$ a S je relácia medzi množinami $\{1, 2, \dots, n\}$ a $\{1, 2, \dots, k\}$. Viete nájsť nejaký vzťah medzi maticou $A_{S \circ R}$ a súčinom matic $A_R \cdot A_S$? (Pozor na výmenu poradia!)

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

c: ULOTRANZUZ}

Úloha 3.1.15. 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 $T := \bigcap \{S \subseteq A \times A; S \supseteq A, S \text{ je tranzitívna}\}$ najmenšou (vzhľadom na inklúziu) reláciou, ktorá obsahuje A a je tranzitívna. (Čiže T je tranzitívny uzáver relácie R .)

Úloha 3.1.16. 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 $f: A \rightarrow B$. Množinu A nazývame *definíčný 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).

Príklad 3.2.3. Jednoduchým príkladom zobrazenia je zobrazenie $id_A: A \rightarrow A$ (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 $f: A \rightarrow B$ je zobrazenie a $C \subseteq A$, tak zobrazenie $f|_C: C \rightarrow B$, 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 $f: A \rightarrow B$ a $g: B \rightarrow C$ ekvivalentne definovať ako

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

Vyplyva 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 $f: A \rightarrow B$, $g: B \rightarrow C$ je $g \circ f$ relácia. Overme, že táto relácia je zobrazením.

Tvrdenie 3.2.5. *Nech $f: A \rightarrow B$, $g: B \rightarrow C$ 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 $f: X \rightarrow Y$ 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, prinaajmenšom 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.

{fun:TVRINVBIIJEK}

Tvrdenie 3.2.7. *Nech $f: A \rightarrow B$ je zobrazenie. Potom f^{-1} je zobrazenie práve vtedy, keď f je bijekcia.*

Dôkaz. \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.)

\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 zobrazenia môžeme ekvivalentne preformulovať tak, že je to zobrazenie, pre ktoré platí

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

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 $f: A \rightarrow B$, $g: B \rightarrow A$ 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) \Rightarrow (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 zobrazenia), 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) \Rightarrow (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 $g \subseteq f^{-1}$. \square

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 $f: \mathcal{S} \rightarrow \bigcup \mathcal{S}$, 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 $f: X \rightarrow Y$ 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.)

²Toto 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.

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

{fun:TVROBRAZ}

Tvrdenie 3.2.13. *Nech $f: X \rightarrow Y$, $g: Y \rightarrow Z$ 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 $A = f^{-1}[f[A]]$;
- {fun:itOBRCAP} (iv) $f[f^{-1}[C]] \subseteq C$ a ak f je surjektívne, tak $f[f^{-1}[C]] = C$;
- {fun:itOBRBIGCAP} (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:itOBRBIGCUP} (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:itOBRBIGCUP} (vii) $f[A \cup B] = f[A] \cup f[B]$;
- {fun:itOBRBIGCUP} (viii) $f[\bigcup_{i \in I} A_i] = \bigcup_{i \in I} f[A_i]$;
- {fun:itOBRBIGCUP} (ix) $f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$;
- {fun:itOBRBIGCUP} (x) $f^{-1}[\bigcap_{i \in I} A_i] = \bigcap_{i \in I} f^{-1}[A_i]$;
- {fun:itOBRBIGCUP} (xi) $f^{-1}[C \cup D] = f^{-1}[C] \cup f^{-1}[D]$;
- {fun:itOBRBIGCUP} (xii) $f^{-1}[\bigcup_{i \in I} A_i] = \bigcup_{i \in I} f^{-1}[A_i]$;
- {fun:itOBRBIGCUP} (xiii) $A \subseteq B \Rightarrow f[A] \subseteq f[B]$ a ak f je injekcia, tak platí aj opačná implikácia;
- {fun:itOBRBIGCUP} (xiv) $C \subseteq D \Rightarrow f^{-1}[C] \subseteq f^{-1}[D]$ a ak f je surjekcia, tak platí aj opačná implikácia;
- {fun:itOBRBIGCUP} (xv) $f[A] \subseteq C \Leftrightarrow A \subseteq f^{-1}[C]$.

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

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 $f: A \rightarrow B$ je zobrazenie. Potom platí:*

- (i) f je surjekcia práve vtedy, keď existuje zobrazenie $g: B \rightarrow A$ také, že $f \circ g = id_B$.
- (ii) Nech navyše $A \neq \emptyset$. Potom f je injekcia práve vtedy, keď existuje zobrazenie $g: B \rightarrow A$ také, že $g \circ f = id_A$.

Dôkaz. (i) \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 $x \neq y$. (Žiadne $a \in A$ sa nemôže zobrazíť na dva rôzne prvky b .)

Potom podľa axiómy výberu (tak ako sme ju preformulovali v poznámke 3.2.11) existuje funkcia $g: B \rightarrow A$ 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 $a \in A$; zvolíme 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 $x = y$. □

Dôsledok 3.2.15. Ak $A \neq \emptyset$ a existuje injekcia $f: A \rightarrow B$, tak existuje surjekcia $f: B \rightarrow A$.

{fun:DOSINJSUR}

Dôkaz. Ak f je injekcia, tak podľa druhej časti tvrdenia 3.2.14 existuje $g: B \rightarrow A$ 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 zdefinujeme 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 $p_1: A \times B \rightarrow A$ a $p_2: A \times B \rightarrow B$, dané predpismi

$$\begin{aligned} p_1(a, b) &= a \\ p_2(a, b) &= b \end{aligned}$$

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 zdefinovať 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 $\bigcup_{i \in I} A_i$ takých, že obraz prvku i patrí do A_i . Označujeme ho $\prod_{i \in I} A_i$.

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

Pre každé $i \in I$ definujeme zobrazenie $p_i: \prod_{i \in I} A_i \rightarrow A_i$

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

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 $f: A \rightarrow C$, $g: B \rightarrow D$ sú zobrazenia. Potom ich *karteziánsky súčin* je zobrazenie $f \times g: A \times B \rightarrow C \times D$ určené predpisom

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

Ak pre každé $i \in I$ je $f_i: A_i \rightarrow B_i$ zobrazenie, tak karteziánsky súčin týchto zobrazení je $g = \prod_{i \in I} f_i: \prod_{i \in I} A_i \rightarrow \prod_{i \in I} B_i$, kde $g(f)$ pre $f \in \prod_{i \in I} A_i$ 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 $\prod_{i \in I} f_i$ je skonštruované pomocou systému zobrazení indexovaného množinou I a je to zobrazenie, ktoré sa na i -tej súradnici správa rovnako ako f_i .

{TVR:funSUCBIJ}

Tvrdenie 3.2.19. Nech $f: A \rightarrow C$, $g: B \rightarrow D$ sú zobrazenia.

- (i) Ak f a g sú injekcie, tak $f \times g$ je injekcia.
- (ii) Ak f a g sú surjekcie, tak $f \times g$ je surjekcia.
- (iii) Ak f a 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 $f(a) = c$, $g(b) = d$. 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 $f_i: A_i \rightarrow B_i$ je zobrazenie pre každé $i \in I$.*

- (i) *Ak f_i je injektívne pre každé $i \in I$, tak $\prod_{i \in I} f_i$ je injektívne.*
- (ii) *Ak f_i je surjektívne pre každé $i \in I$, tak $\prod_{i \in I} f_i$ je surjektívne.*
- (iii) *Ak f_i je bijektívne pre každé $i \in I$, tak $\prod_{i \in I} f_i$ je bijektívne.*

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

- (i) Predpokladajme, že všetky f_i sú injektívne. Nech $f, f' \in \prod_{i \in I} A_i$ 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 $f \in \prod_{i \in I} B_i$. 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 $f \in \prod_{i \in I} B_i$ existuje vzor, čiže g je surjektívne zobrazenie.

- (iii) Ľahko vyplýva z predchádzajúcich dvoch častí. □

Cvičenia

{funcvic:ULOSKLAD}

Úloha 3.2.1. Dokážte, že:

- a) Zloženie dvoch injekcií je injektívne.
- b) Zloženie dvoch surjekcií je surjektívne.
- c) Zloženie dvoch bijekcií je bijektívne.

Úloha 3.2.2. Nech $f: X \rightarrow Y$, $g, h: Y \rightarrow Z$ sú zobrazenia. Dokážte, že:

- a) Ak f je surjektívne, tak platí $g \circ f = h \circ f \Rightarrow g = h$.
- b) Ak $Z \neq \emptyset$ a platí (pre ľubovoľné $g, h: Y \rightarrow Z$) implikácia $g \circ f = h \circ f \Rightarrow g = h$, tak f je surjektívne.

Úloha 3.2.3. Nech $g, h: X \rightarrow Y$, $f: Y \rightarrow Z$ sú zobrazenia. Dokážte, že:

- a) Ak f je injektívne a platí $f \circ g = f \circ h$, tak $g = h$.
- b) Ak $X \neq \emptyset$ a pre ľubovoľné $g, h: X \rightarrow Y$ platí implikácia $f \circ g = f \circ h \Rightarrow g = h$, tak f je injektívne.

Úloha 3.2.4. Ak $f: X \rightarrow Y$ a $g: Y \rightarrow X$ sú zobrazenia také, že $g \circ f = id_X$, tak g je surjektívne a f je injektívne. Ukážte na príklade, že g nemusí byť injektívne a f nemusí byť surjektívne.

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 $f: X \rightarrow Y$ je zobrazenie. Zapište pomocou kvantifikátorov výroky „ f je injektívne“ a „ f je surjektívne“ 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.:

$$(\forall a \in A) a \leq a \quad (\text{R})$$

$$(\forall a, b \in A) a \leq b \wedge b \leq a \Rightarrow a = b \quad (\text{A})$$

$$(\forall a, b, c \in A) a \leq b \wedge b \leq c \Rightarrow a \leq c \quad (\text{T})$$

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.

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

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 upozornenie 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

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

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}, \mid) 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

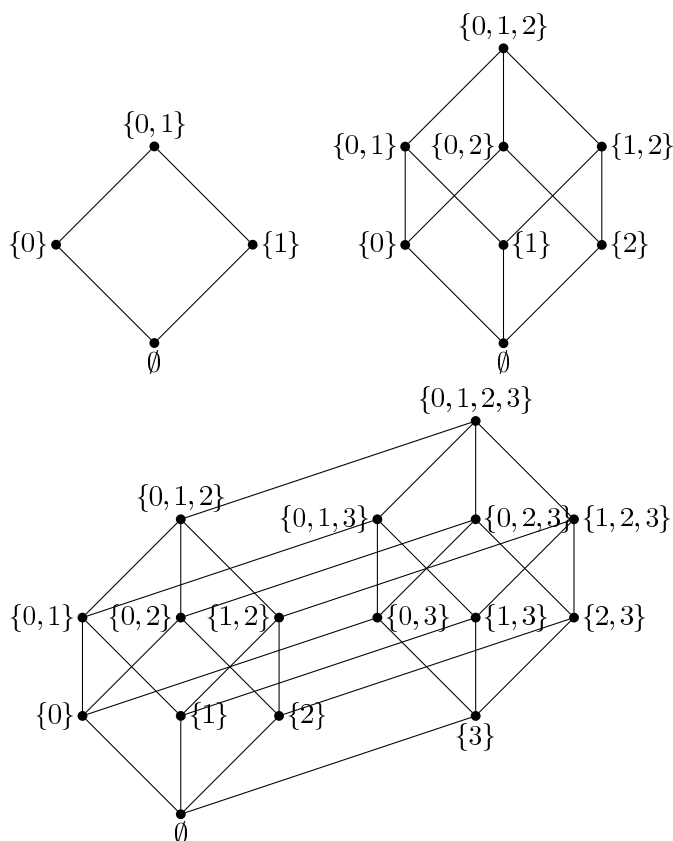
$$a \leq c \leq b \quad \Rightarrow \quad c = a \vee c = b.$$

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.)

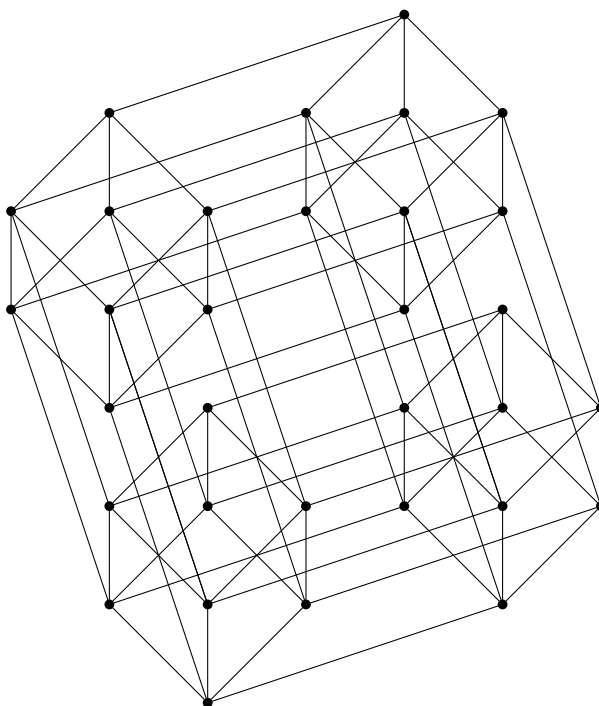
Často sa zvykne kresliť Hasseho diagram tak, že vždy nakreslíme šípku z prvku do jeho nasledovníka. My budeme kresliť Hasseho diagramy bez šípok, ak budú dva prvky spojené hranou, tak nasledovník je ten z nich, ktorý je na obrázku nakreslený vyššie.



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

{cum:FIGHASSEPX}

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.



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

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 $f: X \rightarrow Y$ je zobrazenie. Hovoríme, že zobrazenie f je *monotónne*, ak platí

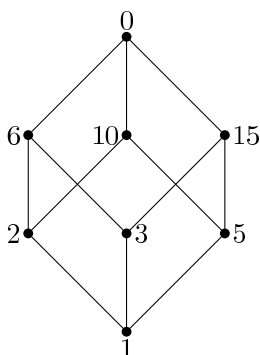
$$(\forall x_1, x_2 \in X) x_1 \leq x_2 \Rightarrow f(x_1) \preceq f(x_2).$$

Niekedy používame aj zápis $f: (X, \leq) \rightarrow (Y, \preceq)$.

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 $(X, \leq) \cong (Y, \preceq)$.

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

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



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

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* 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.

Lahko 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 príkladov (môžete si rozmyslieť, ako je to s čiastočne usporiadanými množinami znázorenými 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.

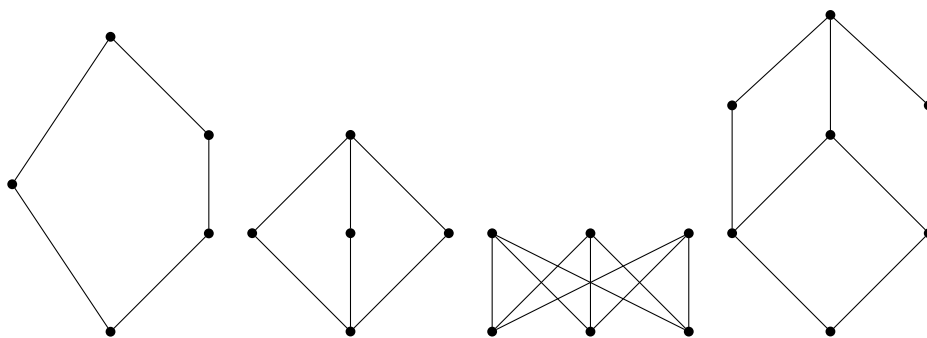
Predchádzajúci príklad súčasne ukazuje, že maximálnych (minimálnych) prvkov môže mať čiastočne usporiadaná množina viacero. Ak však čiastočne usporiadaná množina má najväčší (najmenší) prvok, tak tento prvok je jednoznačne určený.

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 $<$, \subsetneq . (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

$$\begin{aligned} a &\not< a; \\ a < b &\Rightarrow b \not< a; \\ a < b \wedge b < c &\Rightarrow a < c. \end{aligned}$$



Obr. 3.4: Ďalšie príklady Hasseho diagramov

{ cum:FIGMOREH

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.

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. \square

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 . \square

Na základe predchádzajúcich lemm 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 ostrých čiastočných usporiadaní množiny A (a teda tieto priradenia sú bijektívne).

: 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

$$a = b \quad a < b \quad b < a.$$

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:

- Zloženie dvoch monotónnych zobrazení je monotónne zobrazenie;
- 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:

- Relácia $R_1 \cap R_2$ je čiastočné usporiadanie na A .
- Relácia $R_1 \cup R_2$ je čiastočné usporiadanie na A .
- 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.

{cumcvic:ULOPRAZDCUM}

Úloha 3.3.5. Nech A je ľubovoľná množina. Sú relácie $A \times A$, id_A a \emptyset čiastočnými usporiadaniami na množine A ?

Úloha 3.3.6. Môže byť čiastočné usporiadanie na množine A zobrazením z A do A ?

3.4 Dobře 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 takomto 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 súvisi 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.

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

Definícia 3.4.5. Nech (A, \leq_A) , (B, \leq_B) sú čiastočne usporiadané množiny. Potom reláciu \leq na množine $A \times B$ definovanú ako

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

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

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

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

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 3.4.7).

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.

Tvrdenie 3.4.6. *Nech (A, \leq) , (B, \leq) sú čiastočne usporiadané množiny a $(A \times B, \leq)$ je ich (anti)lexikografický súčin. Potom*

{dum:TVRLEXI}

- (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.

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

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

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

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

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

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

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

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

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

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

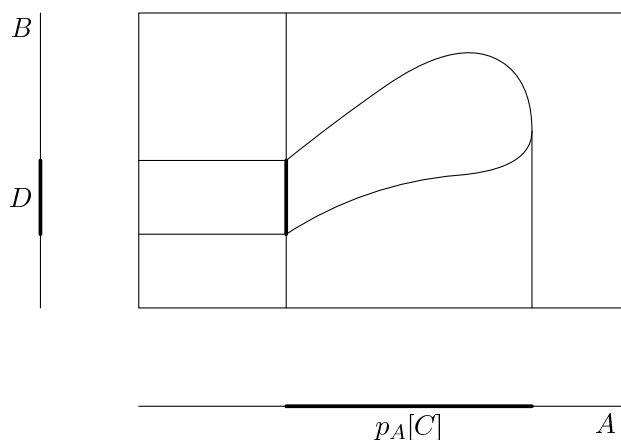
Ak $a = a'$, tak pre prvky b a b' máme opäť dve možnosti. Buď $b \leq b'$, vtedy platí $(a, b) \leq (a', b')$; alebo $b' \leq b$ a v tomto prípade $(a', b') \leq (a, b)$.

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

(iii): Teraz budeme navyše predpokladať, že (A, \leq) a (B, \leq) sú dobre usporiadané. Priopemeňme, že projekcia $p_A: A \times B \rightarrow A$ 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, \leq) je dobre usporiadaná, existuje najmenší prvok a_0 množiny $p_A[C]$.

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, \leq) je dobre usporiadaná množina, existuje najmenší prvok množiny D , označme ho b_0 .



Obr. 3.5: Ilustrácia k dôkazu tvrdenia 3.4.6

{dum:FIGLEXI}

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 $a_0 \leq a$. Ak $a = a_0$, znamená to, že $b \in D$, preto $b_0 \leq b$ a $(a_0, b_0) \leq (a, b)$. Ak $a < a_0$, tak tiež (na základe definície lexikografického usporiadania) platí $(a_0, b_0) \leq (a, b)$. \square

{dum:POZNIZOMLEX}

Poznámka 3.4.7. 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 3.4.6 skutočne stačilo dokázať jednotlivé časti pre jedno z týchto dvoch usporiadaní.)

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

{dum:PRSUCET}

Príklad 3.4.8. Nech (B, \leq_B) a (C, \leq_C) sú čiastočne usporiadané množiny. Na množine $M := \{0\} \times B \cup \{1\} \times C$ zdefinujeme čiastočné usporiadanie \leq takýmto spôsobom:

$(0, b) \leq (1, c)$ pre ľubovoľné $b \in B, c \in C$;

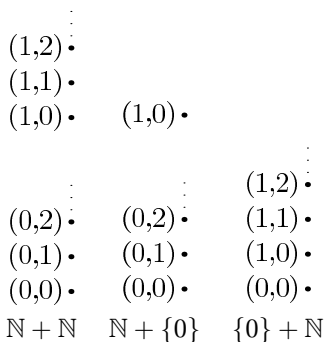
pre $b, b' \in B$ platí $(0, b) \leq (0, b')$ práve vtedy, keď $b \leq_B b'$;

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 (dobře) 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.



Obr. 3.6: Príklady na súčet dobre usporiadaných množín

{dum:FIGSUCET}

{POZNDISJZJED}

Poznámka 3.4.9. 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 3.4.10. *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 $X \setminus U$ je neprázdna podmnožina X . Označme a najmenší prvok množiny $X \setminus U$. Keďže a je najmenší prvok doplnku U , všetky menšie prvky už musia patriť do U , a teda $U \subseteq X_a$.

{dum:TVRIZOMPOCUSEK}

Tvrdenie 3.4.11. *Nech (X, \leq) je lineárne usporiadaná množina a nech $X' = \{X_a; a \in X\}$ je množina všetkých počiatočných úsekov množiny X . Potom zobrazenie $f: X \rightarrow X'$ 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 $x < b$.) \square

Cvičenia

{dumcvic:ULOS}

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 zdefinujeme 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:

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

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

a) Overte, že takto dostaneme čiastočne usporiadanú množinu a navyše, ak všetky použité množiny sú lineárne (dobre) usporiadané, aj $\sum_{a \in A} B_a$ 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 3.4.8.

d) Nech $A = \mathbb{N}$, $B_n = \{0, 1, \dots, n\}$ (v oboch prípadoch s obvyklým usporiadaním prirodzených čísel). Ako vyzerá $\sum_{a \in A} B_a$? (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?)

Literatúra

- [B1] Lev Bukovský. Úvod do matematickej logiky. http://ics.upjs.sk/~novotnyr/home/skola/logika_a_teorija_mnozina/ltm.pdf.
- [B2] Lev Bukovský. *Štruktúra reálnej osi*. Veda, Bratislava, 1979.
- [B3] Lev Bukovský. *Množiny 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 Mathematical 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-Guinness. *The Search for Mathematical Roots 1870–1940*. Princeton University Press, Princeton, 2000.
- [H] Horst Herrlich. *The Axiom of Choice*. Springer-Verlag, Berlin, 2006. Lecture Notes in Mathematics 1876.
- [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 diskretných matematických štruktúr*. Univerzita Komenského, Bratislava, 2007. <http://www.dcs.fmph.uniba.sk/texty/dsmain.pdf>.
- [RF] Branislav Rován 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.
- [ŠS] Tibor Šalát and Jaroslav Smítal. *Teória množín*. UK, Bratislava, 1995.
- [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

- axióma
 - dvojice, 18
 - existencie, 17
 - extenzionality, 17
 - nekonečnej množiny, 20
 - potenčnej množiny, 19
 - regularity, 20
 - výberu, 21, 39
 - zjednotenia množín, 18
- bijekcia, 38
- de Morganove pravidlá, 10
- diagram
 - Hasseho, 45
 - Vennov, 26
- disjunkcia, 9
- dvojica
 - usporiadaná, 28
- ekvivalencia, 9
- formula
 - atomická, 17
- formula teórie množín, 17
- funkcia, 37
- identita, 34
- implikácia, 9
 - obmena, 10
- injekcia, 38
- inklúzia, 21
- izomorfizmus
 - čiastočne usporiadaných množín, 46
- konjunkcia, 9
- kvantifikátor, 11
 - existenčný, 11
 - všoebecný, 11
- množina, 16
 - dobře usporiadaná, 49
- množiny
 - disjunktné, 19
- naivná teória množín, 6
- najmenšia vzhľadom na inklúziu, 35
- nasledovník, 45
- negácia, 9
- obor
 - definičný, 32, 37
 - hodnôt, 32, 37
- obraz množiny, 39
- paradox
 - Berryho, 16
 - Russellov, 15
- podmnožina, 19
 - vlastná, 22
- potenčná množina, 20
- predchodca, 45
- prienik, 19
- projekcia, 41
- prvky
 - porovnateľné, 33
- prvok
 - maximálny, 47
 - minimálny, 47
 - najmenší, 47
 - najväčší, 47
- prázdna množina, 19
- relácia, 32
 - antireflexívna, 33
 - antisymetrická, 33
 - asymetrická, 33
 - inverzná, 33
 - ireflexívna, 33
 - reflexívna, 33
 - symetrická, 33
 - tranzitívna, 33
 - trichotomická, 33

relácia ekvivalencie, 33
rozdiel množín, 25

schéma axióm
 substitúcie, 20, 39
schéma axióma
 vymedzenia, 18
skladanie
 relácií, 33
 zobrazení, 37
surjekcia, 38
symetrická diferencia množín, 25
súčin
 karteziánsky, 29, 42
 funkcií, 42

tranzitívny uzáver, 35

usporiadanie
 antilexikografické, 50
 dobré, 49
 lineárne, 33
 lineárne ostré, 48
 čiasťočné, 33
 čiasťočné ostré, 47

vzor množiny, 39

ZF, 21
ZFC, 21
zjednotenie
 dvojice množín, 18
 systému množín, 18
zloženie
 relácií, 33
 zobrazení, 37
zobrazenie, 37
 bijektívne, 38
 identické, 37
 injektívne, 38
 inverzné, 38
 monotónne, 46
 na, 38
 prosté, 38
 surjektívne, 38
zákony
 de Morganove, 26
zúženie zobrazenia, 37

čiasťočne usporiadaná množina, 33

úsek
 počiatočný, 53

Zoznam symbolov

\neg	9	$\prod_{i \in I} f_i$	42
\wedge	9	\leq	44
\vee	9	$<$	44
\Rightarrow	9	A_a	49
\Leftrightarrow	9	$ X = Y $	54
\forall	11	$ X $	54
\exists	11	$ X \leq Y $	56
\in	16	$ X < Y $	56
$\bigcup A$	18	WO	67
$A \cup B$	18	PM	67
\emptyset	19	ZL	67
$A \cap B$	19	$\text{Ord}(X, \leq)$	74
\subseteq	19	$\text{Ord}(X)$	74
$\mathcal{P}(A)$	20		
$\exists!$	20		
\subsetneq	22		
$\bigcup \mathcal{S}$	23		
$\bigcup_{A \in \mathcal{S}} A$	23		
$\bigcup_{i \in I} A_i$	23		
$\bigcap \mathcal{S}$	23		
$\bigcap_{A \in \mathcal{S}} A$	23		
$\bigcap_{i \in I} A_i$	23		
$A \setminus B$	25		
$A \Delta B$	25		
(a, b)	28		
\times	29		
aRb	32		
$D(R)$	32		
$H(R)$	32		
$S \circ R$	33		
R^{-1}	33		
id_A	34		
$f: A \rightarrow B$	37		
$f _C$	37		
$g \circ f$	37		
$f[A]$	39		
$f^{-1}[B]$	39		
$f^{-1}(b)$	39		
$f(a, b)$	41		
p_1	41		
p_2	41		
p_A	41		
$\prod_{i \in I} A_i$	42		
$f \times g$	42		