Teória množín pre učiteľov

Martin Sleziak

7. marca 2017

Obsah

Kapitola 1

Úvod

Verzia: 7. marca 2017

1.1 Sylaby a literatúra

1.1.1 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 [L, 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 [B2]. Pokiaľ ste schopní čítať text v angličtine, ľahko nájdete veľké množstvo ďalších výborných textov o teórii množín.

1.1.2 Sylaby predmetu

Zermelov-Fraenkelov axiomatický system teórie množín. Kardinálne čísla a kardinálna aritmetika. Spočítateľné a nespočítateľné množiny. Mohutnosť kontinua a kardinalita množín vyskytujúcich sa v školskej matematike. Axióma výberu, jej ekvivalenty a dôsledky.

1.1.3 Stará a nová akreditácia

Explicitne upozorním na to, že pri prechode na novú akreditáciu sa o niečo zmenili obsah predmetu. Tomu som prispôsobil aj učebný text – vynechal časti, ktoré sa nepreberajú a pri preberanej látke mierne upravil poradie. Na mojej stránke nájdete aj text vytvorený keď predmet bežal podľa starej akreditácie [Sl2]. Je možné, že bude pre niekoho zaujímavý – pre ľudí, ktorý absolvujú tento predmet v súčasnej podobe, tam však je pomerne veľa informácií navyše a je pre nich užitočnejší tento text. Aby som ich odlíšil, pri staršom texte som nechal

[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.

pôvodný názov „2-UMA-115 Teória množín“ a nový text je nazvaný „Teória množín pre učiteľov“. (Je to asi o niečo jasnejšie odlíšenie, než ich rozlíšiť iba ako 2-UMA-115/00 a 2-UMA-115/15.)

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

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

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

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

Ako ilustráciu stručne popíšme *Russellov paradox.* (Neskôr sa budeme paradoxami teórie množín zaoberať o niečo podrobnejšie.) Povedali sme si, že základná 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. Možný prístup, ako riešiť tento problém, predstavuje *axiomatická teória*

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

množín, v ktorej sa zavedú axiómy, ktoré obmedzia to aké množiny sa dajú tvoriť a zabránia vzniku Russellovho paradoxu. My sa budeme zaoberať najmä naivnou teóriou množín, axiomatickú teóriu množín spomenieme len stručne ku koncu prednášky.

1.3 Základné označenia

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

Kapitola 2

Množiny a práca s nimi

V tejto kapitole by sme si chceli ukázať základy práce s množinami a niektoré vlastnosti operácií s množinami.

Pracujeme v naivnej teórii množín, kde množinu chápeme jednoducho ako súhrn objektov určených nejakou vlastnosťou.

S množinami budeme pracovať napriek tomu, že sme sme si povedali len pomerne vágnu definíciu množiny a videli sme, že takýto naivný prístup môže viesť k problémom (Russellov paradox v časti 1.2). Na problémy však nenarazíme, ak budeme pracovať so základnými číselnými množinami, ktoré dobre poznáme – ako napríklad $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – a s množinami, ktoré z nich vieme pomocou niektorých operácií vytvoriť.

Ako príklady množín teda môžeme uviesť napríklad:

$$A = \{1, 2, 3, 4\}$$
$$B = \{x \in \mathbb{N}; (\exists a, b \in \mathbb{N}) a^2 + b^2 = x\}$$
$$C = \{2x; x \in \mathbb{N}\}$$

V týchto príkladoch je množina A definovaná tak, že sú vymenované všetky jej prvky. Množina B je množina tých prirodzených čísel, ktoré sa dajú dostať ako súčty dvoch štvorcov. Množina C je množina párnych prirodzených čísel. Ďalšie množiny z nich môžeme vytvárať pomocou rôznych operácií, o ktorých budeme hovoriť v tejto kapitole, t.j. napríklad $A \cap B$, $C \setminus B$, $A \times \mathbb{N}$ a podobne.

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.

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

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

p	$\neg p$
1	0
0	1

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

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

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

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

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 ukážeme overenie jedného z de Morganových pravidiel.

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

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

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

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

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

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

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

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

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

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

Tu je overenie tej istej tautológie tabuľkou:

p	q	$\neg q$	$\neg p$	$p \Rightarrow q$	$\neg q \Rightarrow \neg p$	$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$
1	1	0	0	1	1	1
1	0	1	0	0	0	1
0	1	0	1	1	1	1
0	0	1	1	1	1	1

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 $q \Rightarrow p$.

Disjunktívna normálna forma

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

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

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

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

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

2.1.2 Výroky s kvantifikátormi

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

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

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

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

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

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

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

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

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

Ľavá strana uvedenej ekvivalencie znamená, že nie všetky objekty, s ktorými pracujeme majú vlastnosť $P(x)$. To je ale presne to isté, že medzi nimi existuje aspoň jeden objekt, ktorý túto vlastnosť nemá, a teda spĺňa $\neg P(x)$. (Ak nie je pravda, že všetky 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

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

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

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

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

Príklad 2.1.10. Chceme overiť, či výrok

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

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

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

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

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

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

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

Cvičenia

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) $[p \Rightarrow (q \Rightarrow r)] \Leftrightarrow [p \Rightarrow (q \Rightarrow r)]$

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

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

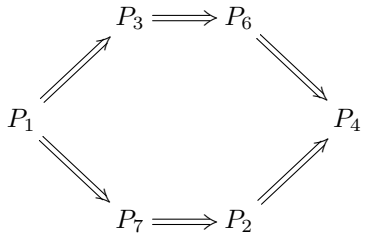
Úloha 2.1.4. Ukážte, že operácie $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ môžeme definovať pomocou:
a) negácie a konjunkcie,
b) negácie a disjunkcie,
c) negácie a implikácie,

d) logickej spojky NAND definovanej ako $P \,\mathrm{NAND}\, Q \Leftrightarrow \neg(P \wedge Q)$,
e) logickej spojky NOR definovanej ako $P \,\mathrm{NOR}\, Q \Leftrightarrow \neg(P \vee Q)$.

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

Úloha 2.1.6. Rozhodnite, či sú uvedené výroky pravdivé. Svoje tvrdenie zdôvodnite.
a) $[(\forall x)P(x) \Rightarrow (\forall x)Q(x)] \Rightarrow (\forall x)(P(x) \Rightarrow Q(x))$
b) $(\exists x)(P(x) \wedge Q(x)) \Leftrightarrow [(\exists x)P(x) \wedge (\exists x)Q(x)]$
c) $(\exists x)(P(x) \vee Q(x)) \Leftrightarrow [(\exists x)P(x) \vee (\exists x)Q(x)]$
d) $(\forall x)(P(x) \wedge Q(x)) \Leftrightarrow [(\forall x)P(x) \wedge (\forall x)Q(x)]$
e) $(\forall x)(P(x) \vee Q(x)) \Leftrightarrow [(\forall x)P(x) \vee (\forall x)Q(x)]$
f) $(\forall x)(P(x) \Rightarrow Q(x)) \Leftrightarrow [(\exists x P(x)) \Rightarrow (\exists x)Q(x)]$
g) $[(\forall x)(\forall y)(R(x,y) \Rightarrow \neg R(y,x))] \Rightarrow (\forall x)\neg R(x,x)$

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



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

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

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

2.2 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.

Asi najdôležitejšia vlastnosť, ktorú budeme používať, je to, že dve množina sa rovnajú práve vtedy, ak majú rovnaké prvky. Inak povedané, množina je jednoznačne určená svojimi prvkami.

Definícia 2.2.1. Hovoríme, že množiny A a B sa rovnajú ak $x \in A$ platí práve vtedy, keď $x \in B$.

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

Dalo by sa povedať, že definícia rovnosti množín bude nahrádzať to, že pojem množiny vlastne nemáme úplne presne definovaný.

Začnime tým, že zadefinujeme vzťah „byť podmnožinou“, ktorý sa zvykne nazývať aj *inklúziou*.

Definícia 2.2.2. Ak A, B sú množiny, tak hovoríme, že A je *podmnožinou* B, ak každý prvok množiny A je prvkom množiny B. Tento fakt označíme $A \subseteq B$.

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

Často budeme potrebovať aj označenie pre množinu, ktorá obsahuje všetky podmnožiny danej množiny.

Definícia 2.2.3. Množinu všetkých podmnožín množiny A nazývame *potenčná množina* množiny A a označujeme $\mathcal{P}(A)$.

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

Nasledujúce tvrdenie zhŕňa základné vlastnosti inklúzie.

Tvrdenie 2.2.4. *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 $A \subseteq C$.*

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 definície 2.2.1 a tautológie z úlohy 2.1.1b)).

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

Tvrdenie 2.2.4(ii) niekedy budeme používať na dôkaz rovnosti množín – môžeme dokazovať to, že množiny A a B sa rovnajú tak, že zvlášť dokážeme inklúzie $A \subseteq B$ a $B \subseteq A$.

Definícia 2.2.5. Ak A je podmnožina B a súčasne $A \neq B$, tak hovoríme, že A je *vlastná podmnožina* množiny B. Označenie $A \subsetneq B$.

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

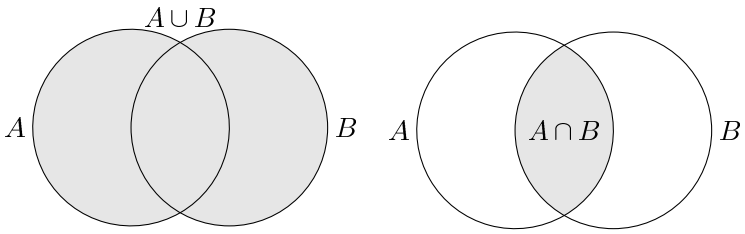
Poznámka 2.2.6. V tomto texte používam $\subseteq$ na označenie podmnožiny a $\subsetneq$ na označenie vlastnej podmnožiny. Toto označenie som zvolil z toho dôvodu, že som sa chcel vyhnúť možným nedorozumeniam. Dosť často sa na označenie inklúzie používa $\subset$, nájdu sa však aj texty (hoci zriedkavejšie), 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 2.2.)



Obr. 2.1: Zjednotenie a prienik dvoch množín

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

Tvrdenie 2.2.7. *Nech A, B, C sú množiny. Potom platí:*

(i) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ (*asociatívnosť operácií* $\cup$ *a* $\cap$);
(ii) $A \cup B = B \cup A$, $A \cap B = B \cap A$ (*komutatívnosť operácií* $\cup$ *a* $\cap$);
(iii) $\emptyset \cup A = A$, $\emptyset \cap A = \emptyset$;
(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*);
(v) $A \cap A = A$, $A \cup A = A$ (*idempotentnosť operácií* $\cup$ *a* $\cap$)
(vi) $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$ (*zákony absorpcie*).

Dôkaz. (i) Dve množiny sa rovnajú práve vtedy, keď obsahujú rovnaké prvky. Teda nám stačí ukázať, že platí

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

Priamo na základe definície zjednotenia môžeme výrok $x \in A \cup (B \cup C)$ prepísať ako $(x \in A) \vee [(x \in B) \vee (x \in C)]$. Podobne výrok na pravej strane ekvivalencie je ekvivalentný

s výrokom $[(x \in A) \vee (x \in B)] \vee (x \in C)$. Ak si teda označíme $p := (x \in A)$, $q := (x \in B)$ a $r := (x \in C)$, tak vlastne máme dokázať

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

čo je presne tautológia z úlohy 2.1.2a).

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

V predchádzajúcom dôkaze sme videli jeden možný spôsob dôkazu množinových identít – založený na tom, že dokazovanú identitu prevedieme na tautológiu, ktorú potom overujeme. Inou možnosťou je dôkaz spočívajúci v algebraickej manipulácii – pokiaľ máme už dokázaný dostatočne veľa identít, môžeme ich použiť na dôkaz nových identít; takýto postup si ukážeme napríklad v príklade 2.2.12. 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.

Definícia 2.2.8. Ak $\mathcal{S}$ je nejaký systém množín, tak množinu

$$\bigcup \mathcal{S} = \{x; (\exists S \in \mathcal{S}) x \in S\}$$

nazývame *zjednotením systému množín* $\mathcal{S}$.

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

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

Dôvod, prečo pri prieniku systému množín vyžadujeme $I \neq \emptyset$ je ten, že pre prázdnu množinu by sme takto dostali množinu všetkých množín resp. všetkých objektov – ako sme už videli pri Russellovom paradoxe, takýto objekt vedie k možným problémom.

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:

Tvrdenie 2.2.9. *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. Použitím definície prieniku dvoch množín a prieniku systému množín dostaneme, že

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

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

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

To je presne ekvivalencia z úlohy 2.1.8a). □

Dokážeme aj niektoré vzťahy medzi množinovými operáciami a reláciou inklúzie.

Tvrdenie 2.2.10. *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. □

Tvrdenie 2.2.11. *Nech A, B, C sú množiny. Potom platí:*

(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 $[(x \in A) \wedge (x \in C)] \Rightarrow [(x \in B) \wedge (x \in C)]$ (na základe tautológie $(p \Rightarrow q) \Rightarrow [(p \wedge r) \Rightarrow (q \wedge r)]$); čo je len inak zapísaná implikácia $x \in A \cap C \Rightarrow x \in B \cap C$. Dôkaz druhej časti sa dá urobiť úplne analogicky.

Skúsme ešte urobiť dôkaz druhej časti pomocou tvrdenia 2.2.10. (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 2.2.7 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

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

□

Ako príklad použitia predchádzajúcich tvrdení uvedieme iný dôkaz tvrdenia 2.2.7(vi).

Príklad 2.2.12. $A \cap (A \cup B) \overset{(1)}{=} (A \cap A) \cup (A \cap B) \overset{(2)}{=} A \cup (A \cap B) \overset{(3)}{=} A$, pričom v jednotlivých rovnostiach sme použili:
(1) distributívnosť – tvrdenie 2.2.7(iv)
(2) idempotentnosť – tvrdenie 2.2.7(v)
(3) fakt, že $A \cap B \subseteq A$ – tvrdenie 2.2.11(ii) – a tvrdenie 2.2.10 pre množiny $A \cap B$ a A.

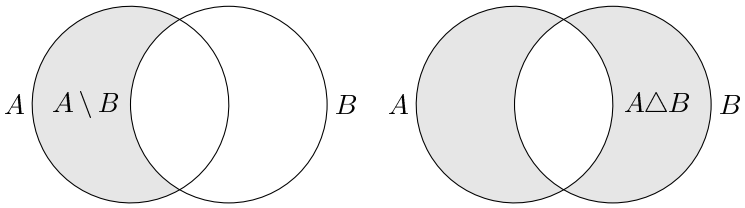
Ďalšie operácie, ktoré budeme niekedy používať, sú rozdiel a symetrická diferencia (symetrický rozdiel) dvoch množín.

Definícia 2.2.13. *Rozdiel množín* A a B je množina

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

Symetrická diferencia množín A a B je množina

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



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

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

Tvrdenie 2.2.14. *Nech A, B, C sú množiny. Potom platí:*

(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) $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$;
(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* $A \setminus \bigcup_{i \in I} B_i = \bigcap_{i \in I} (A \setminus B_i)$.
(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.*

Tvrdenie 2.2.15. *Nech A, B, C sú množiny. Potom platí:*

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

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

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

Pri dokazovaní našej tautológie potom dostávame nasledujúcu tabuľku:

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

□

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 polohe,* t.j. aby sa tam vyskytli „všetky možné“ oblasti. (Napríklad oblasť predstavujúca prvky patriace do A aj B a nepatriace do C, ak kreslíme Vennov diagram pre 3 množiny.)

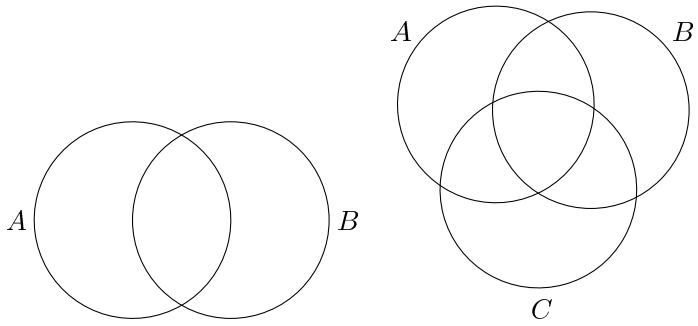
Na obrázku 2.3 sú znázornené 2 resp. 3 množiny v generickej polohe. (Môžete sa pokúsiť vymyslieť, ako by ste kreslili Vennove diagramy pre viac množín.)

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

Príklad 2.2.16. Ako príklad si ukážeme dôkaz asociatívnosti pre operáciu $\triangle$ (tvrdenie 2.2.15(ii)). Dôkaz toho istého tvrdenia overením príslušnej tautológie tabuľkovou metódou sme už videli.

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

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



Obr. 2.3: Generická poloha

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

Cvičenia

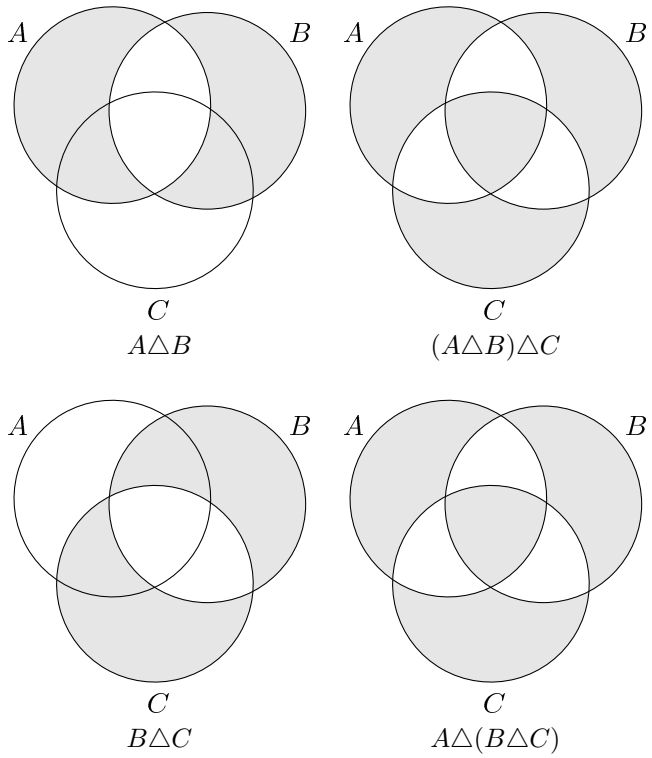
Úloha 2.2.1. Dokážte tvrdenia 2.2.7, 2.2.10, 2.2.11, 2.2.9, 2.2.14, 2.2.15; resp. tie časti uvedených tvrdení, ktoré sme nedokázali v predchádzajúcom texte. (Vyskúšajte si aspoň na niektorom príklade tabuľkovú metódu aj Vennove diagramy; v prípade tvrdení týkajúcich sa inklúzie si môžete vyskúšať dôkaz priamo z definície ako aj použitie tvrdenia 2.2.10.)

Úloha 2.2.2. Pokúste sa vymyslieť nejaké možné nakreslenia Vennovho diagramu pre 4 (prípadne aj viac) množín.

Úloha 2.2.3. 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!
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) $[(\forall x \in A)P(x) \wedge (\forall x \in B)P(x)] \Leftrightarrow (\forall x \in A \cap B)P(x)$.

Úloha 2.2.4. Rozhodnite, či sú nasledujúce tvrdenia pravdivé pre ľubovoľné množiny A, B, C. Tvrdenie dokážte alebo nájdite kontrapríklad.
a) $A \setminus (B \setminus C) = (A \setminus B) \setminus C$

Úloha 2.2.5. Dokážte platnosť daného tvrdenia pre ľubovoľné množiny A, B, C, alebo nájdite kontrapríklad:
a) $A \subseteq B \cap C$ práve vtedy, keď $A \subseteq B$ a $A \subseteq C$;
b) $A \subseteq B \cup C$ práve vtedy, keď $A \subseteq B$ alebo $A \subseteq C$;
c) $A \cup B \subseteq C$ práve vtedy, keď $A \subseteq C$ a $B \subseteq C$;
d) $A \cap B \subseteq C$ práve vtedy, keď $A \subseteq C$ alebo $B \subseteq C$.



Obr. 2.4: Asociatívnosť operácie $\triangle$

Úloha 2.2.6. Nech $\mathcal{S} \subseteq \mathcal{S}'$. Dokážte, že $\bigcup \mathcal{S} \subseteq \bigcup \mathcal{S}'$. Ak navyše predpokladáme $\mathcal{S} \neq \emptyset$, tak $\bigcap \mathcal{S} \supseteq \bigcap \mathcal{S}'$.

2.3 Usporiadané dvojice a karteziánsky súčin

V ďalšom budeme potrebovať pojem karteziánskeho súčinu množín, ktorý je definovaný pomocou usporiadaných dvojíc.

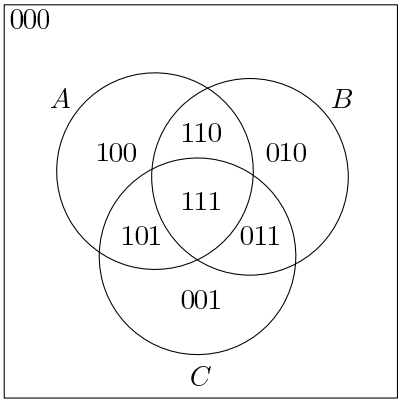
Ak zoberieme dva prvky x a y, tak množinu obsahujúcu práve tieto dva prvky môžeme zapísať viacerými spôsobmi: $\{x, y\} = \{y, x\} = \{x, x, y\}$. Inak povedané, pri množinách nezáleží na poradí v akom uvedieme prvky množiny. (A takisto ani na tom, či ich spomenieme viackrát.)

Teraz sa nám bude hodiť pojem usporiadanej dvojice – t.j. tiež budeme pracovať s dvoma prvkami, ale bude nám záležať i na poradí.

Definícia 2.3.1. *Usporiadanú dvojicu* pozostávajúcu z prvkov a, b budeme označovať (a, b). Dve usporiadané dvojice budeme považovať za rovnaké, ak sa zhodujú ich prvé aj druhé súradnice, t.j.,

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

Opäť sa dá povedať, že sme vlastne neuviedli poriadnu definíciu usporiadanej dvojice – jediné, čo však je pre nás podstatné je to, že vieme povedať, kedy sa dve usporiadané dvojice



Obr. 2.5: Vzťah medzi Vennovým diagramom a tabuľkou

rovnajú. (Podobne sme to urobili pre rovnosť množín v definícii 2.2.1.)

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

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

Tvrdenie 2.3.2. *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. □

Cvičenia

Úloha 2.3.1. Dokážte ostatné časti tvrdenia 2.3.2.

Úloha 2.3.2. Dokážte (priamo, nie s použitím tvrdenia 2.3.2):
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 2.3.3. 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 2.3.4. 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 2.3.5. Dokážte, že množiny A, B sú disjunktné práve vtedy, keď $(A \times B) \cap (B \times A) = \emptyset$.

Úloha 2.3.6. Dokážte, že pre ľubovoľné množiny A, B, C platí $A \times (B \triangle C) = (A \times B) \triangle (A \times C)$.

Úloha 2.3.7. 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.

2.4 Funkcie

Veľmi dôležitú úlohu v niektorých úvahách v ďalších častiach tejto prednášky budú hrať funkcie (alebo tiež zobrazenia, obidva názvy budeme používať ako ekvivalentné). Veľa vecí, ktoré spomenieme v tejto časti, už poznáte z prvého ročníka. Nové by mali byť nanajvýš pojmy vzor a obrazu množiny.

Definícia 2.4.1. *Zobrazenie* (*funkcia*) z množiny A do B je podmnožina $f \subseteq A \times B$ kartoziánskeho súčinu množín A a B taká, že pre každé $a \in A$ existuje práve jedno $b \in B$ s vlastnosťou $(a, b) \in f$.

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

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

Poznámka 2.4.2. 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.

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

Príklad 2.4.3. Jednoduchým príkladom zobrazenia je zobrazenie $id_A \colon A \to A$ definovaná tak, že pre každé $a \in A$ platí

$$id_A(a) = a.$$

Toto zobrazenie zvykneme nazývať *identické zobrazenie.*

Definícia 2.4.4. Ak $f \colon A \to B$ je zobrazenie a $C \subseteq A$, tak zobrazenie $f|_C \colon C \to B$, definované predpisom

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

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

Množinovo môžeme definíciu zúženia zobrazenia zapísať ako

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

Pripomeňme tiež definíciu skladania zobrazení.

Definícia 2.4.5. Ak $f\colon A \to B$ a $g\colon B \to C$ sú zobrazenia, tak zložené zobrazenie $g \circ f\colon A \to C$ definujeme ako zobrazenie určené predpisom:

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

Definícia 2.4.6. Nech $f\colon X \to Y$ je zobrazenie. Hovoríme, že f je *injektívne* (*prosté*) *zobrazenie* (alebo tiež injekcia), ak pre všetky $x, y \in X$ také, že $x \neq y$, platí $f(x) \neq f(y)$.

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

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

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

Niektoré základné vlastnosti injekcií, surjekcií a bijekcií sú zhrnuté v cvičeniach za touto podkapitolou. (Mnohé z nich by ste mali ovládať z prvého ročníka, prinajmenšom celkom určite tie, ktoré sú uvedené v úlohe 2.4.1.)

Definícia 2.4.7. Nech $f\colon A \to B$ je zobrazenie. Ak existuje zobrazenie $g\colon B \to A$ také, že

$$g \circ f = id_A$$
$$f \circ g = id_B$$

tak hovoríme, že g je *inverzné zobrazenie* k zobrazeniu f a označujeme ho f^{-1}.

Definícia inverzného zobrazenia vlastne hovorí, že:

$$(\forall a \in A) g(f(a)) = a$$
$$(\forall b \in B) f(g(b)) = b$$

Môžeme si tiež uvedomiť, že pre inverzné zobrazenie platí

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

Teda vlastne je to predpis, ktorý „obracia“ pôvodné zobrazenie „naopak“.

Z prvého ročníka viete, že podmienkami z definície je inverzné zobrazenie určené jednoznačne. Okrem toho bude pre nás dôležité aj nasledujúce tvrdenie, ktoré hovorí, za akých predpokladov sa k f dá urobiť inverzné zobrazenie:

Tvrdenie 2.4.8. *Nech $f\colon A \to B$ je zobrazenie. Potom inverzné zobrazenie $f^{-1}\colon B \to A$ existuje práve vtedy, keď f je bijekcia.*

Definícia 2.4.9. Nech $f\colon X \to Y$ je zobrazenie, $A \subseteq X$, $B \subseteq Y$.

Potom množinu

$$f[A] := \{f(a); a \in A\}$$

nazývame *obraz množiny* A v zobrazení f a množinu

$$f^{-1}[B] = \{a \in X; f(a) \in B\}$$

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.)

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

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

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

Tvrdenie 2.4.10. *Nech $f\colon X \to Y$, $g\colon Y \to Z$ sú zobrazenia, $A, B \subseteq X$, $C, D \subseteq Y$, $E \subseteq Z$, $A_i \subseteq X$ a $B_i \subseteq Y$ pre každé $i \in I$. Potom platí*

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

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

2.4.1 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 2.4.11. Nech $f\colon A \to C$, $g\colon B \to D$ sú zobrazenia. Potom ich *karteziánsky súčin* je zobrazenie $f \times g\colon A \times B \to C \times D$ určené predpisom

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

Zobrazenie $f \times g$ je vlastne zobrazenie, ktoré sa na prvej súradnici správa rovnako ako f a na druhej súradnici ako g.

Tvrdenie 2.4.12. *Nech $f\colon A \to C$, $g\colon B \to D$ sú zobrazenia.*
(i) *Ak f aj g sú injekcie, tak $f \times g$ je injekcia.*
(ii) *Ak f aj g sú surjekcie, tak $f \times g$ je surjekcia.*
(iii) *Ak f aj g sú bijekcie, tak $f \times g$ je bijekcia.*

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

(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). □

Cvičenia

Úloha 2.4.1. Dokážte, že:
a) Zloženie dvoch injekcií je injekcia.
b) Zloženie dvoch surjekcií je surjekcia.
c) Zloženie dvoch bijekcií je bijekcia.

Úloha 2.4.2. Nech $f\colon X \to Y$, $g,h\colon Y \to Z$ sú zobrazenia. Dokážte, že:
a) Ak f je surjekcia, tak platí $g \circ f = h \circ f \Rightarrow g = h$.
b) Ak $Z \neq \emptyset$ a platí (pre ľubovoľné $g,h\colon Y \to Z$) implikácia $g \circ f = h \circ f \Rightarrow g = h$, tak f je surjekcia.

Úloha 2.4.3. Nech $g,h\colon X \to Y$, $f\colon Y \to Z$ sú zobrazenia. Dokážte, že:
a) Ak f je injekcia a platí $f \circ g = f \circ h$, tak $g = h$.
b) Ak $X \neq \emptyset$ a pre ľubovoľné $g,h\colon X \to Y$ platí implikácia $f \circ g = f \circ h \Rightarrow g = h$, tak f je injekcia.

Úloha 2.4.4. Ak $f\colon X \to Y$ a $g\colon Y \to X$ sú zobrazenia také, že $g \circ f = id_X$, tak g je surjekcia a f je injekcia. Ukážte na príklade, že g nemusí byť injekcia a f nemusí byť surjekcia.

Úloha 2.4.5. Dokážte tvrdenie 2.4.10. Pre časti tvrdenia, ktoré obsahujú inklúziu a nie rovnosť, nájdite príklady ukazujúce, že nerovnosť môže byť ostrá (rovnosť nemusí vždy platiť).

Úloha 2.4.6. Nech $f\colon X \to Y$ je zobrazenie a $A, B \subseteq X$. Pokúste sa dokázať $f[A \cap B] \subseteq f[A] \cap f[B]$ použitím faktu, že pre ľubovoľné $C \subseteq D \subseteq X$ platí $f[C] \subseteq f[D]$. (Inak povedané, skúste dokázať prvú časť tvrdenia 2.4.10 (v) použitím prvej časti tvrdenia 2.4.10 (xiii).)

Úloha 2.4.7. Nech $f\colon X \to Y$ je zobrazenie. Dokážte, že f je injekcia práve vtedy, keď pre ľubovoľné dve podmnožiny $A, B \subseteq X$ platí $f[A \cap B] = f[A] \cap f[B]$.

Úloha 2.4.8. Nech $f\colon X \to Y$ je zobrazenie. Dokážte, že f je injekcia $\Leftrightarrow$ pre ľubovoľné dve podmnožiny $A, B \subseteq X$ platí $f[B \setminus A] = f[B] \setminus f[A]$.

Úloha 2.4.9. Predpokladajme, že $f\colon X \to Y$ je zobrazenie. Zapíšte pomocou kvantifikátorov výroky „f je injekcia“ a „f je surjekcia“ a znegujte tieto výroky.

Kapitola 3

Kardinálne čísla

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

3.1 Porovnávanie mohutností množín

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

Definícia 3.1.1. Hovoríme, že množiny X a Y majú rovnakú *kardinalitu* (*mohutnosť*), ak existuje bijekcia $f\colon X \to Y$. Označujeme $|X| = |Y|$.

Poznámka 3.1.2. Je užitočné si všimnúť, že ak $|X| = |Y|$ a $|Y| = |Z|$, tak aj $|X| = |Z|$. (Vyplýva to z toho, že zložením dvoch bijekcií dostaneme opäť bijekciu.)

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

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

Poznámka 3.1.3. Znak $=$ zvykneme písať medzi nejaké dva objekty v prípade, že sú totožné. V definícii 3.1.1 sme však symbol rovnosti použili v trochu inom význame. Jedna možnosť, ako sa na to pozerať, je skutočne všetky výskyty zápisov tvaru $|X| = |Y|$ chápať ako iný zápis pre to, že existuje bijekcia medzi X a Y. Pozorovanie z poznámky 3.1.2 do istej miery oprávňuje použitie symbolu $=$, lebo ukazuje, že vzťah „mať rovnakú mohutnosť“ má skutočne podobné vlastnosti ako rovnosť.

Oveľa lepšie by bolo, keby sme skutočne boli schopní definovať nejaké objekty, ktoré by zodpovedali symbolu $|X|$. (Inak povedané, chceli by sme ľubovoľnej množine X priradiť konkrétnu množinu, ktorú označíme $|X|$.) To sa skutočne dá urobiť v rámci axiomatickej teórie ZFC. Na tejto prednáške to robiť nebudeme, uspokojíme sa s takýmto (jednoduchším) pohľadom na kardinálne čísla.

Naším najbližším cieľom je presvedčiť sa, že mnohé veci, ktoré vieme robiť s prirodzenými číslami, fungujú aj pre kardinálne čísla. Ako prvú vec sa kardinálne čísla naučíme porovnávať.

Definícia 3.1.4. Hovoríme, že *kardinalita* množiny X je *menšia alebo rovná* ako kardinalita množiny Y, označujeme $|X| \leq |Y|$, ak existuje injekcia z X do Y.

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

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

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

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

Tvrdenie 3.1.5. *Nech X, Y, Z sú ľubovoľné množiny. Potom platí:*
(i) $|X| \leq |X|$;
(ii) $|X| \leq |Y| \wedge |Y| \leq |Z| \Rightarrow |X| \leq |Z|$
(iii) $|X| = |Y| \Rightarrow |X| \leq |Y|$

Dôkaz. (i) $id_X \colon X \to X$ je injekcia.
(ii) Zloženie dvoch injekcií je injekcia.
(iii) Každá bijekcia je injekcia. □

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

Veta 3.1.6 (Cantor-Bernstein)**.** *Nech X, Y sú množiny. Ak platí $|X| \leq |Y|$ a $|Y| \leq |X|$, tak $|X| = |Y|$.*

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

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

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

Uvedieme dva dôkazy tejto vety, základná myšlienka je v oboch veľmi podobná. Budeme sa snažiť ukázať existenciu takej podmnožiny $C \subseteq X$, pre ktorú je $f|_C$ bijekcia medzi C a $f[C]$ a $g|_{Y \setminus f[C]}$ je bijekcia medzi $X \setminus C$ a $Y \setminus f[C]$, pozri obrázok 3.1. Z týchto dvoch bijekcií už potom vieme poskladať bijekciu medzi X a Y.

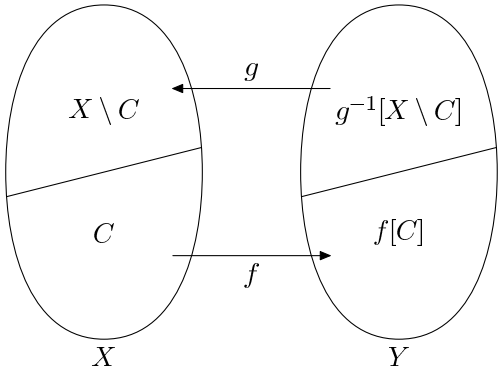
Dôkaz. Nech $f \colon X \to Y$, $g \colon Y \to X$ sú injekcie. Definujme zobrazenie $F \colon \mathcal{P}(X) \to \mathcal{P}(X)$ predpisom

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

Ďalej indukciou definujeme množiny A_n, $n \in \mathbb{N}$ nasledovne:
$A_0 = \emptyset$,
$A_{n+1} = F(A_n)$
a položme $C := \bigcup_{n=1}^{\infty} A_n = \bigcup_{n=0}^{\infty} A_n$.

Potom platí

$$F(C) = F\left(\bigcup_{n=0}^{\infty} A_n\right) = X \setminus g[Y \setminus f[\bigcup_{n=0}^{\infty} A_n]] = X \setminus g[Y \setminus \bigcup_{n=0}^{\infty} f[A_n]] = X \setminus g[\bigcap_{n=1}^{\infty} (Y \setminus f[A_n])] =$$
$$= X \setminus \bigcap_{n=0}^{\infty} g[Y \setminus f[A_n]] = \bigcup_{n=0}^{\infty} (X \setminus g[Y \setminus f[A_n]]) = \bigcup_{n=0}^{\infty} F(A_n) = \bigcup_{n=1}^{\infty} A_n = C.$$



Obr. 3.1: Ilustrácia k dôkazu Cantor-Bernsteinovej vety

V predchádzajúcich úpravách sme použili viackrát tvrdenie 2.4.10 a fakt, že zobrazenia f a g sú injektívne a tiež de Morganove zákony z tvrdenia 2.2.14.

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

$$X \setminus C = g[Y \setminus f[C]].$$

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

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

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

Ukážeme ďalej, že toto zobrazenie je bijektívne. Overme najprv injektívnosť. Nech platí $h(x_1) = h(x_2)$. Rozlíšme tri možnosti, ktoré môžu nastať:
a) Oba prvky sú z množiny C, t.j. $x_1, x_2 \in C$. Potom ak $h(x_1) = h(x_2)$, tak $f(x_1) = f(x_2)$ a z injektívnosti f dostaneme $x_1 = x_2$.
b) Jeden z týchto prvkov je z C a druhý patrí do $X \setminus C$. Nech napríklad $x_1 \in C$ a $x_2 \in X \setminus C$. Ak $h(x_1) = h(x_2)$, tak máme $g(f(x_1)) = x_2$. Potom $x_2 \in g[f[C]]$ a súčasne $x_2 \in X \setminus C = g[Y \setminus f[C]]$, z čoho dostaneme $x_2 \in g[f[C]] \cap g[Y \setminus f[C]] = g[f[C] \cap (Y \setminus f[C])] = g[\emptyset] = \emptyset$, čo je samozrejme spor. (Tu sme využili injektívnosť zobrazenia g, pozri tvrdenie 2.4.10 (v).)
c) Oba prvky sú v $X \setminus C$, t.j. $x_1, x_2 \in X \setminus C$. Potom z $h(x_1) = h(x_2) = y$ vyplýva $g(y) = x_1 = x_2$.

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

Uvedený dôkaz má nevýhodu, že využíva matematickú indukciu a prirodzené čísla. Ak by sme pracovali v rámci axiomatickej teórie množín, musela by tomuto dôkazu predchádzať konštrukcia prirodzených čísel iba na základe axióm. (Aj keď tak ako pracujeme my – v naivnej teórie čísel – by nás zrejme aj takýto dôkaz uspokojil.) Môžeme si však ukázať aj iný dôkaz, ktorý prirodzené čísla ani matematickú indukciu nevyužíva.

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

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

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

Najprv ukážeme, že zobrazenie F je monotónne (vzhľadom na čiastočné usporiadanie $\subseteq$). Ak $A \subseteq B$, tak použitím tvrdení 2.2.14(xi) a 2.4.10 postupne dostaneme

$$\begin{gathered} f[A] \subseteq f[B] \\ Y \setminus f[A] \supseteq Y \setminus f[B] \\ g[Y \setminus f[A]] \supseteq g[Y \setminus f[B]] \\ X \setminus g[Y \setminus f[A]] \subseteq X \setminus g[Y \setminus f[B]] \\ F(A) \subseteq F(B) \end{gathered}$$

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

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

Teda pre každé $B \in \mathcal{S}$ platí $B \subseteq F(B) \subseteq F(C)$, z čoho vyplýva $C = \bigcup\limits_{B \in \mathcal{S}} B \subseteq F(C)$.

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

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

Poznámka 3.1.7. Pre čitateľa, ktorý sa zaoberal teóriou zväzov, môže byť zaujímavé všimnúť si, že sme v dôkaze vlastne zostrojili zobrazenie $F\colon \mathcal{P}(X) \to \mathcal{P}(X)$, ktoré je monotónne. Na dôkaz Cantor-Bernsteinovej vety nám stačilo nájsť pevný bod tohoto zobrazenia. Jeho existencia vyplýva z Knaster-Tarského vety o pevnom bode, keďže $(\mathcal{P}(X), \subseteq)$ je úplný zväz. Takýmto spôsobom je dokázaná Cantor-Bernsteinova veta napríklad v [F, Theorem 3.1.9], [KLŠZ, Príklad 2.3.6]. (V podstate náš dôkaz bol do značnej miery podobný spôsobu, akým sa dokazuje Knaster-Tarského veta, resp. prvý z uvedených dôkazov sa väčšmi ponášal na dôkaz Kleeneho vety o pevnom bode.)

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

Veta 3.1.8. *Nech a, b, c sú kardinálne čísla. Potom platí:*

(i) $a \leq a$;
(ii) $a \leq b \wedge b \leq a \Rightarrow a = b$;
(iii) $a = b \Rightarrow a \leq b$;
(iv) $a \leq b \wedge b \leq c \Rightarrow a \leq c$.

Poznámka 3.1.9. V tomto kontexte je ďalšou prirodzenou otázkou to, či sú ľubovoľné dve kardinálne čísla porovnateľné. Ekvivalentne to môžeme sformulovať aj ako otázku, či pre ľubovoľné dve množiny A, B vždy existuje injekcia $A \to B$ alebo injekcia $B \to A$.

Je to skutočne pravda, dôkaz využíva axiómu výberu.[1] My tento fakt dokazovať nebudeme. Ale to, že naozaj platí, azda stojí za zmienku.

[1] Ak stihneme, axiómu výberu si sformulujeme a niečo málo o nej aj povieme koncom semestra. Pri dôkazoch, ktoré ju používajú, na to upozorníme – hoci sme zatiaľ ani nepovedali, čo vlastne táto axióma hovorí.

Cvičenia

Úloha 3.1.1. Pokúste sa urobiť dôkaz vety 3.1.6 (Cantor-Bernstein) tak, že položíte $C = \bigcap\{B \subseteq X; B \supseteq F(B)\}$.

Úloha 3.1.2. Rozhodnite o platnosti nasledujúceho tvrdenia. (Svoju odpoveď zdôvodnite, t.j. dokážte toto tvrdenie alebo nájdite kontrapríklad.)
Pre ľubovoľné množiny A, B platí $|A| < |B|$ práve vtedy, keď existuje bijekcia medzi množinou A nejakou vlastnou podmnožinou množiny B.

Úloha 3.1.3. Nech A, B sú ľubovoľné množiny. Dokážte (s použitím axiómy výberu), že $|f[A]| \leq |A|$.

3.2 Kardinálna aritmetika

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

Definícia 3.2.1. Nech a, b sú kardinálne čísla a nech A, B sú množiny také, že $|A| = a$, $|B| = b$. Potom:

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

$$a + b = |A \cup B|.$$

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

$$a \cdot b = |A \times B|.$$

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

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

V prvej časti definície navyše požadujeme, aby množiny A a B boli disjunktné. Ak sme už našli množiny A, B spĺňajúce $|A| = a$ a $|B| = b$, tak namiesto nich môžeme zobrať napríklad množiny $A \times \{\emptyset\}$ a $B \times \{\{\emptyset\}\}$. Tieto množiny majú takú istú kardinalitu a určite sú disjunktné.[2]

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

Lema 3.2.2. *Sčitovanie kardinálov je dobre definované.*

Dôkaz. Cvičenie. □

Lema 3.2.3. *Násobenie kardinálov je dobre definované.*

Dôkaz. Máme teda vlastne ukázať, že ak $|A| = |A'|$ a $|B| = |B'|$, tak aj $|A \times B| = |A' \times B'|$. Uvedené predpoklady znamenajú, že existujú bijekcie $f\colon A \to A'$ a $g\colon B \to B'$. Potom podľa tvrdenia 2.4.12 je zobrazenie $f \times g\colon A \times A' \to B \times B'$ tiež bijekcia. □

[2]Stačí si uvedomiť, že bez ohľadu na to aké sú $a \in A$, $b \in B$, určite platí $(a, 0) \neq (b, 1)$.

Lema 3.2.4. *Umocňovanie kardinálov je dobre definované.*

Dôkaz. Teraz chceme ukázať, že existujú bijekcie $f\colon A \to C$ a $g\colon B \to D$, tak existuje aj bijekcia medzi množinami A^B a C^D.

To znamená, že ku každému zobrazeniu $h\colon B \to A$ chceme priradiť zobrazenie z D do C.

$$\begin{array}{ccc} B & \xrightarrow{\ g\ } & D \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle ?} \\ A & \xrightarrow[\ f\ ]{} & C \end{array}$$

Keď si uvedomíme, že g je bijekcia, a teda existuje $g^{-1}\colon D \to B$, tak môžeme definovať $\varphi\colon A^B \to C^D$ predpisom

$$\varphi(h) = f \circ h \circ g^{-1}.$$

Chceli by sme ukázať, že φ je bijekcia. Jedna z možností, ako to overiť, je nájsť inverzné zobrazenie k φ.

Vieme nájsť zobrazenie $\psi\colon C^D \to A^B$ podobným spôsobom ako sme našli φ.

$$\begin{array}{ccc} B & \xrightarrow{\ g\ } & D \\ {\scriptstyle ?}\downarrow & & \downarrow{\scriptstyle k} \\ A & \xrightarrow[\ f\ ]{} & C \end{array}$$

$$\psi(k) = f^{-1} \circ k \circ g.$$

Overme, že ψ je naozaj inverzné zobrazenie k φ.

Pre ľubovoľné $h \in A^B$ máme

$$\psi(\varphi(h)) = f^{-1} \circ (f \circ h \circ g^{-1}) \circ g = (f^{-1} \circ f) \circ h \circ (g^{-1} \circ g) = h.$$

Podobne dostaneme, že

$$\varphi(\psi(k)) = f \circ (f^{-1} \circ k \circ g) \circ g^{-1} = (f \circ f^{-1}) \circ k \circ (g \circ g^{-1}) = k.$$

Zistili sme, že φ má inverzné zobrazenie, čo znamená, že φ je bijekcia. □

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

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

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

Definícia 3.2.5. Ľubovoľné prirodzené číslo n budeme stotožňovať s kardinálnym číslom n-prvkovej množiny. Teda napríklad $|\emptyset| = 0$, $|\{\emptyset\}| = 1$ a $|\{\emptyset, \{\emptyset\}\}| = 2$.

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

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

Poznámka 3.2.6. Zatiaľ ešte nemáme dokázané, že pre každé kardinálne číslo platí buď $a < \aleph_0$ alebo $a \geq \aleph_0$, teda že musí byť buď konečné alebo nekonečné. Ako sme už spomenuli v poznámke 3.1.9, na to aby ľubovoľné dve kardinálne čísla boli porovnateľné potrebujeme axiómu výberu. Pretože s axiómou výberu na tejto prednáške budeme pracovať málo alebo vôbec, uspokojíme sa s takouto definíciou – aj keď s doterajšími vedomosťami nevieme ukázať, že tieto dva prípady už vyčerpávajú všetky možnosti.

Označenie $\mathfrak{c}$ a názov kardinalita kontinua pochádza z toho, že $\mathfrak{c}$ je kardinalita množiny $\mathbb{R}$. Tento fakt overíme neskôr – tvrdenie 3.5.1. Už teraz ukážeme, že $\mathfrak{c} = 2^{\aleph_0}$.

Veta 3.2.7. *Nech X je ľubovoľná množina. Potom platí*

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

Dôkaz. Chceme ukázať existenciu bijekcie medzi množinami $\{0,1\}^X$ a $\mathcal{P}(X)$.

Na to stačí nájsť zobrazenia $f\colon \mathcal{P}(X) \to \{0,1\}^X$ a $g\colon \{0,1\}^X \to \mathcal{P}(X)$, ktoré sú navzájom inverzné. Definujme ich predpisom

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

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

Keďže k zobrazeniu f existuje inverzné zobrazenie, je to bijekcia. □

Dôsledok 3.2.8.

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

3.2.1 Vlastnosti sčitovania kardinálov

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

Veta 3.2.9. *Nech a, b, c sú kardinálne čísla, potom platí*

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

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

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

Veta 3.2.10. *Nech a, b, c sú kardinálne čísla také, že $b \leq c$. Potom*

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

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

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

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

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

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

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

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

To znamená, že pri vhodnej voľbe množiny B môžeme priamo predpokladať $B \subseteq C$. Tým sa dôkaz značne zjednoduší – z tvrdenia 2.2.11(iii) vieme, že potom $A \cup B \subseteq A \cup C$. Z toho už je jasná existencia injekcie definovanej jednoducho ako $x \mapsto x$ pre všetky $x \in A \cup B$.

Príklad 3.2.11. Priamo, konštrukciou príslušnej bijekcie, ukážeme, že platí

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

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

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

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

$$\aleph_0 = 0 + \aleph_0 \leq n + \aleph_0 \leq \aleph_0 + \aleph_0 = \aleph_0$$

Z Cantor-Bernsteinovej vety potom máme

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

Z toho vidíme napríklad aj to, že výsledok analogický k vete 3.2.10 neplatí pre ostrú nerovnosť.

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

Tvrdenie 3.2.12. *Ak a je nekonečné kardinálne číslo, tak $\aleph_0 + a = a$.*

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

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

Teraz už vieme veľmi jednoducho zostrojiť bijekciu medzi $\mathbb{N}\times\{0\}\cup A\times\{1\}$ a A analogickým spôsobom ako v predchádzajúcom príklade.

$$f(n, 0) = 2n, \text{pre } n \in \mathbb{N}$$
$$f(n, 1) = 2n + 1, \text{pre } n \in \mathbb{N}$$
$$f(a, 1) = a, \text{ak } a \in A, a \notin \mathbb{N}$$

□

3.2.2 Vlastnosti násobenia kardinálov

Veta 3.2.13. *Nech a, b, c sú kardinálne čísla, potom platí*

$$ab = ba$$
$$a(bc) = (ab)c$$
$$a(b + c) = ab + ac$$

Dôkaz. Nech A, B, C sú ľubovoľné množiny.

Na dôkaz prvého tvrdenia stačí ukázať existenciu bijekcie medzi $A\times B$ a $B\times A$. Zobrazenie $f\colon A \times B \to B \times A$ definovaní predpisom

$$f\colon (a, b) \mapsto (b, a)$$

pre $a \in A$, $b \in B$ je bijekcia.

Na dôkaz druhej časti stačí nájsť bijekciu $g\colon A \times (B \times C) \to (A \times B) \times C$. Takouto bijekciou je zobrazenie definované ako

$$g\colon (a, (b, c)) \mapsto ((a, b), c)$$

pre $a \in A$, $b \in B$, $c \in C$.

V tretej časti máme, za predpokladu, že B a C sú disjunktné, nájsť bijekciu medzi $A\times(B\cup C)$ a $(A\times B)\cup(A\times C)$. Z tvrdenia 2.3.2 však vieme, že platí dokonca rovnosť $A\times(B\cup C) = (A\times B)\cup(A\times C)$. □

Veta 3.2.14. *Nech a, b, c sú kardinálne čísla také, že $b \leq c$. Potom*

$$ab \leq ac.$$

Dôkaz. Nech $f\colon B \to C$ je injekcia. Potom podľa tvrdenia 2.4.12 je aj zobrazenie $id_A \times f\colon A\times B \to A \times C$ injekcia. □

Opäť platí analogická poznámka ako pri vete 3.2.10. Mohli by sme priamo predpokladať, že $B \subseteq C$ a potom si stačí všimnúť, že $A \times B \subseteq A \times C$ (pozri úlohu 2.3.3).

Príklad 3.2.15. Ukážeme, že platí

$$\aleph_0 \cdot \aleph_0 = \aleph_0. \tag{3.1}$$

Z rovnosti (3.1) dostaneme, že pre každé $n \in \mathbb{N}$, $n > 0$, platí

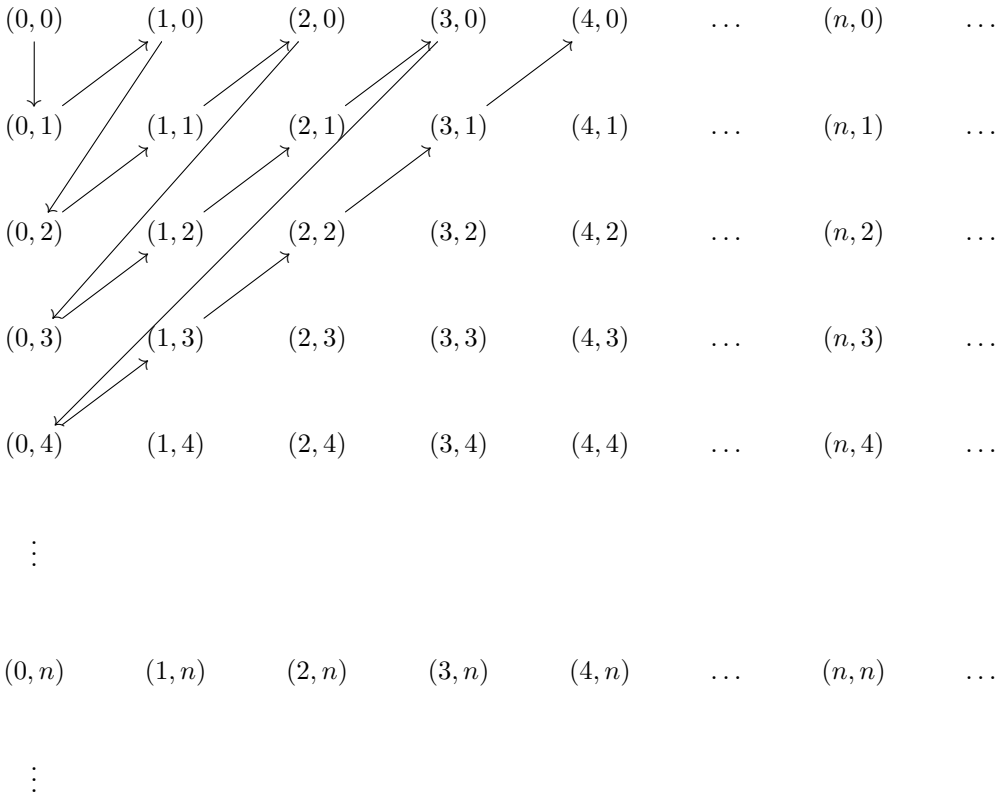
$$\aleph_0 \leq n.\aleph_0 \leq \aleph_0.\aleph_0 = \aleph_0.$$

Z Cantor-Bernsteinovej vety potom vyplýva rovnosť

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

Na dôkaz rovnosti (3.1) nám stačí zostrojiť bijekciu medzi $\mathbb{N} \times \mathbb{N}$ a $\mathbb{N}$. Takýchto bijekcií sa dá nájsť veľa, ako prvú si ukážeme jednu veľmi známu pochádzajúcu už od G. Cantora.

Nasledujúci obrázok nám ukazuje, ako môžeme usporiadané dvojice prirodzených čísel usporiadať do postupnosti:



Zobrazenie $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definujeme tak, že každej dvojici priradíme pozíciu, na ktorej sa nachádza v tejto postupnosti, t.j. $(0,0) \mapsto 0$, $(0,1) \mapsto 1$, $(1,0) \mapsto 2$, $(0,2) \mapsto 3$, $(1,1) \mapsto 4$, $(2,0) \mapsto 5$ atď.

Toto zobrazenie vieme popísať aj jednoduchým predpisom. Všimnime si, že dvojice na tej istej diagonále (t.j. také dvojice (m,n), ktoré majú rovnaký súčet $m+n$) zoraďujeme podľa prvej súradnice a všetky prvky z diagonál, ktoré sú naľavo od nich. Teda ak $m+n=s$, tak $1+2+\cdots+s = \frac{s(s+1)}{2}$ prirodzených čísel sme použili na predchádzajúce diagonály. Poradie na diagonále určíme podľa m, čiže dostaneme

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

(Môžete si túto formulu prekontrolovať pre niektoré konkrétne dvojice.)

O tom, že takéto zobrazenie je bijektívne, by vás snáď mohol presvedčiť obrázok, ktorým sme ho znázornili.

Pokiaľ by vám však takýto argument nestačil, je tu pre vás aj podrobnejší formálny dôkaz.

Dôkaz. Označme $\Delta_a = \sum_{k=1}^{a} k = \frac{a(a+1)}{2}$. (Čiže Δ_a je a-te trojuholníkové číslo.)

Potom funkciu f môžeme zapísať ako

$$f(m,n) = \Delta_{m+n} + m.$$

Ďalej označme $I_a = \{\Delta_a, \Delta_a + 1, \ldots, \Delta_{a+1} - 1\}$ pre každé $a \in \mathbb{N}$. Systém $\{I_a, a \in \mathbb{N}\}$ tvorí rozklad množiny $\mathbb{N}$. (Tento fakt ľahko vyplýva z $\Delta_a = 0$ a $\Delta_a < \Delta_{a+1}$.)

Takisto je zrejmé, že $f(m,n) \in I_{m+n}$. Vďaka tomu z rovnosti $f(m+n) = f(m'+n')$ vyplýva $m+n = m'+n'$. Z $\Delta_{m+n} + m = \Delta_{m+n} + m'$ dostaneme $m = m'$, a teda aj $n = n'$. Tým je dokázaná injektívnosť zobrazenia f.

Overme ešte surjektívnosť. Vieme, že každé $x \in \mathbb{N}$ patrí do niektorej množiny I_a (keďže tieto množiny tvoria rozklad). Stačí teda nájsť m, n tak, že $m+n = a$ a $x = \Delta_a + m$. Z nerovnosti $\Delta_a \leq x \leq \Delta_{a+1} - 1$ a z toho, že $\Delta_{a+1} - \Delta_a = a + 1$ dostaneme, že pre $m = x - \Delta_a$ platí nerovnosť $0 \leq m \leq \Delta_{a+1} - 1 - \Delta_a = a$. Z toho vyplýva, že ak položíme $n = a - m$, tak m aj n sú prirodzené čísla a platí $f(m,n) = a$. □

Inú bijekciu $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ môžeme dostať s použitím faktu, že každé prirodzené číslo väčšie ako 0 sa dá zapísať ako súčin mocniny čísla 2 a nepárneho čísla. (Toto viete odvodiť z poznatkov o deliteľnosti prirodzených čísel, ktoré máte z prvého ročníka [Č].) Teda zobrazenie

$$g(m,n) = 2^m.(2n+1) - 1$$

je bijekcia z $\mathbb{N} \times \mathbb{N}$ do $\mathbb{N}$.

Poznámka 3.2.16. S použitím axiómy výberu sa dá dokázať, že kardinálne sčitovanie a násobenie je jednoduché, pre ľubovoľné nekonečné kardinály a, b totiž platí

$$a + b = a.b = \max\{a, b\}.$$

(Zatiaľ dokonca nevieme ani to, či existuje maximum z kardinálnych čísel a, b; pozri poznámku 3.1.9.)

V tejto kapitole však budeme (v dôkazoch i cvičeniach) využívať iba veci, ktoré sme o kardinálnej aritmetike už dokázali.

3.2.3 Vlastnosti kardinálneho umocňovania

Pri prirodzených číslach sme používali označenie a^2 ako synonymum zápisu $a \cdot a$. (Podobne pre $a^3, a^4, \ldots$) Ukážeme si, že aj pre kardinálne čísla predstavujú tieto dva zápisy to isté.

Tvrdenie 3.2.17. *Ak a je ľubovoľné kardinálne číslo, tak platí*

$$a^2 = a \cdot a.$$

Dôkaz. Máme vlastne ukázať, že pre ľubovoľnú množinu existuje bijekcia medzi $A^{\{0,1\}}$ a $A \times A$.

Definujme $\varphi\colon A^{\{0,1\}} \to A \times A$ ako

$$\varphi(f) = (f(0), f(1)).$$

Súčasne definujme $\psi\colon A \times A \to A^{\{0,1\}}$ tak, že $\psi(a,b)$ je zobrazenie určené predpisom

$$\psi(a,b)(0) = a,$$
$$\psi(a,b)(1) = b.$$

(Namiesto zápisu $\psi((a,b))$ píšeme stručnejšie $\psi(a,b)$.) Ľahko sa overí, že φ a ψ sú navzájom inverzné zobrazenia, čiže φ aj ψ sú bijekcie. □

Takisto by bolo ľahké rozšíriť toto tvrdenie indukciou na ďalšie prirodzené čísla. (Hoci sme zatiaľ stále formálne neskonštruovali prirodzené čísla a ani neukázali, že sú dobre usporiadané a teda na nich funguje indukcia.)

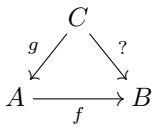
Veta 3.2.18. *Ak a, b, c sú kardinálne čísla také, že $a \leq b$, tak $a^c \leq b^c$.*

Dôkaz. Nech $|A| = a$, $|B| = b$, $|C| = c$. Môžeme priamo predpokladať, $A \subseteq B$. Potom platí aj $A^C \subseteq B^C$. (Každé zobrazenie z C do A je súčasne zobrazením z C do B.) □

Napriek tomu, že máme takýto jednoduchý dôkaz, pokúsme sa ešte urobiť dôkaz priamo z existencie injekcie z A do B. (Aby sme si trochu precvičili prácu so zobrazeniami medzi množinami zobrazení – v ďalších dôkazoch budeme takéto niečo často potrebovať.)

Dôkaz. Vlastne máme dokázať: Ak existuje injekcia $f\colon A \to B$, tak existuje aj injekcia z množiny A^C do množiny B^C. Skúsme teda najprv vymyslieť, ako by sme pomocou zobrazenia f mohli definovať zobrazenie $\varphi\colon A^C \to B^C$ a pri troche šťastia sa nám ho snáď podarí vymyslieť tak, aby bolo injektívne a aj jeho injektívnosť dokázať.

Hľadáme teda zobrazenie, ktoré ľubovoľnej funkcii $g\colon C \to A$ priradí nejakú funkciu z C do B. Našu situáciu si môžeme znázorniť takto:



Hneď vidíme, že f a g určujú zobrazenie z C do B – konkrétne zobrazenie $f \circ g$. Teda asi najprirodzenejší spôsob ak definovať nejaké zobrazenie z A^C do B^C pomocou f je

$$\varphi\colon g \mapsto f \circ g$$
$$\varphi(g) = f \circ g$$

Overme ešte, že toto zobrazenie je injektívne. Pýtame sa, či platí

$$\varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$$
$$f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2$$

Rovnosť $f \circ g_1 = f \circ g_2$ znamená, že pre každé $x \in C$ platí

$$f(g_1(x)) = f(g_2(x)).$$

Pretože f je injektívne, vyplýva z nej rovnosť

$$g_1(x) = g_2(x).$$

Platnosť tejto rovnosti pre každé $x \in X$ znamená rovnosť zobrazení $g_1 = g_2$; čiže presne to, čo sme chceli dokázať. □

Veta 3.2.19. *Ak a, b, c sú kardinálne čísla také, že $a \leq b$ a $c \neq 0$, tak*

$$c^a \leq c^b.$$

Dôkaz. Nech A, B, C sú množiny také, že $|A| = a$, $|B| = b$ a $|C| = c$.

Predpoklad $c \neq 0$ nám hovorí, že $C \neq \emptyset$. Zvoľme si ľubovoľné $c_0 \in C$.

Vieme, že existuje injekcia $f\colon A \to B$. Na základe už viackrát spomenutej úvahy môžeme priamo predpokladať, že $A \subseteq B$. Definujme zobrazenie $\varphi\colon C^A \to C^B$ tak, že

$$\varphi(g)(x) = \begin{cases} g(x) & \text{pre } x \in A, \\ c_0 & \text{pre } x \notin A. \end{cases}$$

pre ľubovoľné $g\colon A \to C$.

Zobrazenie φ je injekcia. Ak platí $\varphi(g) = \varphi(h)$, tak pre každé $x \in A$ platí $g(x) = \varphi(g)(x) = \varphi(h)(x) = h(x)$, a teda $g = h$. □

Ešte si môžeme všimnúť, že v prípade $c = 0$ predchádzajúca veta neplatí. Priamo z definície kardinálneho umocňovania zistíme, že $0^0 = 1$ a $0^a = 0$ pre $a \neq 0$.

Ľubovoľné zobrazenia z X do $\emptyset$ je podmnožina $X \times \emptyset = \emptyset$. Teda ak existuje nejaké zobrazenie $X \to \emptyset$, môže to byť jedine $\emptyset$. V prípade $X = \emptyset$ množina $\emptyset$ spĺňa definíciu zobrazenia, v prípade $X \neq \emptyset$ nie. Teda máme $\emptyset^\emptyset = \{\emptyset\}$ a $\emptyset^A = \emptyset$ pre $A \neq \emptyset$.

Veta 3.2.20. *Pre ľubovoľné kardinálne čísla platí*

$$a^{b+c} = a^b \cdot a^c.$$

Dôkaz. Vlastne máme dokázať, že pre ľubovoľné množiny A, B, C také, že B a C sú disjunktné, existuje bijekcia medzi $A^{B \cup C}$ a $A^B \times A^C$.

T.j. chceli by sme nájsť zobrazenie $\varphi\colon A^{B\cup C} \to A^B \times A^C$ alebo zobrazenie $\psi\colon A^B \times A^C \to A^{B\cup C}$ a ukázať o ňom, že je bijekcia. My budeme postupovať tak, že nájdeme zobrazenia oboma smermi a ak sa nám podarí ukázať, že jedno z nich je inverzné k druhému, tak z toho vieme, že ide o bijekcie.

Aby sme definovali φ, tak vlastne potrebujeme každej funkcii $f\colon B \cup C \to A$ priradiť dvojicu funkcií – prvá z nich ide z B do A a druhá z C do A. Zobrazeniu z $B \cup C$ do A však vieme priradiť zobrazenie na menšej množine veľmi prirodzeným spôsobom – pôjde o zúženie zobrazenia na túto podmnožinu. Môžeme teda definovať zobrazenie $\varphi\colon A^{B\cup C} \to A^B \times A^C$ nasledovne:

$$\varphi\colon f \mapsto (f|_B, f|_C)$$
$$\varphi(f) = (f|_B, f|_C)$$

Ak hľadáme zobrazenie $\psi\colon A^B \times A^C \to A^{B\cup C}$, tak vlastne každej dvojici zobrazení $g\colon B \to A$, $h\colon C \to A$ chceme priradiť zobrazenie z $B \cup C$ do A. Opäť, máme pomerne prirodzený spôsob, ako to môžeme spraviť, dvojici (g, h) priradíme zobrazenie definované predpisom

$$\psi(g,h)(x) = \begin{cases} g(x) & \text{ak } x \in B, \\ h(x) & \text{ak } x \in C. \end{cases}$$

Na tomto mieste využívame fakt, že B a C sú disjunktné – v opačnom prípade by predchádzajúci predpis nemusel definovať zobrazenie.

(Intuitívna predstava za predchádzajúcimi úvahami je asi takáto: Jedným smerom sme postupovali tak, že zobrazenie z $B \cup C$ do A sme rozdelili na 2 zobrazenia na 2 častiach definičného oboru. Zobrazenie ψ zase tieto 2 zobrazenia naspäť zlepí – to je zhruba aj dôvod, prečo sú tieto 2 priradenia jedno k druhému inverzné; overíme to však podrobne.)

To, že ψ je inverzné zobrazenie k φ overíme, tak, že ukážeme, že pri zložení $\varphi \circ \psi$ aj $\psi \circ \varphi$ dostaneme identické zobrazenie.

Skúsme najprv vyrátať, čomu sa rovná $\psi \circ \varphi$. Pre ľubovoľné $f\colon B \cup C \to A$ máme $\psi(\varphi(f)) = \psi(f|_B, f|_C)$ po dosadení $x \in B \cup C$ dostaneme

$$\psi(\varphi(f))(x) = \psi(f|_B, f|_C)(x) = \begin{cases} f|_B(x) = f(x) & \text{ak } x \in B, \\ f|_C(x) = f(x) & \text{ak } x \in C, \end{cases}$$

teda $\psi(\varphi(f))(x) = f(x)$ pre každé $x \in B \cup C$, čiže zobrazenia $\psi(\varphi(f))$ a f sa rovnajú. Dostali sme:

$$(\forall f \in A^{B \cup C})\ \psi(\varphi(f)) = f$$
$$\psi \circ \varphi = id_{A^{B \cup C}}$$

Zostáva nám ešte pozrieť sa na zobrazenie $\varphi \circ \psi\colon A^B \times A^C \to A^B \times A^C$. Ak máme ľubovoľnú dvojicu $g\colon B \to A$, $h\colon C \to A$, tak priamo z definície zobrazenia ψ vidno, že $\psi(g,h)|_B = g$ a $\psi(g,h)|_C = h$, a teda

$$\varphi(\psi(g,h)) = (\psi(g,h)|_B, \psi(g,h)|_C) = (g,h).$$

Teda $\varphi \circ \psi = id_{A^B \times A^C}$.

Zistili sme, že $\psi = \varphi^{-1}$, teda φ aj ψ sú bijekcie. □

Veta 3.2.21. *Pre ľubovoľné kardinálne čísla platí* $(a^b)^c = a^{bc}$.

Dôkaz. Pre ľubovoľné A, B, C chceme nájsť bijekciu medzi $(A^B)^C$ a $A^{B \times C}$. Opäť, pokúsime sa nájsť nejaké zobrazenia $\varphi\colon (A^B)^C \to A^{B \times C}$ a $\psi\colon A^{B \times C} \to (A^B)^C$ a ukázať, že sú navzájom inverzné.

Hľadáme zobrazenie $\varphi\colon (A^B)^C \to A^{B \times C}$. T.j. ak máme dané nejaké zobrazenie $f\colon C \to A^B$, chceli by sme k nemu nájsť niečo, čo dvojiciam $(b,c) \in B \times C$ priradí prvky z A. Pre ľubovoľné $c \in C$ však máme zobrazenie $f(c)\colon B \to A$ – čiže je dosť prirodzené dvojici (b,c) priradiť $f(c)(b)$, t.j.

$$\varphi(f)\colon B \times C \to A$$
$$\varphi(f)(b,c) = f(c)(b)$$

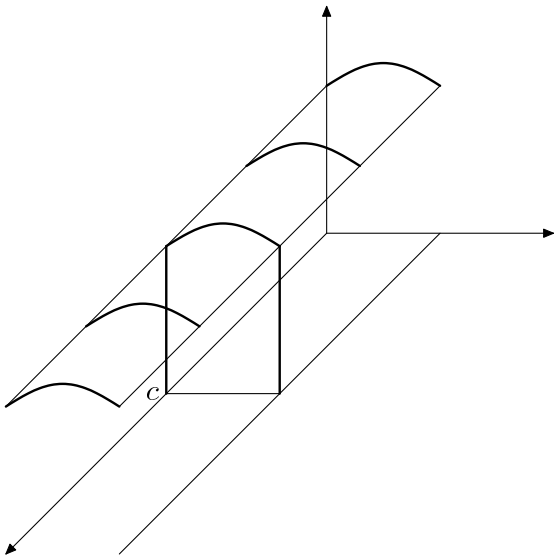
Obrátene, každému zobrazeniu $g\colon B \times C \to A$ by sme chceli priradiť zobrazenie $\psi(g)\colon C \to A^B$, t.j. zobrazenie, ktoré každému prvku z C priradí nejaké zobrazenie z B do A. Ak máme dané zobrazenie z $B \times C$ do A, zafixujeme nejaké $c \in C$ a meníme len prvok $b \in B$ vidíme, že dostaneme zobrazenie z B do A. Presnejšie to môžeme zapísať

$$(\psi(g))(c)\colon B \to A$$
$$(\psi(g))(c)(b) = g(b,c)$$

Toto priradenie je načrtnuté na obr. 3.2, kde $A = \mathbb{R}$, $B = \langle 0,1\rangle$, $C = \langle 0,\infty)$. Rezy načrtnuté na grafe funkcie sú práve funkcie z B do A priradené jednotlivým prvkom z C. (Naschvál som zvolil množiny A, B a C rôzne, aby sa na obrázku dalo vidieť, ktorá množina je ktorá.)

Opäť, priamo dosadením nám vyjde, že $\varphi \circ \psi$ aj $\psi \circ \varphi$ je identita. Počítajme najprv $\varphi \circ \psi\colon A^{B \times C} \to A^{B \times C}$. Pre ľubovoľné $g\colon B \times C \to A$ chceme zistiť, čomu sa rovná zobrazenie $\varphi(\psi(g))\colon B \times C \to A$. Dostaneme (priamo použitím definície zobrazení φ a ψ)

$$\varphi(\psi(g))(b,c) = \psi(g)(c)(b) = g(b,c).$$



Obr. 3.2: Obrázok ilustrujúci postup v dôkaze vety 3.2.21. (Použitá funkcia je $f(x,y) = \frac{3}{2} + \frac{1}{5}\sin \pi x$.)

Vyšlo nám, že $\varphi(\psi(g)) = g$ pre každé $g \in A^{B\times C}$, a teda $\varphi \circ \psi = id_{A^{B\times C}}$.

Skúsme teraz vyrátať $\psi \circ \varphi\colon (A^B)^C \to (A^B)^C$. Ak máme zobrazenie $f\colon C \to A^B$, chceme zistiť, či platí $\psi(\varphi(f)) = f$. Použitím definície φ a ψ máme

$$\psi(\varphi(f))(c)(b) = \varphi(f)(b,c) = f(c)(b).$$

Keďže táto rovnosť platí pre všetky $b \in B$, znamená to rovnosť zobrazení

$$\psi(\varphi(f))(c) = f(c).$$

Opäť, predchádzajúca rovnosť platí pre každé $c \in C$, teda $\psi \circ \varphi(f) = f$. Posledná rovnosť (ktorá platí pre ľubovoľné $f \in (A^B)^C$) znamená rovnosť zobrazení $\psi \circ \varphi = id_{(A^B)^C}$.

Zistili sme, že $\psi = \varphi^{-1}$, preto obe zobrazenia φ aj ψ sú bijekcie. □

Môžeme si ukázať ešte jednu identitu týkajúcu sa umocňovania kardinálov, ktorá má o čosi jednoduchší dôkaz než predošlé tvrdenia. Stručne povedané, ide vlastne o to, že každé zobrazenie $C \to A \times B$ sa dá jednoznačne rozdeliť na dve „zložky“ – na zobrazenia $C \to A$ a $C \to B$. Aj Pokúsime sa teraz dôkaz tohoto faktu aj formálne zapísať. (Urobíme to dokonca dvoma spôsobmi.)

Veta 3.2.22. *Pre ľubovoľné kardinálne čísla a, b, c platí*

$$(ab)^c = a^c \cdot b^c.$$

V dôkaze budeme používať nasledujúce funkcie, ktorým sa často hovorí projekcie. Ak máme karteziánsky súčin dvoch množín A a B, tak môžeme definovať zobrazenia $p_B\colon A\times B \to B$ predpisom

$$p_A(a,b) = a$$
$$p_B(a,b) = b$$

Pre nás bude užitočná táto vlastnosť projekcií: Ak máme ľubovoľný prvok $x \in A \times B$, tak $(p_A(x), p_B(x)) = x$.

$$(\forall x \in A \times B)(p_A(x), p_B(x)) = x \tag{3.2}$$

Platnosť tejto podmienky sa overí vcelku ľahko. Skutočne, každý prvok z karteziánskeho súčinu $A \times B$ je tvaru $x = (a, b)$. Pre takúto usporiadanú dvojicu skutočne dostaneme

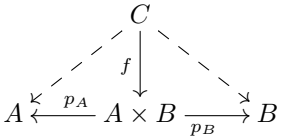
$$(p_A(x), p_B(x)) = (p_A(a, b), p_B(a, b)) = (a, b) = x.$$

Dôkaz. Chceme ukázať existenciu bijekcie medzi množinami $(A \times B)^C$ a $A^C \times A^B$. To by sa nám podarilo, ak by sme vedeli nájsť zobrazenia

$$\varphi\colon (A \times B)^C \to A^C \times B^C$$
$$\psi\colon A^C \times B^C \to (A \times B)^C$$

a ukázať, že tieto zobrazenia sú navzájom inverzné.

Ak chceme zadefinovať zobrazenie φ, tak každej funkcii $f\colon C \to A \times B$ by sme mali priradiť dvojicu zobrazení, ktoré idú z C do A resp. z B do A. Všimnime si, aké zobrazenia máme k dispozícii.



Vidíme, že vieme dostať zobrazenia $p_A \circ f\colon C \to A$ a $p_B \circ f\colon C \to B$.

Môžeme teda zadefinovať

$$\varphi(f) = (p_A \circ f, p_B \circ f).$$

Obrátene, ak máme dvojicu zobrazení $g\colon C \to A$ a $h\colon C \to A$, chceli by sme im priradiť zobrazenie $\psi(g, h)\colon C \to A \times B$. Vcelku prirodzený spôsob je urobiť to takto:

$$\psi(g, h)(c) = (g(c), h(c)).$$

Podobne ako v predošlých dôkazoch sme našli nejaké zobrazenia oboma smermi, stačí už iba overiť, či ψ je inverzné zobrazenie k φ.

Pozrime sa najprv na to, čo dostaneme zložením $\psi \circ \varphi$. Máme

$$\psi(\varphi(f)) = \psi(p_A \circ f, p_B \circ f).$$

chceme overiť, či zobrazenie vpravo je rovné zobrazeniu f. Pozrime sa na to, čo dostaneme dosadením ľubovoľného prvku $c \in C$:

$$\psi(\varphi(f))(c) = \psi(p_A \circ f, p_B \circ f)(c) = (p_A(f(c)), p_B(f(c))) \overset{(3.2)}{=} f(c).$$

V poslednom kroku sme využili platnosť (3.2).

Zistili sme, že

$$\psi \circ \varphi = id_{(A \times B)^C}.$$

Zostáva nám pozrieť sa na ich zloženie v opačnom poradí. Priamo z definície máme

$$\varphi(\psi(g, h)) = (p_A \circ \psi(g, h), p_B \circ \psi(g, h)).$$

Chceme overiť, či dvojica na pravej strane je rovná (g, h) t.j. či

$$p_A \circ \psi(g, h) = g$$
$$p_B \circ \psi(g, h) = h$$

Rovnosť dvoch zobrazení môžeme overiť tak, že dosadíme ľubovoľný prvok $c \in C$. Skutočne dostaneme

$$p_A(\psi(g, h)(c)) = p_A(g(c), h(c)) = g(c)$$
$$p_B(\psi(g, h)(c)) = p_B(g(c), h(c)) = h(c)$$

čo ukazuje uvedené rovnosti.

Platí teda aj

$$\varphi \circ \psi = id_{A^C \times B^C}.$$

Zistili sme, že ψ je inverzné zobrazenie k φ, čo znamená, že φ je bijekcia. □

Skúsme ten istý dôkaz zapísať trochu inak. Nasledujúci dôkaz je vlastne totožný s dôkazom, ktorý sme uviedli, ale vyhli sme sa v ňom používaniu projekcií. Je na vás, aby ste si vybrali, ktorý dôkaz sa vám zdá zrozumiteľnejší. (Samozrejme, pozrieť si môžete oba dôkazy.)

Dôkaz. Chceme nájsť zobrazenia

$$\varphi\colon (A \times B)^C \to A^C \times B^C$$
$$\psi\colon A^C \times B^C \to (A \times B)^C$$

také, že $\varphi \circ \psi$ aj $\psi \circ \varphi$ je identita.

Zobrazenie φ by malo ľubovoľnej funkcii $f\colon C \to A \times B$ priradiť nejakú dvojicu funkcií $\varphi(f) = (g, h)$, kde $g\colon C \to A$, $h\colon C \to B$.

Pre ľubovoľné $c \in C$ je $f(c)$ nejaká usporiadaná dvojica z $A \times B$, t.j. existujú (jednoznačne určené) prvky $a \in A$, $b \in B$ také, že $f(c) = (a, b)$. Takto vieme prvku $c \in C$ priradiť jednoznačne prvok $a \in A$ a tiež prvok $b \in B$. Čiže máme zobrazenia z C do A a z C do B, ktoré môžeme zobrať za $\varphi(f)$.

Voľbu zobrazení g a h môžeme stručne zapísať podmienkou

$$\varphi(f) = (g, h) \qquad \Leftrightarrow \qquad f(c) = (g(c), h(c)). \tag{3.3}$$

Ďalej chceme priradiť dvojici zobrazení $g\colon C \to A$, $h\colon C \to B$ nejaké zobrazenie $C \to A \times B$. Vcelku prirodzený spôsob (rovnaký ako v predošlom dôkaze) je

$$\psi(g, h)(c) = (g(c), h(c)).$$

Teraz chceme overiť, či $\psi(\varphi(f)) = f$. Vieme, že $\varphi(f) = (g, h)$ pre zobrazenia g, h jednoznačne určené podmienkou (3.3). Potom máme

$$\psi(\varphi(f))(c) = \psi(g, h)(c) = (g(c), h(c)) \overset{(3.3)}{=} f(c).$$

Táto rovnosť platí pre ľubovoľné $c \in C$, teda dostávame

$$\psi(\varphi(f)) = f.$$

Opäť z toho, že posledná uvedená rovnosť platí pre ľubovoľné $f\colon C \to A \times B$ dostávame

$$\psi \circ \varphi = id_{(A \times B)^C}.$$

Tiež nás zaujíma, či $\varphi(\psi(g,h)) = (g,h)$. Dvojica zobrazení $\varphi(\psi(g,h))$ je jednoznačne určená podmienkou (3.3), namiesto f však teraz máme dosadiť $\psi(g,h)$. Dostávame

$$\varphi(\psi(g,h)) = (g,h) \qquad \Leftrightarrow \qquad \psi(g,h)(c) = (g(c), h(c)),$$

čo platí priamo na základe definície zobrazenia ψ.

Z uvedenej rovnosti (a z toho, že platí pre ľubovoľné g, h) opäť dostaneme

$$\varphi \circ \psi = id_{A^C \times B^C}.$$

Zistili sme, že ψ je inverzné zobrazenie k φ, čo znamená, že φ je bijekcia. □

Veta 3.2.23. *Pre ľubovoľné kardinálne čísla a, b platí*

$$a^b \leq 2^{ab}.$$

Dôkaz. Ak množiny A, B sú také, že $|A| = a$ a $|B| = b$, tak $A^B \subseteq \mathcal{P}(B \times A)$. (Vyplýva to priamo z definície zobrazenia.)

To ale znamená, že $|A^B| \leq |\mathcal{P}(B \times A)|$ a $a^b \leq 2^{ab}$. □

Ak v predchádzajúcej vete položíme $b = 1$, tak dostaneme

Dôsledok 3.2.24. *Pre ľubovoľné kardinálne číslo a platí*

$$a \leq 2^a.$$

Cvičenia

Úloha 3.2.1. Ukážte, že $|\mathbb{Z}| = \aleph_0$. (T.j. nájdite bijekciu medzi $\mathbb{Z}$ a $\mathbb{N}$.)

Úloha 3.2.2. Ukážte, že $\mathfrak{c}.\mathfrak{c} = \mathfrak{c}$ a $\mathfrak{c}^{\aleph_0} = \mathfrak{c}$.

Úloha 3.2.3. Ukážte, že pre ľubovoľný konečný kardinál n platí $\mathfrak{c} = n.\mathfrak{c} = \mathfrak{c}.\mathfrak{c} = \mathfrak{c}^n = \mathfrak{c}^{\aleph_0}$.

Úloha 3.2.4. Ukážte, že pre ľubovoľný konečný kardinál n platí $2^{\aleph_0} = n^{\aleph_0} = \aleph_0^{\aleph_0} = \mathfrak{c}^{\aleph_0} = \mathfrak{c}$.

Úloha 3.2.5. S využitím faktu, že pre nekonečné kardinály platí $b.b = b$ (ktorý dokážeme neskôr) ukážte, že ak $2 < a \leq b$, kde a, b sú nekonečné kardinály, tak $2^b = a^b$.

Úloha 3.2.6. Ukážte priamo z definície (t.j. konštrukciou bijekcie resp. injekcie), že:
a) Ak $|A| = |B|$, tak $|\mathcal{P}(A)| = |\mathcal{P}(B)|$.
b) Ak $|A| \leq |B|$, tak $|\mathcal{P}(A)| \leq |\mathcal{P}(B)|$.

Úloha 3.2.7. Dokážte dôsledok 3.2.24 bez toho, aby ste sa odvolávali na vetu 3.2.23. Ukážte, ako potom možno z uvedeného dôsledku odvodiť vetu 3.2.23.

Úloha 3.2.8. Ukážte, že ak pre množiny A, B platí $|A \setminus B| = |B \setminus A|$, tak $|A| = |B|$.

Úloha 3.2.9*. Aká je kardinalita množiny všetkých bijekcií z $\mathbb{N}$ do $\mathbb{N}$? (Bijekcie z $\mathbb{N}$ do $\mathbb{N}$ sa niekedy zvyknú nazývať aj permutáciami množiny $\mathbb{N}$. Na základe analógie s prirodzenými číslami by sme kardinalitu takejto množiny mohli nazvať $\aleph_0$-faktoriál.)

3.3 Cantorova veta a diagonálna metóda

Veta 3.3.1 (Cantor)**.** *Pre každú množinu X platí $|X| < |\mathcal{P}(X)|$.*

Cantorovu vetu môžeme ekvivalentne preformulovať tak, že pre každé kardinálne číslo a platí $a < 2^a$.

Dôkaz. Nerovnosť $|X| \leq |\mathcal{P}(X)|$ vyplýva z toho, že $x \mapsto \{x\}$ je injekcia z X do $\mathcal{P}(X)$. (Iné možné zdôvodnenie – dôsledok 3.2.24).

Predpokladajme teraz, že by existovala bijekcia $f\colon X \to \mathcal{P}(X)$. Ďalej označme

$$A := \{x \in X; x \notin f(x)\}.$$

Pretože f je bijekcia, existuje $y \in X$ s vlastnosťou $A = f(y)$.

Sú dve možnosti. Buď platí $y \in A$, čo ale znamená, že $y \notin f(y) = A$; alebo platí $y \notin A$ a v tomto prípade $y \in f(y) = A$. Obidve možnosti vedú k sporu a teda nemôže existovať bijekcia medzi X a $\mathcal{P}(X)$. □

Príklad 3.3.2. Možno nám lepšie pomôže pochopiť tento dôkaz, ak si ho ešte raz osvetlíme na prípade $X = \mathbb{N}$. Budeme sa teda zaoberať kardinalitou množiny $\mathcal{P}(\mathbb{N})$, namiesto nej však môžeme zobrať množinu $\{0,1\}^{\mathbb{N}}$ všetkých postupností núl a jednotiek. Vo vete 3.2.7 sme totiž skonštruovali bijekciu $A \mapsto \chi_A$ medzi týmito dvoma množinami.

Chceme ukázať, že $|\{0,1\}^{\mathbb{N}}| \neq \aleph_0$. Postupujme sporom – predpokladajme, že by existovala bijekcia $f\colon \mathbb{N} \to \{0,1\}^{\mathbb{N}}$. Máme teda postupnosti prirodzených čísel

$$\begin{aligned} f(0) &= (a_0^{(0)}, a_1^{(0)}, a_2^{(0)}, \dots) \\ f(1) &= (a_0^{(1)}, a_1^{(1)}, a_2^{(1)}, \dots) \\ f(2) &= (a_0^{(2)}, a_1^{(2)}, a_2^{(2)}, \dots) \\ &\vdots \end{aligned}$$

Ak definujeme postupnosť $b = (b_n)_{n=0}^{\infty}$ ako

$$b_n = 1 - a_n^{(n)},$$

čiže b_n je 0 ak $a^{(n)} = 1$ a obrátene, tak potom b nie je rovné žiadnej z postupností $f(n)$, $n \in \mathbb{N}$. Od postupnosti $f(n)$ sa totiž líši na n-tom mieste.

Dôkaz vety 3.3.1 je v podstate totožný s postupom z predchádzajúceho príkladu. (Jediný rozdiel je v tom, že sme nemohli prvky $f(x)$, $x \in X$, zapísať do postupnosti, keďže tam sme pracovali s ľubovoľnou množinou X a nie s množinou $\mathbb{N}$.)

Poznámka 3.3.3. Metóda použitá v predchádzajúcom dôkaze pochádza od Cantora a nazýva sa *diagonálna metóda.* (V predchádzajúcom príklade vidno, že sme vlastne menili diagonálne prvky.) Podobný argument je používaný často, aj v iných oblastiach matematiky. Mohli ste sa s ním stretnúť napríklad aj na predmete formálne jazyky a automaty, pri dôkaze, že existujú jazyky, ktoré nie sú rozpoznateľné žiadnym Turingovým strojom [RF, Kapitola 6], [HMU, Chapter 9] (voľne povedané, nie všetko sa dá naprogramovať).

My si ukážeme ešte jednu aplikáciu tejto metódy v príklade 3.5.4.

Môžeme si všimnúť, že na základe Cantorovej vety dostávame nekonečnú hierarchiu kardinálnych čísel. (Pre každé kardinálne číslo existuje kardinál, ktorý je od neho väčší.)

Príklad 3.3.4. Ukážeme, že platí

$$\aleph_0.\mathfrak{c} = \mathfrak{c}.$$

Z Cantorovej vety máme $\aleph_0 < 2^{\aleph_0} = \mathfrak{c}$. Na základe toho dostaneme nerovnosť

$$\aleph_0.\mathfrak{c} \leq \mathfrak{c}.\mathfrak{c} = 2^{\aleph_0}.2^{\aleph_0} = 2^{\aleph_0+\aleph_0} = 2^{\aleph_0} = \mathfrak{c}.$$

Platí aj nerovnosť $\mathfrak{c} \leq \aleph_0.\mathfrak{c}$, takže z Cantor-Bernsteinovej vety dostaneme dokazovanú rovnosť.

Cvičenia

Úloha 3.3.1. Ukážte, že $\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}}$.

3.4 Spočítateľné a nespočítateľné množiny

Definícia 3.4.1. Ak pre množinu A platí $|A| \leq \aleph_0$, tak hovoríme, že A je *spočítateľná.* Spočítateľná množina môže byť buď *konečná spočítateľná* množina, ak $|A| < \aleph_0$, alebo *nekonečná spočítateľná,* ak $|A| = \aleph_0$.

Ak pre množinu A platí $|A| > \aleph_0$, tak A je nespočítateľná.

Opäť platí rovnaká poznámka, ako pri konečných množinách. Ak nespočítateľné množiny definujeme takýmto spôsobom, je to síce to isté ako povedať, že sú to tie množiny, ktoré nie sú spočítateľné, dôkaz tohoto faktu by si však vyžiadal použitie axiómy výberu (pozri poznámku 3.1.9).

Ukážeme, že spočítateľné zjednotenie spočítateľných množín je opäť spočítateľná množina. Dôkaz tohoto faktu súvisí s dôkazom existencie bijekcie medzi $\mathbb{N}\times\mathbb{N}$ a $\mathbb{N}$ (pozri príklad 3.2.15). Je rozumné zdôrazniť, že v tomto dôkaze využijeme axiómu výberu. (Bijekciu medzi $\mathbb{N} \times \mathbb{N}$ a $\mathbb{N}$ sme popísali presným predpisom, čiže tam sme axiómu výberu nepotrebovali.)

Veta 3.4.2. *Nech I je spočítateľná množina a A_i je spočítateľná množina pre každé $i \in I$. (T.j. $\{A_i; i \in I\}$ je spočítateľný systém spočítateľných množín.) Potom aj množina $\bigcup_{i\in I} A_i$ je spočítateľná.*

Dôkaz. Predpokladáme, že $|I| \leq \aleph_0$ a $|A_i| \leq \aleph_0$. Teda existuje injekcia $f\colon I \to \mathbb{N}$ a pre každé $i \in I$ môžeme vybrať nejakú injekciu $f_i\colon A_i \to \mathbb{N}$. (Na tomto mieste využívame axiómu výberu.)

Pomocou zobrazení f a f_i, $i \in I$, zadefinujeme injekciu z $\bigcup_{i\in I} A_i$ do $\mathbb{N}\times\mathbb{N}$. Nech $a \in \bigcup_{i\in I} A_i$. To znamená, že existuje aspoň jedno $i \in I$ také, že $a \in A_i$. Ako i_a označme také $i \in I$, pre ktoré platí $a \in A_i$ a súčasne $f(i)$ je minimálne. (Tu využívame fakt, že každá neprázdna podmnožina $\mathbb{N}$ má najmenší prvok.) Teraz definujme $g\colon \bigcup_{i\in I} A_i \to \mathbb{N}\times\mathbb{N}$ ako

$$g(a) = (f(i_a), f_{i_a}(a)).$$

Toto zobrazenie je injektívne. Ak totiž $g(a) = g(b)$, tak a aj b patria do tej istej množiny A_{i_a} (lebo $f(i_a) = f(i_b)$ a f je injektívne). Potom platí $f_{i_a}(a) = f_{i_a}(b)$ a z injektívnosti zobrazenia f_{i_a} máme $a = b$.

Ukázali sme existenciu injekcie $g\colon \bigcup_{i\in I} A_i \to \mathbb{N}\times\mathbb{N}$. Ak ju zložíme s ľubovoľnou bijekciou $h\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ (dve také bijekcie sme zostrojili v príklade 3.2.15), tak dostaneme injekciu z $\bigcup_{i\in I} A_i$ do $\mathbb{N}$. To znamená, že $|\bigcup_{i\in I} A_i| \leq \aleph_0$ a množina $\bigcup_{i\in I} A_i$ je spočítateľná. □

Tvrdenie 3.4.3. *Množina $\mathbb{Q}$ všetkých racionálnych čísel je nekonečná spočítateľná, t.j.*

$$|\mathbb{Q}| = \aleph_0.$$

Dôkaz. Pretože $\mathbb{N} \subseteq \mathbb{Q}$, platí $\aleph_0 \leq |\mathbb{Q}|$.

Súčasne každé racionálne číslo vieme zapísať jednoznačne v tvare $\frac{p}{q}$, kde $p, q \in \mathbb{Z}$, $q > 0$ a čísla p, q sú nesúdeliteľné. Máme teda injekciu z $\mathbb{Q}$ do $\mathbb{N} \times \mathbb{Z}$, a o tejto množine už vieme, že má kardinalitu $\aleph_0$ ($|\mathbb{N} \times \mathbb{Z}| = |\mathbb{N}| \cdot |\mathbb{Z}| = \aleph_0 \cdot \aleph_0 = \aleph_0$, pozri príklad 3.2.15). Dostávame teda aj druhú nerovnosť $|\mathbb{Q}| \leq \aleph_0$.

Na základe Cantor-Bernsteinovej vety potom máme $|\mathbb{Q}| = \aleph_0$. □

Spočítateľnosť množiny $\mathbb{Q}$ by sme mohli dokázať aj pomocou vety 3.4.2 (rozmyslite si ako). Výhoda dôkazu, ktorý sme uviedli, je v tom, že nevyužíva axiómu výberu.

Pod intervalom v $\mathbb{R}$ budeme rozumieť akúkoľvek množinu I s vlastnosťou

$$a \in I \wedge b \in I \wedge a < x < b \qquad \Rightarrow \qquad x \in I.$$

Tejto definícii vyhovujú aj jednoprvkové množiny, ktoré sa zvyknú nazývať *degenerované* alebo *triviálne* intervaly. Všetky netriviálne intervaly sú tvaru (a, b), $\langle a, b\rangle$, $\langle a, b)$, $(a, b\rangle$, $(-\infty, a)$, $(-\infty, a\rangle$, $\langle a, \infty)$ alebo (a, ∞) pre nejaké $a, b \in \mathbb{R}$.

Tvrdenie 3.4.4. *Ak A je nejaká množina disjunktných netriviálnych intervalov na $\mathbb{R}$, tak množina A je spočítateľná.*

Dôkaz. Každý netriviálny interval obsahuje nejaké racionálne číslo. (Medzi ľubovoľnými dvoma rôznymi reálnymi číslami sa nachádza racionálne číslo.) Ak intervalu $I \in A$ priradíme nejaké racionálne číslo $q_I \in I$, dostaneme injekciu z A do $\mathbb{Q}$. Keďže množina $\mathbb{Q}$ je spočítateľná, musí potom byť spočítateľná aj množina A. □

V predchádzajúcom dôkaze sme použili axiómu výberu na to, aby sme pre každé $I \in A$ vybrali nejaké racionálne číslo $q_I \in I \cap \mathbb{Q}$. Použitiu axiómy výberu sa dá v tomto dôkaze veľmi ľahko vyhnúť. Stačí si všimnúť, že v predchádzajúcom dôkaze sme explicitne popísali injektívne zobrazenie $i\colon \mathbb{Q} \to \mathbb{N} \times \mathbb{N}$. Vieme tiež, že existuje bijekcia medzi $\mathbb{N} \times \mathbb{N}$ a $\mathbb{N}$. Takže v konečnom dôsledku môžeme nájsť injekciu $\mathbb{Q} \to \mathbb{N}$ a teda každej podmnožine $\mathbb{Q}$ priradiť zodpovedajúcu podmnožinu množiny $\mathbb{N}$. Zostáva už len využiť to, že každá neprázdna podmnožina množiny prirodzených čísel má najmenší prvok, čiže vieme z nej explicitným predpisom jeden prvok „vybrať“.

Cvičenia

Úloha 3.4.1. Ukážte, že ak pre kardinálne číslo a platí $a.\aleph_0 = a$, tak $2^a = {\aleph_0}^a$.

Úloha 3.4.2. Ukážte, že ak A je spočítateľná množina, B je nespočítateľná množina a $A \subseteq B$, tak $|B \smallsetminus A| = |B|$. (V tejto úlohe se môže hodiť použitie faktu, že pre každú množinu platí buď $|X| < \aleph_0$ alebo $|X| \geq \aleph_0$, ktorý sme zatiaľ nedokázali. Bez toho, aby sme sa odvolávali na doteraz nedokázané veci vieme dokázať, že z $|B| > \aleph_0$, $|A| \leq \aleph_0$ a $|B \smallsetminus A| \geq \aleph_0$ vyplýva $|B| = |B \smallsetminus A|$.)

Úloha 3.4.3. Ukážte, že množina všetkých konečných podmnožín $\mathbb{N}$ je spočítateľná. (Návod: Jedna z možností je ukázať, že množina n-prvkových množín je spočítateľná pre každé prirodzené číslo n a použiť vetu 3.4.2.)

Úloha 3.4.4. Ukážte, že množina všetkých zobrazení z $\mathbb{Q}$ do $\mathbb{Q}$ nie je spočítateľná. (Môžete vyskúšať použiť diagonálnu metódu aj priamy výpočet kardinality tejto množiny.)

Úloha 3.4.5. Postupnosť (a_n) čísel sa volá *takmer stacionárna,* ak $(\exists m \in \mathbb{N})(\forall n \geq m) a_n = a_m$. Inými slovami, od určitého čísla m sú už všetky členy tejto postupnosti rovnaké.

Dokážte, že:

a) množina všetkých takmer stacionárnych postupností čísel 0, 1 je nekonečná spočítateľná;

b) množina všetkých takmer stacionárnych postupností prirodzených čísel je nekonečná spočítateľná;

c) množina všetkých takmer stacionárnych postupností reálnych čísel má kardinalitu $\mathfrak{c}$.

Úloha 3.4.6*. Existuje nespočítateľný reťazec v $(\mathcal{P}(\mathbb{N}), \subseteq)$? (T.j. existuje taký systém $\mathcal{S}$ podmnožín $\mathbb{N}$, ktorý je nespočítateľný a pre ľubovoľné $A, B \in \mathcal{S}$ platí $A \subseteq B$ alebo $B \subseteq A$?)

Úloha 3.4.7. Nech $S = \mathbb{Q} \times \mathbb{Q}$. Ukážte, že existujú množiny V, H také, že $S = V \cup H$, prienik V sa každou vertikálnou priamkou v rovine $\mathbb{R}^2$ je konečný a prienik H sa každou horizontálnou priamkou je konečný. (T.j. pre každé $x \in \mathbb{Q}$ sú množiny $\{y \in \mathbb{Q}; (x, y) \in V\} = \{x\} \times \mathbb{Q} \cap V$ aj $\{y \in \mathbb{Q}; (y, x) \in H\} = \mathbb{Q} \times \{x\} \cap H$ konečné.)

Úloha 3.4.8. Ak A je nekonečná množina (t.j. $|A| \geq \aleph_0$), tak existuje rozklad $A = \bigcup_{i=1}^{\infty} A_i$ na spočítateľne veľa disjunktných množín taký, že žiadne dve rôzne množiny nemajú rovnakú kardinalitu.

Úloha 3.4.9. Nech A je množina po dvoch disjunktných kruhov v $\mathbb{R}^2$. Ukážte, že A je spočítateľná. Platí to aj pre kružnice?

Úloha 3.4.10. Ukážte, že ak $I_n = \langle a_n, b_n \rangle$ je klesajúca postupnosť uzavretých intervalov (t.j. $I_{n+1} \subseteq I_n$ pre každé $n \in \mathbb{N}$), tak $\bigcap_{n \in \mathbb{N}} I_n \neq \emptyset$. (Tento výsledok by ste mohli poznať z analýzy pod *Cantorova veta,* možno v trochu všeobecnejšom znení – pre kompaktné ohraničené množiny.)

Vedeli by ste pomocou tohoto výsledku dokázať (diagonálnou metódou), že množina $\langle 0, 1 \rangle$ je nespočítateľná? (Hint: Skúste začať tým, že interval $\langle 0, 1 \rangle$ rozdelíte na 3 uzavreté intervaly $\langle 0, 1/3 \rangle$, $\langle 1/3, 2/3 \rangle$, $\langle 2/3, 1 \rangle$.)

Úloha 3.4.11. Nech $f \colon \mathbb{R} \to \mathbb{R}$ je funkcia taká, že pre každé $x \in \mathbb{R}$ platí $f(f(x)) = x$. Dokážte, že existuje iracionálne číslo, ktoré sa funkciou f zobrazí na iracionálne číslo.

3.5 Mohutnosť niektorých v praxi sa vyskytujúcich množín

V predchádzajúcej podkapitole sme skúmali kardinalitu niektorých množín, väčšinou takých, že mali kardinalitu $\aleph_0$. V tejto časti sa budeme venovať ďalším množinám, ktoré sa vyskytujú v matematickej praxi. Množiny, ktoré budeme skúmať v tejto časti, budú zväčša nespočítateľné a budú mať kardinalitu $\mathfrak{c} = 2^{\aleph_0}$.

Ako prvý výsledok si ukážeme veľmi dôležitý fakt, že kardinalita množiny reálnych čísel je $\mathfrak{c} = 2^{\aleph_0}$.

Na úvod si všimnime, že $|(0, 1)| = |\langle 0, 1)| = |\langle 0, 1 \rangle| = |\mathbb{R}|$.

Keďže $(0, 1) \subseteq \langle 0, 1) \subseteq \langle 0, 1 \rangle \subseteq \mathbb{R}$, máme nerovnosti

$$|(0, 1)| \leq |\langle 0, 1)| \leq |\langle 0, 1 \rangle| \leq |\mathbb{R}|.$$

Ak nájdeme bijekciu medzi $(0, 1)$ a $\mathbb{R}$, tak túto nerovnosť môžeme rozšíriť na

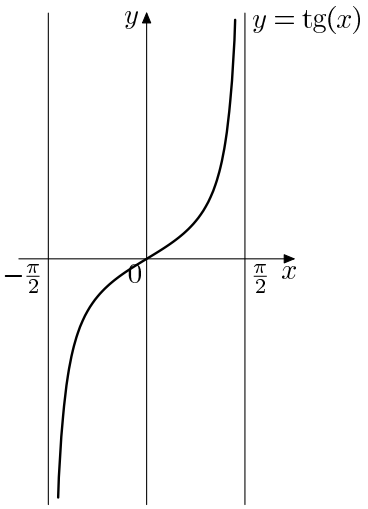
$$|\mathbb{R}| = |(0, 1)| \leq |\langle 0, 1)| \leq |\langle 0, 1 \rangle| \leq |\mathbb{R}|$$

a z Cantor-Bernsteinovej vety potom dostaneme, že všetky uvedené množiny majú rovnakú kardinalitu.

Takýchto bijekcií možno nájsť veľa. Jedna z nich je $f\colon (0,1) \to \mathbb{R}$

$$f(x) = \operatorname{tg}\left(\frac{x}{\pi} + \frac{1}{2}\right).$$

(Dostali sme ju vhodným posunutím a preškálovaním funkcie tangens – pozri obrázok 3.5).



Obr. 3.3: Bijekcia medzi $(-\frac{\pi}{2}, \frac{\pi}{2})$ a $\mathbb{R}$

Ak by ste chceli použiť nejakú elementárnejšiu funkciu, môžete skúsiť vhodne upraviť funkcie z obrázkov 3.4 a 3.5, ktoré sú navzájom inverzné.

Určite by ste ľahko našli bijekciu medzi $(0,1)$ a ľubovoľným otvoreným intervalom, medzi $\langle 0,1\rangle$ a ľubovoľným uzavretým intervalom.

Teda namiesto rovnosti $|\mathbb{R}| = \mathfrak{c}$ môžeme dokázať rovnakú rovnosť pre kardinalitu nejakého uzavretého, polouzavretého alebo otvoreného intervalu.

Predtým, než sa dostaneme k vlastnému dôkazu, povieme si ešte niečo o *binárnom* (*dyadickom*) zápise reálnych čísel. Je to vlastne rozšírenie zápisu v dvojkovej sústave, ktorý z predmetu Elementárna teória čísel [Č] poznáte pre prirodzené čísla. Pre reálne čísla túto konštrukciu možno poznáte z prváckej analýzy [VN, Kapitola V.8].

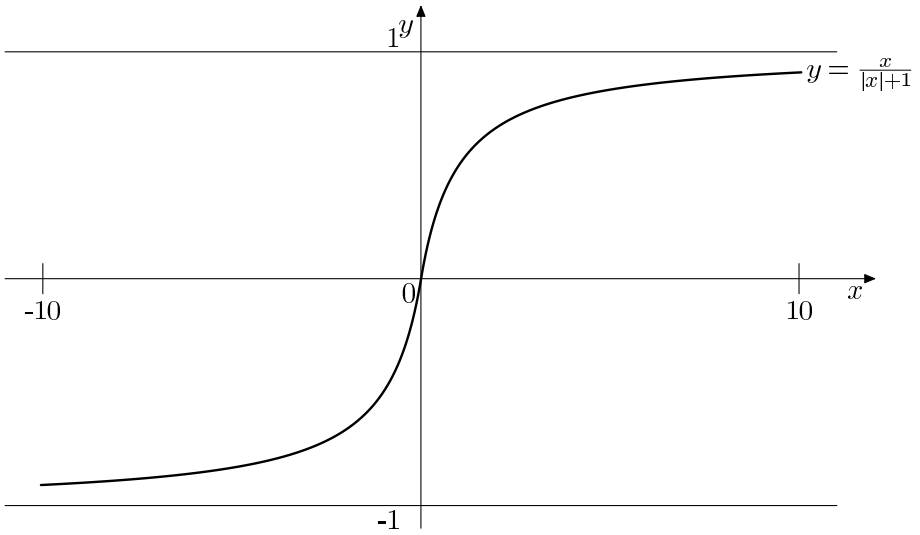
Budú nás zaujímať len reálne čísla z intervalu $\langle 0,1\rangle$, preto sa binárnemu zápisu budeme venovať iba pre tieto čísla.

Ak $(a_n)_{n=0}^{\infty}$ je ľubovoľná postupnosť núl a jednotiek, t.j. $(a_n)_{n=0}^{\infty} \in \{0,1\}^n$, tak takejto postupnosti priradíme číslo

$$r = \frac{a_0}{2} + \frac{a_1}{2^2} + \cdots = \sum_{n=0}^{\infty} \frac{a_n}{2^{n+1}}.$$

Očividne platí $0 \le r \le \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} = 1$, čiže takto dostaneme nejaké číslo z intervalu $\langle 0,1\rangle$. Čísla a_n budeme volať *cifry* binárneho zápisu reálneho čísla r.

Musíme sa však ešte zamyslieť nad dvoma dôležitými otázkami: Dá sa takto zapísať každé číslo z intervalu $\langle 0,1\rangle$? Je takýto zápis reálnych čísel jednoznačný?



Obr. 3.4: Bijekcia medzi $\mathbb{R}$ a $(-1,1)$

O tom, že takýto zápis existuje pre každé reálne číslo z intervalu $\langle 0,1)$ by nás mohla presvedčiť nasledujúca úvaha. Rozdeľme interval $\langle 0,1)$ na dve rovnaké polovice: $\langle 0,\frac{1}{2})$ a $\langle \frac{1}{2},1)$. Číslo r určite patrí do niektorého z týchto intervalov, jeho krajné body označme l_0 a r_0. Platí teda $l_0 \leq r < r_0$. Pritom číslo l_0 je tvaru $\frac{a_0}{2}$, kde $a_0 \in \{0,1\}$, a platí $r_0 - l_0 = \frac{1}{2}$.

V druhom kroku rozdelíme interval $\langle l_0, r_0)$ opäť na dve rovnaké časti. Číslo r patrí do niektorého z intervalov $\langle l_0, \frac{l_0+r_0}{2})$ a $\langle \frac{l_0+r_0}{2}, r_0)$. Koncové body intervalu obsahujúceho r označíme ako l_1, r_1 a opäť si všimneme, že $l_1 = \frac{a_0}{2} + \frac{a_1}{2^2}$ pre nejaké $a_0, a_1 \in \{0,1\}$, a $r_1 - l_1 = \frac{1}{2^2}$.

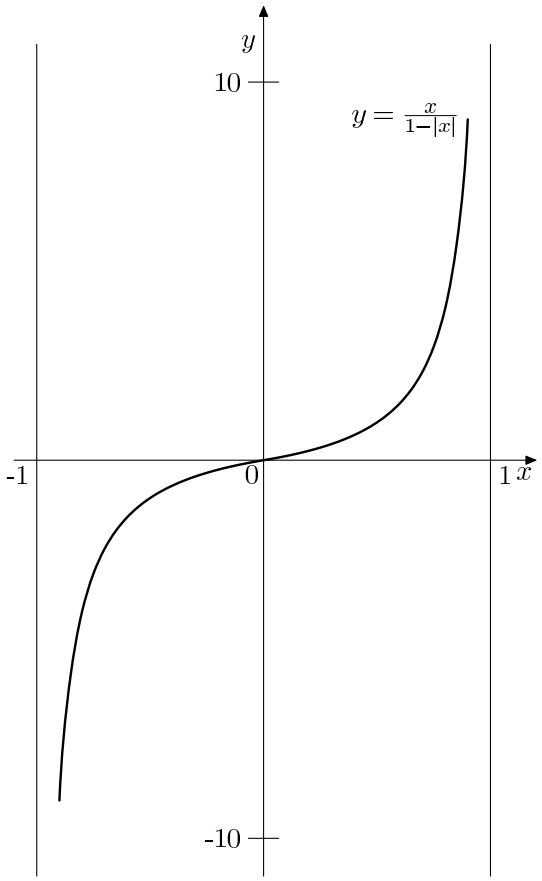
Indukciou môžeme analogicky postupovať ďalej. V indukčnom kroku máme čísla l_n a r_n také, že $r \in \langle l_n, r_n)$, $l_n = \sum_{i=0}^{n} \frac{a_i}{2^{i+1}}$ pre nejaké $a_0, \ldots, a_n \in \{0,1\}$ a $r_n - l_n = \frac{1}{2^{n+1}}$. Opäť platí, že r patrí do niektorého z intervalov $\langle l_n, \frac{l_n+r_n}{2})$ $\langle \frac{l_n+r_n}{2}, r_n)$ dĺžky $\frac{1}{2^{n+2}}$. Tento interval si označíme $\langle l_{n+1}, r_{n+1}\rangle$. Očividne platí $l_{n+1} = l_n$ alebo $l_{n+1} = l_n + \frac{1}{2^{n+2}}$, teda číslo l_{n+1} je tvaru $\sum_{i=0}^{n+1} \frac{a_i}{2^{i+1}}$ pre nejaké $a_0, \ldots, a_{n+1} \in \{0,1\}$, pričom $a_0, \ldots, a_n$ sú tie isté čísla, ktoré určovali číslo l_n.

Indukciou takto zostrojíme postupnosti $(a_n)_{n=0}^{\infty}$, $(l_n)_{n=0}^{\infty}$ a $(r_n)_{n=0}^{\infty}$ také, že pre všetky $n \in \mathbb{N}$ platí

$$0 \leq l_n \leq r < r_n \leq 1$$
$$r_n - l_n = \frac{1}{2^{n+1}}$$
$$l_n = \sum_{i=0}^{n} \frac{a_i}{2^{i+1}}$$
$$a_n \in \{0,1\}$$

Z uvedených vlastností je zrejmé, že obe postupnosti l_n aj r_n konvergujú k číslu r. To znamená, že r je limita postupnosti čiastočných súčtov radu $\sum_{i=0}^{\infty} \frac{a_i}{2^{i+1}}$, čo je len iné vyjadrenie rovnosti

$$r = \sum_{i=0}^{\infty} \frac{a_i}{2^{i+1}}.$$



Obr. 3.5: Bijekcia medzi $(-1, 1)$ a $\mathbb{R}$

Vidíme teda, že každé číslo z intervalu $\langle 0, 1)$ má binárny rozvoj. Tento rozvoj však nemusí byť jednoznačný. Napríklad číslo

$$\frac{1}{2} = \frac{1}{2^2} + \frac{1}{2^3} + \dots$$

sa dá dostať pomocou dvoch rôznych postupností $(1, 0, 0, \dots)$ a $(0, 1, 1, \dots)$ z $\{0, 1\}^{\mathbb{N}}$. Podobným spôsobom vieme dostať dva rôzne rozvoje pre každé, ktoré sa dá binárne zapísať pomocou konečného počtu jednotiek. Stačí, keď posledné číslo tvaru $\frac{1}{2^{n+1}}$, $n \in \mathbb{N}$, ktoré sa vyskytuje v tomto zápise, nahradíme súčtom $\sum_{k=n+2}^{\infty} \frac{1}{2^k}$.

Ukážeme si, že toto je jediný prípad, kedy dochádza k nejednoznačnosti. Inými slovami, ak zakážeme konečné binárne rozvoje, tak pre každé číslo z intervalu $(0, 1)$ budeme už mať jediný rozvoj. To isté platí, ak zakážeme také rozvoje, ktoré počnúc od istého miesta už pozostávajú len zo samých jednotiek.

Predpokladajme, že platí

$$\sum_{k=0}^{\infty} \frac{a_k}{2^{k+1}} = \sum_{k=0}^{\infty} \frac{b_k}{2^{k+1}},$$

pričom postupnosti $(a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty} \in \{0, 1\}^{\mathbb{N}}$ sa nerovnajú. Nech n_0 je prvý index, na

ktorom sa tieto postupnosti líšia. Bez ujmy na všeobecnosti, nech $a_{n_0} = 1$ a $b_{n_0} = 0$. Označme

$$A = \sum_{k=n_0}^{\infty} \frac{a_k}{2^{k+1}}$$
$$B = \sum_{k=n_0}^{\infty} \frac{b_k}{2^{k+1}} = \sum_{k=n_0+1}^{\infty} \frac{b_k}{2^{k+1}}$$

Vieme, že platí $A = B$. Súčasne však $B \leq \sum_{k=n_0+1}^{\infty} \frac{1}{2^{k+1}} = \frac{1}{2^{n_0+1}}$, pričom rovnosť nastane jedine v prípade, že $b_{n_0+1} = b_{n_0+2} = \cdots = 1$. Súčasne platí $A \geq \frac{1}{2^{n_0+1}}$ a rovnosť nastane jedine pre $a_{n_0} = 1$ a $a_{n_0+1} = a_{n_0+2} = \cdots = 0$. teda ide skutočne presne o taký prípad, aký sme pred chvíľou popísali.

Z toho, čo sme doteraz uviedli, je zrejmé, že existuje bijekcia medzi číslami z intervalu $(0, 1\rangle$ a postupnosťami núl a jednotiek s výnimkou tých, ktoré označujú len konečne veľa jednotiek. Postupnostiam z $\{0, 1\}^{\mathbb{N}}$ zasa môžeme bijektívne priradiť podmnožiny $\mathbb{N}$ (pozri dôkaz vety 3.2.7). Teda máme

$$|(0, 1\rangle| = |\{B \subseteq \mathbb{N}; B \text{ nie je konečná}\}|.$$

Keďže z nespočítateľnej množiny $\mathcal{P}(\mathbb{N})$ sme vynechali množinu všetkých konečných podmnožín $\mathbb{N}$, ktorá je spočítateľná (úloha 3.4.3), dostávame podľa úlohy 3.4.2, že $|(0, 1\rangle| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} = \mathfrak{c}$.

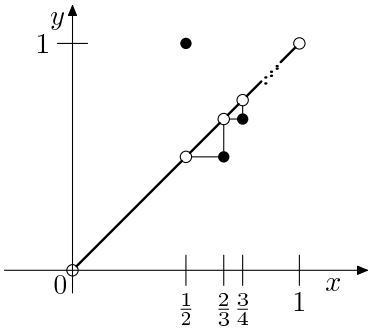
Už sme videli, že $\mathbb{R}$ má rovnakú kardinalitu ako ľubovoľný interval, dostávame teda

Tvrdenie 3.5.1.

$$|(0, 1)| = |\langle 0, 1\rangle| = |\mathbb{R}| = 2^{\aleph_0} = \mathfrak{c}$$

To isté platí aj pre ľubovoľné intervaly tvaru (a, b), $\langle a, b\rangle$, $(a, b\rangle$ či $\langle a, b)$.

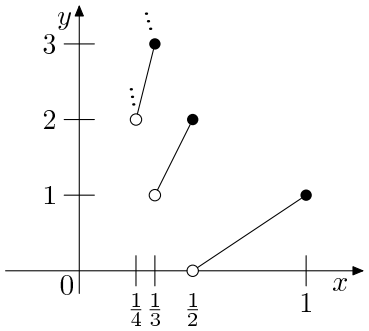
V dôkaze sme používali Cantor-Bernsteinovu vetu, môžete sa pokúsiť nájsť priamo bijekcie medzi množinami $(0, 1)$, $(0, 1\rangle$, $\langle 0, 1)$, $\langle 0, 1\rangle$ a $\mathbb{R}$. Je veľa spôsobov, ako sa to dá urobiť, ku niektorým možnostiam by vás mohli inšpirovať obrázky 3.6 či 3.7.



Obr. 3.6: Bijekcia medzi $(0, 1)$ a $(0, 1\rangle$

Príklad 3.5.2. Skúsme sa ešte raz pozrieť na dyadické rozvoje reálnych čísel, ktoré sme použili v dôkaze tvrdenia 3.5.1, na konkrétnom príklade. (Snáď tento príklad pomôže objasniť, že sa to naozaj podobá na rozvoj v desiatkovej sústave, na ktorý sme zvyknutí.)

Zoberme si nejaké jednoduché číslo, napríklad $x = \frac{2}{3}$. Skúsme postupovať presne podľa algoritmu, ktorý sme použili v dôkaze.



Obr. 3.7: Bijekcia medzi $\langle 0,1\rangle$ a $(0,1\rangle$

Interval $\langle 0,1)$ rozdelíme na polovice a pozrieme sa, do ktorej z nich patrí dané čísla. V tomto prípade do pravej polovice $\langle \frac{1}{2},1)$, teda prvá cifra bude 1. Máme teda zatiaľ x zapísané ako

$$x = \frac{2}{3} = \frac{1}{2} + \dots$$

a chceme sa pozrieť, aké budú ďalšie cifry. Tie by mali byť také, aby nám spolu dali $\frac{2}{3} - \frac{1}{2} = \frac{1}{6}$. Keď znovu spravíme delenie intervalu na polovice, tak sa pýtame, či $\frac{1}{6}$ je v ľavej alebo pravej polovici intervalu dĺžky $\frac{1}{2}$. Keď celú situáciu vhodne preškálujeme, t.j. vynásobíme všetko dvojkou, je to to isté ako pýtať sa, či $2 \cdot \frac{1}{6} = \frac{1}{3}$ je naľavo alebo napravo od $\frac{1}{2}$. Je naľavo, ďalšia cifra je 0.

$$x = \frac{2}{3} = \frac{1}{2} + \frac{0}{4} + \dots$$

Opäť interval rozdelíme na polovice, čo po preškálovaní znamená, že sa pozeráme, kam padne $2 \cdot \frac{1}{3} = \frac{2}{3}$. Čiže opäť sme v tej istej situácii ako na začiatku a vidíme, že sa budú striedavo opakovať cifry 1 a 0.

$$x = \frac{2}{3} = \frac{1}{2} + \frac{0}{4} + \frac{1}{8} + \frac{0}{16} + \frac{1}{32} + \frac{0}{64} + \dots$$

Dostali sme na pravej strane vlastne geometrický rad, kde prvý člen je $\frac{1}{2}$ a kvocient je $\frac{1}{4}$. Ľahko môžeme skontrolovať, že jeho súčet je skutočne

$$x = \frac{1}{2} \cdot \frac{1}{1 - \frac{1}{4}} = \frac{1}{2} \cdot \frac{4}{3} = \frac{2}{3}.$$

Tvrdenie 3.5.3. *Kardinalita množiny všetkých spojitých zobrazení z $\mathbb{R}$ do $\mathbb{R}$ je $\mathfrak{c}$.*

Tento fakt do istej miery kontrastuje s tým, že všetkých zobrazení z $\mathbb{R}$ do $\mathbb{R}$ je $\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}} > \mathfrak{c}$ (pozri úlohu 3.3.1). Dá sa teda povedať, že nespojitých zobrazení je oveľa viac ako spojitých.

Dôkaz. Stačí si uvedomiť, že ak vieme aké hodnoty nadobúda spojité zobrazenie $f\colon \mathbb{R} \to \mathbb{R}$ na racionálnych číslach, tak tým je už toto zobrazenie jednoznačne určené. (Racionálne čísla tvoria hustú podmnožinu reálnych čísel, pre každé reálne číslo existuje postupnosť racionálnych čísel, ktorá k nemu konverguje.) Máme teda injekciu medzi spojitými zobrazeniami z $\mathbb{R}$ do $\mathbb{R}$ a ľubovoľnými zobrazeniami z $\mathbb{Q}$ do $\mathbb{R}$ určenú predpisom $f \mapsto f|_{\mathbb{Q}}$. Kardinalita množiny zobrazení z $\mathbb{Q}$ do $\mathbb{R}$ je

$$|\mathbb{R}|^{|\mathbb{Q}|} = \mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{c}.$$

Teda spojitých zobrazení z $\mathbb{R}$ do $\mathbb{R}$ je nanajvýš $2^{\aleph_0} = \mathfrak{c}$.

Ak si teraz všimneme, že pre každé $a \in \mathbb{R}$ máme spojitú funkciu $f_a(x) = x + a$, tak vidíme, že hľadaná kardinalita je aspoň $|\mathbb{R}| = \mathfrak{c}$. □

Príklad 3.5.4. Síce už vieme, že $|\mathbb{R}| = |\langle 0,1)| = \mathfrak{c}$, a teda tieto množiny sú nespočítateľné, na tomto mieste môžeme však využiť desiatkový rozvoj reálnych čísel na to, aby sme si tento fakt ukázali použitím Cantorovej diagonálnej metódy (poznámka 3.3.3). Postup je veľmi podobný ako v príklade 3.3.2.

Ukážeme, že množina $\langle 0,1)$ je nespočítateľná. Vieme, že každé číslo z tejto množiny sa dá jediným spôsobom zapísať v tvare $x = \sum_{k=0}^{\infty} \frac{a_k}{10^{k+1}}$ a navyše ak vylúčime konečné rozvoje (t.j. také, kde sú od istého miesta všetky čísla nulové), tak je tento rozvoj jednoznačný. Desiatkový zápis budeme zapisovať v tvare $0.a_0a_1a_2\ldots$ (Môžete sa pokúsiť sami si overiť existenciu a jednoznačnosť takéhoto zápisu – postup je podobný ako v prípade dyadického zápisu. Všeobecnejšie tvrdenie, hovoriace o rozvoji pri ľubovoľnom základe, nájdete napríklad v [ŠHHK, kapitola 3.6].)

Predpokladajme, že interval $\langle 0,1)$ je spočítateľný. To znamená, že existuje bijekcia $f\colon \mathbb{N} \to \langle 0,1)$. Každé z čísel $f(0), f(1), f(2), \cdots \in \langle 0,1)$ sa dá zapísať pomocou desiatkového zápisu

$$\begin{aligned} f(0) &= 0.a_0^{(0)}a_1^{(0)}a_2^{(0)}\ldots \\ f(1) &= 0.a_0^{(1)}a_1^{(1)}a_2^{(1)}\ldots \\ f(2) &= 0.a_0^{(2)}a_1^{(2)}a_2^{(2)}\ldots \\ &\vdots \end{aligned}$$

Pomocou týchto desatinných zápisov zadefinujeme nové číslo

$$b = 0.b_0b_1b_2\ldots$$

tak, že $b_k \neq a_k^{(k)}$ a súčasne $b_k \neq 0$. Môžeme napríklad položiť $b_k = a_k^{(k)} + 1$ ak $a_k^{(k)} < 9$ a $b_k = 8$ ak $a_k^{(k)} = 9$. Číslo, ktoré sme takto dostali má nekonečný zápis v desiatkovej sústave rôzny od všetkých čísel $f(n)$, $n \in \mathbb{N}$. (Od čísla $f(n)$ sa líši prinajmenšom na n-tom mieste zápisu, možno aj na nejakých ďalších.)

Teda $b \neq f(n)$ pre žiadne n, čo je v spore s predpokladom, že f je bijekcia.

Cvičenia

Úloha 3.5.1. Ukážte, že kardinalita množiny všetkých iracionálnych čísel je $\mathfrak{c}$.

Úloha 3.5.2. Aká je kardinalita množiny všetkých diferencovateľných zobrazení z $\mathbb{R}$ do $\mathbb{R}$.

Úloha 3.5.3. Aká je kardinalita množiny všetkých divergentných postupností reálnych čísel? Aká je kardinalita množiny všetkých divergentných postupností racionálnych čísel?

3.6 Aplikácie kardinálnych čísel

3.6.1 Existencia transcendentných čísel

Najprv pripomeňme definíciu algebraických a transcendentných čísel.

Definícia 3.6.1. Komplexné číslo a sa nazýva *algebraické,* ak existuje polynóm $f(x) \in \mathbb{Z}[x]$ s celočíselnými koeficientami taký, že $f(a) = 0$, t.j. a je koreňom tohoto polynómu. Komplexné číslo, ktoré nie je algebraické, sa nazýva *transcendentné.*

Ukážeme, že množina algebraických čísel je spočítateľná. Z toho vyplýva, že existujú aj transcendentné čísla.

Tvrdenie 3.6.2. *Množina $\mathbb{A}$ všetkých algebraických čísel je spočítateľná.*

Dôkaz. Využijeme fakt, že každý polynóm $f \in \mathbb{C}[x]$ stupňa n má v $\mathbb{C}$ najviac n koreňov. (Presne n, ak by sme započítali aj ich násobnosť.)

Najprv vypočítajme kardinalitu množiny $\mathbb{Z}[x]$ všetkých polynómov s celočíselnými koeficientami. Každý polynóm stupňa n je jednoznačne určený postupnosťou koeficientov $a_n \in \mathbb{Z} \setminus \{0\}$, $a_{n-1}, \ldots, a_0 \in \mathbb{Z}$. Kardinalita množiny P_n všetkých polynómov stupňa n s celočíselnými koeficientami je teda $\aleph_0^n = \aleph_0$.

Množinu $\mathbb{Z}[x]$ môžeme vyjadriť ako $\mathbb{Z}[x] = \bigcup_{n\in\mathbb{N}} P_n$, čiže ide o spočítateľné zjednotenie spočítateľných množín. Teda dostávame $|\mathbb{Z}[x]| = \aleph_0$.

Každé algebraické číslo je koreňom nejakého polynómu zo $\mathbb{Z}[x]$. Takýto polynóm má najviac n koreňov. Dostávame teda

$$|\mathbb{A}| \leq |\mathbb{Z}[x]|.\aleph_0 = \aleph_0.$$

Súčasne platí $|\mathbb{A}| \geq \aleph_0$, keďže každé celé číslo je algebraické. □

Z predchádzajúceho tvrdenia už dostaneme existenciu transcendentných čísel (pozri úlohu 3.6.1).

Dôsledok 3.6.3. *Kardinalita množiny $\mathbb{C} \setminus \mathbb{A}$ je $\mathfrak{c}$. Z toho dostávame, že existuje aspoň jedno transcendentné číslo.*

Podobne $\mathbb{R} \setminus \mathbb{A}$ má kardinalitu $\mathfrak{c}$, teda existuje aspoň jedno reálne transcendentné číslo.

3.6.2 Vypočítateľné funkcie

V tejto časti si povieme – aspoň veľmi zjednodušene a neformálne – niečo o vypočítateľných funkciách.

Zjednodušene by sme mohli zaviesť pojem vypočítateľnej funkcie takto:

Definícia 3.6.4. Funkcia $f\colon \mathbb{N} \to \mathbb{N}$ sa nazýva *vypočítateľná,* ak existuje *algoritmus* ktorý pre vstup n vráti $f(n)$.

Otázka je, ako by sme mohli spresniť definíciu pojmu *algoritmus,* ktorý sa vyskytuje v predchádzajúcej definícii. Existuje viacero teoretických modelov algoritmu, snáď najrozšírenejší je Turingov stroj. Pre jednoduchosť si však môžete na tomto mieste predstaviť pod pojmom algoritmus program (procedúru) vo vašom obľúbenom programovacom jazyku.

Program nie je vlastne nič iné, než konečný reťazec znakov, ktorý navyše musí spĺňať určité pravidlá. Keďže používame iba konečne veľa znakov, všetkých možných programov je najviac toľko ako konečných postupností prvkov z danej konečnej množiny, čo je $\aleph_0$.

Súčasne vieme, že všetkých zobrazení z $\mathbb{N}$ do $\mathbb{N}$ je $\aleph_0^{\aleph_0} = \mathfrak{c} > \aleph_0$. Z toho vidíme, že existujú funkcie, ktoré nie sú vypočítateľné (nedajú sa naprogramovať). Zaujímavé je snáď aj to, že sa nám ich existenciu podarilo dokázať bez toho, aby sme nejakú konkrétnu nevypočítateľnú funkciu zostrojili.

Cvičenia

Úloha 3.6.1. Ukážte, že množina všetkých transcendentných čísel má kardinalitu $\mathfrak{c}$.

Úloha 3.6.2. Funkcia $f\colon \mathbb{R} \to \mathbb{R}$ sa nazýva funkciou *prvej Bairovej triedy,* ak existuje postupnosť spojitých funkcií $(f_n\colon \mathbb{R} \to \mathbb{R})_{n\in\mathbb{N}}$, ktorá k nej bodovo konverguje (t.j. pre každé $x \in \mathbb{R}$ číselná postupnosť $f_n(x)$ konverguje k $f(x)$). Aká je kardinalita množiny všetkých funkcií prvej Bairovej triedy? Viete na základe kardinality ukázať, že existuje funkcia, ktorá nie je prvej Bairovej triedy?

Úloha 3.6.3. Z daných bodov v rovine vieme vytvárať nové body pomocou pravítka a kružidla takto: Môžeme spojiť dva body priamkou. Môžeme zostrojiť kružnicu takú, že stred bude v niektorom zo zadaných bodov a polomer je vzdialenosť niektorých dvoch zadaných bodov. Dostaneme takto nové body na priesečníkoch takýchto priamok a kružníc.

Nazvime *skonštruovateľnými bodmi* v rovine body $(0, 0)$ a $(0, 1)$ a ďalej všetky body, ktoré vieme z týchto bodov dostať uvedeným spôsobom pomocou konečne veľa krokov.

Aká je kardinalita množiny všetkých skonštruovateľných bodov? Viete na základe toho zdôvodniť, že existujú body v rovine, ktoré z jednotkovej úsečky nedokážeme zostrojiť pomocou pravítka a kružidla?[3]

[3]O tom, že nie všetky konštrukcie sa dajú urobiť pravítkom a kružidlom by ste už mohli vedieť z algebry; dokonca by ste mohli poznať niektoré konkrétne dĺžky, pre ktoré sa nedajú zostrojiť takto dlhé úsečky, ako napríklad $\sqrt[3]{2}$ alebo $\cos\frac{\pi}{9}$. Pozri napríklad [KGGS, Podkapitola 4.1 a 8.2], [DF, Section 13.3], [JMP], [S, Chapter 7], [Sl1].

Tu sme podali alternatívny dôkaz. Má nevýhodu, že nie je konštruktívny. Na druhej strane, princíp dôkazu sa ľahko aplikuje na podobné konštrukcie, kde robíme konečne veľa krokov a pri jednom kroku vieme vytvoriť len konečne veľa bodov. (V našom prípade: Prienik dvoch priamok, priamky a kružnice resp. dvoch kružníc nám pridá najviac dva body.)

Literatúra

[B1] Lev Bukovský. Úvod do matematickej logiky. `http://ics.upjs.sk/~novotnyr/home/skola/logika_a_teoria_mnozin/ltm.pdf`.

[B2] Lev Bukovský. *Množiny a všeličo okolo nich.* Alfa, Bratislava, 1985.

[BŠ] Bohuslav Balcar and Petr Štěpánek. *Teorie množin.* Academia, Praha, 2001.

[Č] Juraj Činčura. Elementárna teória čísel. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/cvicenia/tc/`.

[D] Keith Devlin. *The Joy of Sets.* Springer-Verlag, New York, 1993. Undergraduate Texts in Mathematics.

[DF] David S. Dummit and Richard M. Foote. *Abstract Algebra.* John Willey and Sons, 3rd edition, 2004.

[E] Herbert B. Enderton. *A Mathematcial Introduction to Logic.* Harcourt/Academic Press, San Diego, 2001.

[F] Thomas Forster. *Logic, Induction and Sets.* Cambridge University Press, Cambridge, 2003. LMS Student Texts 56.

[GG] Ivor Grattan-Guiness. *The Search for Mathematical Roots 1870–1940.* Princeton University Press, Princeton, 2000.

[HMU] John E. Hopcroft, Rajeev Motwani, and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Massachusetts, 2nd edition, 2001.

[JMP] Arthur Jones, Sidney A. Morris, and Kenneth R. Pearson. *Abstract Algebra and Famous Impossibilities.* Springer-Verlag, New York, 1991. Universitext.

[KGGS] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a teoretická aritmetika 1.* UK, Bratislava, 2002.

[KLŠZ] M. Kolibiar, A. Legéň, T. Šalát, and Š. Znám. *Algebra a príbuzné disciplíny.* Alfa, Bratislava, 1992.

[L] Seymour Lipschutz. *Schaum's Outline of Theory and Problems of Set Theory and Related Topics.* McGraw-Hill, New York, 1998.

[RF] Branislav Rovan and Michal Forišek. Formálne jazyky a automaty. Poznámky k prednáške, `http://foja.dcs.fmph.uniba.sk/materialy.php`.

[Sl1] Martin Sleziak. 1-MAT-260 Algebra 2. Poznámky k prednáške, http://msleziak.com/vyuka/2011/alg2m/.

[Sl2] Martin Sleziak. Teória množín. 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.

[S] Ian Stewart. *Galois theory.* CRC, Boca Raton, 3rd edition, 2004.

[ŠHHK] T. Šalát, A. Haviar, T. Hecht, and T. Katriňák. *Algebra a teoretická aritmetika 2.* Alfa, Bratislava, 1986.

[ŠS] Tibor Šalát and Jaroslav Smítal. *Teória množín.* UK, Bratislava, 1995.

[VN] J. Vencko and T. Neubrunn. *Matematická analýza.* MFF UK, Bratislava, 1992.

[WIK] Wikipedia. http://en.wikipedia.org.

[Z] Pavol Zlatoš. *Ani matematika si nemôže byť istá sama sebou.* IRIS, Bratislava, 1995. http://thales.doa.fmph.uniba.sk/zlatos/animat/animat.pdf.

Register

Zoznam symbolov