2-UMA-115 Teória množín

Martin Sleziak

26. novembra 2013

Obsah

Kapitola 1

Úvod

Verzia: 26. novembra 2013

1.1 Predhovor

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

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

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

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

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

V texte nájdete množstvo vyriešených úloh. Určite nezaškodí, ak sa ich pokúsite riešiť samostatne – len samostatným uvažovaním si môžete skutočne dôkladne osvojiť niektorú

matematickú disciplínu. Som presvedčený o tom, že v rámci tejto prednášky sa nájde veľa zaujímavých poznatkov. Ako ste však isto spoznali aj z iných predmetov, matematika môže byť zaujímavá a zábavná, vyžaduje si to však najprv nemalé úsilie na strane študenta.

1.2 Sylaby a literatúra

1.2.1 Literatúra

Pri príprave týchto poznámok som čerpal najmä z kníh [BŠ, D, ŠS]. V častiach o histórii teórie množín som čerpal hlavne z [BŠ, GG, Z2]. Samozrejme, pomohli mi aj rôzne internetové zdroje ako napríklad [WIK], blogy rôznych matematikov, s niektorým úlohami, ktoré uvádzam ako cvičenia, som sa stretol na rôznych matematických diskusných fórach. Mnohé cvičenia som prebral z [Li, ŠS].

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

1.2.2 Sylaby predmetu

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

1.2.3 Štátnicové otázky

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

1. Axiomatická metóda v teórii množín, Zermelov-Fraenkelov axiomatický systém teórie množín.
2. Konečné a nekonečné množiny, vlastnosti konečných množín.
3. Spočítateľné množiny, vlastnosti spočítateľných množín, existencia nespočítateľnej množiny.
4. Model Peanovej aritmetiky celých nezáporných čísel v teórii množín. (V súvislosti s touto otázkou môže byť pre vás zaujímavý i text [Č2].)
5. Kardinálne čísla. Súčet a súčin kardinálnych čísel, vlastnosti súčtu a súčinu kardinálnych čísel.

V časti 5.3 sa dotkneme aj otázky: „Konštrukcia oboru (usporiadaného okruhu) celých čísel z oboru celých nezáporných čísel a oboru (usporiadaného poľa) racionálnych čísel z oboru celých čísel.“ Nebudeme sa však ňou zaoberať podrobne.

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

1.3 Niečo z histórie

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

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

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

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

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

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

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

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

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

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

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

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

S použitím axiomatického systému sa podarilo odstrániť všetky dovtedy známe paradoxy. Samozrejme, stále vo vzduchu visela otázka, či sa neobjavia nejaké nové spory v rámci axiomatickej teórie množín. Táto otázka bola jednou z pohnútok, ktoré viedli k tzv. *Hilbertovmu programu.* Jeho ciele boli veľmi ambiciózne, tu spomeňme len dva z nich: Jedným z cieľov bolo sformalizovať celú matematiku v rámci teórie množín. Druhým cieľom bolo ukázať bezospornosť teórie množín, a tým pádom vlastne aj celej matematiky (alebo aspoň tej časti, ktorú budeme schopní v rámci teórie množín sformulovať). Viac o Hilbertovom programe sa môžete dozvedieť napríklad v [Z2, Kapitola 10].

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

Viac o Gödelových vetách (ako aj o niektorých filozofických otázkach súvisiacich s teóriou množín) sa môžete dozvedieť v [Z2]. Tento text je pomerne náročný, rozhodne je vhodné mať zvládnuté základy teórie množín prv, než ho začnete čítať.

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

1.4 Základné označenia

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

{prelim:POZNMNOZN}

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

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

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

Kapitola 2

Axiomatický prístup k teórii množín

2.1 Logika prvého rádu

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

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

2.1.1 Výroková logika

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

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

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

p	$\neg p$
1	0
0	1

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

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

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

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

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

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

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

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

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

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

{logika:PRDEMORGAN}

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

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

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

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

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

{logika:PRTAUTNEPR}

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

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

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

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

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

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.*

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

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

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

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

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

[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.

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“.)

{logika:PRNEGFORALL}

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

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

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

Podobným spôsobom si môžeme ozrejmiť, že platí ekvivalencia

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

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

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

Príklad 2.1.8. Pokúsme sa znegovať výrok

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

Postupne dostaneme

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

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

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

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

Podľa pravidiel, ktoré sme uviedli, je negácia tohoto výroku

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

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

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

Po odbočke venovanej 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

{logika:CVTAUT}

Úloha 2.1.1. Dokážte, že nasledujúce výroky sú tautológie:
a) $(\neg p \vee q) \Leftrightarrow (p \Rightarrow q)$
b) $(p \Leftrightarrow q) \Leftrightarrow [(p \Rightarrow q) \wedge (q \Rightarrow p)]$

c) $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$
d) $((p \wedge q) \Rightarrow r) \Leftrightarrow (p \Rightarrow (q \Rightarrow r))$
e) $(p \Leftrightarrow q) \Leftrightarrow (\neg p \Leftrightarrow \neg q)$
f) $\neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg q)$
g) $(p \Rightarrow \neg q) \Rightarrow \neg p$
h) $((p \Rightarrow \neg p) \Rightarrow p) \Rightarrow ((p \Rightarrow \neg p) \Rightarrow \neg p)$
i) $[p \Leftrightarrow (q \Leftrightarrow r)] \Leftrightarrow [p \Leftrightarrow (q \Leftrightarrow r)]$ j) $[p \Rightarrow (q \Rightarrow r)] \Leftrightarrow [p \Rightarrow (q \Rightarrow r)]$

{logika:CVTAUT2}

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

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

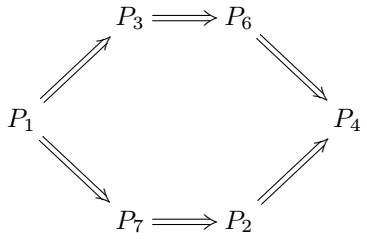
{logika:CVREDUND}

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

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.

{logikacvic:ULODISTRIB}

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

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

2.2 Naivná teória množín a jej paradoxy

{paradox:SECTNAIV}

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

Súčasne s množinami môžeme robiť rôzne operácie, utvárať nové množiny pomocou niektorých vlastností. Napríklad prienik množín A a B je taká množina, do ktorej patria práve

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

prvky spĺňajúce podmienku $(x \in A) \wedge (x \in B)$, čiže opäť je to systém objektov určený nejakou podmienkou. Stručne to môžeme zapísať

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

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

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

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

keďže podmienku $x = x$ spĺňa každý objekt.

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

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

takých množín, ktoré nie sú svojimi vlastnými prvkami. Túto množinu by sme mohli zapísať aj ako

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

Položme si otázku, či do tejto množiny patrí aj množina A.

Ak by platilo $A \in A$, tak množina A musí spĺňať podmienku $x \notin x$, teda platí $A \notin A$. Dostávame platnosť $A \in A$ aj $A \notin A$, čo je spor.

Zostáva teda možnosť $A \notin A$. Lenže potom, opäť na základe definície množiny A, dostaneme $A \in A$, čiže aj táto možnosť vedie k sporu.

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

Berryho paradox Zadefinujeme takúto podmnožinu prirodzených čísel

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

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

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

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

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

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

2.3 Zermelov-Fraenkelov axiomatický systém

{zfc:SECTZFC}

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

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

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

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

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

{zfc:SSECTJAZYK}

2.3.1 Jazyk teórie množín

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

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

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

Definícia 2.3.2.

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

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

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

2.3.2 Axiómy systému ZFC

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

Axióma I (Axióma extenzionality)**.**

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

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

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

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

Axióma IV (Axióma existencie)**.**

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

Existuje aspoň jedna množina.

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

Nasledujú 2 axiómy popisujúce vytváranie množín z iných množín.

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

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

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

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

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

Axióma III (Axióma dvojice)**.**

$$(\forall a)(\forall b)(\exists C)(\forall z)[z \in C \Leftrightarrow (z = a) \vee (z = b)]$$

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

{zfc:TVRZJEDPAIR}

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

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

Ďalšou aplikáciou axiómy dvojice je nasledujúce jednoduché tvrdenie:

{zfc:TVRSINGL

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

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

Túto množinu označujeme $\{a\}$.

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

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

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

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

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

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

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

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

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

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

Túto množinu nazývame prázdna množina.

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

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

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

□

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

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

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

Dôkaz. Množina

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

existuje podľa schémy axióm vymedzenia použitej pre množinu A a formulu $x \in B$.

Jednoznačnosť vyplýva z axiómy extenzionality. □

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

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

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

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

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

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

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

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

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

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

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

Kvôli zostručneniu nasledujúcej axiómy zaveďme ešte jeden symbol.

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

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

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

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

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

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

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

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

Axióma (Axióma regularity)**.**

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

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

Axiómu regularity môžeme teda stručnejšie zapísať ako

$$(\forall A)[A \neq \emptyset \Rightarrow (\exists B \in A)B \cap A = \emptyset]$$

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

{zfc:TVRREGXINX}

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

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

Axióma X (Axióma nekonečnej množiny)**.**

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

Existenciu akej množiny vlastne zaručuje táto axióma? Určite vieme, že $A_0 := \emptyset$ patrí do A. Potom do A patrí aj $A_1 := A_0 \cup \{A_0\} = \{\emptyset\}$. Takto môžeme postupne vytvárať ďalšie množiny.

$$\begin{aligned}
A_0 &= \emptyset \\
A_1 &= A_0 \cup \{A_0\} = \{\emptyset\} \\
A_2 &= A_1 \cup \{A_1\} = \{\emptyset, \{\emptyset\}\} \\
A_3 &= A_2 \cup \{A_2\} = \{\emptyset, \{\emptyset\}, \{\{\emptyset, \{\emptyset\}\}\}\} \\
&\vdots
\end{aligned}$$

Všimnime si, aké množiny sme takto dostali. Dostali sme neklesajúcu postupnosť množín: $A_0 \subseteq A_1 \subseteq A_2 \subseteq \ldots$ Súčasne z tvrdenia 2.3.12 vidíme, že keď sme z množiny x vytvorili novú množinu $x \cup \{x\}$, tak táto množina obsahuje aspoň jeden prvok navyše: máme $x \in x \cup \{x\}$ ale $x \notin x$. Teda všetky inklúzie sú ostré. Dostali sme teda nekonečne veľa prvkov patriacich do A. (Neskôr, v časti 5.2, si ukážeme konštrukciu prirodzených čísel v rámci ZFC. Práve množiny, ktoré sme to označili $A_0, A_1, A_2, \ldots$ budú tvoriť model prirodzených čísel.)

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

Axióma VII (Axióma výberu)**.**

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

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

Axióma výberu je veľmi dôležitá axióma. Neskôr si uvedieme zrozumiteľnejšiu ekvivalentnú formuláciu tejto axiómy. Axiómou výberu sa budeme podrobne zaoberať v kapitole 6. Z formulácie, ktorú sme uviedli, by však mohlo byť jasné, prečo sa nazýva axióma výberu – množina V z každej množiny patriacej do $\mathcal{S}$ „vyberá“ práve jeden prvok.

Veľmi dobre napísané poznámky o motivácii a význame jednotlivých axióm si môžete prečítať napríklad v [Z2, s.79–83][6]. (Môžete si tam prečítať aj o axiómach, ktorými sa v tomto texte podrobne nezaoberáme, ako je axióma regularity.)

{zfc:POZNHRA}

Poznámka 2.3.13. Na odvodenie nejakého tvrdenia v rámci ZFC sa môžeme pozerať aj ako na formálnu hru so symbolmi. Máme presné pravidlá o tom, aké sú naše základné tvrdenia (axiómy), a tiež presné pravidlá o tom, ako z nich odvodzovať nové tvrdenia a zostavovať dôkazy. (Tými sme sa v tomto texte detailne nezaoberali.)

V praxi neodvodzujeme matematické tvrdenia tak, že by sme sa ich snažili zapísať v jazyku teórie množín a odvodzovať každý krok na základe logických axióm. Sú však situácie, kedy je užitočné si aspoň uvedomiť, že takéto niečo je v princípe možné. Napríklad pokiaľ sa zaoberáme tým, či sa nejaké tvrdenie dá alebo nedá dokázať, je dobré mať jasne stanovené axiómy, z ktorých sa ho snažíme dokázať. (Uvedieme viacero príkladov tvrdení, ktoré sa dajú dokázať v ZFC, ale nedajú sa odvodiť v ZF.) Takisto pokiaľ sa zaoberáme bezospornosťou nejakého axiomatického systému, tak ju bude ťažké skúmať bez toho, aby boli jasne stanovené axiómy.

Keď sa na tvrdenia a ich dôkazy pozeráme ako na postupnosti symbolov vyhovujúce určitým pravidlám, zdá sa byť vcelku prirodzenou myšlienka skúsiť ich algoritmicky generovať, alebo aspoň naučiť počítač skontrolovať dôkaz zapísaný v takejto podobe. Ak sme totiž schopný nejaký dôkaz prepísať až do podoby, kedy je už len potrebné kontrolovať, či všetky kroky vyhovujú danými pravidlám, tak kontrola dôkazu je už iba algoritmický proces. Viac o použití počítačov pri verifikácii formálnych dôkazov sa môžete dočítať napríklad v článku [Wi].

2.4 Operácie s množinami

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

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

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

Nasledujúce tvrdenie zhŕňa základné vlastnosti inklúzie.

{oper:TVRSUBSET}
{oper:itSUB1}

Tvrdenie 2.4.1. *Nech A, B, C sú ľubovoľné množiny. Potom platí:*
(i) *Pre každú množinu platí $A\subseteq A$.*

[6] Táto kniha je voľne dostupná na internete

{oper:itSUB2}
{oper:itSUB3}

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

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

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

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

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

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

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

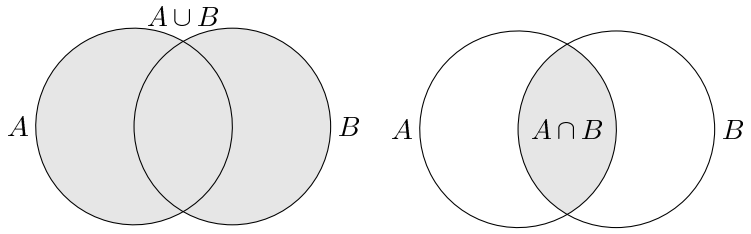
Poznámka 2.4.3. V tomto texte používam $\subseteq$ na označenie podmnožiny a $\subsetneq$ na označenie vlastnej podmnožiny. Toto označenie som zvolil z toho dôvodu, že som sa chcel vyhnúť možným nedorozumeniam. Dosť často sa na označenie inklúzie používa $\subset$, nájdu sa však aj texty (hoci zriedkavejšie),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

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

Pre dvojicu množín sme zatiaľ zadefinovali zjednotenie a prienik množín.

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

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



{oper:FIGZJEDPRIE}

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.)

TVRZJEDPRIEN}

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

{oper:it1ZJEDPRIEN}

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

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

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

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

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

čo je presne tautológia z úlohy 2.1.2a).

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

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

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

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

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

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

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

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

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

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

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

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

{oper:TVRDISTRIBSYSTEM}

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

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

Pokúsme sa (podľa definície) prepísať, čo to znamená, že prvok x patrí do množiny uvedenej na ľavej strane dokazovanej rovnosti. 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.

{oper:TVRSUBEKV}
{oper:it1SUBEKV}
{oper:it2SUBEKV}
{oper:it3SUBEKV}

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

Dôkaz. (i) ⇒ (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) ⇒ (iii) je veľmi podobný ako dôkaz predchádzajúcej časti, ponechávame ho ako cvičenie.

(ii) ⇒ (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) ⇒ (i) opäť prenecháme čitateľovi. □

{oper:TVRSUB}

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

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

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

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

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

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

(iii): Predpokladáme, že $A \subseteq B$, čiže platí implikácia $(x \in A) \Rightarrow (x \in B)$. Potom platí aj $[(x \in A) \wedge (x \in C)] \Rightarrow [(x \in B) \wedge (x \in C)]$ (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 2.4.6. (Touto metódou by sa samozrejme dala dokazovať aj prvá časť tvrdenia.) Vieme teda, že platí $B = A \cup B$ a radi by sme pomocou toho dokázali $(A \cup C) \cup (B \cup C) = B \cup C$. Z tvrdenia 2.4.4 vieme, že operácia $\cup$ je asociatívna (výrazy obsahujúce len túto operáciu môžeme ľubovoľne prezátvorkovať), komutatívna (množiny môžeme vymieňať) a idempotentná. Pomocou týchto vlastností skutočne dostaneme

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

□

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

{oper:PRABSORP}

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

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

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

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

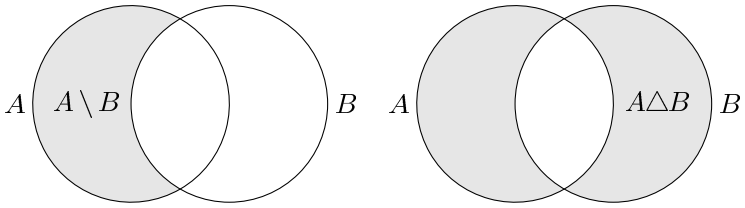
Symetrická diferencia množín A a B je množina

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

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

{oper:TVRSETMINUS}

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



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

{oper:itDEMOR

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

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

{oper:TVRSYMDIF}

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

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

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

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

Pri dokazovaní našej tautológie potom dostávame nasledujúcu tabuľku:

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

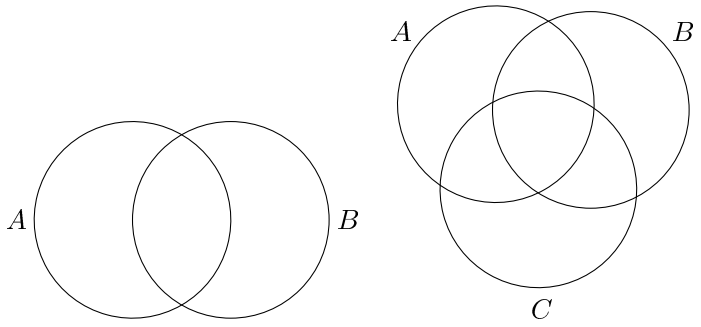
□

Vennove diagramy

{oper:SSSECTVENN}

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

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



Obr. 2.3: Generická poloha

{oper:FIGGENER}

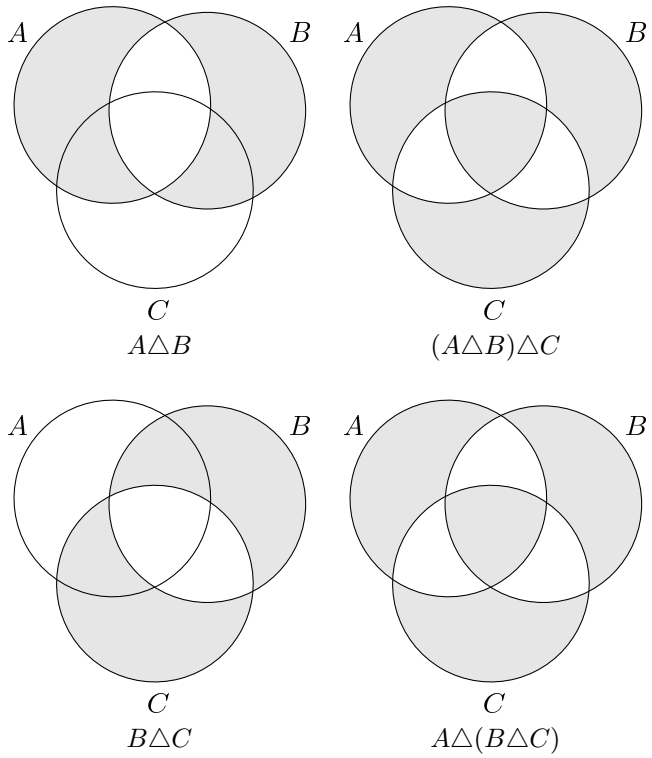
Pri dôkaze postupujeme tak, že vo Vennovom diagrame nakreslíme postupne, ako vyzerajú množiny na ľavej a pravej strane rovnosti a tieto obrázky porovnáme.

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

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

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

Môžete sa pýtať, do akej miery je dôkaz pomocou Vennových diagramov korektný. (Od prvého ročníka na vysokej škole ste už určite veľakrát počuli, že „obrázok nie je dôkaz“.) Odpoveď je, že tento dôkaz je úplne rovnocenný s overením príslušnej tautológie tabuľkovou metódou. Robíme tam totiž presne to isté, čo pri tabuľkovej metóde, len namiesto symbolov



Obr. 2.4: Asociatívnosť operácie △

{oper:FIGSYMD

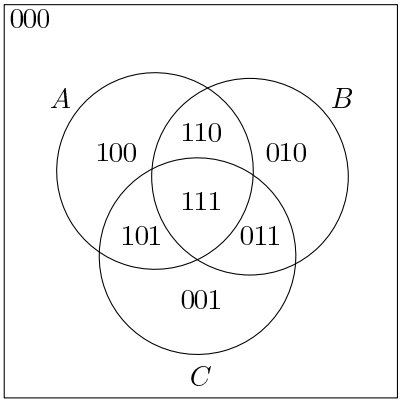
0 a 1 používame farebné zvýraznenie niektorej oblasti – pozri obrázok 2.5. Môžete si teda vybrať ktorúkoľvek z týchto dvoch metód a používať tú, ktorá vám väčšmi vyhovuje a pri ktorej máte menšiu obavu z toho, že by ste spravili chybu.

Cvičenia

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

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

Úloha 2.4.3. Zistite, či sú uvedené tvrdenia pravdivé (pre ľubovoľný výrok $P(x)$). V prípade nepravdivých tvrdení rozhodnite, či aspoň jedna z implikácií je pravdivá. Svoje tvrdenie zdôvodnite!
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) $[(\forall x \in A)P(x) \wedge (\forall x \in B)P(x)] \Leftrightarrow (\forall x \in A \cap B)P(x)$.



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

Úloha 2.4.4. 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 2.4.5. Nech $\mathcal{S} \subseteq \mathcal{S}'$. Dokážte, že $\bigcup \mathcal{S} \subseteq \bigcup \mathcal{S}'$. Ak navyše predpokladáme $\mathcal{S} \neq \emptyset$, tak $\bigcap \mathcal{S} \supseteq \bigcap \mathcal{S}'$.

2.5 Usporiadané dvojice a karteziánsky súčin

{kartez:SECTKARTEZ}

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

{kartez:DEFPAIR}

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

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

nazývame *usporiadanou dvojicou* množín a a b.

Táto definícia sa môže na prvý pohľad zdať neobvyklá. Treba si uvedomiť, že pracujeme iba s množinami a každý objekt chceme definovať ako nejakú množinu. Ľahko si môžete všimnúť, že množina uvedená v definícii skutočne existuje – stačí viackrát použiť axiómu dvojice. Menej zrejmé je, prečo by práve takáto množina mala byť vhodnou definíciou usporiadanej množiny. Odpoveď je, že spĺňa základnú vlastnosť, ktorú od usporiadaných množín vyžadujeme – sformulovanú v nasledujúcom tvrdení. (Pokojne by sme mohli použiť aj akúkoľvek inú definíciu usporiadanej dvojice, ktorá by vyhovovala tejto požiadavke.[7])

{kartez:TVRUSPDVOJ}

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

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

[7] Skutočne sa vyskytlo aj viacero ďalších definícií usporiadanej dvojice, ako sa môžete napríklad presvedčiť na `http://en.wikipedia.org/wiki/Ordered_pair`. Definícia, ktorú sme uviedli my, pochádza od K. Kuratowského.

Dôkaz. Platnosť implikácie $\Leftarrow$ je jasná.

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

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

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

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

Teraz už môžeme zadefinovať karteziánsky súčin dvoch množín.

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

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

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

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

Existencia takejto množiny je zaručená schémou axióm vymedzenia.[8]

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

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

{kartez:TVROPER}

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

(i) $A\times\emptyset=\emptyset\times A=\emptyset$;
(ii) $A\times(B\cup C)=(A\times B)\cup(A\times C)$;
(iii) $A\times(B\cap C)=(A\times B)\cap(A\times C)$;
(iv) $A\times(B\setminus C)=(A\times B)\setminus(A\times C)$.
(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. □

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

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

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

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

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

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

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

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

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

Cvičenia

Úloha 2.5.1. Dokážte ostatné časti tvrdenia 2.5.4.

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

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

{kartezcvic:ULOKARTSUB}

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

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

Úloha 2.5.6. Dokážte, že množiny A, B sú disjunktné práve vtedy, keď $(A \times B) \cap (B \times A) = \emptyset$.

Úloha 2.5.7. Dokážte, že pre ľubovoľné množiny A, B, C platí $A \times (B \triangle C) = (A \times B) \triangle (A \times C)$.

Úloha 2.5.8. Ukážte, že ak $A \times C \subseteq B \times D$ a $A \times C \neq \emptyset$, tak $A \subseteq B$ a $C \subseteq D$. Ukážte na príklade, že bez predpokladu $A \times C \neq \emptyset$ už toto tvrdenie neplatí.

2.5.1 Triedy*

{triedy:SSECT

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

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

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

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

iedy:VTSETISPROPERCLASS}

Veta 2.5.7. *Trieda všetkých množín*

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

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

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

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

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

by bola množina.

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

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

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

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

Kapitola 3

Relácie a funkcie

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

3.1 Relácie

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

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

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

Príklad 3.1.2. Ak A je ľubovoľná množina, tak

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

je relácia na množine A.

{rel:PRIKLKRUZNICA}

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

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

Grafom tejto relácie je kružnica.

{rel:USPN}

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

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

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

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

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

{rel:DEFTRANZ}

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

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

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

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

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

V tejto prednáške sa budeme často zaoberať čiastočnými usporiadaniami.

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

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

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

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

nazývame ju *lineárnym usporiadaním.*

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

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

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

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

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

nazývame *zložením relácií S a R.*

Reláciu

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

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

{rel:TVRINVINV}

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

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

Jednoduchý dôkaz ponechávame ako cvičenie.

{rel:DEFID}

Definícia 3.1.10. Nech A je množina. Potom reláciu

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

na množine A nazývame *identita* na množine A.

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

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

Dôkaz. Označme $T := R \circ id_A$.

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

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

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

{rel:TVRINVZLOZ}

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

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

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

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

Tým je dokázaná rovnosť $L = P$. □

{rel:TVRTRANZSKLAD}

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

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

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

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

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

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

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

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

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

Z reflexívnosti máme $id_A \subseteq R$, z čoho vyplýva $id_A = id_A^{-1} \subseteq R^{-1}$ (pozri úlohu 3.1.12). Táto inklúzia znamená, že R^{-1} je reflexívna.

Antisymetria implikuje, že $R \cap R^{-1} \subseteq id_A$ (pozri Tvrdenie 3.1.13 (iii)), čo je súčasne antisymetria pre reláciu R^{-1}, keďže $(R^{-1})^{-1} = R$.

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

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

Tranzitívny uzáver V niektorých aplikáciách býva užitočný pojem tranzitívneho uzáveru, čo je vlastne relácia obsahujúca danú reláciu R, ktorá sa od R priveľmi nelíši a súčasne je tranzitívna. Nasledujúca definícia spresňuje, čo rozumieme pod pojmom „priveľmi nelíši“. Neskôr, keď sa budeme zaoberať pojmom najmenšieho prvku v čiastočne usporiadanej množine, by malo byť jasnejšie, prečo sme použili práve takúto definíciu.

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

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

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

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

Dôkaz. TODO □

V skutočnosti existenciu tranzitívneho uzáveru by sme mohli ukázať aj trochu iným (snáď jednoduchším) spôsobom, použitím faktu, že prienik tranzitívnych relácií je opäť tranzitívna relácia – úloha 3.1.17. Dôkaz, ktorý sme tu uviedli, má však tú výhodu, že od istej miery aj popisuje, ako tranzitívny uzáver danej relácie vyzerá.

Cvičenia

Úloha 3.1.1. Dokážte tvrdenie 3.1.9 a tvrdenie 3.1.13.

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

Úloha 3.1.3. Nájdite príklad relácie R na trojprvkovej množine, pre ktorú relácia $S = R \cup R^2$ nie je tranzitívna.

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

Úloha 3.1.4. Nech R, S sú relácie na množine A. Pre ktoré z vlastností uvedených v definícii 3.1.5 platí:
a) Ak má danú vlastnosť relácia R, tak ju má aj R^{-1}.
b) Ak majú danú vlastnosť relácie R a S, tak ju má aj $S \circ R$.

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

Úloha 3.1.6. Nech R, S sú čiastočné usporiadania na množine A. Dokážte alebo nájdite kontrapríklad:
a) relácia R^{-1} je čiastočné usporiadanie na A;
b) relácia $R \circ S$ je čiastočné usporiadanie na A;
c) relácia $R \cap S$ je čiastočné usporiadanie na A.

Úloha 3.1.7. Ukážte, že skladanie relácií je asociatívne, t.j. pre relácie R medzi A a B, S medzi B a C, a T medzi C a D platí $T \circ (S \circ R) = (T \circ S) \circ R$.

Úloha 3.1.8. Graficky znázornite dané relácie R, S na množine A; pokúste sa popísať a znázorniť aj relácie R^{-1}, S^{-1}, $S \circ R$, $R \circ S$, $R \circ R$, $S \circ S$. Ktoré z vlastností uvedených v definícii 3.1.5 majú tieto relácie?
a) $A = \langle -1, 1\rangle$, $R = \{(x, y) \in A \times A; x^2 + y^2 = 1\}$, $S = \{(x, y) \in A \times A; x^2 + y^2 \leq 1\}$;
b) $A = \mathbb{R}$; $R = \{(x, y) \in A \times A; |x| \geq |y|\}$, $S = \{(x, y) \in A \times A; |y| \geq |x|\}$;
c) $A = \mathbb{R}$; $R = \{(x, y) \in A \times A; |x - y| < a\}$, $S = \{(x, y) \in A \times A; |x - y| < b\}$, kde a, b sú nejaké (pevne zvolené) reálne čísla;

Úloha 3.1.9. Nech A je konečná množina, ktorá má n prvkov. Koľko relácií, reflexívnych relácií, symetrických relácií existuje na množine A?

Úloha 3.1.10. Dokážte, že ak R je relácia na množine A, ktorá je reflexívna a tranzitívna, tak $R \circ R = R$. Platí aj obrátená implikácia?

Úloha 3.1.11. Nech R, S sú relácie medzi množinami A, B. Dokážte, že $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ a $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$.

{relcvic:ULOSKLADSUB}

Úloha 3.1.12. Dokážte nasledujúce tvrdenia. (V každom z nich implicitne predpokladáme, že ide o relácie medzi takými množinami, aby ich bolo možné skladať.)
a) Ak R, $S_{1,2}$ sú relácie a $S_1 \subseteq S_2$, tak $S_1 \circ R \subseteq S_2 \circ R$. Platí aj obrátená implikácia?
b) Ak $R_{1,2}$, S sú relácie $R_1 \subseteq R_2$, tak $S \circ R_1 \subseteq S \circ R_2$. Platí aj obrátená implikácia?
c) Nech $R_{1,2}$ sú relácie na množine A a $R_1 \subseteq R_2$. Potom $R_1^{-1} \subseteq R_2^{-1}$.
d) Nech R je relácia na množine A taká, že $D(R) = A$. Ak $R \subseteq R^{-1}$, tak $id_A \subseteq R \circ R$. Platí aj obrátená implikácia?

Úloha 3.1.13. Nech $A \neq \emptyset$. Je relácia $\emptyset$ na množine A reflexívna, symetrická, tranzitívna? Ktoré z týchto vlastností platia pre reláciu id_A?

Úloha 3.1.14. Pre reláciu R medzi množinami $\{1, 2, \ldots, m\}$ a $\{1, 2, \ldots, n\}$ definujme *maticu relácie* (označme ju A_R) tak, že $a_{ij} = 1$ ak iRj a v opačnom prípade $a_{ij} = 0$. Nech R je relácia medzi množinami $\{1, 2, \ldots, m\}$ a $\{1, 2, \ldots, n\}$ a S je relácia medzi množinami $\{1, 2, \ldots, n\}$ a $\{1, 2, \ldots, k\}$. Viete nájsť nejaký vzťah medzi maticou $A_{S \circ R}$ a súčinom matíc $A_R.A_S$? (Pozor na výmenu poradia!)

Úloha 3.1.15. Jednotlivé podmienky z definície 3.1.5 prepíšte pomocou kvantifikátorov a znegujte ich.

Úloha 3.1.16. Nájdite príklady čiastočných usporiadaní $\leq$ na množine $\mathbb{N}$ takých, že:
a) Každý prvok $\mathbb{N}$ je minimálnym prvkom $\leq$.
b) $(\mathbb{N}, \leq)$ má najväčší prvok a nemá najmenší prvok.
c) $(\mathbb{N}, \leq)$ nemá najmenší ani najväčší prvok.

{relcvic:ULOTRANZUZ}

Úloha 3.1.17. Nech A je množina.

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

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

Úloha 3.1.18. Nech R je relácia na množine A. Dokážte, že:
a) Najmenšia (vzhľadom na inklúziu) reflexívna relácia obsahujúca R ako svoju podmnožinu je $R \cup id_A$. (Táto relácia sa zvykne nazývať *reflexívny uzáver* relácie R.)
b) Najmenšia (vzhľadom na inklúziu) symetrická relácia obsahujúca R ako svoju podmnožinu je $R \cup R^{-1}$. (Táto relácia sa zvykne nazývať *symetrický uzáver* relácie R.)

3.2 Funkcie

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

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

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

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

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

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

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

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

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

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

Množinovo môžeme definíciu zúženia zobrazenia zapísať ako

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

{fun:TVRINVBIJEK}

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

{fun:POZNAXSUBST}

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

{fun:POZNACFUN}

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

Detailnejšie zdôvodnenie, že ide skutočne o ekvivalentnú formuláciu, je v tvrdení 6.1.2.

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

Potom množinu

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

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

nazývame *obraz množiny* A v zobrazení f a množinu

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

nazývame *vzor množiny* B v zobrazení f.

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

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.

{fun:TVROBRAZVZOR}

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

(i) $g \circ f[A] = g[f[A]]$;
(ii) $(g \circ f)^{-1}[A] = g^{-1}[f^{-1}[A]]$;
(iii) $A \subseteq f^{-1}[f[A]]$ *a ak f je injektívne, tak* $A = f^{-1}[f[A]]$;
(iv) $f[f^{-1}[C]] \subseteq C$ *a ak f je surjektívne, tak* $f[f^{-1}[C]] = C$; {fun:itOBRCAP}
(v) $f[A \cap B] \subseteq f[A] \cap f[B]$ *a ak f je injektívne, tak* $f[A \cap B] = f[A] \cap f[B]$; {fun:itOBRBIGCAP}
(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) $f[A \cup B] = f[A] \cup f[B]$; {fun:itOBRBIGCUP}
(viii) $f[\bigcup_{i\in I} A_i] = \bigcup_{i\in I} f[A_i]$;
(ix) $f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$; {fun:itOBRCAPSYST}
(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;* {fun:itFAC}
(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) $f[A] \subseteq C \Leftrightarrow (\forall a \in A) f(a) \in C \Leftrightarrow (\forall a \in A) a \in f^{-1}[C] \Leftrightarrow A \subseteq f^{-1}[C]$. □

Nasledujúce tvrdenie už možno poznáte z nižších ročníkov, pozri napríklad [Sl2, cvičenia v časti 2.2] alebo [KGGS, Vety 1.3.3,1.3.4]. (Je treba dať pozor na to, že skladanie zobrazení

je v [KGGS] definované opačne ako v tejto prednáške, a preto je aj toto tvrdenie sformulované inak.)

Tu ho uvádzame preto, aby sme zdôraznili použitie axiómy výberu v jednej časti dôkazu tohoto tvrdenia. (V časti 6.1.2 ukážeme, že táto časť tvrdenia je dokonca ekvivalentná s axiómou výberu v systéme ZF.)

{fun:TVRSURJINV} {fun:itSURJ} {fun:itINJ}

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

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

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

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

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

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

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

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

(ii) $\boxed{\Rightarrow}$ Keďže $A \neq \emptyset$, existuje nejaký prvok $a \in A$; zvoľme si jeden taký prvok a označme ho a_0. Zobrazenie g definujeme nasledovne:

$$g(b) = \begin{cases} a, & \text{ak existuje } a \text{ také, že } f(a) = b, \\ a_0, & \text{inak.} \end{cases}.$$

Z injektívnosti f vyplýva, že takýmto spôsobom skutočne dostaneme zobrazenie. Rovnosť $g(f(a)) = a$ (pre každé $a \in A$) je zrejmá z definície zobrazenia g.

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

{fun:DOSINJSUR}

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

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

3.2.1 Karteziánsky súčin systému množín

{fun:SSECTKARTEZ}

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

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

{fun:DEFPROJ}

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

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

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

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

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

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

{kartez:DEFSUCNEK}

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

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

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

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

ktoré nazývame *i-ta projekcia.*

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

3.2.2 Karteziánsky súčin funkcií

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

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

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

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

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

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

{fun:TVRSUCBIJ}

Tvrdenie 3.2.19. *Nech $f\colon A \to C$, $g\colon B \to D$ sú zobrazenia.*
(i) *Ak f aj g sú injekcie, tak $f \times g$ je injekcia.*
(ii) *Ak f aj g sú surjekcie, tak $f \times g$ je surjekcia.*
(iii) *Ak f aj g sú bijekcie, tak $f \times g$ je bijekcia.*

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

(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). □

V dôkaze analogického tvrdenia pre súčin systému množín budeme potrebovať na jednom mieste využiť axiómu výberu; odvoláme sa na jej ekvivalentnú formuláciu, ktorú dokážeme neskôr v kapitole 6.

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

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

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

(ii) Nech každé f_i je surjektívne a nech $f \in \prod_{i\in I} B_i$. Potom pre každé $i \in I$ existuje $a_i \in A_i$ také, že $f_i(a_i) = f(i)$. Inak povedané, $\{a \in A_i; f_i(a) = f(i)\}$ je systém neprázdnych množín. Z ekvivalentnej formulácie axiómy výberu (tvrdenie 6.1.2(iii)) vyplýva existencia zobrazenia h definovaného na I takého, že $h(i) \in \{a \in A_i; f_i(a) = f(i)\}$, čiže $h(i) \in A_i$ a $f_i(h(i)) = f(i)$ pre každé $i \in I$. Posledná rovnosť hovorí presne to, že $g(h) = f$. Ukázali sme, že pre každé $f \in \prod_{i\in I} B_i$ existuje vzor, čiže g je surjektívne zobrazenie.

(iii) Ľahko vyplýva z predchádzajúcich dvoch častí. □

Cvičenia

{funcvic:ULOSKLAD}

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

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

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

{funcvic:ULOINVSURINJ}

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

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

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

Úloha 3.2.6. 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 3.2.7. Nech $f\colon X \to Y$ je zobrazenie. Dokážte, že f je injekcia $\Leftrightarrow$ pre ľubovoľné dve podmnožiny $A, B \subseteq X$ platí $f[B \setminus A] = f[B] \setminus f[A]$.

{funcvic:NEGKVANTINJ}

Úloha 3.2.8. Predpokladajme, že $f\colon X \to Y$ je zobrazenie. Zapíšte pomocou kvantifikátorov výroky „f je injekcia“ a „f je surjekcia“ a znegujte tieto výroky.

3.3 Čiastočne usporiadané množiny

{cum:SECTCUM}

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

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

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

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

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

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

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

Začnime tým, že uvedieme niekoľko príkladov čiastočných usporiadaní.

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

{cum:PRPOMDNCU

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

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

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

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

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

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

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

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

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

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

{cum:DEFNASLED}

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

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

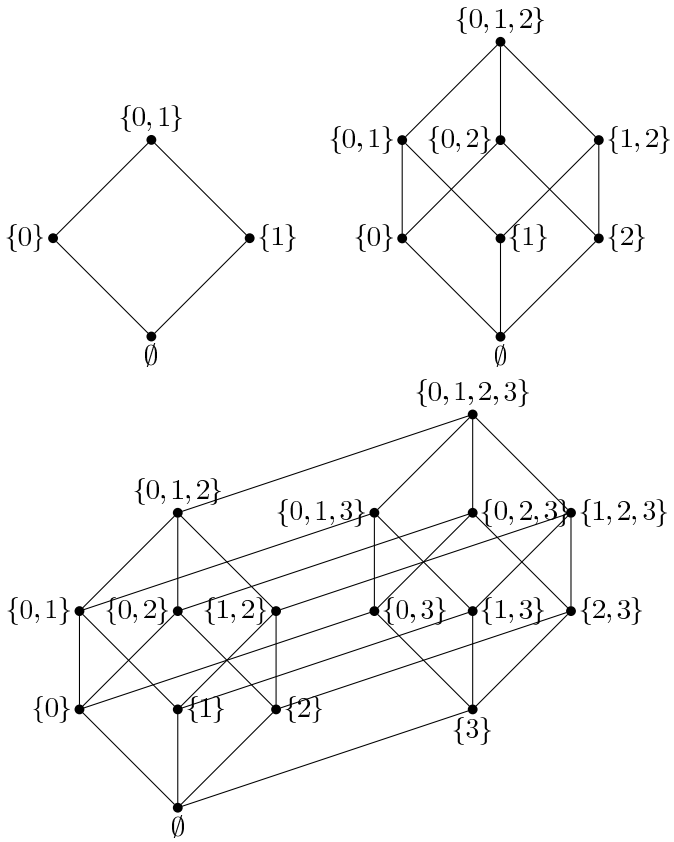
Prvok b sa nazýva *nasledovník* prvku a.

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

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

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

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



m:FIGHASSEPX}

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

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

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

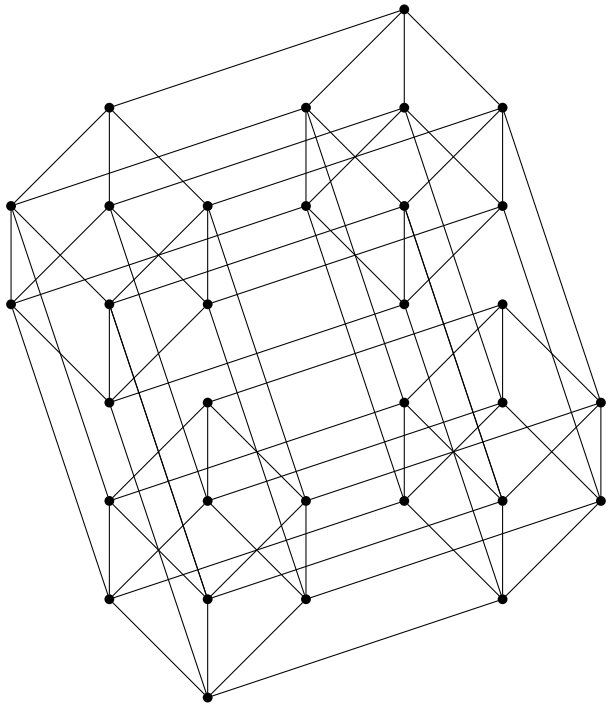
$$(\forall x_1, x_2 \in X) x_1 \leq x_2 \Rightarrow f(x_1) \preceq f(x_2).$$

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

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

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

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



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

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

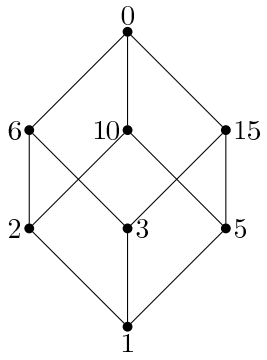
Definícia 3.3.7. Nech $(A, \leq)$ je čiastočne usporiadaná množina a $a \in A$. Hovoríme, že a je
(i) *najmenší prvok* množiny A, ak pre každý prvok $b \in A$ platí $a \leq b$;
(ii) *najväčší prvok* množiny A, ak pre každý prvok $b \in A$ platí $b \leq a$;
(iii) *minimálny prvok* množiny A, ak pre každé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

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

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

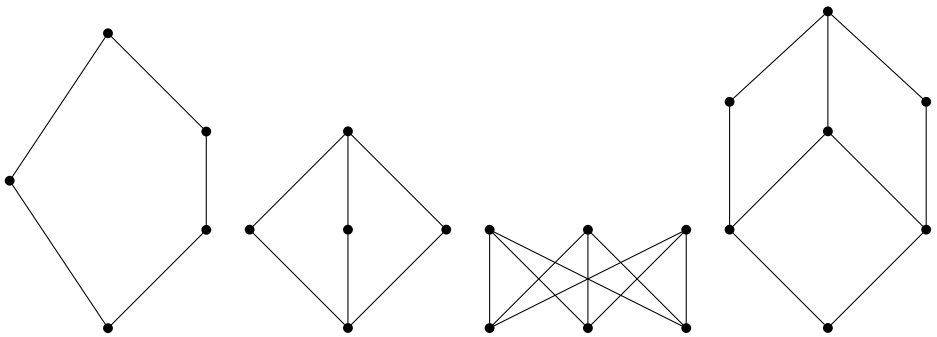
V prípade, že ide o lineárne usporiadanie, tak minimálny prvok je najmenší prvok, maximálny prvok je najväčší prvok. Vo všeobecnosti to však neplatí. Dá sa nájsť veľa jednoduchých príkladov (môžete si rozmyslieť, ako je to s čiastočne usporiadanými množinami znázornenými na obrázku 3.4); my si ukážeme jeden z nich. Ak uvažujeme ľubovoľnú množinu A, ktorá má aspoň dva prvky, tak relácia id_A je čiastočné usporiadanie na množine A. Pri tomto usporiadaní je každý prvok množiny A minimálny (a súčasne aj maximálny), ale množina A nemá najmenší ani najväčší prvok.

Predchádzajúci príklad súčasne ukazuje, že maximálnych (minimálnych) prvkov môže mať čiastočne usporiadaná množina viacero. Ak však čiastočne usporiadaná množina má najväčší



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

(najmenší) prvok, tak tento prvok je jednoznačne určený.



FIGMOREHASSE} Obr. 3.4: Ďalšie príklady Hasseho diagramov

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

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

{cum:DEFOSTRE}

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

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

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

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

Najprv dokážeme dve pomerne jednoduché lemy.

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

(iii) *ak R je tranzitívna, tak aj S je tranzitívna.*

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

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

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

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

Dôkaz. (i) Zrejmé.

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

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

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

{cum:DOSOSTRE}

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

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

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

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

{cum:POZNTRICHOT}

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

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

Čiže ostré čiastočné usporiadanie je trichotomická relácia.

Cvičenia

{cumcvic:ULOJEDNNAJV}

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

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

{cumcvic:ULOIZOMLUM}

Úloha 3.3.3. Ukážte, že ak A, B sú lineárne usporiadané množiny, tak bijektívne monotónne zobrazenie $f\colon A \to B$ je izomorfizmus.

Úloha 3.3.4. Nech A je množina a $R_{1,2}$ sú čiastočné usporiadania na A. Dokážte, alebo vyvráťte:
a) Relácia $R_1 \cap R_2$ je čiastočné usporiadanie na A.
b) Relácia $R_1 \cup R_2$ je čiastočné usporiadanie na A.
c) Ak $R_1 \cup R_2$ je čiastočné usporiadanie na A, tak $R_1 \subseteq R_2$ alebo $R_2 \subseteq R_1$.

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

Úloha 3.3.6. Nájdite pre každý z Hasseho diagramov na obrázku 3.4 množinu $A \subseteq \mathcal{P}(\mathbb{N})$ takú, že čiastočne usporiadaná množina $(A, \subseteq)$ má daný Hasseho diagram.

{cumcvic:ULOPRAZDCUM}

Úloha 3.3.7. Nech A je ľubovoľná množina. Sú relácie $A \times A$, id_A a $\emptyset$ čiastočnými usporiadaniami na množine A?

Úloha 3.3.8. Môže byť čiastočné usporiadanie na množine A zobrazením z A do A?

Úloha 3.3.9. Pre aké množiny A je $(\mathcal{P}(A), \subseteq)$ lineárne usporiadaná množina?

Úloha 3.3.10. Nech A je konečná množina, ktorá má n prvkov. Nech R je čiastočné usporiadanie na A. Aký je maximálny/minimálny možný počet prvkov množiny R? Aká je odpoveď na rovnaké otázky pre reláciu ekvivalencie?

Úloha 3.3.11. Nech $f\colon A \to B$ je ľubovoľné zobrazenie a $(B, \leq)$ je čiastočne usporiadaná množina. Dokážte potom, že relácia $\preceq$ definovaná ako $a \preceq a' \Leftrightarrow f(a) \leq f(a')$ je čiastočným usporiadaním na množine A. Bude $\preceq$ lineárne usporiadanie, ak $\leq$ je lineárne usporiadanie?

3.4 Dobre usporiadané množiny

{dum:SECTDUM}

V tejto časti sa zoznámime s dobre usporiadanými množinami. Dobre usporiadané množiny sú zaujímavá téma sama o sebe – ich užitočnosť spočíva v tom, že veľmi prirodzeným spôsobom ponúkajú zovšeobecnenie matematickej indukcie na ďalšie množiny. Okrem toho ich budeme potrebovať aj na to, aby sme boli schopní sformulovať jednu z ekvivalentných formulácií axiómy výberu v kapitole 6.

{dum:DEFDUM}

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

Ľahko vidno, že dobre usporiadaná množina musí byť lineárne usporiadaná. (Stačí si všimnúť, že ak najmenší prvok množiny $\{a, b\}$ je prvok a, tak platí $a \leq b$, ak je to prvok b, tak platí $b \leq a$. Pozri aj úlohu 3.4.2.)

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

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

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

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

{dum:VTIND}

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

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

Potom $B = A$.

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

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

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

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

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

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

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

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

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

{dum:LMNASLED}

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

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

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

{dum{DEFANTILEXIKO}

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

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

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

Antilexikografické usporiadanie na $A \times B$ definujeme ako

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

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

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

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

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

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

{dum:TVRLEXI}

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

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

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

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

Dôkaz. Všimnime si najprv, že ak $(a, b) \leq (a', b')$, tak $a \leq a'$. (Toto pozorovanie použijeme v dôkaze viackrát.)

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

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

Potom platí $a \leq a'$ aj $a' \leq a$, z čoho dostaneme $a = a'$.

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

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

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

Z týchto nerovností vyplýva $a \leq a'$ a $a' \leq a''$.

Uvažujme najprv prípad, že $a < a'$ alebo $a' < a''$; t.j. že aspoň jedna z týchto dvoch nerovností je ostrá. V ktoromkoľvek z týchto dvoch prípadov dostávame, že $a < a''$, a teda $(a, b) \leq (a'', b'')$.

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

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

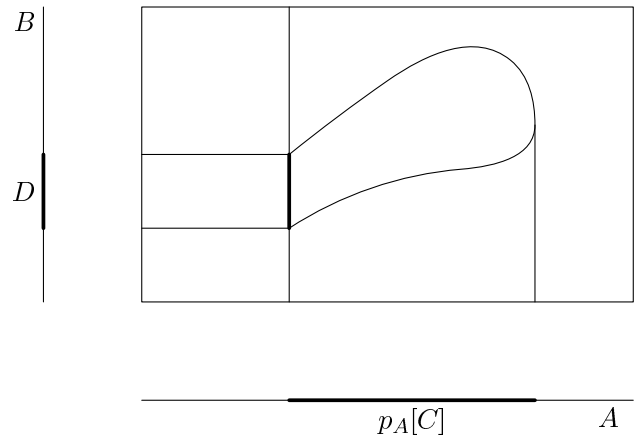
Ak $a < a'$, tak z definície lexikografického usporiadania máme $(a, b) \leq (a', b')$.

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

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

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

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



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

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

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

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

{dum:POZNIZOMLEX}

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

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

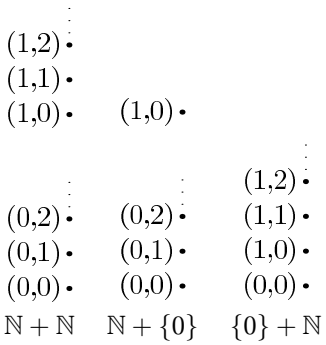
{dum:PRSUCET}

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

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

Ak obe množiny sú lineárne (dobre) usporiadané, platí to aj o výslednej množine – overenie tohoto faktu ponecháme ako cvičenie pre čitateľa. (Zovšeobecnenie tohoto faktu môžete nájsť v úlohe 3.4.4.)

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



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

takto definovaný súčet a antilexikografický súčin dobre usporiadaných množín sa dajú použiť na zavedenie súčtu a súčinu ordinálnych čísel.

{dum:POZNDISJZJED}

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

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

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

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

{dum:TVRIZOMPOCUSEK}

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

$$f(a) = X_a$$

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

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

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

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

Ešte treba overiť, že aj f^{-1} je monotónne. Na to si stačí všimnúť, že ak $X_a \subseteq X_b$, tak $a \leq b$ (Ak by totiž platilo $a > b$, tak $b \in X_a \setminus X_b$, čo je v spore s predpokladom $X_a \subseteq X_b$.)

Iná možnosť – namiesto overovania monotónnosti f^{-1} – je použiť výsledok z úlohy 3.3.3. □

Cvičenia

{dumcvic:ULOSUB}

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

{dumcvic:ULODUMLUM}

Úloha 3.4.2. Ukážte, že $\leq$ je dobré usporiadanie množiny A práve vtedy, keď $\leq$ je lineárne usporiadanie také, že každá neprázdna množina má minimálny prvok. (Dostávame takto ekvivalentnú definíciu dobre usporiadanej množiny. Rozdiely oproti definície 3.4.1: Namiesto čiastočného usporiadania požadujeme lineárne usporiadanie a existenciu najmenšieho prvku sme nahradili existenciou minimálneho prvku.)

Úloha 3.4.3. Nech $(X, \leq)$ je lineárne usporiadaná množina. Ukážte, že $a \in X$ je minimálny prvok množiny X práve vtedy, keď $X_a = \emptyset$.

{dumcvic:SUMSYST}

Úloha 3.4.4. V tejto úlohe zadefinujeme isté zovšeobecnenie lexikografického súčinu.
Nech $(A, \leq_A)$ je čiastočne usporiadaná množina a pre každé $a \in A$ je $(B_a, \leq_a)$ čiastočne usporiadaná množina. Na množine $\bigcup_{a\in A}\{a\} \times B_a$ definujeme reláciu $\leq$ predpisom:

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

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

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

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

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

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

Úloha 3.4.5. Zistite, ktoré z uvedených dobre usporiadaných množín sú izomorfné. Môžete sa pokúsiť ich aj nejako graficky znázorniť.
a) $(\mathbb{N}, \leq)$
b) $(\mathbb{N}, \leq) + (\mathbb{N}, \leq)$
c) $(\mathbb{N}, \leq) + (\{0\}, \leq)$
d) $(\{0\}, \leq) + (\mathbb{N}, \leq)$
e) $(\{0, 1\}, \leq) \times (\mathbb{N}, \leq)$ (lexikografický súčin)
f) $(\mathbb{N}, \leq) \times (\{0, 1\}, \leq)$ (lexikografický súčin)
g) $(\mathbb{N}, \leq) \times (\mathbb{N}, \leq)$ (lexikografický súčin)
h) $\sum_{n\in\mathbb{N}}(\{1, 2, \ldots, n\}, \leq)$
i) $\sum_{n\in\mathbb{N}}(\mathbb{N}, \leq)$

Úloha 3.4.6*. Dokážte, že:
a) (2 body) Každá podmnožina $\mathbb{R}$, ktorá je dobre usporiadaná (pri obvyklom usporiadaní reálnych čísel) je spočítateľná.
b) (2 body) Každá dobre usporiadaná podmnožina $\mathbb{R}$ je izomorfná s podmnožinou $\mathbb{Q}$ (s obvyklým usporiadaním racionálnych čísel).
c) (2 body) Každá spočítateľná dobre usporiadaná množina je izomorfná s podmnožinou $(\mathbb{R}, \leq)$.
(Časti a), b) a c) nemusíte nutne riešiť v uvedenom poradí, zvoľte si také, aké vám vyhovuje najviac.)

Kapitola 4

Kardinálne čísla

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

4.1 Porovnávanie mohutností množín

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

{def:DEFKARD}

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

{def:POZNTRANZEQ}

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

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

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

{def:POZNDEFKARD}

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

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

Odpoveď na túto otázku je, že sa to skutočne dá. Túto množinu $|X|$ budeme nazývať *kardinálne číslo* množiny X. (Kardinálne čísla budeme často označovať malými gréckymi písmenami.) Bohužiaľ zatiaľ nemáme vybudovaný aparát na to, aby sme mohli podať štandardný spôsob, ako sa to v súčasnej teórii množín robí. Čiže zatiaľ vám nezostáva iná možnosť,

iba tomu uveriť a používať pojem kardinálneho čísla s prísľubom, že neskôr uvidíte, že tento pojem sa dá v ZFC zmysluplne vybudovať. (Urobíme to v časti 7.5.)

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

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

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

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

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

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

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

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

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

s množinami, budeme napríklad pracovať s množinami kardinálnych čísel alebo s funkciami definovanými na kardinálnom čísle.

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

KARDINALAMAKARDINALITUA}

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

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

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

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

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

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

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

Poznámka 4.1.6. Už vieme (pozri tvrdenie 3.2.14 a úlohu 3.2.4), že pre $X \neq \emptyset$ je existencia injekcie z X do Y ekvivalentná s existenciou surjekcie z Y do X. (Pričom implikácia $\Leftarrow$ vyžaduje axiómu výberu – dokonca je s ňou ekvivalentná, ako ukážeme v tvrdení 6.1.2(vi).)

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

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

{def:TVRCUM}

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

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

Dôkaz. (i) $id_X \colon X \to X$ 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.

{def:VTCANTBER}

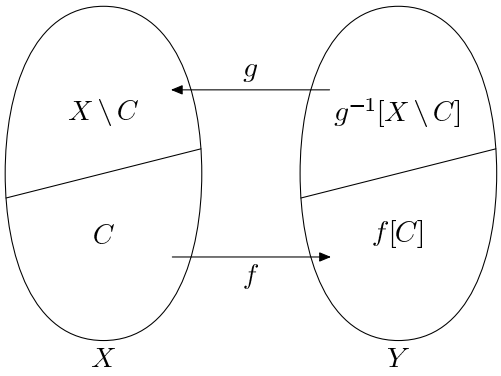
Veta 4.1.8 (Cantor-Bernstein)**.** *Nech X, Y sú množiny. Ak platí $|X| \leq |Y|$ a $|Y| \leq |X|$, tak $|X| = |Y|$.*

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

Inak: Ak existuje injekcia $f \colon X \to Y$ 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 4.1. Z týchto dvoch bijekcií už potom vieme poskladať bijekciu medzi X a Y.



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

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

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

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

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

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

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

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

Tento predpis skutočne definuje zobrazenie: Každý prvok x množiny X buď patrí do C alebo do $X \setminus C$, 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 3.2.13 (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, ktoré sme zatiaľ nedefinovali. (Preto sa ich snažíme využívať iba v príkladoch, nie však v dôležitých dôkazoch.) Nasledujúci dôkaz je len o trošičku komplikovanejší – líši sa od predchádzajúceho vlastne iba na jednom mieste, tento problém v ňom však už nie je.

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

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

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 2.4.10(xi) a 3.2.13 postupne dostaneme

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

Položme $\mathcal{S} := \{B \subseteq X; B \subseteq F(B)\}$ a $C := \bigcup \mathcal{S} = \bigcup \{B \subseteq X; B \subseteq F(B)\}$.
Ak $B \in \mathcal{S}$, tak $B \subseteq C$, a teda $F(B) \subseteq F(C)$.
Teda pre každé $B \in \mathcal{S}$ platí $B \subseteq F(B) \subseteq F(C)$, z čoho vyplýva $C = \bigcup_{B \in \mathcal{S}} B \subseteq F(C)$.

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

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

Poznámka 4.1.9. Pre čitateľa, ktorý sa zaoberal teóriou zväzov, môže byť zaujímavé všimnúť si, že sme v dôkaze vlastne zostrojili zobrazenie $F\colon \mathcal{P}(X) \to \mathcal{P}(X)$, ktoré je monotónne. Na dôkaz Cantor-Bernsteinovej vety nám stačilo nájsť pevný bod tohoto zobrazenia. Jeho existencia vyplýva z Knaster-Tarského vety o pevnom bode, keďže $(\mathcal{P}(X), \subseteq)$ je úplný zväz. Takýmto spôsobom je dokázaná Cantor-Bernsteinova veta napríklad

v [F, Theorem 3.1.9], [KLŠZ, Príklad 2.3.6]. (V podstate náš dôkaz bol do značnej miery podobný spôsobu, akým sa dokazuje Knaster-Tarského veta, resp. prvý z uvedených dôkazov sa väčšmi ponášal na dôkaz Kleeneho vety o pevnom bode.)

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

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

{def:POZNPOROVKARD}

Poznámka 4.1.11. V tomto kontexte je ďalšou prirodzenou otázkou to, či sú ľubovoľné dve kardinálne čísla porovnateľné. Je to skutočne pravda, dôkaz využíva axiómu výberu. Tento fakt ukážeme neskôr pomocou výsledkov o dobre usporiadaných množinách v kapitole o ordinálnych číslach ako dôsledok 7.1.6.

Cvičenia

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

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

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

4.2 Kardinálna aritmetika

{aritm:SECTKARDARITM}

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

Definícia 4.2.1. Nech a, b sú kardinálne čísla a nech A, B sú množiny také, že $|A| = a$, $|B| = b$. Potom:
(i) Predpokladajme navyše, že množiny A a B sú disjunktné. Potom *súčet kardinálnych čísel* a a b je kardinálne číslo množiny $A \cup B$, t.j.

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

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

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

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

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

Táto definícia si zaslúži niekoľko komentárov. V prvom rade sa môžeme zamyslieť nad tým, či vôbec pre ľubovoľné kardinálne číslo a existuje množina A taká, že $|A| = a$. Pokiaľ ste uverili poznámke 4.1.4, tak viete, že môžeme za A zvoliť priamo kardinál a. Tu sa však odvolávame na konštrukciu kardinálov, ktorú urobíme až neskôr v časti 7.5. Ale funguje to aj pri naivnom pohľade na kardinálne čísla – za kardinálne čísla totiž považujeme iba tie „objekty“, ktoré môžeme dostať ako kardinality nejakých množín.

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

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

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

Lema 4.2.2. *Sčitovanie kardinálov je dobre definované.*

Dôkaz. Cvičenie. □

Lema 4.2.3. *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 3.2.19 je zobrazenie $f \times g\colon A \times A' \to B \times B'$ tiež bijekcia. □

Lema 4.2.4. *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.

{aritm:DEFKONKARD}

Definícia 4.2.5. 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 4.2.6. 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 4.1.11, na to aby ľubovoľné dve kardinálne čísla boli porovnateľné potrebujeme axiómu výberu. Keďže my pracujeme v ZFC, tak uvedená definícia je ekvivalentná s takou definíciou, kde by sme nekonečné kardinály zaviedli ako tie, ktoré nie sú konečné.

V teórii množín sa skutočne pracuje s viacerými definíciami konečnosti, ktoré sú ekvivalentné v ZFC, nie všetky z nich sú však ekvivalentné v ZF; pozri napríklad [B2, Problém 1B], [He2, Section 4.1], [ŠS, Kapitoly 7.1 a 7.4]. My sa s týmito dvoma definíciami konečných množín budeme zaoberať v časti 5.4.

Označenie $\mathfrak{c}$ a názov kardinalita kontinua pochádza z toho, že $\mathfrak{c}$ je kardinalita množiny $\mathbb{R}$. Tento fakt overíme neskôr – tvrdenie 4.5.1. Už teraz ukážeme, že $\mathfrak{c} = 2^{\aleph_0}$.

{aritm:VTPX2NAX}

Veta 4.2.7. *Nech X je ľubovoľná množina. Potom platí*

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

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

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

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

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

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

Dôsledok 4.2.8.

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

4.2.1 Vlastnosti sčitovania kardinálov

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

Veta 4.2.9. *Nech a, b, c sú kardinálne čísla, potom platí*

$$a + b = b + a$$
$$a + (b + c) = (a + b) + c$$

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 $A\cup(B\cup C) = (A\cup B)\cup C$. □

{aritm:VTNEROVSUCET}

Veta 4.2.10. *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 vyplýva, že $g(y) \in C$ a $C \cap A = \emptyset$. Teda $y \in A$ a $g(y) = y$, čiže rovnosť $g(x) = g(y)$ znamená priamo $x = y$.

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

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

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

Príklad 4.2.11. 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 4.2.10 neplatí pre ostrú nerovnosť.

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

{aritm:TVRNEKPLUSALNUL}

Tvrdenie 4.2.12. *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.

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

□

4.2.2 Vlastnosti násobenia kardinálov

Veta 4.2.13. *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 2.5.4 však vieme, že platí dokonca rovnosť $A\times(B\cup C) = (A\times B)\cup(A\times C)$. □

Veta 4.2.14. *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 3.2.19 je aj zobrazenie $id_A \times f\colon A\times B \to A \times C$ injekcia. □

Opäť platí analogická poznámka ako pri vete 4.2.10. Mohli by sme priamo predpokladať, že $B \subseteq C$ a potom si stačí všimnúť, že $A \times B \subseteq A \times C$ (pozri úlohu 2.5.4).

{aritm:PRIKLBIJEKNxN}

Príklad 4.2.15. Ukážeme, že platí

{aritm:EQNxN}
$$\aleph_0.\aleph_0 = \aleph_0. \tag{4.1}$$

Z rovnosti (4.1) dostaneme, že pre každé $n \in \mathbb{N}$, $n > 0$, platí

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

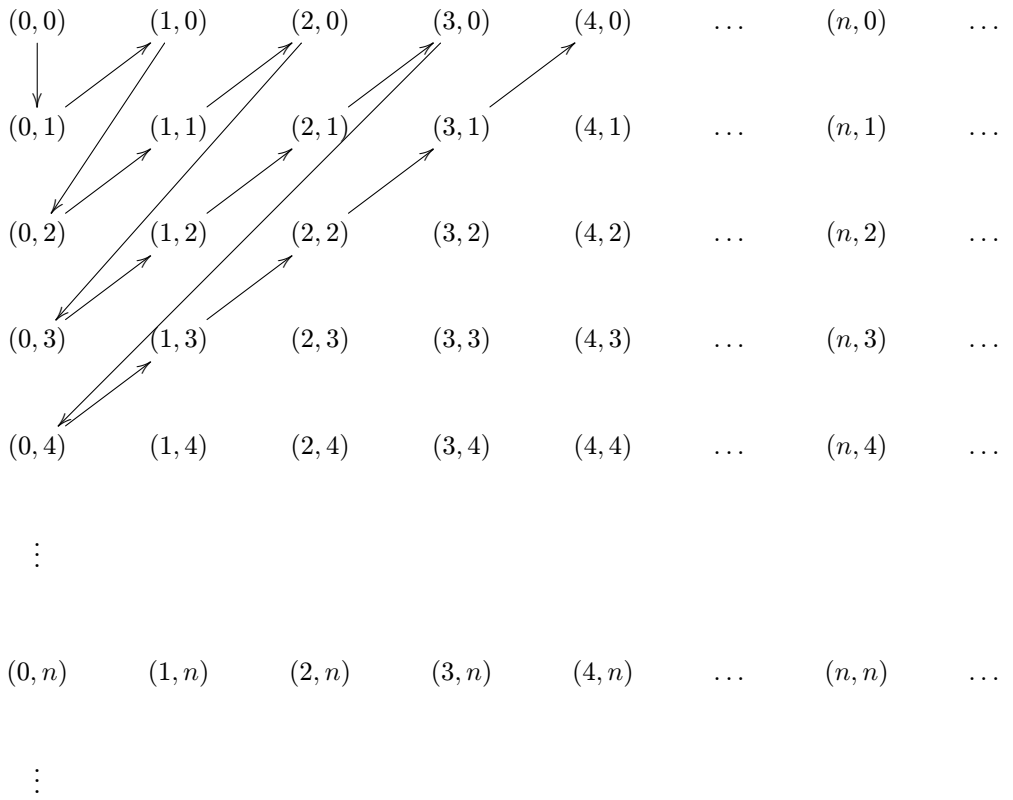
Z Cantor-Bernsteinovej vety potom vyplýva rovnosť

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

Na dôkaz rovnosti (4.1) nám stačí zostrojiť bijekciu medzi $\mathbb{N} \times \mathbb{N}$ a $\mathbb{N}$. Takýchto bijekcií sa dá nájsť veľa, ako prvú si ukážeme jednu veľmi známu pochádzajúcu už od G. Cantora.

Nasledujúci obrázok nám ukazuje, ako môžeme usporiadané dvojice prirodzených čísel

usporiadať do postupnosti:



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

Toto zobrazenie vieme popísať aj jednoduchým predpisom. Všimnime si, že dvojice na tej istej diagonále (t.j. také dvojice (m,n), ktoré majú rovnaký súčet $m+n$) zoraďujeme podľa prvej súradnice a všetky prvky z diagonál, ktoré sú naľavo od nich. Teda ak $m+n=s$, tak $1+2+\cdots+s=\frac{s(s+1)}{2}$ 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 [Č1].) Teda zobrazenie

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

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

{aritm:POZNMAX}

Poznámka 4.2.16. Neskôr ukážeme (vo vete 7.6.1 a dôsledku 7.6.2, dôkaz využíva axiómu výberu), že kardinálne sčitovanie a násobenie je jednoduché, pre ľubovoľné nekonečné kardinály a, b totiž platí

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

(Zatiaľ dokonca nevieme ani to, či existuje maximum z kardinálnych čísel a, b; pozri poznámku 4.1.11.)

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

4.2.3 Vlastnosti kardinálneho umocňovania

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

Tvrdenie 4.2.17. *Ak a je ľubovoľné kardinálne číslo, tak platí*

$$a^2 = a.a.$$

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

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

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

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

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

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

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

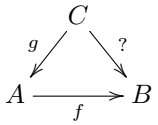
Veta 4.2.18. *Ak a, b, c sú kardinálne čísla také, že $a \leq b$, tak $a^c \leq b^c$.*

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 4.2.19. *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

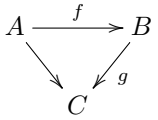
$$\varphi(g)(x) = \begin{cases} g(x) & \text{pre } x \in A, \\ c_0 & \text{pre } x \notin A. \end{cases}$$

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 $g = h$. □

Ukážeme si ešte iný dôkaz. (Oproti predchádzajúcemu má však istú nevýhodu, keďže používame tvrdenie 3.2.14 a úlohu 3.2.4, a teda axiómu výberu.)

Dôkaz. Nech $f\colon A \to B$ je injekcia. Potom pre každé $g\colon B \to C$ máme zobrazenie $g \circ f$.



Definujme zobrazenie $\varphi\colon C^B \to C^A$ ako

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

pre $g\colon B \to C$.

Ukážeme, že toto zobrazenie je surjektívne. Nech $h\colon A \to C$ je ľubovoľný prvok C^A. Predpokladajme navyše, že $A \neq \emptyset$. Podľa tvrdenia 3.2.14 existuje zobrazenie $f'\colon B \to A$ také, že $f' \circ f = id_A$. Potom pre zobrazenie $h \circ f'$ platí $\varphi(h \circ f') = h \circ f' \circ f = h \circ id_A = h$. Ukázali sme, že ľubovoľné zobrazenie $h \in C^A$ má v zobrazení vzor.

Zostáva rozobrať len prípad $A = \emptyset$. Vtedy platí $C^\emptyset = \{\emptyset\}$. Súčasne, keďže $C \neq \emptyset$, takže C^B je aspoň jednoprvková. Teda aj v tomto prípade uvedená nerovnosť platí. □

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 4.2.20. *Pre ľubovoľné kardinálne čísla platí*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

{aritm:VTMOCKARTEZ}

Veta 4.2.21. *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.

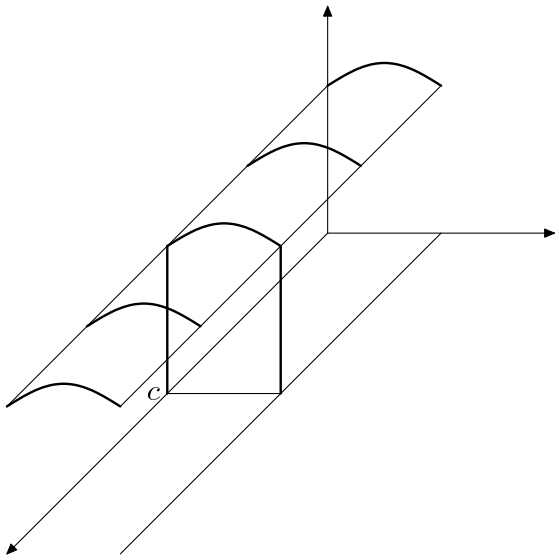
Hľadáme zobrazenie $\varphi\colon (A^B)^C \to A^{B \times C}$. T.j. ak máme dané nejaké zobrazenie $f\colon C \to A^B$, chceli by sme k nemu nájsť niečo, čo dvojiciam $(b,c) \in B \times C$ priradí prvky z A. Pre ľubovoľné $c \in C$ však máme zobrazenie $f(c)\colon B \to A$ – čiže je dosť prirodzené 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. 4.2, kde $A = \mathbb{R}$, $B = \langle 0,1 \rangle$, $C = \langle 0, \infty)$. Rezy načrtnuté na grafe funkcie sú práve funkcie z B do A priradené jednotlivým prvkom z C.



Obr. 4.2: Obrázok ilustrujúci postup v dôkaze vety 4.2.21. (Použitá funkcia je $f(x,y) = \frac{3}{2} + \frac{1}{5}\sin \pi x$.)

{aritm:FIGMOCI

(Naschvál som zvolil množiny A, B a C rôzne, aby sa na obrázku dalo vidieť, ktorá množina je ktorá.)

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

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

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

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

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

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

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

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

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

{aritm:VTANABPOD2NAAB}

Veta 4.2.22. *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

{:DOSAPOD2NAA}

Dôsledok 4.2.23. *Pre ľubovoľné kardinálne číslo a platí*

$$a \leq 2^a.$$

Cvičenia

{aritmcvic:ULOANABEXISTS

Úloha 4.2.1. Ukážte pomocou schémy axióm vymedzenia, že pre ľubovoľné množiny A a B existuje množina všetkých zobrazení z B do A.

Úloha 4.2.2. Ukážte, že $|\mathbb{Z}| = \aleph_0$. (T.j. nájdite bijekciu medzi $\mathbb{Z}$ a $\mathbb{N}$.)

Úloha 4.2.3. Ukážte, že $\mathfrak{c}.\mathfrak{c} = \mathfrak{c}$ a $\mathfrak{c}^{\aleph_0} = \mathfrak{c}$.

Úloha 4.2.4. Ukážte, že pre ľubovoľný konečný kardinál n platí $\mathfrak{c} = n.\mathfrak{c} = \mathfrak{c}.\mathfrak{c} = \mathfrak{c}^n = \mathfrak{c}^{\aleph_0}$.

Úloha 4.2.5. Ukážte, že pre ľubovoľný konečný kardinál n platí $2^{\aleph_0} = n^{\aleph_0} = \aleph_0^{\aleph_0} = \mathfrak{c}^{\aleph_0} = \mathfrak{c}$.

Úloha 4.2.6. S využitím faktu, že pre nekonečné kardinály platí $b.b = b$ (ktorý dokážeme neskôr) ukážte, že ak $2 < a \leq b$, kde a, b sú nekonečné kardinály, tak $2^b = a^b$.

Úloha 4.2.7. 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 4.2.8. Dokážte dôsledok 4.2.23 bez toho, aby ste sa odvolávali na vetu 4.2.22. Ukážte, ako potom možno z uvedeného dôsledku odvodiť vetu 4.2.22.

Úloha 4.2.9. Ukážte, že ak pre množiny A, B platí $|A \setminus B| = |B \setminus A|$, tak $|A| = |B|$.

Úloha 4.2.10*. Aká je kardinalita množiny všetkých bijekcií z $\mathbb{N}$ do $\mathbb{N}$? (Bijekcie z $\mathbb{N}$ do $\mathbb{N}$ sa niekedy zvyknú nazývať aj permutáciami množiny $\mathbb{N}$. Na základe analógie s prirodzenými číslami by sme kardinalitu takejto množiny mohli nazvať $\aleph_0$-faktoriál.)

4.3 Cantorova veta a diagonálna metóda

{cantor:VTCANTOR}

Veta 4.3.1 (Cantor)**.** *Pre každú množinu X platí $|X| < |\mathcal{P}(X)|$.*

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

Dôkaz. Nerovnosť $|X| \leq |\mathcal{P}(X)|$ vyplýva z toho, že $x \mapsto \{x\}$ je injekcia z X do $\mathcal{P}(X)$. (Iné možné zdôvodnenie – dôsledok 4.2.23).

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

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

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

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

{cantor:PRIKL

Príklad 4.3.2. Možno nám lepšie pomôže pochopiť tento dôkaz, ak si ho ešte raz osvetlíme na prípade $X = \mathbb{N}$. Budeme sa teda zaoberať kardinalitou množiny $\mathcal{P}(\mathbb{N})$, namiesto nej však môžeme zobrať množinu $\{0,1\}^{\mathbb{N}}$ všetkých postupností núl a jednotiek. Vo vete 4.2.7 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 4.3.1 je v podstate totožný s postupom z predchádzajúceho príkladu. (Jediný rozdiel je v tom, že sme nemohli prvky $f(x)$, $x \in X$, zapísať do postupnosti, keďže tam sme pracovali s ľubovoľnou množinou X a nie s množinou $\mathbb{N}$.)

{cantor:POZNDIAG}

Poznámka 4.3.3. Metóda použitá v predchádzajúcom dôkaze pochádza od Cantora a nazýva sa *diagonálna metóda.* (V predchádzajúcom príklade vidno, že sme vlastne menili 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 4.5.4.

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

{cantor:PRALNULxC}

Príklad 4.3.4. Ukážeme, že platí

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

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

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

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

Kardinálne čísla tvoria vlastnú triedu

Nadviažeme na časť 2.5.1 a povieme si ešte niečo o vlastných triedach. Aby boli dôkazy výsledkov v tejto časti úplne korektné treba uveriť tomu, že kardinálne čísla sa skutočne dajú zadefinovať formulou jazyka teórie množín a majú vlastnosti, ktoré sme už uviedli (pozri poznámku 4.1.4.)

Pokiaľ chceme ukázať, že nejaký systém množín je vlastnou triedou, často môžeme postupovať sporom – pokúsiť sa ukázať pomocou axióm ZFC, že ak by tento systém bol množinou, bola by množinou aj trieda **Set**. Ukážeme si to na príklade dvoch tvrdení:

{def:TVRSINGLETONSCLASS}

Tvrdenie 4.3.5. *Systém všetkých jednoprvkových množín tvorí vlastnú triedu.*

Dôkaz. Predpokladajme, že by systém všetkých jednoprvkových množín $\{\{x\}; x \in \mathbf{Set}\}$ tvoril množinu. Potom $f\colon \{x\} \mapsto x$ je zobrazenie definované na tejto množine. Jeho obrazom je vlastná trieda **Set**. Podľa schémy axióm substitúcie by potom **Set** bola množina, čo je spor s vetou 2.5.7. □

Iný dôkaz. Predpokladajme, že by systém všetkých jednoprvkových množín $\{\{x\}; x \in \mathbf{Set}\}$ tvoril množinu. Podľa axiómy zjenotenia by potom aj $\bigcup\{\{x\}; x \in \mathbf{Set}\}$ bola množina. Lenže každá množina x patrí do jednoprvkovej množiny $\{x\}$, takže $\bigcup\{\{x\}; x \in \mathbf{Set}\} = \mathbf{Set}$. Dostávame, že **Set** je množina, čo vedie k tomu istému sporu ako v predošlom dôkaze. □

Veľmi podobným spôsobom môžeme ukázať nasledujúce tvrdenie:

{def:TVRGIVENCARDCLASS}

Tvrdenie 4.3.6. *Nech $X \neq \emptyset$ je množina. Potom systém všetkých množín rovnakej mohutnosti ako X tvorí vlastnú triedu.*

Dôkaz. Sporom. Predpokladajme, že $A = \{m; |m| = |X|\}$ je množina. Položme $B = \{m \in A; (\exists x) m = \{x\} \times X\}$. Na základe schémy axióm vymedzenia je aj B množina. Ďalej definujeme formulu $\varphi(y, x)$ ako $y = \{x\} \times X$. Táto formula má tú vlastnosť, že pre každé $y \in B$ existuje práve jedno x také, že platí $\varphi(y, x)$. Existencia vyplýva priamo z definície množiny B a na základe neprázdnosti X dostaneme z $y = \{x_1\} \times X = \{x_2\} \times X$ rovnosti $\{x_1\} = \{x_2\}$ a $x_1 = x_2$. (Pozri tvrdenie 2.5.4.)

Potom zo schémy axióm obrazu, že $\{x; \{x\} \times X \in A\}$ je množina. Ľahko však vidno, že pre každú množinu x existuje bijekcia medzi X a $\{x\} \times X$, čo znamená, že $\{x; \{x\} \times X \in A\} = \mathbf{Set}$. Dostávame spor. □

Iný dôkaz. Sporom. Predpokladajme, že $A = \{m; |m| = |X|\}$ je množina. Stačí nám, podobne ako v prípade predchádzajúceho tvrdenia, ukázať, že $\bigcup A = \mathbf{Set}$.

Ak $x \in \mathbf{Set}$ je ľubovoľná množina, tak existuje $m \in A$ také, že $x \in m$. V prípade, že $x \in X$ je to jasné. Ak $x \notin X$, tak stačí zvoliť nejaké $x_0 \in X$ (čo môžeme urobiť, lebo $X \neq \emptyset$) a položiť $m = X \setminus \{x_0\} \cup X$. Očividne $|m| = |X|$.

Ukázali sme, že každá množina patrí do nejakého prvku množiny A, čo znamená, že $\bigcup A = \mathbf{Set}$. □

{def:VTCNISPROPERCLASS}

Veta 4.3.7. *Systém všetkých kardinálnych čísel tvorí vlastnú triedu. Túto triedu budeme označovať* Cn.

Dôkaz. Sporom. Prepokladajme, že Cn je množina. Potom aj $B = \bigcup \mathrm{Cn}$ je množina, navyše pre každé kardinálne číslo platí $a \subseteq B$. Z toho vyplýva pre každé kardinálne číslo $a \leq |B|$.

Pre kardinálne číslo $2^{|B|}$ máme potom nerovnosť $|B| < 2^{|B|}$ z Cantorovej vety a súčasne $2^{|B|} \leq |B|$ z predchádzajúcej úvahy. Teda $2^{|B|} < 2^{|B|}$, čo je spor. □

Cvičenia

{cantorcvic:ULOCnaC}

Úloha 4.3.1. Ukážte, že $\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}}$.

4.4 Spočítateľné a nespočítateľné množiny

Definícia 4.4.1. Ak pre množinu A platí $|A| \leq \aleph_0$, tak hovoríme, že A je *spočítateľná.* Spočítateľná množina môže byť buď *konečná spočítateľná* množina, ak $|A| < \aleph_0$, alebo *nekonečná spočítateľná,* ak $|A| = \aleph_0$.

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

Opäť platí rovnaká poznámka, ako pri konečných množinách. Ak nespočítateľné množiny definujeme takýmto spôsobom, je to síce to isté ako povedať, že sú to tie množiny, ktoré nie sú spočítateľné, tento fakt ukážeme však až neskôr, s použitím axiómy výberu (pozri poznámku 4.1.11).

Ukážeme, že spočítateľné zjednotenie spočítateľných množín je opäť spočítateľná množina. Dôkaz tohoto faktu súvisí s dôkazom existencie bijekcie medzi $\mathbb{N}\times\mathbb{N}$ a $\mathbb{N}$ (pozri príklad 4.2.15). 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.)

{spoc:VTSPOCZ.

Veta 4.4.2. *Nech I je spočítateľná množina a A_i je spočítateľná množina pre každé $i \in I$. (T.j. $\{A_i; i \in I\}$ je spočítateľný systém spočítateľných množín.) Potom aj množina $\bigcup_{i\in I} A_i$ je spočítateľná.*

Dôkaz. Predpokladáme, že $|I| \leq \aleph_0$ a $|A_i| \leq \aleph_0$. Teda existuje injekcia $f\colon I \to \mathbb{N}$ a pre každé $i \in I$ môžeme vybrať nejakú injekciu $f_i\colon A_i \to \mathbb{N}$. (Na tomto mieste využívame axiómu výberu. Formálnejšie by sme jej použitie vedeli popísať použitím výberovej funkcie na systéme množín $\{B_i; i \in I\}$, kde $B_i = \{j\colon A_i \to \mathbb{N}; j \text{ je injekcia}\}$. Ide o systém neprázdnych množín, teda podľa ekvivalentnej formulácie axiómy výberu – veta 6.1.2(iii) – existuje selektor, čiže funkcia, ktorá z každej množiny B_i vyberie nejaký prvok.)

Pomocou zobrazení f a f_i, $i \in I$, zadefinujeme injekciu z $\bigcup_{i\in I} A_i$ 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. (Také i existuje, lebo $\mathbb{N}$ je dobre usporiadaná množina a $\{f(i); a \in A_i\}$ je neprázdna podmnožina $\mathbb{N}$.) Teraz definujme $g\colon \bigcup_{i\in I} A_i \to \mathbb{N}\times\mathbb{N}$ 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 4.2.15), 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 4.4.3. *Množina $\mathbb{Q}$ všetkých racionálnych čísel je nekonečná spočítateľná, t.j.*

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

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

Súčasne každé racionálne číslo vieme zapísať jednoznačne v tvare $\frac{p}{q}$, kde $p, q \in \mathbb{Z}$, $q > 0$ a čísla p, q sú nesúdeliteľné. Máme teda injekciu z $\mathbb{Q}$ do $\mathbb{N}\times\mathbb{Z}$, 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 4.2.15). 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 4.4.2 (rozmyslite si ako). Výhoda dôkazu, ktorý sme uviedli, je v tom, že nevyužíva axiómu výberu.

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

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

Tejto definícii vyhovujú aj jednoprvkové množiny, ktoré sa zvyknú 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 4.4.4. *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 $i\colon \mathbb{Q} \to \mathbb{N}\times\mathbb{N}$. Na množine $\mathbb{N}\times\mathbb{N}$ máme dobré usporiadanie určené lexikografickým súčinom $(\mathbb{N},\leq)$ a $(\mathbb{N},\leq)$. Z toho dostávame dobré usporiadanie na podmnožine $i[\mathbb{Q}]$, ktoré cez injekciu i vieme preniesť na množinu $\mathbb{Q}$. Namiesto použitia axiómy výberu môžeme zadefinovať q_I takým spôsobom, že je to najmenší prvok množiny $I \cap \mathbb{Q}$ vzhľadom na uvedené dobré usporiadanie množiny $\mathbb{Q}$.

Cvičenia

Úloha 4.4.1. Ukážte, že ak pre kardinálne číslo a platí $a.\aleph_0 = a$, tak $2^a = {\aleph_0}^a$.

{spoccvic:ULONESPOCMINUS

Úloha 4.4.2. 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 $|B| = |B \smallsetminus A|$.)

{spoccvic:ULOKONECPODN}

Úloha 4.4.3. Ukážte, že množina všetkých konečných podmnožín $\mathbb{N}$ je spočítateľná. (Návod: Jedna z možností je ukázať, že množina n-prvkových množín je spočítateľná pre každé prirodzené číslo n a použiť vetu 4.4.2.)

{spoccvic:ULOQdoQNESPOC}

Úloha 4.4.4. Ukážte, že množina všetkých zobrazení z $\mathbb{Q}$ do $\mathbb{Q}$ nie je spočítateľná. (Môžete vyskúšať použiť diagonálnu metódu aj priamy výpočet kardinality tejto množiny.)

Úloha 4.4.5. Postupnosť (a_n) čísel sa volá *takmer stacionárna,* ak $(\exists m \in \mathbb{N})(\forall n \geq m) a_n = a_m$. 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 4.4.6*. 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 4.4.7. 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 4.4.8. 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 4.4.9. Nech A je množina po dvoch disjunktných kruhov v $\mathbb{R}^2$. Ukážte, že A je spočítateľná. Platí to aj pre kružnice?

Úloha 4.4.10. 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 4.4.11. 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.

4.5 Mohutnosť niektorých v praxi sa vyskytujúcich množín

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

Ako prvý výsledok si ukážeme veľmi dôležitý fakt, že kardinalita množiny reálnych čísel je $\mathfrak{c} = 2^{\aleph_0}$. (Stále platí to, čo sme spomínali v poznámke 1.4.1 – reálne čísla sme zatiaľ neskonštruovali v ZFC, až neskôr si ukážeme, ako sa to dá. Budeme pracovať s vedomosťami, ktoré máte o reálnych číslach z nižších ročníkov.)

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

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

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

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

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

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

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

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

{niektore:FIGTAN} (Dostali sme ju vhodným posunutím a preškálovaním funkcie tangens – pozri obrázok 4.5).

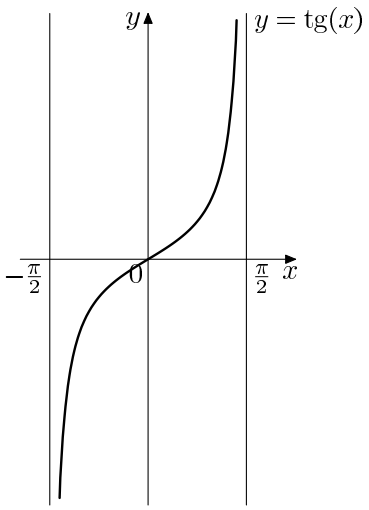
Ak by ste chceli použiť nejakú elementárnejšiu funkciu, môžete skúsiť vhodne upraviť funkcie z obrázkov 4.4 a 4.5, ktoré sú navzájom inverzné.

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

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

Predtým, než sa dostaneme k vlastnému dôkazu, povieme si ešte niečo o *binárnom* (*dyadickom*) zápise reálnych čísel. Je to vlastne rozšírenie zápisu v dvojkovej sústave, ktorý z predmetu Elementárna teória čísel [Č1] 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.



Obr. 4.3: Bijekcia medzi $(-\frac{\pi}{2}, \frac{\pi}{2})$ a $\mathbb{R}$

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

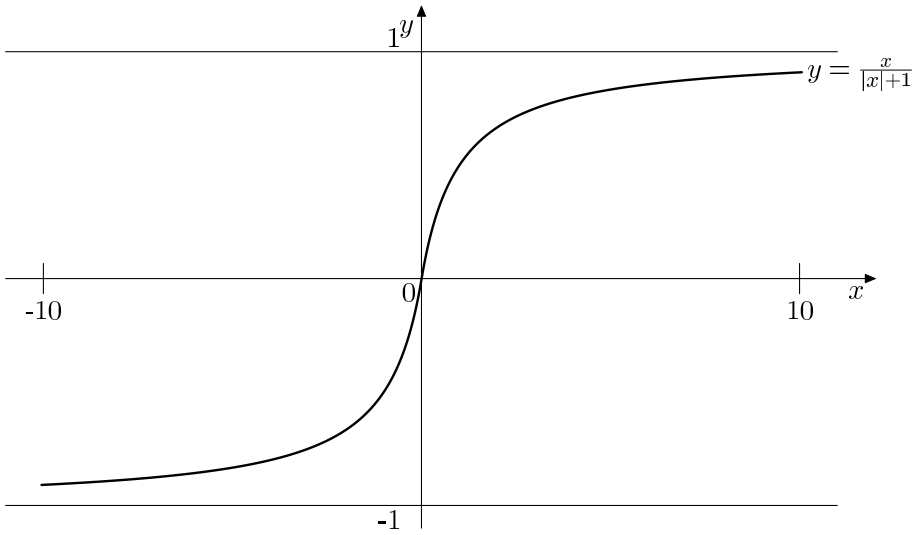
Musíme sa však ešte zamyslieť nad dvoma dôležitými otázkami: Dá sa takto zapísať každé číslo z intervalu $\langle 0, 1\rangle$? Je takýto zápis reálnych čísel jednoznačný?

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



{niektore:ROPINTA}

Obr. 4.4: Bijekcia medzi $\mathbb{R}$ a $(-1, 1)$

$n \in \mathbb{N}$ platí

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

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

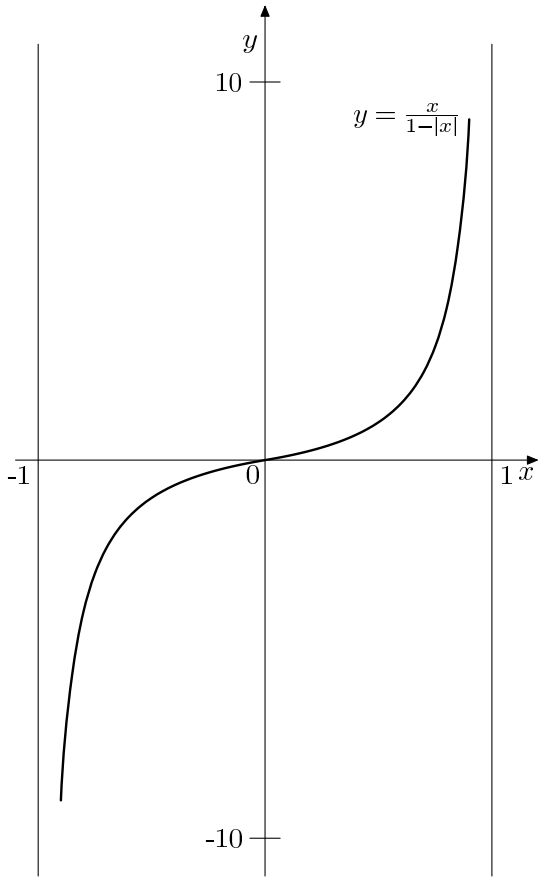
$$r = \sum_{i=0}^{\infty} \frac{a_n}{2^{i+1}}.$$

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

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

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

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



tore:ROPINTB}

Obr. 4.5: Bijekcia medzi $(-1, 1)$ a $\mathbb{R}$

Predpokladajme, že platí

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

pričom postupnosti $(a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty} \in \{0,1\}^{\mathbb{N}}$ sa nerovnajú. Nech n_0 je prvý index, na ktorom sa tieto postupnosti líšia. Bez ujmy na všeobecnosti, nech $a_{n_0} = 1$ a $b_{n_0} = 0$. Označme

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

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

Z toho, čo sme doteraz uviedli, je zrejmé, že existuje bijekcia medzi číslami z intervalu $(0,1\rangle$ a postupnosťami núl a jednotiek s výnimkou tých, ktoré označujú len konečne veľa jednotiek. Postupnostiam z $\{0,1\}^{\mathbb{N}}$ zasa môžeme bijektívne priradiť podmnožiny $\mathbb{N}$ (pozri dôkaz vety 4.2.7). 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 4.4.3), dostávame podľa úlohy 4.4.2, že $|(0,1\rangle| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} = \mathfrak{c}$.

{niektore:TVRKARDR}

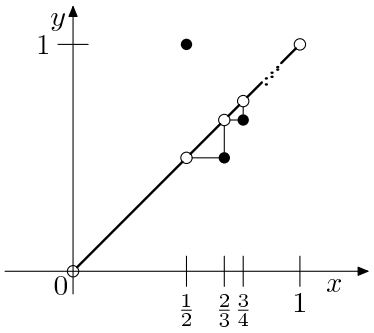
Už sme videli, že $\mathbb{R}$ má rovnakú kardinalitu ako ľubovoľný interval, dostávame teda

Tvrdenie 4.5.1.

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

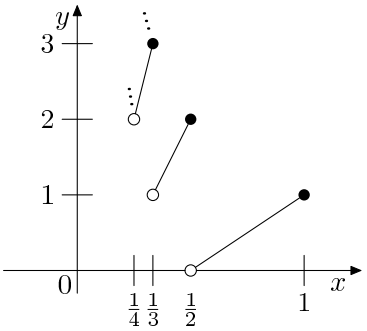
To isté platí aj pre ľubovoľné intervaly tvaru (a,b), $\langle a,b\rangle$, $(a,b\rangle$ či $\langle a,b)$.

V dôkaze sme používali Cantor-Bernsteinovu vetu, môžete sa pokúsiť nájsť priamo bijekcie medzi množinami $(0,1)$, $(0,1\rangle$, $\langle 0,1)$, $\langle 0,1\rangle$ a $\mathbb{R}$. Je veľa spôsobov, ako sa to dá urobiť, ku niektorým možnostiam by vás mohli inšpirovať obrázky 4.6 či 4.7.



{niektore:FIGBIJ0101}

Obr. 4.6: Bijekcia medzi $(0,1)$ a $(0,1\rangle$



niektore:FIGBIJ010INFTY}

Obr. 4.7: Bijekcia medzi $(0,1\rangle$ a $(0,1\rangle$

Príklad 4.5.2. Skúsme sa ešte raz pozrieť na dyadické rozvoje reálnych čísel, ktoré sme použili v dôkaze tvrdenia 4.5.1, 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.

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 4.5.3. *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 4.3.1). Dá sa teda povedať, že nespojitých zobrazení je oveľa viac ako spojitých.

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

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

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

Súčasne vieme ľahko nájsť pre každú podmnožinu $A \subseteq \mathbb{Z}$ spojitú funkciou $f\colon \mathbb{R} \to \mathbb{R}$ takú, že $f|_{\mathbb{Z}} = \chi_A$. (Jednou z možností je lomená čiara.) Z toho máme, že hľadaná kardinalita je aspoň $|\mathcal{P}(\mathbb{Z})| = 2^{\aleph_0} = \mathfrak{c}$. □

{niektore:PRIKLRNESPOC}

Príklad 4.5.4. 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 4.5.4). Postup je veľmi podobný ako v príklade 4.3.2.

Ukážeme, že množina $\langle 0, 1)$ je nespočítateľná. Vieme, že každé číslo z tejto množiny sa dá jediným spôsobom zapísať v tvare $x = \sum_{k=0}^{\infty} \frac{a_k}{10^{k+1}}$ a navyše ak vylúčime konečné rozvoje

(t.j. také, kde sú od istého miesta všetky čísla nulové), tak je tento rozvoj jednoznačný. Desiatkový zápis budeme zapisovať v tvare $0.a_0a_1a_2\ldots$ (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 4.5.1. Ukážte, že kardinalita množiny všetkých iracionálnych čísel je $\mathfrak{c}$.

Úloha 4.5.2. Aká je kardinalita množiny všetkých diferencovateľných zobrazení z $\mathbb{R}$ do $\mathbb{R}$.

Úloha 4.5.3. Aká je kardinalita množiny všetkých divergentných postupností reálnych čísel? Aká je kardinalita množiny všetkých divergentných postupností racionálnych čísel?

4.6 Aplikácie kardinálnych čísel

4.6.1 Existencia transcendentných čísel

Najprv pripomeňme definíciu algebraických a transcendentných čísel.

Definícia 4.6.1. 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 4.6.2. *Množina $\mathbb{A}$ všetkých algebraických čísel je spočítateľná.*

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

Najprv vypočítajme kardinalitu množiny $\mathbb{Z}[x]$ všetkých polynómov s celočíselnými koeficientami. Každý polynóm stupňa n je jednoznačne určený postupnosťou koeficientov $a_n\in$

$\mathbb{Z} \setminus \{0\}$, $a_{n-1}, \ldots, a_0 \in \mathbb{Z}$. 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 4.6.2).

Dôsledok 4.6.3. *Kardinalita množiny $\mathbb{C} \setminus \mathbb{A}$ je $\mathfrak{c}$. Z toho dostávame, že existuje aspoň jedno transcendentné číslo.*

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

4.6.2 Vypočítateľné funkcie

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

Zjednodušene by sme mohli zaviesť pojem vypočítateľnej funkcie takto:

Definícia 4.6.4. Funkcia $f\colon \mathbb{N} \to \mathbb{N}$ sa nazýva *vypočítateľná,* ak existuje *algoritmus* ktorý pre vstup n vráti $f(n)$.

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

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

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

Cvičenia

Úloha 4.6.1. Funkcia $f\colon \mathbb{R} \to \mathbb{R}$ sa nazýva funkciou *prvej Bairovej triedy,* ak existuje postupnosť spojitých funkcií $(f_n\colon \mathbb{R} \to \mathbb{R})_{n\in\mathbb{N}}$, ktorá k nej bodovo konverguje (t.j. pre každé $x \in \mathbb{R}$ číselná postupnosť $f_n(x)$ konverguje k $f(x)$). Aká je kardinalita množiny všetkých funkcií prvej Bairovej triedy? Viete na základe kardinality ukázať, že existuje funkcia, ktorá nie je prvej Bairovej triedy?

{aplikkardcvic:ULOTRANSK

Úloha 4.6.2. Ukážte, že množina všetkých transcendentných čísel má kardinalitu $\mathfrak{c}$.

Kapitola 5

Definícia číselných oborov

Na viacerých miestach sme už spomenuli (pozri poznámku 1.4.1), že množina prirodzených čísel sa dá zadefinovať v rámci systému ZFC. Doteraz sme ju však používali bez jej zavedenie v rámci teórie množín, používali sme tie vlastnosti prirodzených čísel, ktoré poznáte zo strednej školy a z nižších ročníkov. Teraz nastal čas splniť sľub a zaviesť prirodzené čísla.

Čo vlastne znamená, že chceme prirodzené čísla „zadefinovať v teórii množín“? S podobnou – hoci podstatne jednoduchšou – situáciou sme sa stretli pri definovaní usporiadanej dvojice (definícia 2.5.1). Pri jej definícii sme si povedali, aké vlastnosti od usporiadanej dvojice očakávame a potom sa nám podarilo z axióm ZFC ukázať existenciu množiny s týmito vlastnosťami. Takisto sme si povedali, že akákoľvek iná definícia, ktorá by spĺňala tieto základné vlastnosti, by nám vyhovovala rovnako dobre.

Niečo podobné chceme urobiť aj teraz, akurát situácia je o čosi zložitejšia – pretože chceme definovať množinu prirodzených čísel, čo je o dosť zložitejší objekt než usporiadaná dvojica. Preto nasledujúcu časť venujeme tomu, že popíšeme, aké vlastnosti od prirodzených čísel očakávame.

5.1 Peanove axiómy

Peanove axiómy, ktoré si popíšeme v tejto časti, predstavujú obvykle používaný popis vlastností prirodzených čísel.

Pravdepodobne ste zvyknutí uvažovať o prirodzených číslach s ich obvyklým usporiadaním a operáciami $+$ a $\cdot$, ukazuje sa však, že na popis prirodzených čísel stačí popísať vlastnosti význačného prvku 0 a operácie nasledovníka. (Pomocou nich sa dajú potom zadefinovať uvedené operácie i usporiadanie tejto množiny.) Vďaka tomu, že prirodzené čísla popisujeme pomocou menej bohatej štruktúry, máme jednoduchší systém axióm; čo možno považovať za výhodu vždy, keď sme v situácii, že chceme overiť či nejaký systém tieto axiómy spĺňa.

{peano:DEFPEANO}

Definícia 5.1.1. Nech N je množina, 0 je nejaký prvok N a S je zobrazenie definované na N. Hovoríme, že trojica $(N, 0, S)$ spĺňa *Peanove axiómy,* ak platí:

{peano:itPEANO1} (P1) $0 \in N$;

{peano:itPEANO2} (P2) Ak $n \in N$, tak aj $S(n) \in N$.

{peano:itPEANO3} (P3) Ak $n \in N$, tak $S(n) \neq 0$.

{peano:itPEANO4} (P4) Ak $m, n \in N$ a $S(m) = S(n)$, tak $m = n$.

{peano:itPEANO5} (P5) Ak $A \subseteq N$ je podmnožina množiny N taká, že $0 \in A$ a pre každé $n \in A$ aj $S(n) \in A$, tak $A = N$.

S Peanovými axiómami sa môžete stretnúť aj v logike a súvisia tiež s Gödelovými vetami, ktoré sme spomenuli v úvode tohoto textu.

Pokúsime sa ukázať, že tieto vlastnosti naozaj pomerne dobre vystihujú to, čo si predstavujeme pod prirodzenými číslami. Konkrétne si ukážeme, že pomocou nich sa už dá definovať sčitovanie, násobenie a nerovnosť na množine N, ktoré majú vlastnosti, aké by sme od prirodzených čísel očakávali. Drvivá väčšina dôkazov bude založená na vlastnosti (P5), čiže vlastne na tom, že sa dá využívať indukcia.

Základná myšlienka je pomerne jednoduchá – ak chceme ukázať, že nejakú vlastnosť $\varphi(n)$ majú všetky prvky $n \in N$, tak jednoducho označíme $A = \{n \in N; \varphi(n)\}$ a pokúsime sa overiť, že pre túto množinu platia predpoklady z (P5). Ak sa nám to podarí, tak sme vlastne ukázali, že $A = N$, a teda vlastnosť $\varphi(n)$ je splnená pre všetky $n \in N$.

Ukážme si to na nasledujúcom jednoduchom príklade.

{peano:TVRNENULAJENASL}

Tvrdenie 5.1.2. *Nech $(N, 0, S)$ spĺňa Peanove axiómy. Potom pre každé $a \in N$ nastane práve jedna z možností $a = 0$ alebo $a = S(n)$ pre nejaké $n \in N$.*

Dôkaz. Z (P3) vieme, že tieto dve možnosti nemôžu nastať obe súčasne. Stačí teda ukázať, že vždy platí aspoň jedna z nich.

Označme teda $A = \{a \in N; a = 0 \vee (\exists n \in N) a = S(n)\}$.

Očividne $0 \in A$. Súčasne ak $a \in A$, tak $S(a) \in A$. (Stačí zobrať $n = a$.)

Množina A teda spĺňa predpoklady z (P5), z čoho vyplýva $A = N$. Ukázali sme, že pre každé $a \in N$ platí aspoň jedna z uvedených dvoch možností. □

Teraz si dokážeme užitočné tvrdenie, ktoré súčasne formalizuje *definíciu pomocou indukcie.* Dôkaz je síce o niečo zložitejší, výhoda je v tom, že takéto tvrdenie nám potom jednoducho umožní definovať sčitovanie aj násobenie v Peanovej aritmetike (a urobiť ďalšie rekurzívne konštrukcie, keby sme ich chceli definovať.)

{peano:TVRDEFIND}

Tvrdenie 5.1.3. *Nech $(N, 0, S)$ spĺňa Peanove axiómy a X je ľubovoľná množina. Nech $b \in X$ a nech $g\colon N \times X \to X$ je funkcia. Potom existuje* práve jedna *funkcia $f\colon N \to X$ taká, že $f(0) = b$ a pre každé $n \in N$ platí $f(S(n)) = g(n, f(n))$.*

Je to presne to, na čo sme zvyknutí pri definícii matematickou indukciou – predpíšeme ako vyzerá hodnota pre nulu a ako zo známej hodnoty pre n dostaneme hodnotu pre nasledovníka čísla n. Ak poznáme tieto dve veci, objekt, ktorý definujeme, je jednoznačne určený. Formulácia, ktorú sme tu uviedli, nie je zďaleka najvšeobecnejšia možná. Mohli by sme napríklad definovať hodnotu pre $S(n)$ pomocou všetkých doteraz definovaných hodnôt funkcie f.

Dôkaz. Chceme ukázať, že existuje funkcia z N do X s uvedenými vlastnosťami. Začneme tým, že namiesto funkcií sa budeme chvíľu pozerať na relácie medzi N a X, ktoré majú podobné vlastnosti.

Označme ako $\mathcal{M}$ množinu všetkých relácií $R \subseteq N \times X$ takých, že

- $(0, b) \in R$;
- Pre každé $n \in N$ platí: Ak $(n, x) \in R$ tak aj $(S(n), g(n, x)) \in R$.

Cieľom bude nájsť takúto reláciu, ktorá je súčasne funkciou.

Množina $\mathcal{M}$ je neprázdna, lebo relácia $R = N \times X$ spĺňa tieto vlastnosti.

Prienik všetkých relácií z $\mathcal{M}$ tiež patrí do $\mathcal{M}$. Pretože $\mathcal{M} \neq \emptyset$, môžeme zadefinovať

$$f := \bigcap \mathcal{M}.$$

Chceme skontrolovať, či $f \in \mathcal{M}$.

- Pretože $(0, b) \in R$ pre každé $R \in \mathcal{M}$, tak máme aj $(0, b) \in \bigcap \mathcal{M}$.
- Nech $(n, x) \in \bigcap \mathcal{M}$. To znamená, že pre každú reláciu $R \in \mathcal{M}$ platí $(n, x) \in R$. Z toho vyplýva (pretože $R \in \mathcal{M}$), že aj $(S(n), g(n, x)) \in R$ pre každé $M \in \mathcal{R}$. Tým sme ukázali $(S(n), g(n, x)) \in \bigcap \mathcal{M}$.

Ďalšia otázka, ktorú by sme chceli vyriešiť, je *či f je funkcia.* Teda či pre každé $n \in N$ existuje práve jedno $x \in X$ také, že $(n, x) \in f$. Zvlášť sa pozrieme na to, že pre každé $n \in N$ také x existuje a zvlášť na jednoznačnosť.

$D(f) = N$, t.j. pre každé $n \in N$ existuje $x \in X$ také, že $(n, x) \in f$. Označme

$$A = \{n \in N; (\exists x \in X)(n, x) \in f\}.$$

Chceme overiť, či $A = N$.

- $0 \in A$, lebo $(0, b) \in R$ pre každé $R \in \mathcal{M}$, čo znamená, že $(0, b) \in \bigcap \mathcal{M} = f$.
- Nech $n \in A$. To znamená, že existuje $x \in X$ také, že $(n, x) \in R$ pre všetky relácie $R \in \mathcal{M}$. Priamo z definície množiny $\mathcal{M}$ vidíme, že potom aj $(S(n), g(n, x))$ platí do R pre každé $R \in \mathcal{M}$. To znamená, že $(S(n), g(n, x)) \in f$ a $S(n) \in A$.

Z (P5) dostávame, že $A = N$.

f je zobrazenie z N do X. Už vieme, že pre každé $n \in N$ existuje aspoň jedno x také, že $(n, x) \in f$. zostáva nám overiť, že takých x-ov nemôže byť viacero. Označme

$$B = \{n \in N; (\exists! x \in X)(n, x) \in f\}.$$

Opäť chceme ukázať, že $B = N$.

$\boxed{0 \in B}$ Už vieme, že $f \in \mathcal{M}$. Pokúsime sa túto reláciu trochu zmodifikovať tak, že dostaneme znovu reláciu z $\mathcal{M}$. Položme

$$f' = \{(0, b)\} \cup \{(k, x) \in f; k \neq 0\}.$$

Teda v relácii f sme spomedzi dvojíc, ktoré majú na prvej súradnici nulu, nechali iba dvojicu $(0, b)$ a ostatné sme nezmenili. (Teda v f' máme na pre prvú súradnicu rovnú nule iba jedinú možnosť pre druhú súradnicu.) Zrejme platí $f' \subseteq f$.

Ukážme najprv, že $f' \in \mathcal{M}$.

- Platnosť $(0, b) \in f'$ je zjavná z toho, ako sme f' zadefinovali.
- Chceme ešte overiť, že ak $(n, x) \in f'$, tak aj $(S(n), g(n, x)) \in f'$. Ak $(n, x) \in f'$, tak platí aj $(n, x) \in f$. Pretože $f \in \mathcal{R}$, máme potom aj $(S(n), g(n, x)) \in f$. Pretože $S(n) \neq 0$, znamená to aj $(S(n), g(n, x)) \in f'$. (Dvojice, kde je prvá súradnica nenulová, sú v f' práve vtedy, keď sú v f.)

Vieme už teda, že $f' \in \mathcal{M}$ aj $f' \subseteq f$. Pretože $f = \bigcap \mathcal{M}$, tak máme aj $f \subseteq f'$, čo znamená, že $f = f'$.

Súčasne pre $n = 0$ existuje jediné $x = b$ také, že $(n, x) \in f'$. Teda táto vlastnosť je splnená pre f, čím sme skontrolovali, že $0 \in B$.

$\boxed{n \in B \Rightarrow S(n) \in B}$ Predpokladajme teraz, že $n \in B$. To znamená, že existuje jediné $x \in X$ také, že $(n, x) \in f$. Označme takéto x ako x_n. Z toho, že $(n, x_n) \in f$, vieme, že aj $(S(n), g(n, x_n)) \in f$.

Tentokrát položíme

$$f' = \{(S(n), g(n, x_n))\} \cup \{(k, x) \in f; k \neq S(n)\}.$$

Opäť sme f' oproti f zmenili iba „na jednej súradnici“. Takisto je zrejmé, že $f' \subseteq f$.

Poďme overiť, že $f' \in \mathcal{M}$.

- Pretože $(0, b) \in f$, máme aj $(0, b) \in f'$.
- Predpokladajme, že $(j, x) \in f'$. Chceme overiť, že $(S(j), g(j, x)) \in f'$. Rozlíšime dva prípady
  Ak $j \neq n$, tak $(S(j), g(j, x)) \in f$. V tomto prípade to však znamená aj to, že $(S(j), g(j, x)) \in f'$, pretože $S(j) \neq S(n)$.
  Zostáva sa nám pozrieť na prípad $j = n$. Nech $(n, x) \in f'$, čo znamená, že aj $(n, x) \in f$. Ak $(n, x) \in f$, tak máme $x = x_n$. (Lebo x_n je jediný prvok množiny X, ktorý sa vyskytuje v dvojici, kde na prvej súradnici je n.) Pre túto dvojicu platí $(S(n), g(n, x_n)) \in f'$.

Opäť máme $f' \subseteq f$ a z $f \in \mathcal{M}$ dostaneme $f \subseteq f'$ rovnakým argumentom ako minule. (Z toho, že $f = \bigcap \mathcal{M}$.) Teda $f = f'$.

Opäť vidíme, že pre $S(n)$ existuje jediné $x \in X$ také, že $(S(n), x) \in f'$. Pretože $f = f'$, platí to aj pre f, čo znamená, že $S(n) \in B$.

Overili sme, že $0 \in B$ a ak $n \in B$, tak aj $S(n) \in B$. Z (P5) dostaneme, že $B = N$.

Funkcia f spĺňa podmienky z tvrdenia vety. Už sa nám podarilo nejako zostrojiť funkciu f. Treba nám ale ešte skontrolovať, či táto funkcia naozaj spĺňa podmienky uvedené v tvrdení vety.

O funkcii f vieme, že $f \in \mathcal{M}$. To znamená, že $(0, b) \in f$, čo je len iný zápis pre $f(0) = b$.

Takisto ak $f(n) = x$, tak to vlastne znamená $(n, x) \in f$. Pretože $f \in \mathcal{M}$, máme potom aj $(S(n), g(n, x)) \in f$, čo vlastne znamená, že $f(S(n)) = g(n, x) = g(n, f(n))$.

Funkcia f je uvedenými podmienkami určená jednoznačne. Ak $g\colon N \to X$ je nejaká funkcia spĺňajúca podmienky z tvrdenia vety, tak potom $g \in \mathcal{M}$. (Toto sa dá overiť veľmi podobne, ako sme skontrolovali súvis medzi podmienkami z tvrdenia vety a podmienkou $f \in \mathcal{M}$ pre funkciu f v predošlej časti.)

Potom ale máme $f \subseteq g$, pretože $f = \bigcap \mathcal{M}$.

Vezmime si ľubovoľné $n \in N$. Potom platí $(n, f(n)) \in f$. Pretože $f \subseteq g$, máme aj $(n, f(n)) \in g$. Toto je však len iný zápis toho, že $g(n) = f(n)$.

Pretože $g(n) = f(n)$ platí pre každé $n \in N$, tak sa funkcie f a g rovnajú. □

5.1.1 Sčitovanie

{peano:TVRADD}

Tvrdenie 5.1.4. *Nech $(N, 0, S)$ spĺňa Peanove axiómy. Potom existuje práve jedna binárna operácia $+$ na N taká, že pre ľubovoľné $a, n \in N$ platí*
(A1) $a + 0 = a$; {peano:ADD1}
(A2) $a + S(n) = S(a + n)$. {peano:ADD2}

Dôkaz. Na chvíľu sa zaoberajme jedným konkrétnym prvkom $a \in N$. Podľa tvrdenia 5.1.3 existuje práve jedna funkcia $f_a \colon N \to N$ taká, že $f_a(0) = a$ a $f_a(S(n)) = S(f_a(n))$. (Použili sme tvrdenie 5.1.3 pre $X = N$, $b = a$, a $g(n, x) = S(x)$.)

Ak teda definujeme $a+n$ ako $f_a(n)$, tak táto binárna operácia spĺňa uvedené podmienky.

Obrátene, pre každú binárnu operáciu a každé $a \in N$ máme takto určenú funkciu $f_a \colon n \mapsto a+n$, ktorá vyhovuje podmienkam $f_a(0) = a$ a $f_a(S(n)) = S(f_a(n))$. Z jednoznačnosti funkcie f_a pre každé a vyplýva aj jednoznačnosť binárnej operácie $+$. □

Skúsme sa pozrieť na základné vlastnosti operácie $+$, ktorú sme práve definovali. Začnime s komutatívnosťou.

Tvrdenie 5.1.5. *Nech $(N, 0, S)$ spĺňa Peanove axiómy $a +$ je binárna operácia z tvrdenia 5.1.4. Potom pre ľubovoľné $a, b \in N$ platí*

$$0 + a = a \qquad \text{(K1)} \quad \{\texttt{peano:KOM1}\}$$
$$S(0) + a = S(a) \qquad \text{(K2)} \quad \{\texttt{peano:KOM2}\}$$
$$a + S(b) = S(a) + b \qquad \text{(K3)} \quad \{\texttt{peano:KOM3}\}$$
$$a + b = b + a \qquad \text{(K)} \quad \{\texttt{peano:KOM}\}$$

Všetky časti tvrdenia budeme dokazovať pomocou podmienky (P5) – teda v podstate indukciou.

Dôkaz. (K1) Túto prvú vlastnosť overme detailnejšie. Označme ako $A = \{a \in N; 0 + a = a\}$. Chceme ukázať, že $A = N$ a na základe (P5) na to stačí overiť, že $0 \in A$ a platí implikácia $a \in A \Rightarrow S(a) \in A$.

Skutočne máme $0 \in A$, lebo $0 + 0 = 0$ podľa (A1).

Takisto ak $a \in A$, tak platí $0 + S(a) \overset{(A2)}{=} S(0 + a) \overset{IP}{=} S(a)$. (Na mieste označenom ako IP sme využili to, že $a \in A$ – indukčný predpoklad.) □

Princíp ostatných dôkazov v tejto kapitole bude analogický – označíme si ako A množinu tých prvkov, ktoré spĺňajú dokazovanú vlastnosť a overíme, že táto množina spĺňa (P5). Kvôli stručnosti budeme vynechávať definíciu množiny A a overíme len jednotlivé časti podmienky (P5). (T.j. že dokazovanú vlastnosť má 0 a ak ju má a, tak ju má aj $S(a)$.)

Dôkaz. (K2) 1° Pre $a = 0$ máme $S(0) + 0 \overset{(A1)}{=} S(0)$.

2° Ak $S(0) + a = S(a)$, tak platí aj

$$S(0) + S(a) \overset{(A2)}{=} S(S(0) + a) \overset{IP}{=} S(S(a)).$$

(V skutočnosti sme rovnosť $S(0) + 0 = S(0)$ v indukčnom kroku nepoužili, čiže v tomto prípade nešlo o dôkaz indukciou ale o rozdelenie na dva možné prípady, že dané číslo je 0 alebo nasledovník.)

(K3) Chceme ukázať, že každé $b \in N$ má vlastnosť $(\forall a \in N) a + S(b) = S(a) + b$.

1° Ak $b = 0$, tak platí $a + S(0) \overset{(A2)}{=} S(a + 0) \overset{(A1)}{=} S(a) \overset{(A1)}{=} S(a) + 0$.

2° Nech $a + S(b) = S(a) + b$ platí pre ľubovoľné $a \in N$. Potom máme

$$a + S(S(b)) \overset{(A2)}{=} S(a + S(b)) \overset{IP}{=} S(S(a) + b) \overset{(A2)}{=} S(a) + S(b).$$

(K) Chceme ukázať, že každé $a \in N$ spĺňa podmienku $(\forall b \in A)a + b = b + a$.

1° Ak $a = 0$, tak $0 + b \overset{(K1)}{=} b$ a súčasne $b + 0 \overset{(A1)}{=} b$.

2° Nech platí $a + b = b + a$ (pre ľubovoľné b). Potom

$$S(a) + b \overset{(K3)}{=} a + S(b) \overset{IP}{=} S(b) + a \overset{(K3)}{=} b + S(a)$$

□

{peano:TVRKRAT} Ďalej overíme, že pre takto definované sčitovanie platí asociatívnosť a zákony o krátení.

Tvrdenie 5.1.6. *Nech $(N, 0, S)$ spĺňa Peanove axiómy $a +$ je binárna operácia z tvrdenia 5.1.4. Potom pre ľubovoľné $a, b, c \in N$ platí*

{peano:ASOC} $$(a + b) + c = a + (b + c) \tag{A}$$

{peano:KRAT} $$b + a = c + a \Rightarrow b = c \tag{C}$$

Dôkaz. (A) Chceme overiť vlastnosť $(\forall a, b \in N)(a + b) + c = a + (b + c)$.

1° Ak $c = 0$, tak $(a + b) + 0 = a + b$ a súčasne $a + (b + 0) = a + b$ (v oboch prípadoch sme použili (A1)).

2° Predpokladajme platnosť $(a + b) + c = a + (b + c)$. Pre $S(c)$ dostaneme

$$(a + b) + S(c) \overset{(A1)}{=} S((a + b) + c) \overset{IP}{=} S(a + (b + c)) \overset{(A2)}{=} a + S(b + c) \overset{(A2)}{=} a + (b + S(c)).$$

(C) Chceme overiť vlastnosť $(\forall b, c \in N)b + a = c + a \Rightarrow b = c$.

1° Ak $a = 0$, tak $b + 0 = b$ a $c + 0 = c$ podľa (A1). Teda v tomto prípade tvrdenie platí.

2° Predpokladajme, že platí implikácia $b + a = c + a \Rightarrow b = c$. Potom z

$$b + S(a) = c + S(a)$$

dostaneme na základe (A2)

$$S(b + a) = S(c + a).$$

Z (P4) potom vyplýva $b + a = c + a$ a z indukčného predpokladu máme

$$b = c.$$

□

{peano:LMSUCNULA} Ešte pridajme jedno jednoduché pozorovanie, ktoré sa nám bude hodiť vo viacerých ďalších dôkazoch:

Lema 5.1.7. *Nech $(N, 0, S)$ spĺňa Peanove axiómy $a +$ je binárna operácia z tvrdenia 5.1.4. Potom pre ľubovoľné $a, b \in N$ platí*

$$a + b = 0 \qquad \Rightarrow \qquad a = 0 \wedge b = 0$$

Dôkaz. Predpokladajme, že by platilo $b \neq 0$. To znamená, že $b = S(b')$ pre nejaké $b' \in N$ (tvrdenie 5.1.2). Dostaneme

$$a + b = a + S(b') = S(a + b').$$

Podľa (P3) potom $a + b$ nemôže byť 0. Dostávame teda spor.

Zatiaľ sme ukázali, že z $a + b = 0$ vyplýva $b = 0$.

Pretože sme už dokázali komutatívnosť sčitovania (K), platí aj $a = 0$. □

5.1.2 Nerovnosť

{peano:INEQDEF}

Definícia 5.1.8. Nech $(N, 0, S)$ spĺňa Peanove axiómy a $+$ je binárna operácia z tvrdenia 5.1.4. Potom definujeme reláciu $\leq$ na množine N ako

$$a \leq b \Leftrightarrow (\exists c \in N) b = a + c. \tag{I}$$

V nasledujúcom tvrdení ukážeme, že relácia $\leq$ je lineárne usporiadanie na množine N.

{peano:TVRLUM}

Tvrdenie 5.1.9. *pre ľubovoľné $a, b, c \in N$ platí*

$$a \leq a \tag{IR}$$ {peano:REFLEX}

$$a \leq b \wedge b \leq a \Rightarrow a = b \tag{IA}$$ {peano:ANTISYM}

$$a \leq b \wedge b \leq c \Rightarrow a \leq c \tag{IT}$$ {peano:TRANZ}

$$0 \leq a \tag{5.1}$$ {peano:MINIM}

$$a \leq 0 \Rightarrow a = 0 \tag{5.2}$$ {peano:MINIM2}

$$a \leq S(a) \tag{5.3}$$ {peano:INEQSA}

$$a \leq b \Leftrightarrow S(a) \leq S(b) \tag{5.4}$$ {peano:INEQNASLEQUIV}

$$a \leq S(b) \Rightarrow a \leq b \vee a = S(b) \tag{5.5}$$ {peano:INEQNASL2}

$$a \leq b \vee S(b) \leq a \tag{5.6}$$ {peano:POROV2}

$$a \leq b \vee b \leq a \tag{IL}$$ {peano:POROV}

Najdôležitejšie výsledky predchádzajúceho tvrdenia môžeme stručne zhrnúť v konštatovaní, že:

{peano:DOSLUM}

Dôsledok 5.1.10. *Množina $(N, \leq)$ je lineárne usporiadaná množina.*

Dôkaz. Stačí si všimnúť podmienky (IR), (IA), (IT) a (IL) v tvrdení 5.1.9. □

Dôkaz tvrdenia 5.1.9. (IR) Podľa (A1) platí $a + 0 = a$, čo znamená, že $a \leq a$.

(IA) Nech platí $a \leq b$ a $b \leq a$. Teda existujú $c, d \in N$ také, že $a + c = b$ a $b + d = a$. Dostávame teda

$$a + (c + d) \overset{(A)}{=} (a + c) + d = a = a + 0.$$

Z (C) potom vyplýva $c + d = 0$. Potom musí platiť $c = d = 0$ podľa lemy 5.1.7. Dostávame teda, že $b = a + 0 = a$.

(IT) Úloha 5.1.5.

(5.1): Pre ľubovoľné $a \in N$ máme $0 + a = a$, čo znamená $0 \leq a$.

(5.2): Ak $a \leq 0$, tak máme $a + b = 0$ pre nejaké $b \in N$. Podľa lemy 5.1.7 potom platí $a = 0$.

(5.3): $S(a) \overset{(A1)}{=} S(a + 0) \overset{(A2)}{=} a + S(0)$

(5.4): $\boxed{\Rightarrow}$ Ak $b = a + c$ pre nejaké $c \in N$, tak $S(b) = S(a + c) \overset{(A2)}{=} a + S(c) \overset{(K3)}{=} S(a) + c$.

$\boxed{\Leftarrow}$ Podobným spôsobom z $S(b) = S(a) + c$ dostaneme: $S(b) = S(a) + c \overset{(K3)}{=} a + S(c) \overset{(A2)}{=} S(a + c)$. Na základe (P4) z rovnosti $S(b) = S(a + c)$ vyplýva $b = a + c$.

(5.5): Ak $a \leq S(b)$, znamená to, že $S(b) = a + c$ pre nejaké $c \in N$. Podľa tvrdenia 5.1.2 platí buď $c = 0$ alebo $c = S(d)$, pre nejaké $d \in N$.

V prípade, že $c = 0$ máme $a = S(b)$, čo znamená, že dokazované tvrdenie platí.

Ak $c = S(d)$, tak

$$S(b) = a + S(d) \overset{(A2)}{=} S(a + d)$$

a z (5.4) potom dostaneme $b = a + d$, čo znamená, že $a \leq b$. Teda dokazované tvrdenie platí i v tomto prípade.

(5.6): Všimnime si najprv, že uvedená vlastnosť platí pre $b = 0$. Ak $a = 0$, tak máme $0 \leq 0$. Ak $a \neq 0$, tak $a = S(a')$ a z $a' \geq 0$ dostaneme na základe (5.4) $a = S(a') \geq S(0)$.

Vo zvyšku dôkazu tejto vlastnosti budeme teda predpokladať, že máme nejaké (pevne zvolené) $b \neq 0$. Opäť využijeme, že potom $b = S(b')$ pre nejaké $b' \in N$ (podľa tvrdenia 5.1.2).

Označme $A = \{a \in N; a \leq b \vee S(b) \leq a\}$. Chceme ukázať, že $A = N$.

Evidentne $0 \in A$.

Teraz predpokladajme, že $a \in A$. Teda pre a platí niektorá z možností $a \leq b$ resp. $S(b) \leq a$.

Ak $S(b) \leq a$, tak z $a \leq S(a)$ a tranzitívnosti (IT) dostávame $S(b) \leq S(a)$. Teda $S(a) \in A$.

Druhá možnosť je, že $a \leq b = S(b')$. Podľa (5.5) potom platí $a \leq b'$ alebo $a = S(b')$. Na každú z týchto možností sa pozrime zvlášť.

Ak $a \leq b'$, tak podľa (5.4) aj $S(a) \leq S(b')$, čo je len iným spôsobom zapísaná podmienka $S(a) \leq b$. V tomto prípade teda $S(a) \in A$.

Ak $a = S(b') = b$, tak aj $S(a) = S(b)$. Znamená to, že $S(b) \leq S(a)$, a teda aj v tomto prípade $S(a) \in A$.

Overili sme, že množina A spĺňa predpoklady (P5), čo znamená, že $A = N$.

(IL): Podľa (5.6) vieme, že buď platí $a \leq b$ alebo $S(b) \leq a$. V druhom prípade z $b \leq S(b)$ a $S(b) \leq a$ na základe tranzitívnosti dostaneme $b \leq a$. □

Už teda vieme, že $(N, \leq)$ je lineárne usporiadaná množina. Pomerne ľahko už teraz vieme ukázať, že ide dokonca o dobré usporiadanie.

Tvrdenie 5.1.11. *Množina $(N, \leq)$ je dobre usporiadaná.*

Dôkaz. Nech $A \subseteq N$. Predpokladajme, že A nemá najmenší prvok. (Naším cieľom je ukázať, že potom $A = \emptyset$.)

Označme

$$B = \{n \in N; (\forall x \in N) x \leq n \Rightarrow x \notin A\}.$$

Ukážeme, že $B = N$.

1° Ak $x \leq 0$, tak $x = 0$ podľa (5.2). Z (5.1) potom ale vidíme, že ak by platilo $x = 0 \in A$, tak x by bol najmenší prvok množiny A.

2° Predpokladajme, že $n \in B$, t.j. platí $x \leq n \Rightarrow x \notin A$. Chceme ukázať, že aj $S(n) \in B$.

Ak $x \leq S(n)$, tak podľa (5.5) máme $x \leq n$ alebo $x = S(n)$.

Ak $x \leq n$, tak $x \notin A$ (lebo $n \in A$).

Zostáva nám rozmyslieť si prípad $x = S(n)$. Ak by prvok $S(n)$ patril do A, bol by to najmenší prvok množiny A. Pre každé $a \in A$ totiž podľa (5.6) platí $a \leq n$ alebo $S(n) \leq a$. Prvá z týchto dvoch možností však nemôže nastať (opäť vďaka tomu, že $n \in A$.)

Dokázali sme teda, že $B = N$. Z toho už vyplýva, že $A = \emptyset$. (Ak by nejaký prvok n patril do A, tak pre $x = n$ máme $x \leq n$ a súčasne $x \in A$, čo by znamenalo, že $n \notin B$.) □

Keď už sme pomocou Peanových axióm zadefinovali sčitovanie a nerovnosť a ukázali niektoré ich základné vlastnosti, oplatí sa azda aj pozrieť na niektoré vlastnosti, ktoré sa týkajú sčitovania i nerovnosti.

{peano:TVRINEQADD}

Tvrdenie 5.1.12. *Nech $(N, 0, S)$ spĺňa Peanove axiómy. Pre ľubovoľné $a, b, c \in N$ platí*

{peano:INEQADD}

$$a \leq b \qquad \Leftrightarrow \qquad c + a \leq c + b \tag{M}$$

Dôkaz. Ak $a \leq b$, tak existuje $d \in N$ také, že $a + d = b$. Potom

$$(c + a) + d \overset{(A)}{=} c + (a + d) = c + b,$$

čo znamená, že $c + a \leq c + b$.

Obrátene, ze $c + a \leq c + d$ máme existenciu takého $d \in N$, že $(c + a) + d = c + b$, čo nám na základe asociatívnosti (A) dá

$$c + (a + d) = c + b$$

a na základe platnosti zákona o krátení (C) dostaneme

$$a + d = b,$$

čo je, podľa definície, to isté ako $a \leq b$. □

Keďže už vieme, že $S(0) + n = S(n)$, tak z (M) dostaneme ako špeciálny prípad

$$a \leq b \qquad \Leftrightarrow \qquad S(a) \leq S(b).$$

Túto vlastnosť sme už predtým dokázali v (5.4).

Tiež sa možno oplatí uvedomiť, že keď máme lineárne usporiadanie $\leq$ na množine N, tak súčasne máme aj jemu zodpovedajúce ostré lineárne usporiadanie $<$ (pozri definíciu 3.3.8 a korešpondenciu medzi ostrým a neostrým usporiadaním uvedenú v dôsledku 3.3.11). Keďže toto ostré usporiadanie zodpovedá lineárnemu usporiadaniu, má vlastnosť trichotómie (pozri poznámku 3.3.12).

Aj pre neostré usporiadanie platí monotónnosť:

{peano:DOSINEQADD}

Dôsledok 5.1.13. *Nech $(N, 0, S)$ spĺňa Peanove axiómy. Pre ľubovoľné $a, b, c \in N$ platí*

$$a < b \qquad \Leftrightarrow \qquad c + a < c + b \tag{M'}$$

{peano:INEQADD2}

Dôkaz. Ak platí $a < b$, znamená to, že $a \leq b$ a súčasne $a \neq b$. Z (M) máme $c + a \leq c + b$. Platnosť krátenia (C) pre operáciu $+$ môžeme ekvivalentne preformulovať ako $a \neq b \Rightarrow c + a \neq c + b$. Spolu teda dostávame $c + a < c + b$.

Obrátene, ak $c + a < c + b$, tak z (M) máme $a \leq b$. Súčasne z $c + a \neq b + a$ vyplýva $a \neq b$, lebo $+$ je binárna operácia na N. Spolu teda máme $a < b$. □

Z tvrdenia 5.1.12 dostaneme, že nerovnosti môžeme sčitovať.

{peano:DOSINEQSCIT}

Dôsledok 5.1.14. *Nech $(N, 0, S)$ spĺňa Peanove axiómy a nech $a_1, a_2, b_1, b_2 \in N$. Ak $a_1 \leq a_2$, $b_1 \leq b_2$, tak $a_1 + b_1 \leq a_2 + b_2$.*

Dôkaz. Viacnásobným použitím tvrdenia 5.1.12 (a komutatívnosti sčitovania) dostaneme:

$$a_1 + b_1 \leq a_1 + b_2 \leq a_2 + b_2.$$

Z už dokázanej tranzitívnosti (IT) potom máme

$$a_1 + b_1 \leq a_2 + b_2.$$

□

Podobné tvrdenie platí pre súčet ostrej a neostrej nerovnosti.

{peano:DOSINE

Dôsledok 5.1.15. *Nech $(N, 0, S)$ spĺňa Peanove axiómy a nech $a_1, a_2, b_1, b_2 \in N$. Ak $a_1 < a_2$, $b_1 \leq b_2$, tak $a_1 + b_1 < a_2 + b_2$.*

Dôkaz. Najprv použijeme dôsledok 5.1.13 a dostaneme

$$a_1 + b_1 < a_2 + b_1.$$

Súčasne máme

$$a_2 + b_1 \leq a_2 + b_2$$

na základe tvrdenia 5.1.12. Tieto dve nerovnosti nám spolu dajú

$$a_1 + b_1 < a_2 + b_2.$$

□

5.1.3 Násobenie

Podobne ako sčitovanie, dá sa indukciou definovať aj násobenie.

{peano:TVRMULT}

Tvrdenie 5.1.16. *Nech $(N, 0, S)$ spĺňa Peanove axiómy. Potom existuje práve jedna binárna operácia $\cdot$ na N taká, že pre ľubovoľné $a, b \in N$ platí*
(M1) $a \cdot 0 = 0$;
(M2) $a \cdot S(b) = a \cdot b + a$.

{peano:MULT1}
{peano:MULT2}

Dôkaz. S drobnými zmenami môžeme zopakovať dôkaz tvrdenia 5.1.4. □

Základné vlastnosti násobenia sa overia podobne ako pri sčitovaní.

{peano:TVRMULTKOM}

Tvrdenie 5.1.17. *Nech $(N, 0, S)$ spĺňa Peanove axiómy $a \cdot$ je operácia z tvrdenia 5.1.16. Potom pre ľubovoľné $a, b, c \in N$ platí*
(i) $a \cdot S(0) = a$
(ii) $0 \cdot a = 0$
(iii) $S(b) \cdot a = b \cdot a + a$
(iv) $a \cdot b = b \cdot a$

{peano:itMULTS0}
{peano:itMULTKOM0}
{peano:itMULTKOM1}
{peano:itMULTKOM}

Dôkaz. (i) $a \cdot S(0) \overset{(M2)}{=} a \cdot 0 + a \overset{(M1)}{=} 0 + a \overset{(K1)}{=} a$.
(ii) 1° Ak $a = 0$, tak z (M1) máme $0 \cdot 0 = 0$.
2° Prepokladajme, že $0 \cdot a = 0$. Potom aj $0 \cdot S(a) \overset{(M2)}{=} 0 \cdot a + 0 = 0 \cdot a = 0$.
(iii) Platnosť $S(b) \cdot a = b \cdot a + a$ pre ľubovoľné b ukážeme indukciou na a:
1° $S(b) \cdot 0 = 0 = b \cdot 0 = b \cdot 0 + 0$.
2° Predpokladajme, že $S(b) \cdot a = b \cdot a + a$. Potom

$$S(b) \cdot S(a) \overset{(M2)}{=} S(b) \cdot a + S(b) \overset{IP}{=} b \cdot a + a + S(b) \overset{(K3)}{=} b \cdot a + S(a) + b \overset{(K)}{=} b \cdot a + b + S(a) \overset{(M2)}{=} b \cdot S(a) + S(a).$$

(V predošlom odvodení sme vynechávali zátvorky, čo znamená, že sme tam súčasne využívali asociatívnosť sčitovania.)
(iv) Indukciou na b.
1° Pre $b = 0$ máme $a \cdot 0 = 0$ a podľa (ii) $0 \cdot a = 0$.
2° Predpokladajme platnosť $a \cdot b = b \cdot a$. Potom

$$a \cdot S(b) \overset{(M2)}{=} a \cdot b + a \overset{IP}{=} b \cdot a + a \overset{(iii)}{=} S(b) \cdot a.$$

□

Máme teda dokázanú komutatívnosť násobenia. Pred dôkazom asociatívnosti sa nám hodí ukázať najprv distributívnosť.

:MULTTVRASOC}

Tvrdenie 5.1.18. *Nech $(N, 0, S)$ spĺňa Peanove axiómy $a \cdot$ je operácia z tvrdenia 5.1.16. Potom pre ľubovoľné $a, b, c \in N$ platí*

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{(D)} \quad \{\texttt{peano:itDISTRIB}\}$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \text{(MA)} \quad \{\texttt{peano:itMULTASOC}\}$$

Proof. (D) 1° Pre $c = 0$ platí $a \cdot (b + 0) = a \cdot b$ a súčasne $a \cdot b + a \cdot c = a \cdot b + 0 = a \cdot b$.

2° Predpokladajme, že $a \cdot (b + c) = a \cdot b + a \cdot c$. Potom máme

$$a \cdot (b + S(c)) \overset{(A2)}{=} a \cdot S(b + c) \overset{(M2)}{=} a \cdot (b + c) + a$$

$$a \cdot b + a \cdot S(c) \overset{(M2)}{=} a \cdot b + (a \cdot c + a) \overset{(A)}{=} (a \cdot b + a \cdot c) + a$$

Výrazy na pravých stranách sa podľa indukčného predpokladu rovnajú.

(MA) 1° Pre $c = 0$ máme $a \cdot (b \cdot 0) = a \cdot 0 = 0$ aj $(a \cdot b) \cdot 0 = a \cdot 0$ podľa (M2).

2° Predpokladáme, že $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Potom

$$(a \cdot b) \cdot S(c) \overset{(M2)}{=} (a \cdot b) \cdot c + a \cdot b$$

$$a \cdot (b \cdot S(c)) \overset{(M2)}{=} a \cdot (b \cdot c + b) \overset{(D)}{=} a \cdot (b \cdot c) + a \cdot b$$

Podľa indukčného predpokladu sa výrazy na pravých stranách rovnajú. □

Pozrime sa teraz na to, ako sa násobenie správa k nerovnostiam.

{peano:TVRINEQMULT}

Tvrdenie 5.1.19. *Nech $(N, 0, S)$ spĺňa Peanove axiómy. Pre ľubovoľné $a, b, c \in N$ platí*

$$a \leq b \qquad \Rightarrow \qquad c \cdot a \leq c \cdot b \qquad (5.7) \quad \{\texttt{peano:INEQMULT}\}$$

Dôkaz. Ak $b = a + b'$, tak

$$c \cdot b = c \cdot (a + b') \overset{(D)}{=} c \cdot a + c \cdot b',$$

čo znamená, že $c \cdot a \leq c \cdot b$. Dostali sme platnosť (M). □

{peano:TVRMULTKRAT}

Tvrdenie 5.1.20. *Nech $(N, 0, S)$ spĺňa Peanove axiómy $a \cdot$ je operácia z tvrdenia 5.1.16. Potom pre ľubovoľné $a, b, c \in N$ platí*

$$c \neq 0 \wedge a \cdot c = b \cdot c \Rightarrow a = b \qquad (5.8) \quad \{\texttt{peano:itMULTKRAT}\}$$

Dôkaz. Indukciou na d dokážeme $a \cdot S(d) = b \cdot S(d) \Rightarrow a = b$. Toto je ekvivalentné formuláciou uvedenou v tvrdení, pretože podľa tvrdenia 5.1.2 je každé $c \neq 0$ tvaru $c = S(d)$ pre nejaké $d \in N$.

1° Pre $d = 0$ máme $a \cdot S(0) \overset{(i)}{=} a$, $b \cdot S(0) \overset{(i)}{=} b$. Teda z $a \cdot S(0) = b \cdot S(0)$ skutočne vyplýva $a = b$.

2° Nech $a \cdot S(S(d)) = b \cdot S(S(d))$. Z (M2) dostaneme

$$a \cdot S(d) + a = b \cdot S(d) + b.$$

Na základe trichotómie relácie $<$ vieme, že nastane práve jedna z možností $a < b$, $a = b$, $a > b$.

Predpokladajme najprv $a < b$. Potom z (5.7) dostaneme

$$a \cdot S(d) \leq b \cdot S(d).$$

Na základe dôsledku 5.1.15 máme potom aj

$$a \cdot S(d) + a < b \cdot S(d) + b.$$

Toto je v spore s predpokladom $a \cdot S(d) + a = b \cdot S(d) + b$, čím sme ukázali, že možnosť $a < b$ nemôže nastať.

Podobným spôsobom sa ukáže, že nenastane ani možnosť $a > b$. Musí teda platiť $a = b$ □

Keď už máme dokázaný zákon o krátení aj pre násobenie, tak sa nám o niečo jednoduchšie bude dokazovať ako sa správa násobenie k ostrej nerovnosti a tiež opačná implikácia k implikácii z tvrdenia 5.1.19.

Tvrdenie 5.1.21. *Nech $(N, 0, S)$ spĺňa Peanove axiómy $a \cdot$ je operácia z tvrdenia 5.1.16 a nech $a, b, c \in N$. Potom platí:*

{peano:INEQMULTOST}
$$c \neq 0 \wedge a < b \quad \Rightarrow \quad c \cdot a < c \cdot b \tag{5.9}$$

{peano:INEQMULTOST2}
$$c \neq 0 \wedge c \cdot a < c \cdot b \quad \Rightarrow \quad a < b \tag{5.10}$$

{peano:INEQMULT2}
$$c \neq 0 \wedge c \cdot a \leq c \cdot b \quad \Rightarrow \quad a \leq b \tag{5.11}$$

Dôkaz. (5.9) Ak $a < b$, tak z (5.7) máme $c \cdot a \leq c \cdot b$. Súčasne ak by platilo $c \cdot a = c \cdot b$ tak z (5.8) dostaneme $a = b$, čo je v spore s $a < b$. Teda musí platiť ostrá nerovnosť $c \cdot a < c \cdot b$.

(5.10) Opäť využijeme, že na základe trichotómie nastane práve jedna z možností $a < b$, $a = b$, $a > b$.

V prípade $a = b$ by platilo $c \cdot a = c \cdot b$. V prípade $a > b$ by podľa (5.9) platí $c \cdot a > c \cdot b$. Obe tieto možnosti teda vedú k sporu. Musí platiť zostávajúca možnosť $a < b$.

(5.11) Dôkaz môžeme urobiť rozobratím jednotlivých prípadov ako v predchádzajúcej časti. □

5.1.4 Umocňovanie

Poznámka 5.1.22. Pod pojmom *Peanova aritmetika* sa obvykle rozumie systém vyhovujúci Peanovým axiómam spolu s operáciami sčitovania a násobenia. Viac-menej na precvičenie práce s Peanovými axiómami si ukážeme, ako sa dá zadefinovať umocňovanie a odvodiť jeho základné vlastnosti.

{peano:TVREXP}
Tvrdenie 5.1.23. *Nech $(N, 0, S)$ je spĺňa Peanove axiómy. Potom existuje práve jedna binárna operácia* exp *na množine N taká, že pre ľubovoľné $a, n \in N$ platí*

$$\exp(a, 0) = S(0)$$
$$\exp(a, S(n)) = \exp(a, n) \cdot a$$

Namiesto označenia $\exp(a, n)$ budeme používať – tak ako ste zvyknutí – označenie a^n. Potom definíciu umocňovania môžeme zapísať takto:

$$a^0 = S(0)$$
$$a^{S(n)} = a^n \cdot a$$

Dôkaz. Opäť môžeme zopakovať podobný dôkaz ako v tvrdení 5.1.4. □

Tvrdenie 5.1.24. *Nech $(N, 0, S)$ je spĺňa Peanove axiómy. Potom pre ľubovoľné $a, b, c \in N$ platí*

{peano:itEXPS0}
{peano:itEXPADD}
{peano:itEXPMULT}

(i) $a^{S(0)} = a$;
(ii) $a^{b+c} = a^c \cdot a^c$;
(iii) $a^{b \cdot c} = (a^b)^c$; {peano:INEQEXP1}
(iv) $a \leq b \Rightarrow a^c \leq b^c$; {peano:INEQEXP0}
(v) $c \neq 0 \Rightarrow c^b \geq S(0)$; {peano:INEQEXP2}
(vi) $c \neq 0 \wedge a \leq b \Rightarrow c^a \leq c^b$.

Dôkaz. (i) Úloha 5.1.6.
(ii) Úloha 5.1.7.
(iii) Úloha 5.1.8.
(iv), (v) a (vi): Úloha 5.1.9. □

Cvičenia

Úloha 5.1.1. Nech trojica $(N, 0, S)$ spĺňa Peanove axiómy a nech $N' = \{S(n); n \in N\}$. Spĺňa aj $(N', S(0), S|_{N'})$ Peanove axiómy? Svoju odpoveď zdôvodnite!

Úloha 5.1.2. Nájdite príklad trojice $(N, 0, S)$, pre ktorú neplatí (P3), ale spĺňa všetky ostatné Peanove axiómy.

Úloha 5.1.3. Nájdite príklad trojice $(N, 0, S)$, pre ktorú neplatí (P4), ale spĺňa všetky ostatné Peanove axiómy.

Úloha 5.1.4. Nájdite príklad trojice $(N, 0, S)$, pre ktorú neplatí (P5), ale spĺňa všetky ostatné Peanove axiómy.

{peanocvic:ULOTRANZ}

Úloha 5.1.5. Dokážte platnosť (IT), t.j. že pre nerovnosť definovanú v definícii (5.1.8) vyplýva z Peanových axióm tranzitívnosť.

Vo všetkých úlohách týkajúcich sa umocňovania predpokladáme, že $(N, 0, S)$ spĺňa Peanove axiómy a a^b je operácia z tvrdenia 5.1.23, t.j. vyhovuje podmienkam (5.1.4) a (5.1.4). Pri riešení jednotlivých úloh môžete používať veci už dokázané v predchádzajúcich úlohách.

{peanocvic:ULOEXPS0}

Úloha 5.1.6. Dokážte, že pre ľubovoľné $a \in N$ platí $a^{S(0)} = a$.

{peanocvic:ULOEXPADD}

Úloha 5.1.7. Dokážte, že pre ľubovoľné $a \in N$ platí $a^{b+c} = a^c \cdot a^c$.

{peanocvic:ULOEXPMULT}

Úloha 5.1.8. Dokážte, že pre ľubovoľné $a \in N$ platí $a^{b \cdot c} = (a^b)^c$.

{peanocvic:ULOINEQ}

Úloha 5.1.9. Dokážte, že pre ľubovoľné $a \in N$ platí
(i) $a \leq b \Rightarrow a^c \leq b^c$;
(ii) $c \neq 0 \Rightarrow c^b \geq S(0)$;
(iii) $c \neq 0 \wedge a \leq b \Rightarrow c^a \leq c^b$.

5.2 Prirodzené čísla

{priro:SECTPRIRO}

V tejto časti chceme zadefinovať v ZFC množinu prirodzených čísel a tiež usporiadanie, sčitovanie a násobenie na tejto množine. Súčasne si ukážeme nejaké základné vlastnosti, ktoré táto množina má. (Medziiným aj to, že spĺňa Peanove axiómy.)

Iný text, kde si môžete prečítať niečo o konštrukcii prirodzených čísel, je napríklad [Č2].

Pri konštrukcii prirodzených čísel využijeme axiómu nekonečnej množiny.

Axióma X (Axióma nekonečnej množiny)**.**

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

Definícia 5.2.1. Množinu, ktorá spĺňa podmienku

$$\emptyset \in A \wedge (\forall x)(x \in A \Rightarrow x \cup \{x\} \in A)$$

budeme nazývať *induktívna množina.*

Axióma nekonečnej množiny teda vlastne postuluje existenciu aspoň jednej induktívnej množiny. Množinu prirodzených čísel potom zadefinujeme ako najmenšiu induktívnu množinu. (Rovnaký prístup je použitý napríklad v [BŠ, Kapitola I.6], [Č2].)

Definícia 5.2.2. *Množina prirodzených čísel* $\mathbb{N}$ je taká induktívna množina, že pre každú induktívnu množinu B platí $\mathbb{N} \subseteq B$.

Prvky tejto množiny nazývame *prirodzené čísla.*

Pre každé prirodzené číslo n budeme $S(n) = n \cup \{n\}$ nazývať *nasledovníkom* čísla n.

Aby sme s uvedenou definíciou prirodzených čísel mohli ďalej pracovať, musíme ukázať, že takáto množina existuje.

{priro:LMPRIENINDUK}

Lema 5.2.3. *Prienik ľubovoľného neprázdneho systému induktívnych množín je induktívna množina.*

Dôkaz. Nech $\mathcal{S} \neq \emptyset$ je množina taká, že každý jej prvok $A \in \mathcal{S}$ je induktívna množina. Ukážeme, že $\bigcap \mathcal{S}$ je tiež induktívna množina.

Pretože $(\forall A \in \mathcal{S})\emptyset \in A$, máme $\emptyset \in \bigcap \mathcal{S}$.

Podobne ak $x \in \bigcap \mathcal{S}$, znamená to, že $(\forall A \in \mathcal{S})x \in A$. Keďže každá množina $A \in \mathcal{S}$ je induktívna, platí potom aj $(\forall A \in \mathcal{S})x \cup \{x\} \in A$, a teda $x \cup \{x\} \in \bigcap \mathcal{S}$. □

Tvrdenie 5.2.4. *Existuje práve jedna množina* $\mathbb{N}$ *taká, že* $\mathbb{N}$ *je induktívna a pre každú induktívnu množinu platí* $\mathbb{N} \subseteq B$.

Dôkaz. Jednoznačnosť. Ak uvedenú vlastnosť spĺňajú množiny N_1 aj N_2, tak máme $N_1 \subseteq N_2$ a $N_2 \subseteq N_1$, čo znamená, že $N_1 = N_2$.

Existencia. Podľa axiómy nekonečnej množiny existuje aspoň jedna induktívna množina A. Položme

$$\mathcal{S} = \{B \subseteq A; B \text{ je induktívna}\}$$

a

$$\mathbb{N} = \bigcap \mathcal{S}.$$

Nech teraz B je ľubovoľná induktívna množina. Potom podľa lemy 5.2.3 aj množina $B \cap A$ je induktívna, navyše platí $B \cap A \subseteq A$. To znamená, že $B \cap A \in \mathcal{S}$. Pretože množina $\mathbb{N}$ je prienik systému $\mathcal{S}$, dostávame

$$\mathbb{N} \subseteq B \cap A \subseteq B.$$

□

Podarilo sa nám teda ukázať, existenciu nejakej množiny, ktorú sme označili $\mathbb{N}$. Ako ďalší krok by bolo dobre ukázať, že táto množina naozaj v nejakom zmysle zodpovedá prirodzeným číslam a našej intuícii o nich.

Číslo 0 stotožníme s prázdnou množinou. Pre každé prirodzené číslo n dostaneme nasledujúce číslo ako $n \cup \{n\}$. Priamo z definície vidno, že čísla

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

patria do $\mathbb{N}$.

Nasledujúca veta bude veľmi dôležitá pri dôkaze rôznych vlastností množiny $\mathbb{N}$. Táto veta zdôvodňuje, prečo na dôkaz rôznych tvrdení o prirodzených číslach môžeme používať matematickú indukciu.

{priro:VTIND}

Veta 5.2.5 (Indukcia na množine prirodzených čísel)**.** *Nech $A \subseteq \mathbb{N}$ je množina taká, že*

(i) $\emptyset \in A$*;*

(ii) $(\forall n \in \mathbb{N})\ n \in A \Rightarrow S(n) \in A$*;*

t.j. A obsahuje 0 a s každým prirodzeným číslom obsahuje aj jeho nasledovníka.
Potom platí $A = \mathbb{N}$.

Dôkaz. Uvedené vlastnosti vlastne znamenajú, že A je induktívna množina. Priamo z definície $\mathbb{N}$ potom máme $\mathbb{N} \subseteq A$, a teda $A = \mathbb{N}$. □

Pomocou matematickej indukcie už vieme dokázať mnohé vlastnosti prirodzených čísel.

{priro:LMNJETRANZ}
{priro:itnNOTINn}
{priro:itNONZERONASL}
{priro:itnPODN}
{priro:itINRASUB}
{priro:itINJETRANZ}
{priro:itSUBRAIN}
{priro:it0INn}

Lema 5.2.6. *Pre ľubovoľné prirodzené čísla m, n, k platí*
(i) $n \notin n$*;*
(ii) $n = \emptyset \vee (\exists n_1 \in \mathbb{N}) n = S(n_1)$
(iii) $n \subseteq \mathbb{N}$*;*
(iv) $m \in n \Rightarrow S(m) \subseteq n$*;*
(v) *Ak $m \in n$ a $n \in k$, tak $m \in k$.*
(vi) $m \subseteq n \Rightarrow m = n \vee m \in n$*;*
(vii) $n = \emptyset \vee \emptyset \in n$.

Dôkaz. (i) Vyplýva z axiómy regularity.

(ii) Nech $A = \{n \in \mathbb{N}; n = \emptyset \vee (\exists n_1 \in \mathbb{N}) n = S(n_1)\}$. Očividne $\emptyset \in A$ a ak $n \in A$, tak aj $S(n) \in A$. Z vety 5.2.5 potom vyplýva, že $A = \mathbb{N}$, čiže dokazovaná vlastnosť platí pre každé prirodzené číslo.

(iii) Uvedená vlastnosť očividne platí pre $n = \emptyset$, keďže $\emptyset \subseteq \mathbb{N}$.

Ak pre nejaké $n \in \mathbb{N}$ máme $n \subseteq \mathbb{N}$, tak z $n \subseteq \mathbb{N}$ a $\{n\} \subseteq \mathbb{N}$ spolu vyplýva, že $S(n) = n \cup \{n\} \subseteq \mathbb{N}$.

Teda množina prirodzených čísel spĺňajúcich dokazovanú vlastnosť je celé $\mathbb{N}$.

(iv) Uvažujme množinu $A = \{n \in \mathbb{N}; (\forall m \in \mathbb{N})(m \in n \Rightarrow S(m) \subseteq n)\}$.

Predpoklad $m \in \emptyset$ nie je splnený pre žiadne m, teda implikácia $m \in \emptyset \Rightarrow S(m) \subseteq \emptyset)$ platí.

Predpokladajme teraz, že $n \in A$, ukážeme, že aj $S(n) = n \cup \{n\} \in A$. Ak $m \in S(n)$, tak sú dve možnosti. Buď platí $m \in n$, a vtedy $S(m) \subseteq n \subseteq n \cup \{n\} = S(n)$. Druhá možnosť je, že $m = n$, čo znamená, že $S(m) = S(n)$.

Z vety 5.2.5 potom vyplýva, že $A = \mathbb{N}$, čiže dokazovaná vlastnosť platí pre každé prirodzené číslo.

(v) Ak $n \in k$, tak podľa (iv) platí $S(n) \subseteq k$, čiže dostávame $m \in n \subseteq S(n) \subseteq k$. To znamená, že $m \in k$.

(vi) Indukciou vzhľadom na n; nech $A = \{n \in \mathbb{N}; (\forall m \in \mathbb{N}) m \subseteq n \Rightarrow m = n \vee m \in n\}$.

Ak $n = \emptyset$, tak z $m \subseteq \emptyset$ dostaneme $m = \emptyset$, čiže $\emptyset \in A$.

Nech teraz $n \in A$ a nech $m \subseteq S(n) = n \cup \{n\}$ pre nejaké $m \in \mathbb{N}$. Uvažujme najprv prípad, že $n \in m$. Potom podľa (iv) $S(n) \subseteq m$. Z platnosti oboch inklúzií $m \subseteq S(n)$ aj $S(n) \subseteq m$ máme $m = S(n)$.

Druhá možnosť je, že $n \notin m$ a vtedy dostaneme $m \subseteq n$. Keďže $n \in A$, máme buď $m = n \in S(n)$, alebo $m \in n$. V druhom prípade z $m \in n$ a $n \in S(n)$ vyplýva $m \in S(n)$ na základe (v).

(vii) Špeciálny prípad (vi) pre $m = \emptyset$. □

Z doteraz dokázaných výsledkov ľahko dostaneme:

{priro:DOSSMSN}
{priro:itINLRASUB}
{priro:itSMSN}

Dôsledok 5.2.7. *Pre ľubovoľné $m, n \in \mathbb{N}$ platí:*

(i) $m \subsetneq n \Leftrightarrow m \in n$.

(ii) $m \in n \Rightarrow S(m) \in S(n)$.

Dôkaz. (i) $\boxed{\Rightarrow}$ Vyplýva z 5.2.6 (vi).

$\boxed{\Leftarrow}$ Ak $m \in n$, tak z lemy 5.2.6 (iv) máme $S(m) = m \cup \{m\} \subseteq n$. Pretože $m \subsetneq S(m)$, platí $m \subsetneq n$.

(ii) Ak $m \in n$, tak podľa prvej časti tvrdenia máme $m \subsetneq n$, z čoho dostávame $m \cup \{m\} \subsetneq n \cup \{n\}$. Teda $S(m) \subsetneq S(n)$, čo je ekvivalentné s $S(m) \in S(n)$. □

Na tomto mieste už vieme overiť, že množina $\mathbb{N}$ (spolu s jej prvkom $\emptyset$ a funkciou S.) spĺňa Peanove axiómy z definície 5.1.1. Niektoré z nich už sme už vlastne dokázali. Platnosť podmienky (P5) vyplýva z vety 5.2.5 o indukcii. Platnosť (P1) a (P2) je zrejmá priamo z definície množiny $\mathbb{N}$. Takisto platnosť (P3) je jasná. Zostáva už overiť len vlastnosť (P4).

{priro:TVRPEANO}

Tvrdenie 5.2.8. *Pre ľubovoľné prirodzené čísla m, n platí*

$$S(m) = S(n) \qquad \Rightarrow \qquad m = n.$$

Dôkaz. Ak $S(m) = S(n)$, tak špeciálne máme $m \in S(n) = n \cup \{n\}$, čo znamená, že $m = n$ alebo $m \in n$. Ak nastane prvá z uvedených možností, tak tvrdenie platí. Stačí nám teda ukázať, že druhá možnosť nastať nemôže.

Predpokladajme teda, že by súčasne platilo $m \in n$ aj $S(m) = S(n)$. Podľa lemy 5.2.6(iv) potom platí $S(m) \subseteq n$, a teda $n \notin S(m)$ podľa lemy 5.2.6(i). Súčasne však $n \in S(n)$, dospeli sme teda k sporu s predpokladom, že $S(m) = S(n)$. □

5.2.1 Usporiadanie reláciou $\in$

Ďalej by sme na množine $\mathbb{N}$ chceli zaviesť usporiadanie. Malo by zodpovedať našej obvyklej predstave o usporiadaní prirodzených čísel, špeciálne by to malo byť dobré usporiadanie a malo by platiť $(\forall n \in \mathbb{N}) n < S(n)$. Toto usporiadanie zadefinujeme pomocou vzťahu $\in$.

Definícia 5.2.9. Na množine $\mathbb{N}$ definujeme reláciu $<$ tak, že pre $m, n \in \mathbb{N}$

$$m < m \Leftrightarrow m \in n.$$

Reláciu $\leq$ zavedieme tak, že

$$m \leq n \Leftrightarrow m = n \vee m < n.$$

Poznámka 5.2.10. Keďže už vieme, že prirodzené čísla spĺňajú Peanove axiómy, mohli by sme sa odvolať na to, že vieme dostať lineárne usporiadanie spôsobom uvedeným v časti 5.1.2. Dokonca platí, že by sme oboma spôsobmi dostali to isté usporiadanie. (Tento fakt nebudeme dokazovať.)

Napriek tomu, že pri odvolaní na predošlé výsledky by sme mali usporiadanie množiny $\mathbb{N}$ „zadarmo“, zdalo sa mi vhodné uviesť tu aj tento prístup. Jeden z dôvodov je, že pri dokazovaní Peanových axióm sme súčasne dokázali viacero tvrdení, ktoré sa nám budú hodiť aj pri dôkaze, že $(\mathbb{N}, \in)$ je dobre usporiadaná množina; takže už máme pomerne veľa pomocných vecí pripravených. Ďalší dôvod je ten, že to súvisí s ordinálnymi číslami (kapitola 7), kde je ako usporiadanie použitá tiež relácia $\in$.

Z dôsledku 5.2.7 (i) okamžite vidíme, že pre $m, n \in \mathbb{N}$ platí

$$m \leq n \Leftrightarrow m \subseteq n \tag{5.12}$$ {priro:EQ<LRASUB}

a

$$m < n \Leftrightarrow m \in n \Leftrightarrow m \subsetneqq n. \tag{5.13}$$ {priro:EQINLRASUB}

Z (5.13) je zrejmé, že $(\mathbb{N}, \leq)$ je čiastočne usporiadaná množina. Ďalej by sme chceli ukázať, že ide o lineárne usporiadanie. Rozmyslime si najprv, čo presne znamená, že ostré usporiadanie je lineárne. Pre čiastočné usporiadanie sme linearitu definovali tak, že pre ľubovoľné prvky platí $a \leq b \vee b \leq a$. Ostrému čiastočnému usporiadaniu $<$ zodpovedá čiastočné usporiadanie definované ako $a \leq b \overset{\text{def}}{\Leftrightarrow} a < b \vee a = b$. Teda o lineárne usporiadanie pôjde, ak platí

$$(\forall a, b \in X) a < b \vee a = b \vee b < a;$$

čiže relácia $<$ je trichotomická.

Overme teda, že relácia $\in$ na množine $\mathbb{N}$ je trichotomická. {priro:TVRTRICHO}

Tvrdenie 5.2.11. *Pre ľubovoľné $m, n \in \mathbb{N}$ platí*

$$m \in n \vee m = n \vee n \in m.$$

Dôkaz. Označme $A = \{n \in \mathbb{N}; (\forall m \in \mathbb{N}) m \in n \vee m = n \vee n \in m\}$.

Z lemy 5.2.6 (vii) máme $\emptyset \in A$.

Nech teraz $n \in A$ a m je ľubovoľné prirodzené číslo. Ak $m = \emptyset$, tak opäť z lemy 5.2.6 (vii) máme $m \in n \vee m = n$. Ak $m \neq \emptyset$, tak $m = S(m_1)$ pre nejaké $m_1 \in \mathbb{N}$ (lema 5.2.6 (ii)). Pretože $n \in A$, nastane niektorá z možností $m_1 \in n$, $m_1 = n$, $n \in m_1$. Na základe dôsledku 5.2.7 (ii) potom dostávame pre $S(m_1) = m$ v jednotlivých prípadoch $m \in S(n)$, $m = S(n)$, $S(n) \in m$. □

Keď už máme dokázanú linearitu nášho usporiadania na $\mathbb{N}$, vcelku ľahko sa dá ukázať, že je to dobré usporiadanie. {priro:TVRNJEDUM}

Tvrdenie 5.2.12. *Množina $(\mathbb{N}, \leq)$ je dobre usporiadaná množina.*

Dôkaz. Chceme ukázať, že každá neprázdna podmnožina $\mathbb{N}$ má najmenší prvok.

Sporom. Nech $B \neq \emptyset$, $B \subseteq \mathbb{N}$ a B nemá najmenší prvok.

Označme $A = \{n \in \mathbb{N}; (\forall b \in B) n < b\}$. Všimnime si, že ak $n \in A$, tak žiadny prvok $m \in \mathbb{N}$ taký, že $m \leq n$ nemôže patriť do B.

Zrejme, $\emptyset \in A$, inak by platilo $\emptyset \in B$ a $\emptyset$ by potom bol najmenší prvok množiny B.

Nech teraz $n \in A$. Potom aj $S(n) \in A$. Ak by totiž platilo $S(n) \notin A$, tak musí existovať $b \in B$ s vlastnosťou $b \leq S(n)$. Lenže už vieme, že pre všetky $m \leq n$ platí $m \notin B$. Potom ale $S(n) \in B$ a $S(n)$ je najmenší prvok množiny B, čo vedie k sporu.

Množina A teda spĺňa predpoklady vety 5.2.5, čiže potom $A = \mathbb{N}$. Keďže ale $A \subseteq \mathbb{N} \setminus B$, dostávame $B = \emptyset$, čo je hľadaný spor. □

Cvičenia

Úloha 5.2.1. Ukážte, že pre $m, n \in \mathbb{N}$ platí $S(m) \in S(n) \Rightarrow m \in n$. (Ide vlastne o obrátenú implikáciu k implikácii dokázanej v dôsledku 5.2.7(ii)).

5.3 Celé, racionálne a reálne čísla

{QaR:SECTOBORY}

Napriek tomu, že to nepatrí do sylabu tohoto predmetu a do istej miery takto vznikne prekryv s látkou, ktorú budete preberať na teoretickej aritmetike [Č3], aspoň stručne sa zmienime aj o tom, ako z prirodzených čísel môžeme vybudovať ďalšie číselné obory.

5.3.1 Iné konštrukcie prirodzených čísel

{QaR:SSECTINEPRIR}

Možno ešte skôr než sa začneme venovať ďalším číselným oborom, oplatí sa spomenúť, že konštrukcia prirodzených čísel z predchádzajúcej kapitoly rozhodne nie je jedinou možnosťou, ako ich môžeme zaviesť (hoci je v množinovo-teoretických textoch najrozšírenejšia). Napríklad v knihe [ŠS] sa prirodzené čísla definujú ako konečné kardinály. Dajú sa pre ne zaviesť operácie S, $+$, $\cdot$ i relácia $<$, ktoré spĺňajú všetky vlastnosti, ktoré sme uviedli v predchádzajúcej časti. Táto konštrukcia sa samozrejme opiera o existenciu kardinálnych čísel, ktorú (ako už dlhšie sľubujeme) dokážeme neskôr. (Snáď sa oplatí spomenúť, že pri našej definícii kardinálnych čísel budú tieto dve konštrukcie v konečnom dôsledku totožné.)

5.3.2 Celé čísla

Celé čísla sa dosť často zavádzajú ako triedy rozkladu množiny $\mathbb{N} \times \mathbb{N}$ určené reláciou ekvivalencie

$$(m, n)R(m', n') \Leftrightarrow m + n' = n + m'.$$

Dvojica m, n potom zodpovedá číslu $m - n$.

Prirodzeným spôsobom sa dajú na tejto množine zaviesť operácie $+$, $\cdot$ a relácia $<$ pomocou analogických operácií už zavedených pre prirodzené čísla.

$$[(m, n)] + [(k, l)] = [(m + k, n + l)]$$
$$[(m, n)].[(k, l)] = [(mk + nl, ml + nk)]$$
$$[(m, n)] \leq [(k, l)] \Leftrightarrow m + l \leq k + n$$

(Uvedené definície sú veľmi prirodzené, keď si uvedomíme, že majú zodpovedať výsledkom operácií $(m - n) + (k - l)$, $(m - n).(k - l)$ a nerovnosti $m - n \leq k - l$.)

Samozrejme, aby bola táto definícia úplná, treba overiť, že R je skutočne relácia ekvivalencie a že výsledky uvedených operácií resp. platnosť nerovnosti nezávisia od výberu reprezentanta príslušnej triedy. (Podrobné dôkazy môžete nájsť v [Č3].)

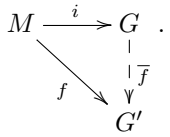
Určite by ste vedeli vymyslieť aj iné konštrukcie, ktoré by splnili tento účel rovnako dobre. (Napríklad by sme každé celé číslo mohli určovať pomocou dvojice znamienko a prirodzené číslo a nejako pre ne zadefinovať všetky operácie a nerovnosť.) Na tomto mieste by som sa aspoň stručne zmienil o dvoch argumentoch v prospech výberu práve tejto konštrukcie.

Jeden z dôvodov je ten, že sa táto konštrukcia veľmi podobá na konštrukciu racionálnych čísel, ktoré spomenieme o chvíľu – a takýmto spôsobom dosiahneme istú jednotnosť.

Ďalším argumentom v prospech uvedenej konštrukcie by mohlo byť to, že ak si všímame iba operáciu $+$, tak konštrukcia $(\mathbb{Z}, +)$ sa dá ľahko zovšeobecniť na nasledovnú situáciu:

TVRPOLOGRUPA}

Tvrdenie 5.3.1. *Ak $(M, *)$ je komutatívna pologrupa s krátením, tak existuje grupa $(G, \circ)$ a injektívny homomorfizmus $i\colon M \to G$ taký, že pre každý homomorfizmus $f\colon M \to G'$ z M do grupy G' existuje práve jeden homomorfizmus $\overline{f}\colon G \to G'$ taký, že $f = \overline{f} \circ i$.*



Inak povedané, každú komutatívnu pologrupu s krátením možno vnoriť do grupy a táto grupa i príslušné vnorenie sú určené jednoznačne až na izomorfizmus.

Pripomeňme, že dvojicu $(M, *)$ voláme *pologrupa* ak $*$ je asociatívna binárna operácia na množine M. O pologrupe *s krátením* hovoríme vtedy, ak navyše platia zákony o krátení, t.j.

$$(\forall a, b, c \in M) a * b = a * c \Rightarrow b = c$$
$$(\forall a, b, c \in M) b * a = c * a \Rightarrow b = c$$

Môžete si vyskúšať dokázať toto tvrdenie ako precvičenie vašich znalostí z algebry. (Prípadne sa k nemu môžete vrátiť, keď sa budete učiť o konštrukcii celých čísel a skúsiť si uvedomiť, že uvedený postup funguje pre ľubovoľnú komutatívnu pologrupu s krátením.)

5.3.3 Racionálne čísla

Racionálne čísla z celých čísel vieme dostať konštrukciou, ktorú by ste mali poznať z algebry vo všeobecnejšej podobe. Viete totiž, že pre každý obor integrity existuje podielové pole – najmenšie pole, ktoré ho obsahuje (pozri napríklad [KGGS, podkapitola 4.5]).

5.3.4 Reálne čísla

Ak už máme zostrojené racionálne čísla, dajú sa z nich dostať reálne čísla viacerými spôsobmi. (Každý z nich má výhody i nevýhody.)

Jeden pomerne častý spôsob je pomocou *zúplnenia.* Z matematickej analýzy by ste mali vedieť, že pre každý metrický priestor sa dá zostrojiť jeho zúplnenie, čo je úplný metrický priestor v ktorom je pôvobný priestor hustou podmnožinou. Zúplnenie sa obvykle konštruuje ako množina tried ekvivalencií cauchyovských postupností. V prípade, že zúplňujeme metrický priestor $(\mathbb{Q}, d)$, $d(x, y) = |x - y|$, dá sa na priestore, ktorý dostaneme, pomerne prirodzeným spôsobom zaviesť usporiadanie, sčitovanie i násobenie.

Často sa vyskytuje aj konštukcia reálnych čísel pomocou *Dedekindových rezov.* Reálne čísla tu definujeme ako dvojice (A, B) také, že

(i) $A \cup B = \mathbb{Q}$;
(ii) $x \in A \wedge y \leq x \Rightarrow y \in A$;
(iii) $x \in B \wedge y \geq x \Rightarrow y \in B$;
(iv) $x \in A \wedge y \in B \Rightarrow x \leq y$;
(v) Množina A nemá najväčší prvok.

Napríklad reálnemu číslu $\sqrt{2}$ zodpovedá dvojica (A, B) taká, že $A = \{x \in \mathbb{Q}; x \leq 0 \vee x^2 \leq 2\}$ a $B = \{x \in \mathbb{Q}; x \geq 0, x^2 \geq 2\}$. Racionálnemu číslu q by zodpovedala dvojica (A, B) taká, že $A = \{x \in \mathbb{Q}; x < 0\}$ a $B = \{x \in \mathbb{Q}; x \geq 0\}$.

5.4 Konečné a nekonečné množiny

{konec:SECT}

Doteraz sme používali ako definíciu konečnej množiny podmienku $|A| < \aleph_0$. Uvedieme dve ďalšie možné definície konečnej množiny. Ako sa napokon ukáže, tieto definície sú ekvivalentné v ZFC. Čo je možno do istej miery prekvapivé (a zaujímavé), bez axiómy výberu už ekvivalencia definícií, ktoré tu uvedieme, platiť nemusí. Keďže chceme zdôrazniť miesta, kde bude potrebné použiť axiómu výberu, budeme v tejto kapitole pri všetkých tvrdeniach zdôrazňovať to, či sme v dôkaze použili len axiómy systému ZF alebo aj AC.

5.4.1 Dedekindova definícia konečnej množiny

Ako už bolo spomenuté, nakoniec ukážeme (v ZFC) ekvivalenciu všetkých definícii konečnosti, ktorými sa tu budeme zaoberať. Aby sme boli schopní rozlíšiť, s ktorou definíciou práve pracujeme, budeme v názve používať aj prvé písmeno mena autora definície. (Takáto terminológia asi nie je celkom štandardná, ale potrebovali sme definície nejako odlíšiť.)

Nasledujúca definícia pochádza od nemeckého matematika Richarda Dedekinda.

Definícia 5.4.1. Množinu X budeme nazývať *D-nekonečná,* ak existuje vlastná podmnožina $Y \subsetneqq X$ taká, že $|Y| = |X|$. Ak množina X nie je D-nekonečná, voláme ju *D-konečná.*

D-nekonečná je teda taká množina, ktorá má rovnakú mohutnosť ako niektorá jej vlastná podmnožina. Nasledujúce tvrdenie ukazuje súvislosť tohoto pojmu s kardinálnym číslom $\aleph_0$.

Príklad 5.4.2. Množina $\mathbb{N}$ je D-nekonečná. Stačí zobrať bijekciu $f\colon \mathbb{N} \to \mathbb{N} \setminus \{0\}$, $f\colon n \mapsto n+1$.

{konec:TVRDNEKONEKV}

Tvrdenie 5.4.3 (ZF)**.** *Nech X je ľubovoľná množina. Nasledujúce podmienky sú ekvivalentné:*

{konec:itD1} (i) *X je D-nekonečná;*

{konec:itD2} (ii) $\aleph_0 \leq |X|$*;*

{konec:itD3} (iii) $|X| = |X| + 1$.

Ešte pred dôkazom si môžeme uvedomiť, že podmienka $|X| = |X| + 1$ vlastne znamená, že existuje bijekcia medzi X a $X \cup \{X\}$. (Z axiómy regularity vieme, že $X \notin X$; čiže X a $\{X\}$ sú disjunktné.)

Dôkaz. (i) $\Rightarrow$ (ii) Nech Y je vlastná podmnožina množiny X a $g\colon X \to Y$ je bijekcia. Nech $x \in X \setminus Y$. Definujme zobrazenie $f\colon \mathbb{N} \to X$ ako[1]

$$f(0) = x,$$
$$f(n+1) = g(f(n)).$$

Matematickou indukciou (veta 5.2.5) možno overiť, že tento predpis skutočne jednoznačne určuje zobrazenie z $\mathbb{N}$ do X.

Toto zobrazenie je navyše injektívne. Jediný prvok, ktorý sa zobrazí na x, je 0, lebo ak $m \neq 0$, tak $m = n+1$ pre nejaké n, a teda $f(m) \in g[X] = Y$. Predpokladajme, že by f nebolo injektívne. Potom množina

$$A = \{n \in \mathbb{N}; (\exists m \in \mathbb{N}) m \neq n \wedge f(m) = f(n)\}$$

[1] Budeme už používať aj označenie $n+1$, ktoré je asi obvyklejšie, namiesto $S(n)$, ktorého sme sa dôsledne pridržiavali pri zavedení prirodzených čísel.

by bola neprázdna, teda by mala najmenší prvok. Označme ho n_0. Už sme zdôvodnili, že $n_0 \neq 0$. Teda $n_0 = n+1$ pre nejaké n. Potom dostávame $f(n_0) = f(m)$ a súčasne $n_0 = n+1$, $m = k+1$ pre nejaké $n, k \in \mathbb{N}$, $n \neq k$. Lenže z definície zobrazenia f potom vyplýva $g(f(n)) = g(f(k))$. Na základe injektívnosti zobrazenia g máme $f(n) = f(k)$, z čoho dostaneme $n \in A$, čo je spor s minimalitou n_0.

(ii) $\Rightarrow$ (iii) Ak $\aleph_0 \leq |X|$, tak existuje injekcia $g\colon \mathbb{N} \to X$. Definujme $f\colon X \cup \{X\} \to X$ takto:

$$f(x) = \begin{cases} g(n+1) & \text{ak } x = g(n), \\ g(0) & \text{ak } x = X, \\ x & \text{ak } x \notin g[\mathbb{N}]. \end{cases}$$

Takto definované zobrazenie f je bijekcia.

(iii) $\Rightarrow$ (i) Nech $f\colon X \cup \{X\} \to X$ je bijekcia. Potom $f|_X$ je bijekcia medzi množinou X a jej vlastnou podmnožinou $X \setminus \{f(X)\}$. □

5.4.2 Tarskiho definícia konečnej množiny

Autorom inej často používanej definície konečných množín je poľský matematik Alfred Tarski.

Definícia 5.4.4. Hovoríme, že množina X je *T-konečná,* ak každá neprázdna množina $\mathcal{A}$ podmnožín množiny X má minimálny prvok vzhľadom na inklúziu.

$$\mathcal{A} \subseteq \mathcal{P}(X) \wedge \mathcal{A} \neq \emptyset \Rightarrow (\exists A \in \mathcal{A})(B \in \mathcal{A} \wedge B \subseteq A \Rightarrow B = A)$$

Ak X nie je T-konečná, budeme ju volať *T-nekonečná.*

Pretože zobrazenie $A \mapsto X \setminus A$ obracia inklúzie (tvrdenie 2.4.10 (i)), je zrejmé, že ak nahradíme v uvedenej definícii slovo „minimálny“ slovom „maximálny“, dostaneme ekvivalentnú definíciu.

Príklad 5.4.5. Množina $\mathbb{N}$ je T-nekonečná, keďže systém $\{A_n; n \in \mathbb{N}\}$, kde $A_n = \{m \in \mathbb{N}, m \geq n\}$ nemá minimálny prvok.

{konec:LMTKONEC}

Lema 5.4.6 (ZF)**.**
(i) *Množina $\emptyset$ je T-konečná.*
(ii) *Ak X je T-konečná množina a x je ľubovoľná množina, tak aj $X \cup \{x\}$ je T-konečná.*

Dôkaz. Prvá časť tvrdenia zrejmá.

(ii) Ak $x \in X$, tak uvedené tvrdenie triviálne platí. Budeme teda predpokladať, že $x \notin X$. Nech $\mathcal{A} \neq \emptyset$ je nejaký neprázdny systém podmnožín množiny $X \cup \{x\}$. Položme $\mathcal{B} = \{A \cap X; A \in \mathcal{A}\}$.

Ak $\mathcal{B} = \emptyset$, znamená to, že $\mathcal{A} \subseteq \mathcal{P}(\{x\})$. Jednoprvková množina je T-konečná, preto $\mathcal{A}$ má minimálny prvok.

Teraz už budeme predpokladať, že $\mathcal{B} \neq \emptyset$. Pretože $\mathcal{B} \subset \mathcal{P}(X)$ a X je T-konečná, existuje minimálny prvok B systému $\mathcal{B}$. Ak $B \in \mathcal{A}$, tak B je súčasne minimálny prvok množiny $\mathcal{A}$. Ak $B \notin \mathcal{A}$, tak $B \cup \{x\}$ je minimálny prvok množiny $\mathcal{A}$. □

Nasledujúce tvrdenie poskytuje ekvivalentnú charakterizáciu konečnosti v zmysle Tarskiho definície.

{konec:TVRTKONIND}

Tvrdenie 5.4.7 (ZF)**.** *Nech X je ľubovoľná množina. Nasledujúce podmienky sú ekvivalentné:*
(i) *X je T-konečná;*

(ii) *ak množina $\mathcal{A} \subseteq \mathcal{P}(X)$ spĺňa podmienky*
(a) $\emptyset \in \mathcal{A}$;
(b) $A \in \mathcal{A}$, $x \in X \Rightarrow A \cup \{x\} \in \mathcal{A}$,
tak $X \in \mathcal{A}$.

Dôkaz. $\boxed{\Rightarrow}$ Ak X je T-konečná, tak systém $\mathcal{A}$ má (vzhľadom na inklúziu) maximálny prvok A. Ukážeme, že $A = X$, z čoho už priamo vyplýva $X \in \mathcal{A}$.

Nech by platilo $A \subsetneqq X$. Potom existuje $x \in X$ také, že $x \notin A$. Z predpokladu, že $\mathcal{A}$ spĺňa podmienku (a), dostaneme $A \cup \{x\} \in \mathcal{A}$. Lenže $A \subsetneqq A \cup \{x\}$, čo je spor s maximalitou A.

$\boxed{\Leftarrow}$ Nech $\mathcal{A}$ je množina všetkých T-konečných podmnožín X. Z lemy 5.4.6 vyplýva, že $\mathcal{A}$ spĺňa podmienky (a), (b). Teda $X \in \mathcal{A}$, čiže X je T-konečná. □

5.4.3 Vlastnosti konečných množín

Priamo z definície vieme ukázať viaceré jednoduché vlastnosti T-konečných množín. Keďže napokon ukážeme, že T-konečnosť je presne to isté, čo sme doteraz rozumeli pod pojmom konečnosť, môžeme priamo hovoriť o vlastnostiach konečných množín.

{konec:TVRTKONPOD}

Tvrdenie 5.4.8 (ZF)**.** *Ak X je T-konečná množina a $Y \subseteq X$, tak aj Y je T-konečná.*

Dôkaz. Ak $\emptyset \neq \mathcal{A} \subseteq \mathcal{P}(Y)$, tak aj $\emptyset \neq \mathcal{A} \subseteq \mathcal{P}(X)$, a teda $\mathcal{A}$ má minimálny prvok vzhľadom na inklúziu. □

{konec:TVR1}

Tvrdenie 5.4.9 (ZF)**.** *Ak X a Y sú T-konečné množiny, tak aj $X \cup Y$ je T-konečná.*

Dôkaz. Bez ujmy na všeobecnosti môžeme predpokladať, že X a Y sú disjunktné. (Ak nie, tak Y nahradíme $Y \setminus X$. Už vieme, že podmnožina T-konečnej množiny je opäť T-konečná.)

Nech $\mathcal{A} \subseteq \mathcal{P}(X \cup Y)$ a $\mathcal{A} \neq \emptyset$. Označme $\mathcal{B} = \{A \cap X; A \in \mathcal{A}\}$. Potom existuje $B \subseteq X$, ktoré je minimálnym prvkom $\mathcal{B}$. Ďalej položme $\mathcal{C} = \{A \cap Y; A \in \mathcal{A} \wedge A \cap X = B\}$. (Pretože $B \in \mathcal{B}$, existuje také $A \in \mathcal{A}$, že $A \cap X = B$, preto je systém $\mathcal{C}$ neprázdny.) Keďže ide o podmnožinu T-konečnej množiny Y, existuje minimálny prvok C množiny $\mathcal{C}$. Potom množina $B \cup C$ je minimálnym prvkom $\mathcal{A}$.

(Najprv si uvedomme, že $B \cup C$ patrí do $\mathcal{A}$. Vyplýva to z toho, že existuje taký prvok $A \in \mathcal{A}$, pre ktorý $A \cap X = B$ a $A \cap Y = C$. Potom $A = A \cap (X \cup Y) = (A \cap X) \cup (A \cap Y) = B \cup C$.

Podobný argument použijeme aj na zdôvodnenie, že je to minimálny prvok. Nech pre nejaké $A \in \mathcal{A}$ platí $A \subseteq B \cup C$. Potom $A \cap X \in \mathcal{B}$ a $A \cap X \subseteq (B \cup C) \cap B = B$, a teda z minimality B dostaneme $A \cap X = B$. Z toho ďalej vyplýva, že $A \cap Y \in \mathcal{C}$ a podobnou úvahou dostaneme $A \cap Y = C$. Pretože $A \subseteq X \cup Y$, platí $A = A \cap (X \cup Y) = (A \cap X) \cup (A \cap Y) = B \cup C$.) □

{konec:TVR2}

Tvrdenie 5.4.10 (ZF)**.** *Ak $\mathcal{S}$ je T-konečný systém T-konečných množín, tak aj množina $\bigcup \mathcal{S}$ je T-konečná.*

Dôkaz. Označme $\mathcal{A} = \{\mathcal{B} \subseteq \mathcal{S}; \bigcup \mathcal{B}$ je T-konečná množina$\}$. Zrejme $\emptyset \in \mathcal{A}$ a z tvrdenia 5.4.9 dostaneme, že ak $\mathcal{B} \in A$ a $B \in \mathcal{S}$, tak aj $\mathcal{B} \cup \{B\} \in \mathcal{A}$. (Stačí si uvedomiť, že $\bigcup(\mathcal{B} \cup \{B\}) = (\bigcup \mathcal{B}) \cup B$ je zjednotenie dvoch T-konečných množín.) Podľa tvrdenia 5.4.7 platí potom $\mathcal{S} \in \mathcal{A}$, a teda množina $\bigcup \mathcal{S}$ je T-konečná. □

{konec:TVR4}

Tvrdenie 5.4.11 (ZF)**.** *Obraz T-konečnej množiny je T-konečná množina, t.j. ak X je T-konečná a $f\colon X \to Y$ je surjekcia, tak Y je T-konečná.*

Dôkaz. Nech $\mathcal{A} \subseteq \mathcal{P}(X)$ a $\mathcal{A} \neq \emptyset$. Potom $\mathcal{B} = \{f^{-1}[A]; A \in \mathcal{A}\}$ je neprázdna podmnožina $\mathcal{P}(X)$. Táto množina má minimálny prvok, ktorý musí byť tvaru $f^{-1}[A_0]$, pre nejaké $A_0 \in \mathcal{A}$. Ukážeme, že A_0 je minimálny prvok množiny $\mathcal{A}$.

Nech $B \in \mathcal{A}$ a $B \subseteq A_0$. Potom aj $f^{-1}[B] \subseteq f^{-1}[A_0]$. Pretože $f^{-1}[B] \in \mathcal{B}$, dostaneme na základe minimality $f^{-1}[B] = f^{-1}[A_0]$.

Potom ale

$$B = f[f^{-1}[B]] = f[f^{-1}[A_0]] = A_0.$$

(Využili sme, že pre surjektívnu funkciu $f\colon X \to Y$ a $C \subseteq Y$ platí $f[f^{-1}[C]] = C$.) □

Z uvedeného tvrdenia ľahko vidíme, že T-konečnosť sa prenáša bijekciami.

{konec:DOSBIJEK}

Dôsledok 5.4.12 (ZF). *Ak X je T-konečná množina a $|X| = |Y|$, tak Y je T-konečná.*

V kombinácii s tvrdením 5.4.8 dostaneme

{konec:DOSINJEK}

Dôsledok 5.4.13 (ZF). *Ak Y je T-konečná množina a $|X| \leq |Y|$, tak X je T-konečná.*

{konec:TVR3}

Tvrdenie 5.4.14 (ZF). *Ak množina X je T-konečná, tak je T-konečná aj množina $\mathcal{P}(X)$.*

Dôkaz. Označme $\mathcal{A} = \{A \subseteq X; \mathcal{P}(A) \text{ je T-konečná}\}$. Očividne $\emptyset \in \mathcal{A}$.

Nech $A \in \mathcal{A}$ a $x \in X$. Ak $x \in A$, tak $A \cup \{x\} = A \in \mathcal{A}$. Predpokladajme teda, že $x \notin A$. Potom $\mathcal{P}(A \cup \{x\}) = \mathcal{P}(A) \cup \{B \cup \{x\}; B \in \mathcal{P}(A)\}$. Množina $\mathcal{P}(A)$ je T-konečná. Keďže $B \mapsto B \cup \{x\}$ je bijekcia medzi $\mathcal{P}(A)$ a $\{B \cup \{x\}; B \in \mathcal{P}(A)\}$, aj táto množina je T-konečná. Potom $\mathcal{P}(A \cup \{x\})$ je zjednotenie dvoch T-konečných množín, čiže je to tiež T-konečná množina.

Ukázali sme, že $\mathcal{A}$ spĺňa podmienky (a), (b) z tvrdenia 5.4.7. Teda aj $X \in \mathcal{A}$ a množina $\mathcal{P}(X)$ je T-konečná. □

5.4.4 Vzťah rôznych definícií konečnosti

T-konečnosť môžeme charakterizovať pomocou prirodzených čísel nasledovne:

{konec:TVRTKONN}

Tvrdenie 5.4.15 (ZF). *Nech X je ľubovoľná množina. Nasledujúce podmienky sú ekvivalentné:*

{konec:itTN1}

(i) *X je T-konečná;*

{konec:itTN3}

(ii) *existuje $n \in \mathbb{N}$ také, že $|X| = n$;*

{konec:itTN2}

(iii) *existuje $n \in \mathbb{N}$ také, že $|X| \leq n$.*

Vlastnosť $|X| = n$ vlastne znamená existenciu bijekcie medzi X a $n = \{k \in \mathbb{N}; k < n\}$. Podobne, $|X| \leq n$ znamená existenciu injekcie z X do n.

Dôkaz. (i) ⇒ (ii) Nech X je T-konečná množina $\mathcal{A} = \{A \subseteq X; (\exists n \in \mathbb{N})|A| = n\}$. Očividne $\emptyset \in \mathcal{A}$. Ďalej nech $A \in \mathcal{A}$ a $x \in X$. Ak $x \in A$, tak $A \cup \{x\} = A \in \mathcal{A}$. Ak $x \notin A$ a existuje bijekcia $f\colon A \to n$, tak aj zobrazenie $g\colon A \cup \{x\} \to S(n)$ určené tým, že $g|_A = f$ a $g(x) = n$ je bijekcia medzi $A \cup \{x\}$ a $S(n) = n \cup \{n\}$.

(ii) ⇒ (iii) Zrejmé.

(iii) ⇒ (i) Vďaka dôsledku 5.4.13 nám stačí ukázať, že každé prirodzené číslo je T-konečná množina. To sa ľahko overí indukciou na množine $\mathbb{N}$ (veta 5.2.5) s použitím lemy 5.4.6.

□

Ďalej ukážeme, že T-konečnosť je ekvivalentná s definíciou konečnosti, ktorú sme používali doteraz (definícia 4.2.5). V dôkaze tohoto tvrdenia sa nám bude hodiť nasledujúca lema.

{konec:LMNEOH

Lema 5.4.16 (ZF)**.** *Nech $A \subseteq \mathbb{N}$ a A je neohraničená (t.j. $(\forall n \in \mathbb{N})(\exists a \in A) n < a$). Potom $|A| = \aleph_0$.*

Dôkaz. Je zrejmé, že $|A| \leq \aleph_0$, stačí teda dokázať existenciu injekcie z $\mathbb{N}$ do A.

Položme $f(0) = \min A$ a $f(S(n)) = \min(A \setminus \{f(k); k \leq n\})$. (Z neohraničenosti A vyplýva, že množina $A \setminus \{f(k); k \leq n\}$ je neprázdna pre každé $n \in \mathbb{N}$.) Indukciou na množine $\mathbb{N}$ (veta 5.2.5) sa dá overiť, že $f(S(n)) > f(n)$, teda táto funkcia bud rastúca. A tiež indukciou dostaneme to, že $A \setminus \{f(k); k \leq n\}$ je neprázdna; pretože prvky množiny $\{f(k); k \leq n\}$ nepresiahnu $f(n)$. Teda $f(S(n))$ uvedené podmienky skutočne jednoznačne definujú funkciu z $\mathbb{N}$ do A (berieme minimum z neprázdnej množiny, jeho existencia je zaručená tým, že $\mathbb{N}$ je dobre usporiadaná).

Pretože funkcia f je ostro rastúca, je aj prostá. □

{konec:TVRTKONALNUL}

Tvrdenie 5.4.17 (ZF)**.** *Množina X je T-konečná práve vtedy, keď $|X| < \aleph_0$.*

Dôkaz. $\boxed{\Rightarrow}$ Podľa tvrdenia 5.4.15 už vieme, že existuje bijekcia medzi X a nejakou množinou $n \subseteq \mathbb{N}$. Teda $|X| \leq \aleph_0$. Súčasne nemôže existovať bijekcia medzi X a $\mathbb{N}$, lebo to by znamenalo, že $\mathbb{N}$ je T-konečná množina (dôsledok 5.4.12). Teda dostávame $|X| \neq \aleph_0$ a celkovo $|X| < \aleph_0$.

$\boxed{\Leftarrow}$ Pretože $|X| \leq \aleph_0$, existuje bijekcia medzi X a nejakou podmnožinou $A \subseteq \mathbb{N}$. Pretože $|X| \neq \aleph_0$, takáto podmnožina A je nutne ohraničená. Teda $A \subseteq n$ pre nejaké n. Podľa tvrdenia 5.4.15 je tento fakt už ekvivalentný s T-konečnosťou. □

{konec:TVRTKONJEDKON}

Tvrdenie 5.4.18 (ZF)**.** *Každá T-konečná množina je D-konečná.*

Dôkaz. Nech množina X je D-nekonečná, čo podľa tvrdenia 5.4.3 znamená, že existuje injekcia $f\colon \mathbb{N} \to X$. Ak položíme $A_n = \{f(m); m \in \mathbb{N}, m \geq n\}$, tak $\mathcal{A} = \{A_n; n \in \mathbb{N}\}$ je systém podmnožín X, ktorý nemá minimálny prvok. Teda X je T-nekonečná. □

{konec:TVRDKONJETKON}

Tvrdenie 5.4.19 (AC)**.** *Každá D-konečná množina je T-konečná.*

Dôkaz. Nech X nie je T-konečná. Teda existuje neprázdna množina $\mathcal{A} \subseteq \mathcal{P}(X)$, ktorá nemá maximálny prvok vzhľadom na inklúziu.

Matematickou indukciou zostrojíme injekciu $f\colon \mathbb{N} \to X$.

Vyberme ľubovoľnú množinu $X_0 \in \mathcal{A}$. Pretože X_0 nie je maximálny prvok $\mathcal{A}$, existuje $X_1 \supsetneq X_0$. Vyberme nejaký prvok $t_0 \in X_1 \setminus X_0$.

Ak už máme definované t_k a X_k pre $k \in \{1, \ldots, n\}$, tak opäť existuje $X_{k+1} \in \mathcal{A}$ také, že $X_{k+1} \supsetneq X_k$ a $t_{k+1} \in X_{k+1} \setminus X_k$. Takto dostaneme rastúcu postupnosť X_k, $k \in \mathbb{N}$ a prvky $t_k \in X_{k+1} \setminus X_k$ pre $k \in \mathbb{N}$. Funkciu f potom definujeme ako $f(k) = t_k$ pre ľubovoľné $k \in \mathbb{N}$. (V každom kroku vyberáme X_k a t_k, teda využívame axiómu výberu.) Táto funkcia je injektívna.

Ukázali sme, že $\aleph_0 \leq |X|$, čo znamená podľa tvrdenia 5.4.3, že X je D-nekonečná. □

Azda je zaujímavé spomenúť, že uvedené tvrdenie neplatí v ZF. Dokonca pre D-konečné množiny v ZF nemusia platiť tvrdenia analogické k tvrdeniam 5.4.10, 5.4.11 a 5.4.14, ktoré sme dokázali pre T-konečné množiny (pozri napríklad [He2, Section 4.1]).

Existujú aj ďalšie definície konečnosti, ktoré sú ekvivalentné v ZFC ale nie všetky z nich sú ekvivalentné v ZF (pozri napríklad [B2, Problém 1B], [HR, Note 94]).

Tiež si môžeme všimnúť, že v ZFC máme, že každá množina je buď konečná alebo nekonečná (pre ktorúkoľvek z uvedených definícií – v ZFC sú ekvivalentné), čiže sme vlastne dokázali, že pre každú množinu X platí

{konec:EQTRICHALNUL}

$$|X| < \aleph_0 \qquad \vee \qquad \aleph_0 \leq |X|. \tag{5.14}$$

Neskôr ukážeme podobné tvrdenie pre ľubovoľný kardinál – dôsledok 7.1.6.

Cvičenia

Úloha 5.4.1. Ukážte, že množina X je D-nekonečná práve vtedy, keď $\aleph_0 + |X| = |X|$.

Kapitola 6

Axióma výberu

{CHCHOICE}

Axióma výberu sa do istej miery líši od ostatných axióm ZFC. Hlavný rozdiel je v tom, že kým ostatné vlastnosti zaručujú existenciu nejakej množiny, ktorá je explicitne popísaná pomocou nejakej vlastnosti prvkov tejto množiny, tu sa postuluje existencia výberovej množiny, ale takýto popis tejto množiny axióma výberu neposkytuje.

Táto odlišnosť a tiež to, že z axiómy výberu sa podarilo odvodiť niektoré zdanlivo dosť paradoxné výsledky viedli k tomu, že medzi matematikmi sa našli aj takí, ktorí tejto axióme nedôverovali, odmietali ju alebo sa snažili navrhnúť nejaké alternatívy, ktoré by ju nahradili.

Na druhej strane, ako sa budeme snažiť ilustrovať i v tejto kapitole, axiómu výberu používame vo viacerých veľmi základných a často používaných matematických výsledkoch. V našej matematickej praxi sme ju teda zvyknutí používať, preto môže pre nás byť práca v systéme ZF bez axiómy výberu pomerne neobvyklá. Veľmi ľahko sa môže stať, že si ani nevšimneme, že používame axiómu výberu. V tejto kapitole si budeme obzvlášť dávať pozor na to, či používame axiómu výberu, alebo nie. Pokiaľ pre nejaké tvrdenie máme aj dôkaz, ktorý ju nevyužíva, uprednostíme ho pred dôkazom založenom na axióme výberu. (V súčasnej matematike je dosť rozšíreným zvykom čitateľa upozorniť na použitie axiómy výberu.)

Z uvedených dôvodov vzniklo mnoho matematických prác, ktoré sa podrobne venujú tomu, aké výsledky je možné odvodiť bez axiómy výberu a pre aké je nevyhnutná. Takisto sa študuje mnoho slabších foriem axiómy výberu. Štúdium takéhoto typu problémov je jedna z oblastí teórie množín, ktorá sa v posledných rokoch teší veľmi živému záujmu.

Axióme výberu je venovaná veľmi rozsiahla literatúra, môžeme spomenúť napríklad knihy [He2, HR, J, M]. Uvedené knihy sú možno na prvé čítanie pomerne náročné, v prípade, že by ste sa o túto problematiku zaujímali hlbšie, možno by mohla byť pre vás zaujímavá kniha [B2], v ktorej sa striktne rozlišujú výsledky používajúce axiómu výberu a je tu napríklad odvodených viacero výsledkov, na ktoré stačí axióma výberu pre spočítateľný systém podmnožín nejakej spočítateľnej množiny. Niektoré úvahy o axióme výberu a jej možných alternatívach nájdete aj v [Z2]. Tieto knihy majú navyše tú výhodu, že sú v slovenčine. Stručný prehľad o axióme výberu a ordinálnych číslach podáva aj článok [Z1] (tiež v slovenčine).

Axióma výberu má dôležité aplikácie v mnohých oblastiach matematiky. V teórii množín je to napríklad už spomínaná porovnateľnosť ľubovoľných dvoch kardinalít, môžeme však spomenúť aj Hahn-Banachovu vetu, či Krein-Milmanovu vetu vo funkcionálnej analýze, Tichonovovu vetu vo všeobecnej topológii, existenciu algebraického uzáveru poľa v algebre. Po prečítaní tejto kapitoly by ste sa mohli (celkom oprávnene) pýtať na to, prečo som v nej uviedol len veľmi málo aplikácií axiómy výberu, keď tvrdím, že sa axióma výberu používa takmer v každom odvetví matematiky a má veľký význam. Dôvody sú dva. Jedným z nich je, že som sa snažil uviesť aplikácie, ktoré nevyžadujú príliš veľké znalosti z nejakej oblasti.

(Ak by som napríklad chcel ukázať Tichonovovu vetu – súčin kompaktných priestorov je opäť kompaktný – musel by som predtým ako prípravu povedať dosť veľa o topologických priestoroch všeobecne a špeciálne o kompaktných topologických priestoroch.) Druhý dôvod je ten, že niektoré dôsledky axiómy výberu si dokážeme až neskôr, keď sa naučíme používať transfinitnú indukciu.

6.1 Ekvivalentné formy axiómy výberu

Základnú formu axiómy výberu, ktorú sme uviedli v časti 2.3, môžeme preformulovať viacerými ekvivalentnými spôsobmi.

Na tomto mieste je snáď vhodné vysvetliť, že budeme v dôkazoch o ekvivalencii axiómy výberu s niektorými ďalšími tvrdeniami pracovať v ZF a nie v ZFC. Je to veľmi prirodzené – pokiaľ chceme ukázať, že axióma výberu je ekvivalentná s nejakým iným výrokom, musíme pracovať v systéme, ktorý túto axiómu neobsahuje.

Začnime tým, že pripomenieme, ako sme zaviedli axiómu výberu v časti 2.3:

Axióma VIII (Axióma výberu)**.**

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

Pre každý systém neprázdnych po dvoch disjunktných množín existuje výberová množina, t.j. taká množina, ktorá má s každou z množín tohoto systému jednoprvkový prienik.

Axióma výberu sa často zvykne označovať AC (z anglického „axiom of choice“).

Pomerne jednoducho vieme nájsť niekoľko príbuzných tvrdení, ktoré sú (v ZF) ekvivalentné s axiómou výberu. V ďalšom budeme vcelku bežne používať i časti (ii) a (iii) tvrdenia 6.1.2 používať pod pomenovaním axióma výberu.

Definícia 6.1.1. Nech $\mathcal{S}$ je množina. Zobrazenie $f\colon\mathcal{S}\to\bigcup\mathcal{S}$ sa nazýva *selektor* alebo tiež *výberová funkcia* na množine $\mathcal{S}$, ak platí

$$(\forall x\in\mathcal{S})f(x)\in x.$$

Pomenovanie výberová funkcia je pomerne prirodzené – je to funkcia, ktorá z každej množiny v $\mathcal{S}$ vyberá nejaký jej prvok.

{ekviv:TVRACEKVPROD}
{ekviv:itAC}
{ekviv:itSELDISJ}
{ekviv:itSEL}
{ekviv:itPROD}

Tvrdenie 6.1.2 (ZF)**.** *Nasledujúce podmienky sú ekvivalentné* (*ako tvrdenia ZF*)*:*

(i) *axióma výberu;*
(ii) *pre každý systém neprázdnych po dvoch disjunktných množín existuje selektor;*
(iii) *pre každý systém neprázdnych množín existuje selektor;*
(iv) *karteziánsky súčin ľubovoľného systému neprázdnych množín je neprázdny, t.j.*

$$(\forall i\in I)X_i\neq\emptyset\qquad\Rightarrow\qquad\prod_{i\in I}X_i\neq\emptyset;$$

{ekviv:itREL}

(v) *ak R je relácia medzi množinami A a B taká, že pre každé $a\in A$ existuje $b\in B$ s vlastnosťou aRb, tak existuje funkcia $f\colon A\to B$ taká, že $f\subseteq R$;*

{ekviv:itSURJ}

(vi) *ak $f\colon A\to B$ je surjekcia, tak existuje $g\colon B\to A$ také, že $f\circ g=id_B$.*

Dôkaz. (i) $\Rightarrow$ (ii): Ak $\mathcal{S}$ je systém neprázdnych po dvoch disjunktných množín, tak podľa (i) existuje množina V s vlastnosťou, že $V\cap A=\{x\}$ je jednoprvková množina pre každé $A\in\mathcal{S}$. Potom môžeme definovať funkciu f na množine $\mathcal{S}$ tak, že $f(A)$ je práve taký prvok

x, pre ktorý $x \in V \cap A$. Z toho, že $V \cap A$ je vždy jednoprvková množina vyplýva, že takto skutočne definujeme zobrazenie. Takisto vidíme, že platí $f(A) = x \in A$. Z toho, že $x \in A \in \mathcal{S}$ je zrejmé, že $f(A) = x$ je prvkom $\bigcup \mathcal{S}$, čiže ide skutočne o zobrazenie do množiny $\bigcup \mathcal{S}$.

(ii) $\Rightarrow$ (i): Ak $\mathcal{S}$ je systém neprázdnych po dvoch disjunktných množín a $f\colon \mathcal{S} \to \bigcup \mathcal{S}$ je selektor na $\mathcal{S}$, tak stačí položiť $V = \{f(A); A \in \mathcal{S}\}$. Očividne platí $V \cap A = \{f(A)\}$.

(ii) $\Rightarrow$ (iii): Nech $\mathcal{S}$ je ľubovoľný systém neprázdnych množín. Definujme $\mathcal{S}'$ ako

$$\mathcal{S}' = \{A \times \{A\}; A \in \mathcal{S}\}.$$

Potom $\mathcal{S}'$ je systém neprázdnych množín, ktoré sú navyše po dvoch disjunktné. (Ak totiž $A \times \{A\}$ a $B \times \{B\}$ obsahujú nejaký spoločný prvok, tak tento prvok je usporiadanou dvojicou a na druhej súradnici máme v jednom prípade A a v druhom B. To znamená, že $A = B$.)

Nech teraz f je selektor na množine $\mathcal{S}'$. Potom môžeme definovať zobrazenie $g\colon \mathcal{S} \to \bigcup \mathcal{S}$ takým spôsobom, že $g(A) = x$, kde x je taký prvok, pre ktorý $(x, A) = f(A)$. Potom máme $(x, A) \in A \times \{A\}$ a $x \in A$, čiže g je selektor. (Stručne by sme mohli napísať, že $g = p_1 \circ f$, kde p_1 označuje projekciu z $(\bigcup \mathcal{S}) \times \mathcal{S}$ na prvú súradnicu.)

(iii) $\Rightarrow$ (ii): Zrejmé.

(iii) $\Leftrightarrow$ (iv): Vyplýva priamo z definície karteziánskeho súčinu systému množín a definície selektora.

(iii) $\Rightarrow$ (v): Pre každé $a \in A$ označme $B_a = \{b \in B; aRb\}$. Systém $\{B_a; a \in A\}$ je systém neprázdnych množín a selektor f pre tento systém je funkcia s požadovanými vlastnosťami. (Pre každé $a \in A$ platí $f(a) \in B_a$, čiže $aRf(a)$, teda každá dvojica $(a, f(a))$ patrí do R, čo znamená, že $f \subseteq R$.)

(v) $\Rightarrow$ (iii): Nech $\mathcal{S}$ je ľubovoľná množina, označme $B := \bigcup \mathcal{S}$ a uvažujme reláciu $R := \{(A, x) \in \mathcal{S} \times B; x \in A\}$ medzi množinami $\mathcal{S}$ a B. Potom existuje funkcia $f\colon \mathcal{S} \to \bigcup \mathcal{S}$ s vlastnosťou, že pre všetky $A \in \mathcal{S}$ platí $(A, f(A)) \in R$, t.j. $f(A) \in A$. Táto funkcia je selektor na $\mathcal{S}$.

(ii) $\Rightarrow$ (vi): Túto implikáciu sme už dokázali v tvrdení 3.2.14.

(vi) $\Rightarrow$ (ii): Nech $\mathcal{S}$ je systém neprázdnych disjunktných množín. Definujme zobrazenie $f\colon \bigcup \mathcal{S} \to \mathcal{S}$ tak, že $f(x) = A$ ak $x \in A$. Tento predpis skutočne definuje zobrazenie, lebo vďaka disjunktnosti systému $\mathcal{S}$ každému x môžeme priradiť len jednu množinu. Z toho, že každé množina v $\mathcal{S}$ je neprázdna, vyplýva, že toto zobrazenie je surjektívne.

Potom existuje zobrazenie $g\colon \mathcal{S} \to \bigcup \mathcal{S}$ také, že $f(g(A)) = A$, čo znamená, že $g(A) \in A$. Teda g je selektor na $\mathcal{S}$. □

Uvedené tvrdenia boli v podstate len jednoduchými preformulovaniami axiómy výberu. Zvyšok tejto podkapitoly budeme venovať ďalším tvrdeniam, ktoré sú (v ZF) ekvivalentné s AC. Tieto tvrdenia sú v matematike veľmi často používané a preto snáď aj o čosi zaujímavejšie, než výsledky z predchádzajúceho tvrdenia; aj niektoré z dôkazov budú o dosť náročnejšie.

Ešte pred dokázaním najdôležitejšej vety tejto časti dokážeme lemu, ktorá sa nám bude viackrát hodiť v niektorých dôkazoch.

Definícia 6.1.3. Podmnožinu čiastočne usporiadanej množiny $(P, \leq)$, ktorá je usporiadaním $\leq$ lineárne usporiadaná, budeme nazývať *reťazec* v P.

{ekviv:LMCHAINOFPOSETS}

Lema 6.1.4. *Nech A je množina a $\mathcal{C} \neq \emptyset$ je systém čiastočných usporiadaní na množine A taký, že pre ľubovoľné $C, D \in \mathcal{C}$ platí $C \subseteq D$ alebo $D \subseteq C$. (Inak povedané, $\mathcal{C}$ je reťazec v množine všetkých relácií čiastočného usporiadania na A čiastočne usporiadanej reláciou $\subseteq$.) Potom $R := \bigcup \mathcal{C}$ je tiež čiastočné usporiadanie na A.*

Navyše, ak všetky čiastočné usporiadania v $\mathcal{C}$ sú lineárne, tak aj R je lineárne usporiadanie.

Dôkaz. Je očividné, že $R = \bigcup \mathcal{C}$ je relácia na A. Pre túto reláciu chceme overiť reflexívnosť, antisymetriu a tranzitívnosť.

Reflexívnosť. Nech $a \in A$. Keďže $\mathcal{C} \neq \emptyset$, existuje $C \in \mathcal{C}$. Relácia C je reflexívna, čiže $(a, a) \in C$. Potom aj $(a, a) \in R = \bigcup \mathcal{C}$.

Antisymetria. Nech $a, b \in A$. Nech platí $(a, b) \in R$ aj $(b, a) \in R$. To znamená, že existujú $C_{1,2} \in \mathcal{C}$ také, že $(a, b) \in C_1$ a $(b, a) \in C_2$. Podľa predpokladov lemy ale platí $C_1 \subseteq C_2$ alebo $C_2 \subseteq C_1$. Bez ujmy na všeobecnosti predpokladajme, že $C_1 \subseteq C_2$ (druhá možnosť je symetrická). Potom máme aj $(a, b) \in C_2$ a z antisymetrie relácie C_2 dostávame $a = b$.

Tranzitívnosť. Nech $a, b, c \in A$ a platí $(a, b) \in R$ aj $(b, c) \in R$. Potom existujú $C_{1,2} \in \mathcal{C}$ také, že $(a, b) \in C_1$ a $(b, c) \in C_2$. Opäť, bez ujmy na všeobecnosti, nech $C_1 \subseteq C_2$. Máme $(a, b) \in C_1 \subseteq C_2$ a $(b, c) \in C_2$. Z tranzitívnosti relácie C_2 dostaneme, že $(a, c) \in C_2$, a teda aj $(a, c) \in R$.

Teraz predpokladajme navyše, že všetky čiastočné usporiadanie patriace do $\mathcal{C}$ sú aj lineárne. Nech $a, b \in A$. Keďže $\mathcal{C} \neq \emptyset$, existuje aspoň jedno lineárne usporiadanie $C \in \mathcal{C}$. Prvky a a b sú v usporiadaní C porovnateľné, čiže platí $(a, b) \in C \vee (b, a) \in C$. Keďže $C \subseteq R$, máme potom aj $(a, b) \in R \vee (b, a) \in R$, čiže R je skutočne lineárne usporiadanie. □

{ekviv:VTEKVACWO}

Veta 6.1.5 (ZF)**.** *Nasledujúce podmienky sú (ako tvrdenia systému ZF) ekvivalentné s axiómou výberu:*

(WO) *Na každej množine existuje dobré usporiadanie.*

(PM) *Pre každý reťazec v čiastočne usporiadanej množine $(P, \leq)$ existuje maximálny reťazec, ktorý ho obsahuje.*

(ZL) *Ak každý reťazec v čiastočne usporiadanej množine $(P, \leq)$ má horné ohraničenie, tak $(P, \leq)$ má maximálny prvok.*

Tvrdenie WO sa zvykne nazývať *princíp dobrého usporiadania,* PM je *princíp maximality* (alebo tiež Hausdorffov princíp maximality) a ZL sa zvyčajne volá *Zornova lema.*

Ako budeme vidieť aj v tejto kapitole, pri použití princípu maximality a Zornovej lemy sa veľmi často ako čiastočné usporiadanie volí $\subseteq$.

{ekviv:POZNACEMPS}

Poznámka 6.1.6. Skôr než sa začneme venovať dôkazu ekvivalencie medzi uvedenými formami axiómy výberu, všimnime si, že všetky platia pre prázdnu množinu. To nám umožní v dôkazoch sa zaoberať už len netriviálnymi prípadmi.
AC: Selektor na prázdnom systéme množín je prázdne zobrazenie.
WO: Jediné možné čiastočné usporiadanie na $\emptyset$ je prázdna relácia $\emptyset$, ide o dobré usporiadanie prázdnej množiny.
PM: Ak $P = \emptyset$, tak jediný reťazec v P je prázdny reťazec. Čiže každý reťazec je obsiahnutý v prázdnom reťazci $\emptyset$.
ZL: Jediný možný reťazec $\emptyset$ nemá horné ohraničenie v $\emptyset$. Teda predpoklad implikácie je nepravdivý a implikácia uvedená v Zornovej leme platí.

Jednotlivé implikácie v dôkaze vety 6.1.5 dokážeme samostatne, najprv sa pozrieme na tú z nich, ktorá je najjednoduchšia.

Dôkaz implikácie WO $\Rightarrow$AC. Nech $\mathcal{S}$ je systém neprázdnych množín. Podľa WO existuje dobré usporiadanie $\leq$ na množine $\bigcup \mathcal{S}$. Zobrazenie f definované predpisom

$$f(A) = \min A,$$

t.j. každej množine z $\mathcal{S}$ priradíme jej najmenší prvok vzhľadom na usporiadanie $\leq$, je selektor na $\mathcal{S}$. (Pre každé $A \in \mathcal{S}$ existuje najmenší prvok, lebo ide o neprázdnu podmnožinu dobre usporiadanej množiny $(\bigcup \mathcal{S}, \leq)$.) □

Dôkaz implikácie ZL ⇒WO. Nech A je množina, chceme ukázať, že existuje dobré usporiadanie na A.

Nech P je systém všetkých dvojíc (B, R), kde $B \subseteq A$ a R je dobré usporiadanie na B. Na P zavedieme čiastočné usporiadanie

$$(B, R) \leq (B', R') \Leftrightarrow (B, R) \text{ je počiatočným úsekom } (B', R');$$

t.j. $B \subseteq B'$, R je zúžením relácie R' na množinu B a B má tú vlastnosť, že ak $b \in B$ a $b'R'b$, tak aj $b' \in B$.

Pomerne ľahko sa overí, že $\leq$ je čiastočné usporiadanie na P. Aby sme mohli použiť Zornovu lemu, musíme ešte ukázať, že každý reťazec v P má horné ohraničenie.

Nech $\mathcal{C}$ je reťazec v $(P, \leq)$. Položme

$$\overline{B} := \bigcup_{(B,R)\in\mathcal{C}} B,$$
$$\overline{R} := \bigcup_{(B,R)\in\mathcal{C}} R.$$

Inak povedané, $(\overline{B}, \overline{R})$ sme definovali tak, že sme zjednotili všetky prvky reťazca; relácia $\overline{R}$ na každej množine B splýva s príslušnou reláciou R. Očividne pre ľubovoľné $(B, R) \in \mathcal{C}$ platí $B \subseteq \overline{B}$ a $R \subseteq \overline{R}$. Ak teda ukážeme, že $(\overline{B}, \overline{R}) \in P$, tak $(\overline{B}, \overline{R})$ je horným ohraničením pre reťazec $\mathcal{C}$.

Je zrejmé, že $\overline{B} \subseteq A$, treba overiť, že $\overline{R}$ je dobré usporiadanie na $\overline{B}$. Z lemy 6.1.4 vieme, že $\overline{R}$ je čiastočné usporiadanie.

Ešte ukážme, že $(\overline{B}, \overline{R})$ je dobre usporiadaná množina. Nech A je neprázdna podmnožina $\overline{B}$. Z neprázdnosti vyplýva, že existuje $a \in A$ a z definície množiny $\overline{B}$ vyplýva, že existuje $(B, R) \in \mathcal{C}$ tak, že $a \in B$. Položme $m := \min_R(A \cap B)$, t.j. m je najmenší prvok množiny $A \cap B$ v usporiadaní R. (Takýto prvok existuje vďaka tomu, že (B, R) je dobre usporiadaná množina.) Tvrdíme, že potom m je najmenší prvok množiny a v usporiadaní $\overline{R}$.

Nech $a' \in A$. Keďže $A \subseteq \overline{B}$, existuje $(B', R') \in \mathcal{C}$ také, že $a' \in B'$. Pretože $\mathcal{C}$ je reťazec, jeho prvky (B, R) a (B', R') sú porovnateľné. Môžu nastať dva prípady:
Ak $(B', R') \leq (B, R)$, tak $B' \subseteq B$, čo znamená, že $a' \in A \cap B$, a teda mRa' (keďže m je najmenší prvok množiny $A \cap B$), čiže aj $m\overline{R}a'$.
Druhý možný prípad je $(B, R) \leq (B', R')$. Ak $a \in B$, tak môžeme bezo zmeny zopakovať úvahu z predchádzajúceho prípadu. Zostáva teda len prípad $a \in B' \setminus B$. Potom však nemôže platiť $aR'm$, lebo B je počiatočný úsek B' a z podmienky $m \in B$ by sme potom dostali aj $a \in B$. Keďže R' je lineárne usporiadanie, zostáva len druhá možnosť $mR'a$. To ale znamená, že $m\overline{R}a$.

Ukázali sme, že $(P, \leq)$ spĺňa predpoklady Zornovej lemy. Teda v $(P, \leq)$ existuje maximálny prvok, označme ho (B_0, R_0). Ak ukážeme, že $B_0 = A$, tak R_0 je dobré usporiadanie na A.

Sporom. Nech by $A \setminus B_0 \neq \emptyset$. Potom existuje $a \in A \setminus B_0$. Na množine $B_0 \cup \{a\}$ zadefinujeme reláciu $R = R_0 \cup (B_0 \cup \{a\}) \times \{a\}$, inak povedané, pre $x, y \in B_0 \cup \{a\}$

$$xRy \Leftrightarrow xR_0y \vee y = a.$$

Ľahko sa overí, že R je dobré usporiadanie na množine $B_0 \cup \{a\}$ a (B_0, R_0) je počiatočným úsekom $(B_0 \cup \{a\}, R)$, čiže

$$(B_0, R_0) < (B_0 \cup \{a\}, R).$$

To je ale spor s predpokladom, že (B_0, R_0) je maximálny prvok $(P, \leq)$. □

Napriek tomu, že implikácia ZL $\Rightarrow$ AC vyplýva z už dokázaných implikácií, rozhodli sme sa podať aj tento dôkaz, pretože je typickou ukážkou použitia Zornovej lemy. (Ako čiastočné usporiadanie sa použije inklúzia.)

Dôkaz implikácie ZL $\Rightarrow$AC. Nech R je relácia medzi množinami A a B taká, že pre každé $a \in A$ existuje aspoň jedno $b \in B$ s vlastnosťou aRb. Definujeme

$$P = \{f \colon A' \to B, A' \subseteq A, f \subseteq R\},$$

čiže P je množina všetkých zobrazení, ktorých definičný obor leží pod A' a ktoré sú podmnožinami R; a na tejto množine použijeme čiastočné usporiadanie $\subseteq$. Vieme, že $(P, \subseteq)$ je čiastočne usporiadaná množina.

Všimnime si, že ak pre zobrazenia $f \colon A_1 \to B$, $g \colon A_2 \to B$ platí $f \subseteq g$, tak aj $A_2 \subseteq A_2$.

Overme, že táto množina spĺňa predpoklady Zornovej lemy. Nech $\mathcal{C}$ je reťazec v $(P, \leq)$. Definujme

$$g := \bigcup_{f \in \mathcal{C}} f.$$

Ak ukážeme, že $g \in P$, tak g je očividne horným ohraničením reťazca $\mathcal{C}$.

Je zrejmé, že $g \subseteq R$. Treba teda už len overiť, že g je zobrazenie

Položme $D := \{a \in A; (\exists b \in B)(a, b) \in g\}$. Naším cieľom je ukázať, že pre $a \in D$ existuje jediné b s vlastnosťou $(a, b) \in g$.

Ak $(a, b) \in g$, znamená to, že existuje $f \in \mathcal{C}$ také, že $f(a) = b$. Ukážeme, že pre každé b' s vlastnosťou $(a, b') \in g$ platí $b' = b$. Z $(a, b') \in g$ máme existenciu $f' \in \mathcal{C}$ takého, že $f'(a) = b'$. Keďže $\mathcal{C}$ je reťazec, tak $f \subseteq f'$ alebo $f \subseteq f'$. Nech napríklad $f \subseteq f'$ (druhý možný prípad sa vyrieši analogicky). Potom $(a, b) \in f \subseteq f'$. Máme teda $(a, b) \in f'$ a súčasne $(a, b') \in f'$. Podľa definície zobrazenia ale ku každému a existuje iba jeden prvok s takouto vlastnosťou, a teda $b = b'$. Ukázali sme, že g je skutočne zobrazeníe.

Zatiaľ sme overili, že množina P spĺňa predpoklady Zornovej lemy. Potom ale táto množina má maximálny prvok. Označme ho f. Tvrdíme, že f je zobrazenie definované na celom A.

Dokážeme to sporom. Nech by f bolo definované na vlastnej podmnožine $A' \subsetneq A$. To znamená, že existuje $a_0 \in A \setminus A'$ a k tomuto a_0 existuje $b \in B$ také, že $a_0 R b$. Definujme zobrazenie $\overline{f}$ na množine $A' \cup \{a_0\}$ tak, že

$$\overline{f}(a) = \begin{cases} f(a) & a \in A', \\ b & a = a_0; \end{cases}$$

inak povedané $\overline{f}|_{A'} = f$ a $\overline{f}(a_0) = b$. Očividne $\overline{f} \in P$ a $f \subsetneq \overline{f}$. To je ale spor s predpokladom, že f je maximálny prvok $(P, \subseteq)$. □

Predchádzajúce dôkazy by nás mali presvedčiť, že Zornova lema je pomerne silným prostriedkom na dokazovanie – akonáhle si osvojíme metódu jej použitia, sú takéto dôkazy vcelku ľahké. (V odborných článkoch a pokročilejších textoch často nájdete napísané len „vyplýva z Zornovej lemy“.)

Teraz ukážeme, že Zornova lema a pricíp maximality sú ekvivalentné v ZF. Dôkaz implikácie ZL $\Rightarrow$ PM je veľmi podobný na použitie Zornovej lemy v predchádzajúcom dôkaze, snáď jediná komplikácia je to, že tu budeme pracovať s reťazcami reťazcov.

Dôkaz implikácie ZL $\Rightarrow$PM. Nech $(P, \leq)$ je čiastočne usporiadaná množina, $P \neq \emptyset$ a $\mathcal{C}$ je reťazec v P. Chceme ukázať, že existuje maximálny reťazec obsahujúci $\mathcal{C}$.

Bez ujmy na všeobecnosti môžeme predpokladať, že $\mathcal{C} \neq \emptyset$. Ak by totiž $\mathcal{C}$ bola prázdna množina, môžeme do nej pridať ľubovoľný prvok $p \in P$ a dokazovať ďalej tvrdenie pre reťazec

$\{p\}$. Z platnosti uvedeného tvrdenia pre tento jednoprvkový reťazec vyplýva aj jeho platnosť pre prázdny reťazec.

Označme

$$U = \{\mathcal{D}; \mathcal{D} \text{ je reťazec v } (P, \leq) \text{ a } \mathcal{D} \supseteq \mathcal{C}\},$$

čiže U je množina všetkých reťazcov v P, ktoré obsahujú C. Chceme použiť Zornovu lemu na čiastočne usporiadanú množinu $(U, \subseteq)$, potrebujeme teda overiť jej predpoklady – že každý reťazec v $(U, \subseteq)$ má horné ohraničenie.

Nech teda $\mathcal{R}$ je reťazec v U a $\mathcal{E} := \bigcup \mathcal{R}$. Ak ukážeme, že $\mathcal{E} \in U$, tak $\mathcal{E}$ je horné ohraničenie pre $\mathcal{R}$ v $(U, \subseteq)$.

Priamo z definície $\mathcal{E}$ je zrejmé, že $\mathcal{E} \supseteq \mathcal{C}$. Podľa lemy 6.1.4 je $\mathcal{E}$ reťazec.

Teda $(U, \subseteq)$ spĺňa predpoklady Zornovej lemy. Z nej potom vyplýva, že existuje maximálny prvok v U, čiže maximálny reťazec obsahujúci $\mathcal{C}$. □

Dôkaz implikácie PM ⇒ZL. Nech $(P, \leq)$ je čiastočne usporiadaná množina, kde každý reťazec má horné ohraničenie.

Potom reťazec $\emptyset$ je obsiahnutý v nejakom maximálnom reťazci $\mathcal{C}$. Nech m je horné ohraničenie reťazca $\mathcal{C}$. (Horné ohraničenie každého reťazca existuje podľa predpokladov Zornovej lemy). Tvrdíme, že m je potom maximálny prvok v $\mathcal{C}$.

Ukážeme to sporom. Ak by $m < m'$, tak $\mathcal{C} \cup \{m'\}$ by bol reťazec s vlastnosťou, $\mathcal{C} \cup \{m'\} \supsetneq \mathcal{C}$, teda reťazec $\mathcal{C}$ by nebol maximálny. □

Aby sme mali dokázanú ekvivalenciu všetkých podmienok uvedených vo vete 6.1.5, stačí nám už len dokázať AC ⇒ ZL, resp. AC ⇒ PM. Tento dôkaz uvedieme neskôr, v časti 7.6.2, keď budeme mať k dispozícii ako dôkazový prostriedok transfinitnú indukciu. Pre čitateľa, ktorý z nejakého dôvodu chce vidieť dôkaz bez použitia transfinitnej indukcie (či už z netrpezlivosti alebo preto, že sa rozhodne vynechať kapitolu o ordinálnych číslach a teda aj transfinitnú indukciu) môžeme odporučiť napríklad článok [Lew] alebo dôkaz uvedený v [Ha, Section 16].

6.2 Aplikácie axiómy výberu

Táto podkapitola sleduje dva hlavné ciele. Jedným z nich je ukázať, že v matematike bežne používame axiómu výberu, dokonca sme na to tak zvyknutí, že si to často ani nevšimneme. Druhým cieľom je ukázať na nejakých výsledkoch ukázať, že axióma výberu (alebo jej niektoré ekvivalentné formy) môžu byť užitočné pri dôkaze niektorých zaujímavých výsledkov. Na záver si ukážeme niektoré menej príjemné a trochu antiintuitívne dôsledky AC, ktoré by aspoň do istej miery mohli osvetliť, prečo táto axióma bola prijímaná s oveľa väčšou nedôverou, než ostatné axiómy.

Jeden príklad tvrdenia, ktoré poznáte z nižších ročníkov a jeho dôkaz využíva axiómu výberu, je existencia pravého inverzného zobrazenie k ľubovoľnej surjekcii – pozri tvrdenie 3.2.14(i). Dokonca sme v tvrdení 6.1.2(vi) ukázali, že v ZF je toto tvrdenie s axiómou výberu ekvivalentné. Ďalším príkladom takéhoto tvrdenia je ekvivalencia Cauchyho a Heineho definícia spojitosti.

6.2.1 Cauchyho a Heineho definícia spojitosti

Na úvod si pripomeňme definíciu spojitosti reálnej funkcie v bode:

Definícia 6.2.1 (Cauchyho definícia spojitosti)**.** Funkcia $f\colon \mathbb{R} \to \mathbb{R}$ je *spojitá* v bode $a \in \mathbb{R}$, ak

$$(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x \in \mathbb{R})|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

Spojitosť (a limita) reálnej funkcie v nejakom bode sa dá popísať aj pomocou konvergencie postupností.

Definícia 6.2.2 (Heineho definícia spojitosti)**.** Funkcia $f\colon \mathbb{R} \to \mathbb{R}$ je *sekvenciálne spojitá* v bode $a \in \mathbb{R}$, ak pre každú postupnosť $(x_n)_{n=0}^{\infty}$ reálnych čísel takú, že $\lim\limits_{n\to\infty} x_n = a$, platí $\lim\limits_{n\to\infty} f(x_n) = f(a)$.

Definícia sekvenciálne spojitej funkcie vlastne hovorí, že ak nejaká postupnosť $(x_n)_{n=0}^{\infty}$ reálnych čísel konverguje k a, tak postupnosť $(f(x_n))_{n=0}^{\infty}$ konverguje k $f(a)$. Voľne povedané, funkcia f zachováva konvergenciu postupností. Namiesto názvu „sekvenciálne spojitá“ sa často používa aj termín *spojitá v Heineho zmysle.*

Nasledujúce tvrdenie poznáte z matematickej analýzy. Na tomto mieste chceme zdôrazniť, na ktorom mieste dôkazu sa využíva AC.

Tvrdenie 6.2.3. *Nech $f\colon \mathbb{R} \to \mathbb{R}$ je ľubovoľná funkcia a $a \in \mathbb{R}$. Funkcia f je spojitá v bode a práve vtedy, keď je sekvenciálne spojitá v bode a.*

Dôkaz. $\boxed{\Rightarrow}$ Predpokladajme, že f je spojitá v bode a a $\lim\limits_{n\to\infty} x_n = a$. Priamo overením definície limity postupnosti ukážeme, že $\lim\limits_{n\to\infty} f(x_n) = f(a)$. Nech $\varepsilon > 0$ a nech $\delta > 0$ je také, že platí implikácia $|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon$. (Existencia takého δ vyplýva zo spojitosti f.) Potom z konvergencie postupnosti $(x_n)_{n=0}^{\infty}$ k číslu a vyplýva, že existuje n_0 také, že $n \geq n_0 \Rightarrow |x_n - a| < \delta$. Potom ale dostávame pre všetky $n \geq n_0$ platnosť nerovnosti

$$|f(x_n) - f(a)| < \varepsilon.$$

$\boxed{\Leftarrow}$ Budeme postupovať sporom. Predpokladajme, že funkcia f je sekvenciálne spojitá v bode a, ale nie je v tomto bode spojitá. Nespojitosť f v bode a znamená

$$(\exists \varepsilon > 0)(\forall \delta > 0)(\exists x \in \mathbb{R})|x - a| < \delta \wedge |f(x) - f(a)| \geq \varepsilon.$$

Špeciálne ak položíme $\delta_n = \frac{1}{n}$ tak máme pre každé n zaručenú existenciu čísla $x \in \mathbb{R}$ takého, že $|x - a| < \frac{1}{n}$ a súčasne $|f(x) - f(a)| \geq \varepsilon$. (Inak povedané, pre každé $n \in \mathbb{N}$ je množina $A_n = \{x \in \mathbb{R}; |x - a| < \frac{1}{n} \wedge |f(x) - f(a)| \geq \varepsilon\}$ neprázdna.) Pre každé n nejaké také x vyberieme a označíme ho x_n. (Formálnejšie: Postupnosť x_n definujeme ako selektor na množine $\{A_n; n \in \mathbb{N}\}$.)

Potom pre túto postupnosť platí $\lim\limits_{n\to\infty} x_n = a$ a súčasne $(\forall n \in \mathbb{N})|f(x_n) - f(a)| \geq \varepsilon$, čo znamená, že $f(x_n)$ nekonverguje k $f(a)$, čím dostávame hľadaný spor. □

Uvedené tvrdenie hovorí o spojitosti funkcie v bode. Pokiaľ by sme sa zaoberali spojitosťou funkcie $f\colon \mathbb{R} \to \mathbb{R}$ na celom $\mathbb{R}$, tak ekvivalencia Cauchyho a Heineho definície platí už v ZF [He2, Theorem 3.15]. Dôkaz je však o niečo náročnejší v porovnaní s dôkazom, ktorý sme tu uviedli pre spojitosť v bode. Tento výsledok pochádza od W. Sierpińskeho. [1]

Z platnosti ekvivalencie uvedených dvoch definícií spojitosti pre reálne funkcie v bode už vyplýva platnosť axiómy výberu pre spočítateľné systémy podmnožín $\mathbb{R}$ (t.j. pre každý systém $\{A_i \in \mathcal{P}(\mathbb{R}); i \in \mathbb{N}\}$ neprázdnych množín existuje výberová funkcia) [He1, Theorem 1.1], [He2, Theorem 4.54].

[1] Pozri aj `http://thales.doa.fmph.uniba.sk/sleziak/texty/rozne/AC/cont.pdf`

6.2.2 Hamelova báza

Hamelova báza je istým zovšeobecnením pojmu bázy, ktorý poznáte z prvého ročníka pre konečnorozmerné vektorové priestory. Ukážeme, že Hamelova báza existuje pre ľubovoľný vektorový priestor.

Zaradenie dôkazu existencie Hamelovej bázy je motivované viacerými dôvodmi. Tento dôkaz predstavuje typické použitie Zornovej lemy. (V drvivej väčšine prípadov sú dôkazy využívajúce Zornovu lemu „na jedno kopyto“. Takže ak zvládnete niekoľko aplikácií, ľahko takýto dôkazu budete vedieť urobiť v iných situáciach vhodných na využitie Zornovej lemy.) Ďalší dôvod je jeho elementárnosť – okrem poznatkov z tejto prednášky úplne pri dôkaze vystačíme s tým, čo vieme z prváckej lineárnej algebry. A zaujímavé je aj to, že z existencie Hamelovej bázy budeme vedieť odvodiť niektoré zaujímavé výsledky.

Definícia 6.2.4. Nech V je vektorový priestor nad poľom F.

Podmnožinu $A \subseteq V$ nazývame *lineárne nezávislou* podmnožinou, ak ľubovoľný konečný počet vektorov z A tvorí lineárne nezávislý systém vektorov, čiže pre ľubovoľné $n \in \mathbb{N}$, $c_1, \dots, c_n \in F$ a $\vec{\alpha}_1, \dots, \vec{\alpha}_n \in A$ platí

$$c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = \vec{0} \qquad \Rightarrow \qquad c_1 = \cdots = c_n = 0.$$

Hovoríme, že podmnožina $A \subseteq V$ *generuje* priestor V, ak každý vektor z A sa dá napísať ako lineárna kombinácia (konečného počtu) vektorov z A, t.j. pre každé $\vec{\alpha} \in V$ existujú $n \in \mathbb{N}$, $c_1, \dots, c_n \in F$ a $\vec{\alpha}_1, \dots, \vec{\alpha}_n \in A$ také, že

$$\vec{\alpha} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n.$$

Označujeme $[A] = V$.

Podmnožina A sa nazýva *Hamelova báza* priestoru V, ak je lineárne nezávislá a $[A] = V$.

Uvedené pojmy sú pomerne prirodzeným zovšeobecnením lineárnej nezávislosti a generujúcej množiny ako sme ich definovali v konečnorozmernom prípade.

Úplne rovnakým spôsobom, ako ste to dokázali pre bázu konečnorezmerného vektorového priestoru v prvom ročníku, sa dá overiť, že B je Hamelova báza priestoru V práve vtedy, keď každý vektor $\vec{\alpha}$ sa dá jednoznačne zapísať v tvare $\vec{\alpha} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n$.

Príklad 6.2.5. Pre niektoré konkrétne priestory vieme explicitne popísať Hamelovu bázu. Už sme spomenuli, že v prípade konečnorozmerných vektorových priestorov je to presne pojem bázy, ktorý poznáte z prvého ročníka.

Ukážme si aspoň jeden príklad priestoru, ktorého báza je nekonečná.

Nech F je množina všetkých postupností reálnych čísel, ktoré majú iba konečne veľa nenulových hodnôt. (Inak povedané, postupnosť $(x_n)_{n=0}^{\infty}$ patrí do množiny F práve vtedy, keď existuje n_0 také, že $x_n = 0$ pre každé $n \geq n_0$.) Sčitovanie a násobenie skalárom zadefinujeme obvyklým spôsobom t.j. súčet postupností $(x_n)_{n=0}^{\infty}$ a $(y_n)_{n=0}^{\infty}$ je postupnosť

$$(x_n + y_n)_{n=0}^{\infty}$$

a c-násobok postupnosti $(x_n)_{n=0}^{\infty}$ je postupnosť $(cx_n)_{n=0}^{\infty}$.

Ľahko sa overí, že F s týmito operáciami tvorí vektorový priestor. Nulovým vektorom je konštantná postupnosť pozostávajúca zo samých núl.

Báza tohoto priestoru je $B = \{e^{(n)}; n \in \mathbb{N}\}$, kde postupnosť $e^{(n)}$ je zložená zo samých núl, iba na n-tom mieste má jednotku;

$$e_k^{(n)} = \begin{cases} 1 & n = k, \\ 0 & n \neq k. \end{cases}$$

Táto množina je skutočne lineárne nezávislá; ak totiž

$$c_1 e^{(i_1)} + \cdots + c_k e^{(i_k)} = 0,$$

tak postupnosť na ľavej strane rovnosti má na i_j-tom mieste hodnotu c_j, čiže z uvedenej rovnosti vyplýva $c_j = 0$. Dostali sme, že $c_1 = \cdots = c_k = 0$.

Takisto je vcelku ľahko vidieť, že ak $x_n = 0$ pre $n \geq n_0$, tak $(x_n)_{n=0}^{\infty}$ vieme dostať ako lineárnu kombináciu postupností e_i, $i = 0, \ldots, n_0 - 1$.

Existencia Hamelovej bázy pre ľubovoľný vektorový priestor vyplynie z nasledujúceho výsledku, ktorý pre konečnorozmerný prípad poznáte z prvého ročníka. Táto veta hovorí, že každá lineárne nezávislá množina sa dá rozšíriť na bázu.

Veta 6.2.6. *Nech V je vektorový priestor nad poľom F a A je lineárne nezávislá podmnožina V. Potom existuje Hamelova báza B taká, že $A \subseteq B$.*

Dôkaz. Použijeme Zornovu lemu pre množinu

$$P = \{C \subseteq V; A \subseteq C, C \text{ je lineárne nezávislá}\}$$

čiastočne usporiadanú inklúziou.

Najprv overme, že $(P, \subseteq)$ spĺňa predpoklady Zornovej lemy. Nech $\mathcal{R}$ je ľubovoľný reťazec v P. Tvrdíme, že potom $D = \bigcup \mathcal{R} \in P$, čo znamená, že D je horným ohraničením reťazca $\mathcal{R}$.

Inklúzia $D \supseteq A$ je zrejmá, treba overiť len lineárnu nezávislosť množiny D. Ak máme nejaký konečný počet vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in D$, tak pre každé $\vec{\alpha}_i$ existuje $C_i \in \mathcal{R}$ tak, že $\vec{\alpha}_i \in C_i$. Keďže množina $\{C_i; i = 1, \ldots, n\}$ je konečná lineárne usporiadaná množina, existuje i_0 také, že $C_{i_0} = \bigcup_{i=1}^{n} C_i$, a teda $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in C_i$. Pretože C_i je lineárne nezávislá množina, vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé.

Podľa Zornovej lemy existuje teda množina B, ktorá je maximálnym prvkom čiastočne usporiadnej množiny $(P, \subseteq)$. Ukážeme, že táto množina je Hamelovou bázou priestoru V.

Priamo z toho, že $B \in P$, vyplýva, že B je lineárne nezávislá množina. Chceme ukázať ešte, že B generuje V. Postupujme sporom. Nech by existoval vektor $\vec{\alpha} \notin [B]$, t.j. $\vec{\alpha}$ sa nedá napísať ako lineárna kombinácia vektorov z B. Stačí ukázať, že množina $B \cup \{\vec{\alpha}\}$ je tiež lineárne nezávislá, pretože tým dostaneme spor s predpokladom, že B je maximálny prvok množiny $(P, \subseteq)$.

Nech teda platí

$$c\vec{\alpha} + c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = \vec{0},$$

pre nejaké $c, c_1, \ldots, c_n \in F$ a $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in B$. Ak $c = 0$, tak aj $c_1 = \cdots = c_n = 0$, pretože množina B je lineárne nezávislá. V prípade, že $c \neq 0$ však dostaneme

$$\vec{\alpha} = -c_1 c^{-1}\vec{\alpha}_1 - \cdots - c_n c^{-1}\vec{\alpha}_n,$$

čiže $\vec{\alpha}$ je lineárnou kombináciou vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in B$, a teda $\vec{\alpha} \in [B]$. Predpoklad, že $c \neq 0$ teda vedie k sporu s predpokladom $\vec{\alpha} \notin [B]$. □

Ukážeme si tiež, že – podobne ako v konečnorozmernom prípade – ľubovoľné dve Hamelove bázy vektorového priestoru majú rovnakú kardinalitu.

Tvrdenie 6.2.7. *Nech V je vektorový priestor nad poľom F. Nech $B_{1,2}$ sú Hamelove bázy priestoru V. Potom $|B_1| = |B_2|$.*

Dôkaz. Ak niektorá z týchto báz je konečná, znamená to, že priestor V je konečnorozmerný. V tomto prípade ide o vetu, ktorú poznáte z prváckej lineárnej algebry [Sl2]. Budeme sa zaoberať teda len prípadom, že B_1 aj B_2 sú nekonečné.

Z definície Hamelovej bázy vyplýva, že pre každé $\vec{\alpha} \in B_1$ existuje jednoznačne určená konečná množina $B_2(\vec{\alpha})$ vektorov z B_2, ktorých lineárnou kombináciou je $\vec{\alpha}$. (Existencia vyplýva z toho, že $\vec{\alpha} \in [B_2]$. Jednoznačnosť je dôsledkom lineárnej nezávislosti B_2.)

Najprv ukážeme, že pre každé $\vec{\beta} \in B_2$ existuje také $\vec{\alpha} \in B_1$, že $\vec{\beta} \in B_2(\vec{\alpha})$.

Nech by to tak nebolo, teda $\vec{\beta} \notin B_2(\vec{\alpha})$ pre každé $\vec{\alpha} \in B_1$. Potom $B_1 \subseteq [B_2 \setminus \{\vec{\beta}\}]$. Keďže B_1 je báza, tak potom $[B_2 \setminus \{\vec{\beta}\}] = X$, a teda $\vec{\beta}$ je lineárna kombinácia prvkov z $B_2 \setminus \{\vec{\beta}\}$. Ukázali sme, že B_2 nie je lineárne nezávislá, čo je spor s predpokladom, že je to Hamelova báza.

Máme teda ukázané $(\forall \vec{\beta} \in B_2)(\exists \vec{\alpha} \in B_1)\vec{\beta} \in B_2(\vec{\alpha})$. Platí potom $B_2 = \bigcup_{\vec{\alpha} \in B_1} B_2(\vec{\alpha})$. Pre kardinality dostávame $|B_2| = |(\bigcup_{\vec{\alpha} \in B_1} B_2(\vec{\alpha}))| \leq |B_1|.\aleph_0 = |B_1|$ (v poslednej rovnosti sme využili, že $|B_1|$ je nekonečná.[2])

Rovnakým spôsobom ako $|B_2| \leq |B_1|$ môžeme ukázať nerovnosť $|B_1| \leq |B_2|$. Z týchto dvoch nerovností (podľa Cantor-Bernsteinovej vety) dostaneme $|B_2| = |B_1|$. □

Cauchyho funkcionálna rovnica

Cauchyho funkcionálnou rovnicou nazývame rovnicu

{aplik:EQCAUCHY}
$$(\forall x, y \in \mathbb{R}) f(x+y) = f(x) + f(y), \tag{6.1}$$

kde f je funkcia z $\mathbb{R}$ do $\mathbb{R}$.

Termín funkcionálna rovnica používame preto, že v tomto prípade je neznámou funkcia. Inak povedané, $f\colon \mathbb{R} \to \mathbb{R}$ je riešením tejto funkcionálnej rovnice, ak spĺňa podmienku (6.1). Viacero riešení tejto rovnice vieme uhádnuť. Napríklad funkcia $f(x) = 0$ ako aj každá lineárna funkcia $f(x) = ax$ pre $a \in \mathbb{R}$ tejto rovnici vyhovujú. Otázka je, či sú to už všetky riešenia. Najprv si ukážeme, že za istých dodatočných podmienok má skutočne každé riešenie tvar lineárnej funkcie.

Vo viacerých dôkazoch nám pomôže táto úvaha.

{aplik:LMQLIN}
Lema 6.2.8. *Ak f je riešenie funkcionálnej rovnice* (6.1)*, tak*

{aplik:EQLINEAR}
$$(\forall r \in \mathbb{Q})(\forall x \in \mathbb{R}) f(rx) = rf(x) \tag{6.2}$$

Dôkaz. Ak položíme $x = y = 0$ v (6.1), tak dostaneme $f(0) = f(0) + f(0)$, čiže $f(0) = 0$.

Z (6.1) dostávame $f(2x) = 2f(x)$ pre $x = y$. Matematickou indukciou pre každé $n \in \mathbb{N}$ dostaneme

$$f(nx) = nf(x)$$

pre ľubovoľné $x \in \mathbb{R}$

Ďalej ak položíme v (6.1) $y = -x$, tak máme $f(x) + f(-x) = 0$, čiže

$$f(-x) = -f(x).$$

Vďaka tomu rovnosť $f(zx) = zf(x)$ pre všetky $z \in \mathbb{Z}$, $x \in \mathbb{R}$.

[2] Využívame rovnosť $a.b = \max\{a, b\}$ platnú pre nekonečné kardinály, ktorú dokážeme v časti 7.6.1.

Nech teraz $r = \frac{p}{q}$ je ľubovoľné racionálne číslo ($p \in \mathbb{Z}$, $q \in \mathbb{N} \setminus \{0\}$). Potom máme

$$qf\left(\frac{px}{q}\right) = f(px) = pf(x)$$
$$f\left(\frac{px}{q}\right) = \frac{p}{q}f(x)$$
$$f(rx) = rf(x)$$

pre ľubovoľné $r \in \mathbb{Q}$, $x \in \mathbb{R}$. □

{aplik:TVRCAUCHYSPOJ}

Tvrdenie 6.2.9. *Ak f je spojité riešenie funkcionálnej rovnice* (6.1)*, tak $f(x) = ax$ pre nejaké $a \in \mathbb{R}$.*

Dôkaz. Nech $x \in \mathbb{R}$ a (q_n) je postupnosť racionálnych čísel, ktorá konverguje k x. (Taká postupnosť existuje pre každé reálne číslo.) Označme $f(1) = a$.

Podľa lemy 6.2.8 platí

$$f(q_n) = q_n f(1) = q_n a$$

a zo spojitosti f dostaneme

$$f(x) = \lim_{n\to\infty} f(q_n) = \lim_{n\to\infty} q_n a = az.$$

□

Toto tvrdenie sa dá o trochu vylepšiť – stačí dokonca spojitosť funkcie f v jednom bode.

Tvrdenie 6.2.10. *Ak f je riešenie funkcionálnej rovnice* (6.1) *a f je spojité v nejakom bode $x_0 \in \mathbb{R}$, tak f je spojité na celom $\mathbb{R}$, a teda f má tvar $f(x) = ax$ pre nejaké $a \in \mathbb{R}$.*

Dôkaz. Nech $x \in \mathbb{R}$. Ukážeme, že f je spojité v bode x.

Majme $\varepsilon > 0$. Potom existuje $\delta > 0$ také, že $|y - x_0| < \delta \Rightarrow |f(y) - f(x_0)| < \varepsilon$.

Nech $|y' - x| < \delta$ a označme $d := y' - x$. Potom $f(y') = f(x) + f(d)$, čiže nám stačí ukázať, že $|f(d)| < \varepsilon$.

Súčasne platí $|(x_0 + d) - x_0| < \delta$, teda aj $|f(x_0 + d) - f(x_0)| < \varepsilon$. Z (6.1) však dostaneme $f(x_0 + d) = f(x_0) + f(d)$, čiže

$$|f(d)| = |f(x_0 + d) - f(x_0)| < \varepsilon.$$

□

{aplik:TVRCAUCHYOHR}

Tvrdenie 6.2.11. *Ak funkcia $f\colon \mathbb{R} \to \mathbb{R}$ vyhovuje rovnici* (6.1) *a je ohraničená na nejakom netriviálnom intervale I, tak $f(x) = ax$ pre nejaké $a \in \mathbb{R}$.*

Dôkaz. Môžeme predpokladať, že interval I je ohraničený interval tvaru $I = \langle b, c\rangle$.

Označme $a = f(1)$. Nech $g(x) = f(x) - ax$. Funkcia g tiež spĺňa rovnicu (6.1) a je ohraničená na intervale I. Navyše však platí $g(1) = 0$ a z lemy 6.2.8 potom dostaneme $f(r) = 0$ pre každé racionálne číslo $r \in \mathbb{Q}$.

Pre ľubovoľné reálne číslo x existuje racionálne číslo rv intervale $\langle x - c, x - b\rangle$. Potom $x - r \in \langle b, c\rangle$ a

$$g(x) = g(x - r) + g(r) = g(x - r).$$

Zistili sme teda, že funkcia g je ohraničená na celom $\mathbb{R}$. Z toho už ale vyplýva, že $g(x) = 0$ pre každé $x \in \mathbb{R}$. (Ak by existovalo x_0 také, že $g(x_0) \neq 0$, tak postupnosť $|g(nx_0)| = n|g(x_0)|$ je neohraničená.)

Pre každé $x \in \mathbb{R}$ teda platí rovnosť

$$g(x) = f(x) - ax = 0,$$

čo znamená, že $f(x) = ax$. □

{aplik:TVRCAUCHYMONOT}

Tvrdenie 6.2.12. *Ak f je monotónne riešenie funkcionálnej rovnice* (6.1)*, tak $f(x) = ax$ pre nejaké $a \in \mathbb{R}$.*

Dôkaz. Označme $f(1) = a$

Nech napríklad f je neklesajúca. (Prípad, že f je nerastúca, sa dá riešiť podobne alebo previesť na tento prípad prechodom k opačnej funkcii.) Pre každé reálne číslo x existuje rastúca postupnosť racionálnych čísel $(r_n)_{n=0}^{\infty}$, ktorá konverguje k x zdola a klesajúca postupnosť racionálnych čísel $(s_n)_{n=0}^{\infty}$, ktorá konverguje k x zhora. Potom platí

$$\begin{gathered}(\forall n \in \mathbb{N}) f(r_n) \leq f(x) \leq f(s_n) \\ \lim_{n\to\infty} f(r_n) \leq f(x) \leq \lim_{n\to\infty} f(s_n) \\ \lim_{n\to\infty} ar_n \leq f(x) \leq \lim_{n\to\infty} as_n \\ ax \leq f(x) \leq ax.\end{gathered}$$

Zistili sme, že pre každé $x \in \mathbb{R}$ platí $f(x) = f(ax)$. □

Ďalší výsledok podobného typu je, že každá merateľná funkcia, ktorá je riešením (6.1), musí byť tvaru $f(x) = ax$. Toto tvrdenie nebudeme dokazovať, pekný dôkaz sa dá nájsť v [He2, Theorem 5.4].

S využitím Hamelovej bázy však vieme dokázať i existenciu riešení, ktoré nie sú lineárne.

Veta 6.2.13 (AC)**.** *Existujú nelineárne riešenia rovnice* (6.1) (*t.j. riešenia, ktoré nie sú tvaru $f(x) = ax$*)*.*

Budeme pracovať s vektorovým priestorom $V = \mathbb{R}$ nad poľom $\mathbb{Q}$. Všimnime si, že lineárne zobrazenie z V do V je presne zobrazenie, ktoré spĺňa rovnosti (6.1) a (6.2). Pretože v tomto dôkaze pojem lineárna funkcia (lineárne zobrazenie) používame v dvoch významoch – raz ako pomenovanie funkcií z $\mathbb{R}$ do $\mathbb{R}$ tvaru $f(x) = ax$ a raz pre funkcie, ktoré zachovávajú sčitovanie a násobenie skalárom z $\mathbb{Q}$, čiže pre linearitu v priestore V – dohodnime sa, že v prvom prípade budeme hovoriť o $\mathbb{R}$-lineárnej funkcii a v druhom prípade budeme používať termín $\mathbb{Q}$-*lineárna funkcia* alebo $\mathbb{Q}$-*lineárne zobrazenie*, aby sme predišli možným zmätkom.

Dôkaz. Už sme ukázali, že funkcia $f\colon \mathbb{R} \to \mathbb{R}$ je riešením rovnice (6.1) práve vtedy, keď f je $\mathbb{Q}$-lineárna funkcia z V do V.

Nech teraz B je ľubovoľná Hamelova báza priestoru V a $b \in B$ je jej ľubovoľný prvok. Ak zvolíme $f(b) = 1$ a $f(b') = 0$ pre $b' \in B \setminus \{b\}$, tak je tým jednoznačne určené $\mathbb{Q}$-lineárne zobrazenie $f\colon V \to V$. (Každý prvok $x \in \mathbb{R}$ sa dá jednoznačne vyjadriť ak $x = c_1b_1 + \cdots + c_nb_n$, kde $c_1, \ldots, c_n \in \mathbb{Q}$ a $b_1, \ldots, b_n \in B$. Z $\mathbb{Q}$-linearity f už dostávame jednoznačne určený obraz $f(x) = c_1f(b_1) + \cdots + c_nf(b_n)$. Týmto predpisom je teda definované zobrazenie f, o ktorom sa ľahko overí, že je skutočne $\mathbb{Q}$-lineárne.) Takéto f je riešením rovnice (6.1).

Všimnime si tiež, že $B \setminus \{b\} \neq \emptyset$. Ak by totiž platilo $B = \{b\}$, t.j. Hamelova báza $\mathbb{R}$ ako vektorového priestoru nad $\mathbb{Q}$ by bola jednoprvková, tak by každé reálne číslo bolo vyjadriteľné v tvare $q.b$ pre nejaké $q \in \mathbb{Q}$, čiže reálnych čísel by bolo spočítateľne veľa.

Z toho vidíme, že existujú $b, b' \neq 0$ také, že $f(b) \neq 0$ a súčasne $f(b') = 0$, čo znamená, že funkcia f nie je $\mathbb{R}$-lineárna. □

Pridajme si ešte jeden výsledok ukazujúci, že nespojité riešenia (6.1) majú pomerne patologické vlastnosti. Môžeme si všimnúť, že z nasledujúceho výsledku vyplývajú tvrdenia 6.2.12 a 6.2.11 ako jednoduché dôsledky.

Tvrdenie 6.2.14. *Ak $f\colon \mathbb{R} \to \mathbb{R}$ je nespojité riešenie* (6.1)*, tak graf tejto funkcie*

$$G(f) = \{(x, f(x)); x \in \mathbb{R}\}$$

je hustá podmnožina $\mathbb{R}^2$.

Pripomeňme, že A je hustá podmnožina $\mathbb{R}^2$, ak pre ľubovoľné reálne čísla x_0, y_0 a $\varepsilon > 0$ existuje nejaký prvok $(x, y) \in A$ taký, že $|x - x_0| < \varepsilon$ a $|y - y_0| < \varepsilon$. (Množina $\{(x, y) \in \mathbb{R}; |x - x_0| < \varepsilon \wedge |y - y_0| < \varepsilon\}$ je presne guľa s polomerom ε okolo (x_0, y_0) pri metrike $d((x, y), (x', y')) = \max|x - x'|, |y - y'|$. Táto metrika dáva na $\mathbb{R}^2$ obvyklú euklidovskú topológiu. Nasledujúci dôkaz by sa prakticky nezmenil keby sme si zvolili niektorú z ostatných bežne používaných metrík.)

Dôkaz. Ak f je nespojité riešenie (6.1), tak podľa tvrdenia 6.2.9 nemôže mať tvar $f(x) = ax$, čiže nemôže platiť, že $\frac{f(x)}{x}$ je konštanta. To znamená. že existujú body $x_{1,2} \in \mathbb{R}$ také, že

$$\frac{f(x_1)}{x_1} \neq \frac{f(x_2)}{x_2}.$$

Z $\frac{f(x_1)}{x_1} - \frac{f(x_2)}{x_2} = \frac{f(x_1)x_2 - x_1 f(x_2)}{x_1 x_2} \neq 0$ vidíme, že nasledujúci determinant je nenulový:

$$\begin{vmatrix} x_1 & f(x_1) \\ x_2 & f(x_2) \end{vmatrix} \neq 0.$$

To znamená, že vektory $(x_1, f(x_1))$ a $(x_2, f(x_2))$ sú lineárne nezávislé, čiže tvoria bázu vektorového priestoru $\mathbb{R}^2$. (Teraz už $\mathbb{R}^2$ chápeme ako vektorový priestor nad $\mathbb{R}$, tak ako obvykle.)

Na to, aby sme ukázali, že $G(f)$ je hustá množina, úplne stačí, ak sa nám podarí ukázať, že pre ľubovoľné $x_0, y_0 \in \mathbb{R}$ a $\varepsilon > 0$ existuje nejaký bod $(x, f(x)) \in G(f)$ taký, že $|x - x_0| < \varepsilon$ a $|f(x) - f(x_0)| < \varepsilon$.

Zvoľme si teda ľubovoľné $\varepsilon > 0$ a bod (x_0, y_0).

Pretože $(x_1, f(x_1))$ a $(x_2, f(x_2))$ tvoria bázu, existujú reálne konštanty a, b tak, že

$$a(x_1, f(x_1)) + b(x_2, f(x_2)) = (x_0, y_0).$$

Ak zvolíme racionálne čísla $a', b' \in \mathbb{Q}$ dostatočne blízko k číslam a a b, tak vieme dosiahnuť, že bod $a'(x_1, f(x_1)) + b'(x_2, f(x_2))$ bude dostatočne blízko[3] k (x_0, y_0), t.j. $|a'x_1 + b'x_2 - x_0| < \varepsilon$ a $|a'f(x_1) + b'f(x_2) - y_0| < \varepsilon$.

Označme $x = a'x_1 + b'x_2$. Použitím (6.1) a (6.2) dostaneme

$$f(x) = f(a'x_1 + b'x_2) = f(a'x_1) + f(b'x_2) = a'f(x_1) + b'f(x_2).$$

Vidíme teda, že bod $(a'x_1 + b'x_2, a'f(x_1) + b'f(x_2)) = (x, f(x))$ patrí do množiny $G(f)$. □

[3]Pokiaľ chcete, môžete sa pokúsiť vyjadriť, čo presne znamená „dostatočne blízko“. Snáď sa ale uspokojíte i s takým argumentom, že ide vlastne o lineárne zobrazenie v premenných a, b a každé lineárne zobrazenie z $\mathbb{R}^2$ do $\mathbb{R}^2$ je spojité. Pri spojitom zobrazení malá zmena parametra znamená malú zmenu hodnoty.

6.2.3 Linearizácia čiastočne usporiadanej množiny

{aplik:TVRLINI

Tvrdenie 6.2.15. *Pre každú čiastočne usporiadanú množinu* $(A, \leq)$ *existuje* linearizácia $(A, \preceq)$*, t.j. také lineárne usporiadanie na množine* A*, že pre ľubovoľné* $a, b \in A$ *platí*

$$a \leq b \qquad \Rightarrow \qquad a \preceq b.$$

(*Inak povedané, relácia* $\preceq$ *obsahuje reláciu* $\leq$*; t.j.* $\leq \subseteq \preceq$.)

Dôkaz. Uvažujme množinu všetkých čiastočných usporiadaní R na A, ktoré obsahujú $\leq$. Túto množinu označme P a ako čiastočné usporiadanie použijeme $\subseteq$.

Najprv overme, že $(P, \subseteq)$ spĺňa predpoklady Zornovej lemy. Nech $\mathcal{C}$ je ľubovoľný reťazec v $(P, \subseteq)$; položme $\overline{R} = \bigcup C$. Podľa lemy 6.1.4 je $\overline{R}$ čiastočné usporiadanie na A a očividne $\overline{R}$ obsahuje $\leq$. Teda $\overline{R} \in P$ a je to horné ohraničenie reťazca $\mathcal{C}$.

Potom existuje maximálny prvok v $(P, \subseteq)$, označme ho $\preceq$. Z definície P vyplýva, že $\preceq$ je čiastočné usporiadanie, ukážeme, že toto čiastočné usporiadanie je lineárne.

Sporom. Nech by prvky $a, b \in A$ neboli porovnateľné vzhľadom na $\preceq$. Definujme reláciu

$$\preceq' = \preceq \cup \{(c, d) \in A \times A; (c \preceq a) \wedge (b \preceq d)\}.$$

(Intuícia za touto definíciou je taká, že sme pridali dvojicu (a, b) a všetky ďalšie dvojice, ktoré si vynúti tranzitívnosť.)

Ukážeme, že $\preceq'$ je čiastočné usporiadanie na A. Akonáhle budeme mať dokázaný tento fakt, tak dostávame spor s tým, že $\preceq$ je maximálny prvok P, lebo $\preceq'$ je prvok P, ktorý je od neho ostro väčší v usporiadaní inklúziou.

Overme teda, že $\preceq'$ je čiastočné usporiadanie. *Reflexívnosť* platila už pre menšiu reláciu $\preceq$, čiže platí aj pre $\preceq'$.

Antisymetria. Nech $x \preceq' y$ aj $y \preceq' x$. Rozoberieme jednotlivé možnosti:
a) Ak $x \preceq y$ a $y \preceq x$; potom $x = y$ z antisymetrie relácie $\preceq$.
b) Možnosť $x \preceq y$ a súčasne $y \preceq a$ a $b \preceq x$, nemôže nastať, lebo z tranzitívnosti relácie $\preceq$ by sme dostali $b \preceq a$, ale predpokladáme, že a a b sú neporovnateľné.
c) Možnosť $x \preceq a$, $b \preceq y$ a $y \preceq x$ je symetrická s predchádzajúcou možnosťou.
d) Posledná možnosť, ktorá zostáva, je súčasná platnosť $x \preceq a$, $b \preceq y$, $y \preceq a$ a $b \preceq x$. Opäť z tranzitívnosti máme $b \preceq x \preceq a$, čiže b a a by boli porovnateľné.

Tranzitívnosť. Predpokladajme, že $x \preceq' y$ a $y \preceq' z$. Chceme ukázať, že aj $x \preceq' y$. Opäť jednoducho rozoberieme možnosti, ktoré môžu nastať:
a) Ak $x \preceq y$ a $y \preceq z$, tak platí $x \preceq z$, a teda aj $x \preceq' z$.
b) Ak $x \preceq y$ a súčasne $y \preceq a$ a $b \preceq z$, tak opäť z tranzitívnosti máme $x \preceq a$ a $b \preceq z$, čo znamená, že $x \preceq' z$.
c) Overenie prípadu $x \preceq a$, $b \preceq y$ a $y \preceq z$ je podobné ako v b).
d) Zostáva možnosť, že platí $x \preceq a$, $b \preceq y$, $y \preceq a$ a $b \preceq z$. Lenže potom $b \preceq y \preceq a$, čiže b a a sú porovnateľné. Táto možnosť teda nemôže nastať. □

6.2.4 Nepríjemné dôsledky axiómy výberu

Výsledky uvedené v tejto časti by mohli aspoň sčasti osvetliť, prečo u niektorých matematikov vyvolávala axióma výberu nedôveru a hľadali k nej rôzne alternatívy.

Existencia nemerateľnej množiny

Najprv pripomeňme definíciu miery, s ktorou ste sa už stretli na matematickej analýze.

Definícia 6.2.16. Množina $\mathcal{S} \subseteq \mathcal{P}(X)$ sa nazýva *σ-algebra* na množine X, ak platí

(i) $X \in \mathcal{S}$;
(ii) $A \in \mathcal{S} \Rightarrow X \setminus A \in \mathcal{S}$; (množina $\mathcal{S}$ je uzavretá vzhľadom na vytváranie doplnkov)
(iii) $A_n \in \mathcal{S}$ pre $n \in \mathbb{N} \Rightarrow \bigcup_{n\in\mathbb{N}} A_n \in \mathcal{S}$; (množina $\mathcal{S}$ je uzavretá vzhľadom na spočítateľné zjednotenia).

Ak $\mathcal{S}$ je nejaká σ-algebra na X, tak funkcia $m\colon \mathcal{S} \to \langle 0, \infty\rangle$ z $\mathcal{S}$ ak platí

$$m\left(\bigcup_{n\in\mathbb{N}} A_n\right) = \sum_{n\in\mathbb{N}} m(A_n)$$

pre každý spočítateľný systém $\{A_n; n \in \mathbb{N}\}$ disjunktných množín z $\mathcal{S}$.

Prvky σ-algebry $\mathcal{S}$ sa v takomto prípade zvyknú nazývať *merateľné množiny.*

Stručne môžeme povedať, že miera je funkcia zo σ-algebry do $\mathbb{R}$, ktorá je nezáporná a σ-aditívna. (Vlastnosť uvedená v definícia sa nazýva σ-aditivita.)

Priamo z definície sa ľahko overí, že miera je *monotónna,* t.j.

$$A \subseteq B \wedge A, B \in \mathcal{S} \Rightarrow m(A) \leq m(B).$$

Budeme potrebovať ešte jednu špeciálnu vlastnosť miery.

Definícia 6.2.17. Miera $m\colon \mathcal{S} \to \langle 0, \infty\rangle$ na množine $\mathbb{R}$ sa nazýva *invariantná na posun* alebo *translačne invariantná,* ak pre každú množinu $A \in \mathcal{S}$ a $x \in \mathbb{R}$ aj množina

$$x + A = \{x + a; a \in A\}$$

patrí do $\mathcal{S}$ a platí

$$m(x + A) = m(A).$$

Inak povedané, miera množiny sa nezmení ak ju posunieme.

Miera na množine $\mathbb{R}$, s ktorou ste sa pravdepodobne stretli, je Lebesguova miera. Táto miera spĺňa $m(I) = b - a$ pre každý interval I s koncovými bodmi $a < b$, t.j. miera intervalu je jeho dĺžka. Táto miera je navyše translačne invariantná.

Podmienka, že miera intervalu je rovná dĺžke je pomerne prirodzená. Otázka je, či vieme dĺžku intervalu nejako rozšíriť na mieru na $\mathcal{P}(X)$, t.j. či vieme merať všetky množiny. Nasledujúce tvrdenie ukazuje, že (v ZFC) takáto miera neexistuje.

Tvrdenie 6.2.18. *Neexistuje translačne invariantná miera $m\colon \mathcal{P}(\mathbb{R}) \to \langle 0, \infty\rangle$ taká, že $m(\langle a, b\rangle) = b - a$ pre ľubovoľné $a < b$, $a, b \in \mathbb{R}$.*

Dôkaz – Vitaliho konštrukcia. Predpokladajme, že $m\colon \mathcal{P}(\mathbb{R}) \to \langle 0, \infty\rangle$ je translačne invariantná miera s uvedenými vlastnosťami.

Uvažujme rozklad grupy $(\mathbb{R}, +)$ podľa podgrupy $\mathbb{Q}$. Triedy tohoto rozkladu sú množiny tvaru

$$a + \mathbb{Q} = \{a + q; q \in \mathbb{Q}\}$$

pre $a \in \mathbb{R}$.

Pre každé $a \in \mathbb{R}$ je množina $(a + \mathbb{Q}) \cap \langle 0, 1\rangle$ neprázdna a tieto množiny tvoria rozklad $\langle 0, 1\rangle$ (sú po dvoch disjunktné). Definujme V ako výberovú množinu $\{(a+\mathbb{Q})\cap\langle 0, 1\rangle; a \in \mathbb{R}\}$, t.j. V je taká množina, že pre každé $a \in \mathbb{R}$ je množina $(a + \mathbb{Q}) \cap \langle 0, 1\rangle \cap V$ jednoprvková. (Z každej triedy rozkladu sme vybrali jedného reprezentanta, navyše sme to urobili tak, že tento reprezentant je z intervalu $\langle 0, 1\rangle$.)

Ukážeme, že

$$\langle 0, 1\rangle \subseteq \bigcup_{q\in\mathbb{Q}\cap\langle -1,1\rangle} q + V \subseteq \langle -1, 2\rangle,$$

kde $q + V = \{q + v; v \in V\}$.

Pre každé reálne číslo $a \in \mathbb{R}$ existuje $v \in V$, také, že $a + \mathbb{Q} = v + \mathbb{Q}$, čo je ekvivalentné s podmienkou $a - v \in \mathbb{Q}$. Navyše vieme, že $v \in \langle 0, 1\rangle$.

Ak $a \in \langle 0, 1\rangle$, tak z toho, že aj $v \in \langle 0, 1\rangle$, dostaneme že ich rozdiel $a - v$ je v intervale $\langle -1, 1\rangle$. Teda pre $q = a - v \in \mathbb{Q} \cap \langle -1, 1\rangle$ a máme $a = q + v \in q + V$. Tým sme dokázali inklúziu $\langle 0, 1\rangle \subseteq \bigcup_{q\in\mathbb{Q}\cap\langle -1,1\rangle} q + V$.

Súčasne ak $a \in q + V$ pre nejaké $q \in \langle -1, 1\rangle$, tak a sa dá zapísať ako $q + v$, kde $v \in V \subseteq \langle 0, 1\rangle$. Potom $a = q + v \in \langle -1, 2\rangle$. Teda platí aj inklúzia $\bigcup_{q\in\mathbb{Q}\cap\langle -1,1\rangle} q + V \subseteq \langle -1, 2\rangle$.

Čo vieme povedať o množine $B := \bigcup_{q\in\mathbb{Q}\cap\langle -1,1\rangle} q + V$? Táto množina je spočítateľné disjunktné zjednotenie množín tvaru $q + V$. Keďže miera m je translačne invariantná, platí $m(q + V) = m(V)$ a zo σ-aditivity potom dostaneme

$$m(B) = \sum_{q\in\mathbb{Q}\cap\langle -1,1\rangle} m(q + V) = \sum_{q\in\mathbb{Q}\cap\langle -1,1\rangle} m(V).$$

V závislosti od hodnoty $m(V)$ je teda $m(B)$ buď 0 alebo $+\infty$.

Súčasne však z monotónnosti m a z už dokázaných inklúzií máme

$$1 = m(\langle 0, 1\rangle) \leq m(B) \leq m(\langle -1, 2\rangle) = 3,$$

čím dostávame spor. □

Dôsledok 6.2.19. *Existuje lebesguovsky nemerateľná podmnožina* $\mathbb{R}$.

Existencia lebesguovsky nemerateľnej množiny sa nedá dokázať v ZF.

Banach-Tarskiho paradox

Ešte spomenieme bez dôkazu jeden veľmi známy a veľmi kontraintuitívny dôsledok axiómy výberu.

Veta 6.2.20 (Banach-Tarski)**.** *Pre ľubovoľné dve ohraničené množiny* $A, B \subseteq \mathbb{R}^n$, $n \geq 3$ *existujú rozklady* $A = A_1 \cup \cdots \cup A_k$ *a* $B = B_1 \cup \cdots \cup B_k$ *na konečný počet množín také, že* A_i *a* B_i *sú kongruentné* (*t.j. jednu z druhej možno získať posunutím a otočením*).

Tento výsledok znie naozaj veľmi paradoxne. Znamená, že guľu je možné rozložiť na konečný počet častí, tie popresúvať a poskladať do dvojice gúľ rovnakej veľkosti. Samozrejme, jednotlivé časti rozkladu sú nemerateľné množiny (ak by boli merateľné, kongruentné množiny by mali rovnaký objem/Lebesguovu mieru).

Kniha [Wa] je vcelku príjemné čítanie o histórii tohoto paradoxu. Prístupným spôsobom sa snaží vysvetliť tento paradox a naznačiť jeho dôkaz. Obsahuje aj viacero historických zaujímavostí zo života matematikov, ktorých výsledky sa v tejto knihe spomínajú.

Cvičenia

Úloha 6.2.1. Ukážte na príklade, že linearizácia čiastočne usporiadanej množiny nemusí byť jednoznačne určená.

Úloha 6.2.2. a) Nájdite všetky spojité riešenia funkcionálnej rovnice $f(x+y) = f(x).f(y)$; $f\colon \mathbb{R} \to \mathbb{R}$. Existujú aj nespojité riešenia?
b) Nájdite všetky spojité riešenia funkcionálnej rovnice $f(xy) = f(x) + f(y)$; $f\colon (0,\infty) \to \mathbb{R}$. Existujú aj nespojité riešenia?
c) Nájdite všetky spojité riešenia funkcionálnej rovnice $f(xy) = f(x).f(y)$; $f\colon \langle 0,\infty) \to \mathbb{R}$. Existujú aj nespojité riešenia?

Úloha 6.2.3. Použitím Hamelovej bázy ukážte, že grupy $(\mathbb{R},+)$ a $(\mathbb{C},+)$ sú izomorfné.

6.3 Relatívna konzistentnosť a niektoré nerozhodnuteľné problémy v teórii množín

Na tomto mieste si môžeme povedať niekoľko zaujímavých faktov (bez dôkazov, keďže tie sú dosť náročné) o vzťahu medzi ZF a ZFC a tiež o niektorých tvrdeniach, ktoré sa v ZFC dokázať nedajú.

6.3.1 Relatívna konzistenosť AC a CH

Už sme spomenuli, že axióma výberu vyvolávala u niektorých matematikov prinajmenšom rozpačité reakcie. Preto boli pokusy dokázať AC z axióm systému ZF, alebo naopak, dokázať, že táto axióma v ZF neplatí. Žiadny z týchto pokusov však nebol úspešný.

Ďalší problém, ktorý pomerne dlho odolával snahe o rozriešenie bola hypotéza kontinua (CH, continuum hypothesis), ktorá hovorí, že neexistuje kardinálne číslo medzi $\aleph_0$ a $2^{\aleph_0}$.

V roku 1938 Kurt Gödel dokázal, že ak je systém ZF bezosporný, tak spor nemôžeme dostať ani po pridaní axiómy výberu. (Tento fakt sa často formuluje aj tak, že systém ZFC je *relatívne bezosporný* vzhľadom na ZF. Ak veríme, že ZF je bezosporný, tak sme súčasne uverili aj bezospornosti ZFC.) To znamená, že AC sa nedá vyvrátiť pomocou axióm systému ZF, za predpokladu, že ZF je bezosporný.

To isté ukázal aj o CH – systém ZFC+CH je relatívne bezosporný. Tento výsledok teda znamená, že CH sa nedá vyvrátiť v ZFC.

Až oveľa neskôr, v roku 1963 Paul Cohen dokázal, že v ZF nemožno dokázať AC a v ZFC nemožno dokázať CH. (Presnejšie povedané, ukázal, že ZF+$\neg$AC i ZFC+$\neg$CH sú relatívne bezosporné.)

Platí teda, že axiómu výberu ani jej negáciu nemožno dokázať v ZF. Axióma výberu je *nezávislá* od axióm ZF. Podobne, hypotéza kontinua je nezávislá od axióm systému ZFC. Postupne sa v teórii množín i v ďalších odvetviach matematiky podarilo o mnohých ďalších tvrdeniach ukázať, že sa v rámci ZFC nedajú dokázať ani vyvrátiť. (Systém ZFC je *neúplný*.)

Kapitola 7

Ordinálne čísla

{CHORD}

7.1 Základná veta o dobre usporiadaných množinách

{dum2:SECTDUM2}

Skôr než sa dostaneme k definícii a vlastnostiam ordinálnych čísel, budeme potrebovať ešte niektoré ďalšie výsledky o dobrých usporiadaniach.

{dum2:TVRFAA}

Tvrdenie 7.1.1. *Nech $(A, \leq)$ je dobre usporiadaná množina a $f\colon A \to A$ je injektívne monotónne zobrazenie. Potom pre každé $a \in A$ platí $a \leq f(a)$.*

Dôkaz. Sporom. Predpokladajme, že tvrdenie neplatí, čo znamená, že množina $B := \{a \in A; a > f(a)\}$ je neprázdna. Potom existuje jej najmenší prvok $b = \min B$.

Zrejme platí $b > f(b)$. Z monotónnosti máme $f(b) \geq f(f(b))$, keď navyše využijeme injektívnosť, tak vidíme, že $f(b) > f(f(b))$.

Zistili sme, že $f(b) \in B$, súčasne však platí $f(b) < b$, čo je spor s predpokladom, že b je najmenší prvok množiny B. □

Z predošlého tvrdenia ľahko dostaneme nasledujúci výsledok:

{dum2:LMFAA}

Lema 7.1.2. *Nech $(A, \leq)$ je dobre usporiadaná množina. Ak $f\colon A \to A$ je izomorfizmus, tak $f = id_A$.*

Dôkaz. Pre ľubovoľné $a \in A$ máme

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

(Využili sme dvakrát tvrdenie 7.1.1, raz pre zobrazenie f a raz pre f^{-1}.) □

Dôsledok 7.1.3. *Ak $(A, \leq)$ a $(B, \leq)$ sú dobre usporiadané množiny, tak existuje najviac jeden izomorfizmus medzi A a B.*

Dôkaz. Nech $f, g\colon A \to B$ sú izomorfizmy medzi danými dobre usporiadanými množinami. Potom $g^{-1} \circ f$ je izomorfizmus z A do A, čo podľa lemy 7.1.2 znamená, že $g^{-1} \circ f = id_A$, a teda $g = g \circ id_A = g \circ (g^{-1} \circ f) = (g \circ g^{-1}) \circ f = id_B \circ f = f$. □

dum2:DOSNEEXIZOMPOCUSEK}

Dôsledok 7.1.4. *Nech $(A, \leq)$ je dobre usporiadaná množina, B je počiatočný úsek množiny A a $f\colon A \to B$ je izomorfizmus. Potom $B = A$ a $f = id_A$. (Inak povedané: Dobre usporiadaná množina nemôže byť izomorfná s vlastným počiatočným úsekom seba samej.)*

Dôkaz. Zobrazenie f môžeme chápať ako zobrazenie $f\colon A \to A$, pretože $B \subseteq A$. Teda podľa tvrdenia 7.1.1 pre každé $a \in A$ platí $a \leq f(a)$. Keďže $f(a) \in f[A] = B$ a B je počiatočný úsek, dostávame z tejto nerovnosti, že aj $a \in B$.

Ukázali sme, že každý prvok množiny A patrí do B, čo znamená, že $A \subseteq B$.

Máme už teda dokázanú rovnosť $A = B$ a vieme, že $f\colon A \to A$ je bijektívne monotónne zobrazenie. Podľa lemy 7.1.2 to znamená, že $f = id_A$. □

Nasledujúci výsledok bude pre nás pomerne dôležitý:

{dum2:VTZAKL}

Veta 7.1.5 (Základná veta o dobre usporiadaných množinách)**.** *Ak $(A, \leq)$ a $(B, \leq)$ sú dobre usporiadané množiny, tak buď $(A, \leq)$ je izomorfná s nejakým počiatočným úsekom množiny B alebo $(B, \leq)$ je izomorfná s nejakým počiatočným úsekom množiny A.*

Dôkaz. Budeme sa chvíľu zaoberať bijekciami medzi počiatočnými úsekmi množín A a B. Naším prvým cieľom bude ukázať, že všetky takéto zobrazenia sú v istom zmysle „kompatibilné“ – to neskôr využijeme na dôkaz tvrdenia vety.

Ukážeme najprv nasledujúci fakt: Ak $A_1, A_2 \subseteq A$, $B_1, B_2 \subseteq B$ sú počiatočné úseky a $f_1\colon A_1 \to B_1$, $f_2\colon A_2 \to B_2$ sú izomorfizmy medzi príslušnými počiatočnými úsekmi množiny A a nejakými počiatočnými úsekmi B, tak sa tieto zobrazenia na $A_1 \cap A_2$ zhodujú, t.j. $f_1|_{A_1 \cap A_2} = f_2|_{A_1 \cap A_2}$.

Uvažujme ľubovoľné $x \in A_1 \cap A_2$ a označme $f_1(x) = y_1$, $f_2(x) = y_2$. Označme $C := \{a \in A; a \leq x\}$ a $D_1 := \{b \in B; b \leq f_1(x)\}$. Ukážeme, že $f_1|_C$ je bijekcia medzi C a D_1, ktorá zachováva usporiadanie.

Najprv si musíme uvedomiť, že ide skutočne o zobrazenie, teda, že platí $f_1(c) \in D_1$ pre každé $c \in C$. To vyplýva z toho, že f_1 zachováva usporiadanie, preto z $c \in C$ vyplýva $c \leq x$ $\Rightarrow f_1(c) \leq f_1(x) = y_1$, a teda $f_1(c) \in D_1$.

Keďže $f_1|_C$ je zúženie injekcie zachovávajúcej usporiadanie, aj toto zobrazenie zachováva usporiadanie a je injektívne. (Tieto vlastnosti sa zachovajú pri zúžení.) Zostáva nám ukázať surjektívnosť. Zo surjektívnosti f_1 dostaneme, že pre každé $d \in D_1$ (teda $d \leq y_1$) existuje $c \in A_1$ také, že $f(c) = d$. Súčasne z toho, že f_1 zachováva usporiadanie vidíme, že nemôže platiť $d > x$. Teda sme našli v C vzor pre d, čím sme ukázali, že aj $f_1|_C$ je surjektívne zobrazenie.

Rovnakým spôsobom môžeme ukázať, že $f_2|_C$ je bijekcia medzi C a $D_2 := \{b \in B; b \leq f_2(x)\}$.

Fakt, že máme 2 takéto bijekcie využijeme na dôkaz toho, že $y_1 = y_2$. Bez ujmy na všeobecnosti predpokladajme, že $y_1 \leq y_2$. Máme bijekciu $g := (f_1|_C) \circ (f_2|_C)^{-1}\colon D_2 \to D_1$. Keďže $D_1 \subseteq D_2$ (lebo $y_1 \leq y_2$), môžeme g súčasne chápať ako zobrazenie z D_2 do D_2, z čoho vyplýva na základe tvrdenia 7.1.1 nerovnosť $y_2 \leq g(y_2)$. Súčasne $g(y_2) \in D_2$, a teda $g(y_2) \leq y_1$. Spolu máme

$$y_2 \leq g(y_2) \leq y_1,$$

dostali sme teda obe nerovnosti $y_1 \leq y_2$ aj $y_2 \leq y_1$, čo znamená, že $y_1 = y_2$, čiže $f_1(x) = f_2(x)$.

Označme $\mathcal{S} = \{D \subseteq A; D$ je počiatočný úsek množiny A a existuje bijekcia medzi D a nejakým počiatočným úsekom množiny $B\}$. Ak tieto množiny zjednotíme, dostaneme množinu $C = \bigcup \mathcal{S}$, ktorá je opäť počiatočným úsekom A. Navyše, môžeme definovať zobrazenie $f\colon C \to B$, tak, že $f(x)$ je spoločná hodnota všetkých bijekcií z počiatočných úsekov obsahujúcich x. Takéto zobrazenie opäť zachováva usporiadanie a je to bijekcia na nejaký počiatočný úsek množiny B. (Konkrétne je to počiatočný úsek $\bigcup_{D \in \mathcal{S}} f[D]$.)

Ak $C = A$, našli sme bijekciu medzi A a počiatočným úsekom B. Ak $f[C] = B$, tak máme bijekciu medzi počiatočným úsekom A a celou množinou B. Jediný prípad, ktorý nevyhovuje dokazovanému tvrdeniu je ten, že by obe tieto podmnožiny boli vlastné. Ukážeme, že takýto prípad nemôže nastať.

Sporom. Nech $A \setminus C \neq \emptyset$ aj $B \setminus f[C] \neq \emptyset$. Definujme $a := \min(A \setminus C)$, $b := \min(B \setminus f[C])$. Máme bijekciu $f\colon A \to f(A)$. Potom aj zobrazenie $\hat{f}\colon C \cup \{a\} \to f[C] \cup \{b\}$ definované ako

$$\hat{f}(x) = \begin{cases} f(x) & x \in C, \\ b & x = a. \end{cases}$$

je bijekcia medzi počiatočnými úsekmi množín A a B, ktorá zachováva usporiadanie. Potom aj $A \cup \{a\} \in \mathcal{S}$, čo je spor s tým, že $a \notin \bigcup \mathcal{S}$. □

S využitím vety 7.1.5 už vieme ukázať (s použitím AC, presnejšie WO), že ľubovoľné dve kardinálne čísla sú porovnateľné.

{dum2:DOSPOROVKARD}

Dôsledok 7.1.6. *Pre ľubovoľné dve kardinálne čísla a, b platí $a \leq b$ alebo $b \leq a$.*

Dôsledok 7.1.6 môžeme ekvivalentne preformulovať aj takýmto spôsobom:

Dôsledok 7.1.7. *Pre ľubovoľné množiny X, Y existuje injekcia z X do Y alebo existuje injekcia z Y do X.*

Na základe úlohy 3.2.4 by sme mohli druhú časť v predchádzajúcej formulácii nahradiť existenciou surjekcie z Y do X.

Dôkaz. Nech X, Y sú ľubovoľné dobre usporiadané množiny. Podľa vety 6.1.5 existuje na množine X dobré usporiadanie $\leq_X$ a na množine Y dobré usporiadanie $\leq_Y$. Z vety 7.1.5 dostávame, že existuje buď $(X, \leq_X)$ je izomorfné s nejakým počiatočným úsekom $(Y, \leq_Y)$, čo implikuje existenciu injekcie z X do Y, alebo obrátene. □

7.2 Definícia ordinálnych čísel

Cieľom tejto kapitoly je zadefinovať ordinálne čísla. Veľmi stručne sa dá vysvetliť o čo ide na základe analógie s kardinálnymi číslami. Pre každú množinu existuje kardinálne číslo a dve množiny majú rovnaké kardinálne čísla práve vtedy, keď medzi nimi existuje bijekcia. Inak povedané, z každej „triedy ekvivalencie“ všetkých množín rovnakej mohutnosti sme vybrali jedného reprezentanta. Pri ordinálnych číslach pôjde o niečo podobné, ale hovoriť budeme o dobre usporiadaných množinách (čiže okrem množiny bude na nej dané aj nejaké dobré usporiadanie) a ekvivalencia bude určená existenciou izomorfizmu medzi nim.

Poznámka 7.2.1. Ordinálne čísla chceme zaviesť už skutočne v ZFC, t.j. definícia ktorú uvedieme by sa dala prepísať ako formula jazyka teórie množín a z axióm ZFC sa dá ukázať, že objekty spĺňajúce túto vlastnosť skutočne reprezentujú v uvedenom zmysle všetky dobre usporiadané množiny. Pokiaľ je čitateľ ochotný uveriť tomu, že sa takéto niečo dá urobiť v ZFC alebo je spokojný s naivným prístupom k ordinálnym číslam ako typom dobre usporiadaných množín (podobne ako sme to urobili pre kardinálne čísla – pozri poznámku 4.1.3), tak v podstate môže preskočiť definíciu ordinálnych čísel, bude si však musieť samostatne rozmyslieť, ako pri naivnom prístupe definujeme nerovnosť ordinálnych čísel a operácie s nimi. Takisto si bude musieť samostatne dokázať tvrdenia, ktoré tu uvedieme. (S výnimkou tvrdení o vzťahu medzi $\alpha \in \beta$, $\alpha \subsetneq \beta$ a $\alpha < \beta$ – tie treba akceptovať a v ďalšom chápať tieto výroky o ordináloch ako ekvivalentné.)

Myslím si však, že axiomatický prístup k ordinálnym číslam nie je až taký komplikovaný, takže nie je veľmi výhodné zvoliť naivný prístup. (Resp. pri voľbe naivného prístupu by bolo asi vhodnejšie ďalší text a poradie, v akom tvrdenia dokazujeme, organizovať inak.)

7.2.1 Tranzitívne množiny

Najprv zavedieme pojem tranzitívnej množiny a ukážeme si niektoré jeho základné vlastnosti.

Definícia 7.2.2. Množina X je *tranzitívna,* ak pre každé $x \in X$ platí $x \subseteq X$.

Definíciu tranzitívnej množiny môžeme ekvivalentne preformulovať tak, že platí

$$(\forall x, y) y \in x \in X \Rightarrow y \in X \tag{7.1}$$ {defordnew:EQTRANZ}

alebo tiež $y \in x \wedge x \in X \Rightarrow y \in X$. (Z (7.1) a z podmienky (iii) v leme 7.2.3 vidno, odkiaľ sa vzalo pomenovanie tranzitívna množina.)

Podľa lemy 5.2.6 je množina prirodzených čísel $\mathbb{N}$ príkladom tranzitívnej množiny.

{defordnew:LMTRANZSUBSET

Lema 7.2.3.

(i) *Ak X a Y sú tranzitívne množiny, tak aj $X \cap Y$ a $X \cup Y$ je tranzitívna množina.*

(ii) *Ak každý prvok $X \in \mathcal{S}$ je tranzitívna množina, tak aj $\bigcap \mathcal{S}$ a $\bigcup \mathcal{S}$ sú tranzitívne.* {defordnew:itSUBSETTRANZ

(iii) *Ak X je tranzitívna množina, tak relácia $\in$ je tranzitívna na X práve vtedy, keď každý prvok $x \in X$ je tranzitívna množina.*

{defordnew:itTRANZNASL}

(iv) *Ak X je tranzitívna množina, tak aj množina $X \cup \{X\}$ je tranzitívna.*

Dôkaz. (i) Ak $x \in X \cap Y$, tak $x \in X$ aj $x \in Y$. Z tranzitívnosti množín X a Y dostaneme $x \subseteq X$ a $x \subseteq Y$, z čoho vyplýva $x \subseteq X \cap Y$.

Podobne, ak $x \in X \cup Y$, tak $x \in X$ alebo $x \in Y$. V prvom prípade máme $x \subseteq X \subseteq X \cup Y$, v druhom $x \subseteq Y \subseteq X \cup Y$.

(ii) Ak $x \in \bigcap \mathcal{S}$, tak $x \in X$ pre každé $X \in \mathcal{S}$. Potom pre každé $X \in \mathcal{S}$ máme $x \subseteq X$, a teda $x \subseteq \bigcap S$.

Ak $x \in \bigcup \mathcal{S}$, tak $x \in X$ pre nejaké $X \in \mathcal{S}$. Pre takéto X platí $x \subseteq X$, z čoho dostávame $x \subseteq \bigcup \mathcal{S}$.

(iii) $\boxed{\Rightarrow}$ Predpokladajme, že relácia $\in$ je tranzitívna na X a nech $x \in X$. Ak $z \in y \in x$, tak z tranzitívnosti máme $z \in x$, čo podľa (7.1) znamená, že množina x je tranzitívna.

$\boxed{\Leftarrow}$ Teraz predpokladáme, že každý prvok X je tranzitívnou množinou. Ak $x, y, z \in X$ a platí $x \in y \in z$, tak z toho, že z je tranzitívna a z (7.1) dostaneme $x \in z$.

(iv) Označme $X' = X \cup \{X\}$. Ak $y \in X'$, tak nastane jedna z týchto dvoch možností: Buď platí $y \in X$ alebo $y = X$. V oboch prípadoch máme $y \subseteq X \subseteq X'$. Ukázali sme, že X' je tranzitívna. □

Poznámka 7.2.4. Keď hovoríme o relácii $\in$ na množine A, máme na mysli množinu usporiadaných dvojíc $\{(a, b) \in A \times A; a \in b\}$. (Hovoriť o $\in$ nie je úplne presné – korektnejšie by azda bolo zaviesť nový symbol – budeme to však takto používať, keďže takéto vyjadrovanie je stručné a aj rozšírené v literatúre.)

7.2.2 Ordinálne čísla ako tranzitívne množiny

Definícia 7.2.5. Množina α sa nazýva *ordinálne číslo* alebo *ordinál,* ak α je tranzitívna množina a $\in$ je dobré ostré usporiadanie na α.

Ordinálne čísla budeme obvykle označovať gréckymi písmenami.

Pripomeňme, že ostrému čiastočnému usporiadaniu sme sa venovali na konci časti 3.3. Ide o reláciu, ktorá je antireflexívna, asymetrická a súčasne tranzitívna. Predchádzajúcu definíciu by sme ekvivalentne mohli sformulovať aj tak, že relácia $\in \cup\, id_\alpha$ je dobré usporiadanie na α.

Zadefinovali sme pojem ordinálu, zatiaľ však nevieme ani to, či nejaké ordinály vôbec existujú. Nasledujúce tvrdenie nám ukáže, že všetky prirodzené čísla (tak ako sme ich zadefinovali v časti 5.2) sú ordinálmi.

Tvrdenie 7.2.6.

(i) $\emptyset$ *je ordinálne číslo;*

(ii) *ak* α *je ordinálne číslo, tak aj* $S(\alpha) = \alpha \cup \{\alpha\}$ *je ordinálne číslo.*

Ordinálne číslo $S(\alpha)$ *nazývame* (*ordinálny*) nasledovník *ordinálu* α.

Dôkaz. (i) Zrejmé.

(ii) Podľa tvrdenia 7.2.3 (iv) je $S(\alpha)$ tranzitívna množina. Stačí nám teda už len ukázať, že $\in$ je ostré dobré usporiadanie na $S(\alpha)$. Na to si stačí uvedomiť, že to, čo dostaneme, je to isté, ako keď použijeme konštrukciu z príkladu 3.4.9 pre (ostro) dobre usporiadané množiny $(\alpha, \in)$ a $(\{\alpha\}, \in)$. (V tomto prípade ide o disjunktné množiny, takže by sme vôbec nemuseli používať zdisjunktnenie ako v uvedenom príklade.)

Skutočne, ak $\beta \in S(\alpha) \setminus \{\alpha\}$, tak platí $\beta \in \alpha$ a súčasne $\alpha \notin \beta$. (Ak by platilo $\alpha \in \beta$, tak máme $\alpha \in \beta \in \alpha$ a z tranzitívnosti množiny α potom platí $\alpha \in \alpha$, čo je spor s axiómou regularity.) Takže jediný rozdiel oproti relácii definovanej v príklade 3.4.9 je ten, že tu používame ostré usporiadanie. □

Prirodzené čísla sme zaviedli takým spôsobom, že každé prirodzené číslo sa rovnalo množine všetkých prirodzených čísel od neho menších. Rovnakú vlastnosť majú aj ordinálne čísla. Nasledujúce tvrdenie ukazuje, že všetky prvky ordinálu sú opäť ordinály.

Tvrdenie 7.2.7. *Ak* α *je ordinál a* $\beta \in \alpha$*, tak* β *je ordinál.*

Dôkaz. Keďže α je dobre usporiadaná reláciou $\in$, to isté platí o jej podmnožine β. (Z tranzitívnosti množiny α máme, že $\beta \subseteq \alpha$.)

Z lemy 7.2.3 (iii) vyplýva, že β je tranzitívna množina. □

Tvrdenie 7.2.8. *Pre ľubovoľné dva ordinály* α*,* β *platí*

$$\alpha \in \beta \Leftrightarrow \alpha \subsetneqq \beta.$$

Dôkaz. $\boxed{\Rightarrow}$ Z tranzitívnosti množiny β máme $\alpha \subseteq \beta$. Súčasne nemôže platiť $\alpha = \beta$, lebo by sme dostali $\beta \in \beta$, čo je spor s axiómou regularity.

$\boxed{\Leftarrow}$ Ak $\alpha \subsetneqq \beta$, tak $\beta \setminus \alpha \neq \emptyset$, preto má množina $\beta \setminus \alpha$ najmenší prvok vzhľadom na ostré usporiadanie $\in$. Označme tento najmenší prvok γ. Ukážeme, že $\alpha = \gamma$.

$\boxed{\alpha \subseteq \gamma}$ Ak $\delta \in \alpha$, tak $\delta \in \gamma$ (lebo γ je horné ohraničenie α vzhľadom na ostré lineárne usporiadanie $\in$).

$\boxed{\gamma \subseteq \alpha}$ Nech $\delta \in \gamma$. Z tranzitívnosti množiny β vyplýva, že δ je prvkom β. Ak by platilo $\delta \notin \alpha$, tak $\delta \in (\beta \setminus \alpha)$, čo je spor s tým, že γ je najmenší prvok množiny $\beta \setminus \alpha$. Na základe linearity čiastočného usporiadania $\in$ potom zostáva len možnosť $\delta \in \alpha$. □

Definícia 7.2.9. Nech α, β sú ordinálne čísla. Hovoríme, že α je menšie ako β, ak $\alpha \in \beta$. Používame označenie $\alpha < \beta$.

Ďalej definujeme

$$\alpha \leq \beta \overset{\text{def}}{\Leftrightarrow} \alpha < \beta \vee \alpha = \beta.$$

:POZNEKVPODM}

Poznámka 7.2.10. Podobne ako pre prirodzené čísla, aj pre ordinály platí

$$\alpha < \beta \Leftrightarrow \alpha \in \beta \Leftrightarrow \alpha \subsetneqq \beta$$

a

$$\alpha \leq \beta \Leftrightarrow \alpha \subseteq \beta.$$

Priamo z definície ordinálu (a z toho, že prvky ordinálu sú opäť ordinály) je jasné, že relácia $\leq$ je dobré usporiadanie na každom ordinále α.

Poznámka 7.2.11. Keďže už vieme, že podmienky $\alpha < \beta$ a $\alpha \in \beta$ sú ekvivalentné, budeme používať ktorúkoľvek z nich. (Niekedy sa nám lepšie hodí používať reláciu $\in$, hlavne v prípade, že chceme používať množinovú reprezentáciu ordinálu ako tranzitívnej množiny.) Pokiaľ budete čítať nejakú knihu alebo článok, v ktorom sa vyskytujú ordinály, treba počítať s tým, že sa tam budú vyskytovať ktorákoľvek z týchto troch ekvivalentných podmienok.

Vidíme teda, že každý ordinál je presne množina všetkých ordinálov od neho menších. Veľmi ľahko vieme dostať ešte jednu ekvivalentnú charakterizáciu nerovnosti medzi ordinálmi.

{defordnew:TVRNEROVUSEK}

Tvrdenie 7.2.12. *Nech α, β sú ordinály. Potom*

$$\beta \in \alpha \Leftrightarrow \beta = \alpha_\beta.$$

Dôkaz. $\boxed{\Leftarrow}$ Množina α_β je vlastnou podmnožinou α. Z $\beta = \alpha_\beta$ máme teda $\beta \subsetneqq \alpha$, čo je ekvivalentné s $\beta \in \alpha$.

$\boxed{\Rightarrow}$ Nech $\beta \in \alpha$. Keďže na α uvažujeme ostré usporiadanie $\in$, máme

$$\alpha_\beta = \{\gamma \in \alpha; \gamma \in \beta\} = \alpha \cap \beta = \beta.$$

(Posledná rovnosť vyplýva z $\beta \subseteq \alpha$.)

□

Na základe ekvivalencie podmienok uvedených v poznámke 7.2.10 už vieme ukázať, že $S(\alpha)$ sa vzhľadom na nerovnosť ordinálov správa rovnako ako nasledovník v dobre usporiadanej množine.

{defordnew:TVRSAJENASLED

Tvrdenie 7.2.13. *Nech α, β sú ordinály. Potom $\alpha < \beta \Leftrightarrow S(\alpha) \leq \beta$*

Dôkaz. $\alpha < \beta \Leftrightarrow \alpha \subseteq \beta \wedge \alpha \in \beta \Leftrightarrow S(\alpha) = \alpha \cup \{\alpha\} \subseteq \beta \Leftrightarrow S(\alpha) \leq \beta$ □

Z tvrdenia 7.2.12 a vety 7.1.5 okamžite dostaneme:

{defordnew:DOSTRICHO}

Dôsledok 7.2.14. *Pre ľubovoľné ordinály α, β platí práve jedna z možností*

$$\alpha < \beta \vee \alpha = \beta \vee \alpha > \beta.$$

Dôkaz. Označme $\gamma = \alpha \cup \beta$. Potom $\alpha, \beta \in S(\gamma)$. Keďže $<$ je (ostré) lineárne usporiadanie na ordinále $S(\gamma)$, tak skutočne platí práve 1 z uvedených podmienok. □

Z doteraz dokázaných výsledkov sa už dá vidieť, že počiatočné vnorenia zo základnej vety o dobre usporiadaných množinách popisujú nerovnosť medzi ordinálmi. (Toto by teda bol prístup ako definovať nerovnosť medzi ordinálnymi číslami, ak by sme chceli použiť naivný prístup. I pri práci v ZFC je však nasledujúci výsledok často užitočný.)

{defordnew:TVl

Tvrdenie 7.2.15. *Nech α, β sú ordinálne čísla. Potom:*
$\alpha \leq \beta$ práve vtedy, keď α je izomorfné s nejakým počiatočným úsekom dobre usporiadanej množiny $(\beta, \in)$;
$\alpha < \beta$ práve vtedy, keď α je izomorfné s nejakým vlastným počiatočným úsekom $(\beta, \in)$.

Dôkaz. $\boxed{\Rightarrow}$ Ak $\alpha < \beta$, tak $\alpha = \beta_\alpha$.

$\boxed{\Leftarrow}$ Sporom. Nech by platilo $\beta < \alpha$ a súčasne by bol ordinál β izomorfný s nejakým počiatočným úsekom množiny α. To by znamenalo, že $f\colon \beta \to \alpha$, $f(\gamma) = \gamma$, je vnorenie β, ktorého obraz je vlastná podmnožina α. Súčasne existuje vnorenie $g\colon \beta \to \alpha$ ordinálu β na počiatočný úsek α. Potom $f \circ g\colon \alpha \to \alpha$ je injektívne monotónne zobrazenie, ktoré zobrazí α na vlastný počiatočný úsek ordinálu α. Podľa tvrdenia 7.1.1 platí potom pre každé $\gamma \in \alpha$ nerovnosť $\gamma \leq f \circ g(\gamma)$.

Keďže ale $f \circ g[\alpha]$ je vlastný počiatočný úsek α, existuje taký ordinál γ, ktorý neleží v počiatočnom úseku $f \circ g[\alpha]$. To znamená, že na γ sa nezobrazí žiaden prvok α a špeciálne $f \circ g(\gamma) < \gamma$. Spor. □

{defordnew:TVRSUBSETLE}

Tvrdenie 7.2.16. *Nech α je ordinál a $B \subseteq \alpha$. Nech β je ordinálny typ množiny B. Potom $\beta \leq \alpha$.*

Dôkaz. Sporom. Nech by platilo $\alpha < \beta$. To znamená, že existuje vnorenie $f\colon \alpha \to \beta$, ktoré zobrazí ordinál α na vlastný počiatočný úsek množiny β. Súčasne existuje izomorfizmus medzi β a B, z ktorého vieme dostať vnorenie $g\colon \beta \to \alpha$. Spolu dostávame injektívne monotónne zobrazenie $f \circ g\colon \beta \to \beta$, ktoré zobrazí β na vlastný počiatočný úsek množiny α. To už vedie k sporu. (Rovnakým spôsobom ako v dôkaze tvrdenia 7.2.15.) □

{defordnew:LMZJEDSYS}

Lema 7.2.17. *Ak $\mathcal{S} \neq \emptyset$ je množina ordinálnych čísel, tak aj $\bigcup \mathcal{S}$ a $\bigcap \mathcal{S}$ sú ordinálne čísla.*

Predpoklad $\mathcal{S} \neq \emptyset$ sme pridali preto, aby malo zmysel hovoriť o prieniku systému $\mathcal{S}$. (Pre zjednotenie tento predpoklad nepotrebujeme – vtedy je však tvrdenie lemy triviálne.)

Dôkaz. Z lemy 7.2.3 vieme, že $\bigcup \mathcal{S}$ sú tranzitívne množiny. Zostáva nám teda overiť, či $\in$ je na týchto množinách dobré usporiadanie.

Ostré čiastočné usporiadanie. Antireflexívnosť vyplýva z axiómy regularity (tvrdenie 2.3.12).

Asymetrickosť: Nech $\alpha, \alpha' \in \bigcup \mathcal{S}$. Potom existujú β, β' tak, že $\alpha \in \beta$ a $\alpha' \in \beta'$. Keďže β a β' sú ordinály, nastane jedna z inklúzií $\beta \subseteq \beta' \vee \beta' \subseteq \beta$ (dôsledok 7.2.14). Bez ujmy na všeobecnosti, predpokladajme, že $\beta' \subseteq \beta$. Potom $\alpha, \alpha' \in \beta$. Keďže $\in$ je ostré čiastočné usporiadanie na β, musí platiť práve jedna z možností $\alpha \in \alpha'$, $\alpha = \alpha'$ alebo $\alpha' \in \alpha$.

Dôkaz pre $\bigcap \mathcal{S}$ je ešte jednoduchší, lebo tu za β obsahujúce α i α' môžeme zvoliť ktorýkoľvek prvok $\mathcal{S}$.

Tranzitívnosť: Základná ide dôkazu je identická ako v predošlej časti: Pre $\alpha, \alpha', \alpha''$ z $\bigcup \mathcal{S}$ (resp. z $\bigcap \mathcal{S}$) treba nájsť ordinál β, ktorý obsahuje všetky tri prvky. Detaily prenecháme čitateľovi.

Dobré usporiadanie. Začnime s jednoduchším prípadom – množinou $\bigcap \mathcal{S}$. Ak A je neprázdna podmnožina $\bigcap \mathcal{S}$, tak je súčasne neprázdna podmnožina α pre každé $\alpha \in \mathcal{S}$. Pretože α je ordinál, a teda dobre usporiadaná množina, existuje najmenší prvok množiny A.

Teraz sa pozrime na množinu $\bigcup \mathcal{S}$. Ak A je neprázdna podmnožina $\bigcup \mathcal{S}$, tak existuje také $\alpha \in \mathcal{S}$, že $A \cap \alpha \neq \emptyset$. O množine α vieme, že je dobre usporiadaná (je to ordinál), takže každá jej neprázdna podmnožina má najmenší prvok. Označme $a := \min(A \cap \alpha)$. Ukážeme, že a je najmenší prvok množiny A.

Pre každé $b \in A$ existuje $\beta \in \mathcal{S}$ také, že $b \in \beta$. Opäť z toho, že α a β sú ordinály, vieme, že $\alpha \subseteq \beta$ alebo $\beta \subseteq \alpha$. Takisto pre prvok b máme dve možnosti: buď $b \in \alpha$ alebo $b \notin \alpha$. Ak $b \in \alpha$, tak $a \leq b$, lebo a je najmenší prvok množiny $A \cap \alpha$. Ak $b \notin \alpha$, tak $b \in \beta \setminus \alpha$. To znamená, že neplatí $\beta \subseteq \alpha$, a teda musí platiť $\alpha \subseteq \beta$. Toto je ale ekvivalentné s tým, že $\alpha = \beta_\alpha$, čo znamená, že pre $b \in \beta \setminus \alpha$ platí $b > a$. (Prvok b je väčší než akýkoľvek prvok počiatočného úseku β_α neobsahujúceho b.) □

{defordnew:DOSMNOZORDJED

Dôsledok 7.2.18. *Ľubovoľná množina $\mathcal{S}$ ordinálnych čísel je dobre usporiadaná reláciou $\in$.*

Dôkaz. Je to podmnožina dobre usporiadanej množiny $\bigcup S$. □

{defordnew:DEFSUPINF}

Definícia 7.2.19. Ak $\mathcal{S}$ je množina ordinálov, tak ordinál $\bigcup \mathcal{S}$ označujeme $\sup \mathcal{S}$ a nazývame *suprémum* ordinálnych čísel z množiny $\mathcal{S}$.

$$\sup \mathcal{S} = \bigcup \mathcal{S}.$$

Podobne definujeme

$$\inf \mathcal{S} = \bigcap \mathcal{S}.$$

Ak je množina $\mathcal{S} = \{\alpha, \beta\}$ dvojprvková, tak obvykle namiesto supréme a infime hovoríme o maxime a minime, označujeme $\min\{\alpha, \beta\}$ a $\max\{\alpha, \beta\}$.

Všimnime si, že takto zadefinované suprémum má presne tie vlastnosti, na ktoré sme zvyknutí (napríklad pri supréme v $\mathbb{R}$).

{defordnew:TVRSUP}

Tvrdenie 7.2.20. *Nech $\mathcal{S}$ je množina ordinálov a β je ordinál. Potom $\beta = \sup \mathcal{S}$ práve vtedy, keď β spĺňa nasledujúce podmienky:*

{defornew:itSUP1}
{defornew:itSUP2}

(i) *je horným ohraničením – pre každé $\alpha \in \mathcal{S}$ platí $\alpha \leq \beta$;*
(ii) *je najmenším horným ohraničením – čiže ak nejaký ordinál γ spĺňa podmienku $(\forall \alpha \in \mathcal{S})\alpha \leq \gamma$, tak $\beta \leq \gamma$.*

Dôkaz. Ukážme najprv, že ak $\beta = \sup \mathcal{S} = \bigcup \mathcal{S}$, tak sú obe uvedené podmienky splnené.

(i) Pre každé $\alpha \in \mathcal{S}$ platí $\alpha \subseteq \beta$, čo znamená $\alpha \leq \beta$.

(ii) $(\forall \alpha \in \mathcal{S})\alpha \leq \gamma \Rightarrow (\forall \alpha \in \mathcal{S})\alpha \subseteq \gamma \Rightarrow \beta = \bigcup \mathcal{S} \subseteq \gamma \Rightarrow \beta \leq \gamma$.

Je pomerne jasné, že β je týmito vlastnosťami jednoznačne určené. Ak by totiž ordinály β aj β' spĺňali obe uvedené podmienky, tak dostaneme $\beta \leq \beta'$ aj $\beta' \leq \beta$, z čoho dostaneme $\beta = \beta'$. □

Takisto je vcelku jasné, že tieto dve vlastnosti suprémum množiny ordinálov charakterizujú.

Analogické vlastnosti sa dajú ukázať pre infimum, maximum a minimum.

{defordnew:TVRORDJETRIED

Tvrdenie 7.2.21. *Neexistuje množina všetkých ordinálnych čísel.*

Predchádzajúce tvrdenie vlastne hovorí, že systém všetkých ordinálnych čísel tvorí vlastnú triedu – pozri časť 2.5.1.

Dôkaz. Predpokladajme, že

$$\mathrm{On} = \{\alpha; \alpha \text{ je ordinál}\}$$

by bola množina. Podľa lemy 7.2.17 je aj $\beta := \bigcup \mathrm{On}$ ordinál.

Ďalej si uvedomme, že pre každý ordinál α platí $\alpha \in S(\alpha) \in \mathrm{On}$, a teda $\alpha \in \bigcup \mathrm{On} = \beta$.

Dostávame, že platí $\beta \in \beta$, čo je spor s axiómou regularity. □

Už sme spomenuli, že ordinálne čísla zavádzame s tým zámerom. aby sme dostali typy ordinálnych množín. Teda chceme ukázať, že každý dobre usporiadaná množina je izomorfná s práve jedným ordinálnym číslom.

{defordnew:VT

Veta 7.2.22. *Pre každú dobre usporiadanú množinu $(X, <)$ existuje práve jedno ordinálne číslo α také, že $(X, <)$ a $(\alpha, \in)$ sú izomorfné, t.j. $(X, <) \cong (\alpha, \in)$.*

Dôkaz. Nech $(X, \leq)$ je dobre usporiadaná množina. Budeme postupovať sporom. Predpokladajme, že by množina $(X, \leq)$ nebola izomorfná so žiadnym ordinálnym číslom.

Nech α je ľubovoľné ordinálne číslo. Podľa vety 7.1.5 môže nastať niektorá z týchto 3 možností:

a) $(\alpha, \in)$ a $(X, <)$ sú izomorfné, čo je však v spore s naším predpokladom.

b) $(X, <)$ je izomorfné s nejakým počiatočným úsekom α_β dobre usporiadanej množiny $(\alpha, \in)$. (Pre nejaké $\beta \in \alpha$.) To by ale znamenalo, že $(X, <)$ je izomorfné s ordinálom β (tvrdenie 7.2.12), čo je opäť spor s predpokladom, že X nie je izomorfné so žiadnym ordinálom.

c) Zostáva teda možnosť, že existuje x také, že $X_x \cong \alpha$. Takéto x navyše môže existovať najviac jedno. Označme x s touto vlastnosťou ako x_α.

Ďalej ukážeme, že priradenie[1] $\alpha \mapsto x_\alpha$ je injektívne. Na to nám stačí ukázať $\beta < \alpha \Rightarrow x_\beta < x_\alpha$.

Postupujme opäť sporom. Nech by pre nejaké ordinály α a β platilo $\alpha < \beta$ a súčasne $x_\alpha \geq x_\beta$. Potom $X_{x_\beta} \subseteq X_{x_\alpha}$. Poskladaním izomorfimu z β do X_{x_β}, inklúzie z X_{x_β} do X_{x_α} a izomorfizmu z X_{x_α} do α dostaneme injektívne monotónne zobrazenie $f\colon \beta \to \alpha$. Pre toto zobrazenie očividne platí $f(\alpha) < \alpha$, čo je v spore s tvrdením 7.1.1.

Teraz definujme pre každé $x \in X$ ordinál α_x, tak, že ak $x = x_\alpha$ pre nejaké α, tak položíme α_x rovné práve tomuto α a v opačnom prípade definujeme $\alpha_x = 0$. Takto sme každému $x \in X$ priradili[2] práve jeden ordinál α_x. Potom ale podľa schémy axióm obrazu je

$$\{\alpha_x; x \in X\}$$

množina. Táto množina však ale obsahuje všetky ordinálne čísla, čiže dostávame spor s tvrdením 7.2.21. □

Definícia 7.2.23. (Jednoznačne určený) ordinál, ktorý je izomorfný s dobre usporiadanou množinou X nazývame *ordinálny typ* množiny X.

7.3 Ordinálna aritmetika

{aritmord:SECTORDARIT}

Už sme sa naučili ordinálne čísla porovnávať. V tejto podkapitole zavedieme súčet a súčin ordinálov a budeme sa zaoberať základnými vlastnosťami týchto operácií, podobne ako sme to predtým urobili pre kardinálne čísla. (Neskôr zadefinujeme aj umocňovanie ordinálov, jeho definícia je však o dosť komplikovanejšia.) Ako ihneď uvidíte, v skutočnosti sme sa so sčitovaním a násobením ordinálnych čísel už stretli, vtedy sme však hovorili o dobre usporiadaných množinách (keďže sme nemali vybudovaný pojem ordinálu).

[1] Hovoríme o priradení, nie o zobrazení; keďže sme prvok z X priradili každému ordinálnemu číslu a ordinálne čísla netvoria množinu. Aj pre takéto triedové funkcie však má zmysel hovoriť o injektívnosti.

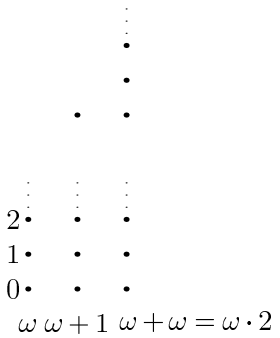
[2] Môžete si všimnúť, že sme vlastne úplne presne zopakovali postup z dôkazu tvrdenia 3.2.14(ii) s tým rozdielom, že opäť nemôžeme hovoriť o zobrazeniach, keďže ordinálne čísla netvoria množinu.

7.3.1 Súčet ordinálnych čísel

d:SSECTSUCET}

Definícia 7.3.1. Nech α a β sú ordinálne čísla. Potom ich *súčet* $\alpha + \beta$ definujeme ako ordinálny typ dobre usporiadanej množiny $\{0\} \times \alpha \cup \{1\} \times \{\beta\}$ s usporiadaním $\leq$ definovaným tak, že
a) $(0, \gamma) \leq (1, \delta)$ pre ľubovoľné $\gamma \in \alpha$, $\delta \in \beta$;
b) $(0, \gamma) \leq (0, \gamma')$ pre $\gamma, \gamma' \in \alpha$ práve vtedy, keď $\gamma \leq \gamma'$;
c) $(1, \delta) \leq (1, \delta')$ pre $\delta, \delta' \in \beta$ práve vtedy, keď $\delta \leq \delta'$.

Vidíme, že ide presne o čiastočné usporiadanie z príkladu 3.4.9, kde sme sa venovali aj tomu, že takto dostaneme (z dobre usporiadaných množín) dobré usporiadanie. Niektoré príklady sú znázornené na obrázku 7.1.



Obr. 7.1: Príklady na súčet ordinálnych čísel {aritmord1:FIGSUCET}

Na rozdiel od sčitovania kardinálov, táto operácia nie je komutatívna, ako ukazuje tento príklad:

$$1 + \omega = \omega \neq \omega + 1.$$

Základné vlastnosti sa dajú pomerne ľahko odvodiť priamo z definície (podobným spôsobom, ako sme to robili pre kardinály; tu namiesto bijekcie konštruujeme izomorfizmus medzi dobre usporiadanými množinami).

{aritmord1:TVRSUC0}

Tvrdenie 7.3.2. *Ak α je ľubovoľný kardinál, tak $S(\alpha) = \alpha + 1$ a*

$$0 + \alpha = \alpha + 0 = \alpha.$$

Pre ľubovoľné ordinály α, β, γ platí

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma,$$

t.j. sčitovanie ordinálov je asociatívne.

Dôkaz. Ponechávame ako cvičenie čitateľovi. □

Môžeme si všimnúť, že ako špeciálny prípad asociatívnosti dostávame $\alpha + (\beta + 1) = (\alpha + \beta) + 1$, t.j.

$$\alpha + S(\beta) = S(\alpha + \beta). \tag{7.2}$$

{aritmord1:EQPLUSNASL}

Podobne ako pri kardinálnych číslach, aj tu nás bude zaujímať, či sčitovanie ordinálov zachováva nerovnosti.

{aritmord1:TVI

Tvrdenie 7.3.3. *Nech α, β, γ sú ľubovoľné ordinály.*
(i) *Ak $\beta < \gamma$, tak $\alpha + \beta < \alpha + \gamma$.*
(ii) *Ak $\alpha \leq \beta$, tak $\alpha + \gamma \leq \beta + \gamma$.*

Dôkaz. (i): Ak $\beta < \gamma$, tak $f\colon \beta \to \gamma$, $f(\delta) = \delta$ je vnorenie β na vlastný počiatočný úsek dobre usporiadanej množiny $(\gamma, \in)$. Pomocou neho môžeme zadefinovať zobrazenie $g\colon \alpha \times \{0\} \cup \beta \times \{1\} \to \alpha \times \{0\} \cup \gamma \times \{1\}$ predpisom

$$g(\delta, 0) = (\delta, 0);$$
$$g(\delta, 1) = (f(\delta), 1).$$

Ľahko sa overí, že ide o vnorenie na vlastný počiatočný úsek. Potom pre ordinálne typy týchto množín platí $\alpha + \beta < \alpha + \gamma$.

(ii): Tentokrát máme vnorenie $f\colon \alpha \to \beta$, $f(\delta) = \delta$, ordinálu α na počiatočný úsek ordinálu β. Potom zobrazenie $g\colon \alpha \times \{0\} \cup \gamma \times \{1\} \to \beta \times \{0\} \cup \gamma \times \{1\}$ definované ako

$$g(\delta, 0) = (f(\delta), 0);$$
$$g(\delta, 1) = (\delta, 1);$$

zobrazí množinu ordinálneho typu $\alpha + \gamma$ na podmnožinu množiny ordinálneho typu $\beta + \gamma$. Podľa tvrdenia 7.2.16 z toho vyplýva, že $\alpha + \gamma \leq \beta + \gamma$. □

Ľahko môžeme nájsť príklad ukazujúci, že druhá časť predchádzajúceho tvrdenia už neplatí, ak by sme neostrú nerovnosť nahradili ostrou. Napríklad $0 < 1$ ale

$$0 + \omega = 1 + \omega = \omega.$$

Pomocou sčitovania ordinálov vieme charakterizovať aj nerovnosť medzi ordinálmi.

{aritmord1:TVRROZD}

Tvrdenie 7.3.4. *Nech α, β sú ordinály. Potom $\alpha \leq \beta$ platí práve vtedy, keď existuje ordinál γ taký, že $\beta = \alpha + \gamma$.*

$$\alpha \leq \beta \qquad \Leftrightarrow \qquad (\exists\gamma)\beta = \alpha + \gamma$$

Dôkaz. $\boxed{\Leftarrow}$ Pre každý ordinál platí $\gamma \geq 0$. Z tvrdenia 7.3.3 potom máme $\beta = \alpha + \gamma \geq \alpha + 0 = \alpha$.

$\boxed{\Rightarrow}$ Stačí za γ zvoliť ordinálny typ množiny $\beta \setminus \alpha$. □

{aritmord1:TVRSUCSPOJ}

Tvrdenie 7.3.5. *Nech α je ordinál a $\{\beta_i; i \in I\}$ je množina ordinálov. Potom*

{aritmord1:EQSUCSPOJ}
$$\alpha + \sup_{i\in I} \beta_i = \sup_{i\in I}(\alpha + \beta_i) \tag{7.3}$$

{aritmord1:EQSUP}
$$(\sup_{i\in I} \beta_i) + \alpha \geq \sup_{i\in I}(\beta_i + \alpha) \tag{7.4}$$

Dôkaz. Rovnosť (7.3): Označme $\lambda = \alpha + \sup_{i\in I} \beta_i$ a $\rho = \sup_{i\in I}(\alpha + \beta_i)$.

Pretože pre každé $i \in I$ platí $\beta_i \leq \sup_{i\in I} \beta_i$, dostávame $\alpha + \beta_i \leq \alpha + \sup_{i\in I} \beta_i = \lambda$. Z platnosti tejto nerovnosti pre každé $i \in I$ dostaneme

$$\rho = \sup_{i\in I}(\alpha + \beta_i) \leq \lambda.$$

Súčasne je zrejmé, že $\rho \geq \alpha$, teda existuje ordinál γ taký, že $\rho = \alpha + \gamma$. Tvrdíme, že $(\forall i \in I)\beta_i \leq \gamma$. Sporom. Ak by to tak nebolo, tak existuje nejaké $i \in I$ s vlastnosťou $\beta_i > \gamma$. Potom ale podľa tvrdenia 7.3.3 $\alpha + \beta_i > \alpha + \gamma = \rho$, čo je spor.

Z platnosti nerovnosti $\beta_i \leq \gamma$ pre všetky $i \in I$ máme $\sup_{i\in I} \beta_i \leq \gamma$, a teda

$$\lambda = \alpha + \sup_{i\in I} \beta_i \leq \alpha + \gamma = \rho.$$

Nerovnosť (7.4): Pre každé $i \in I$ platí z $\beta_i \leq \sup_{i\in I} \beta_i$, a teda aj $\beta_i + \alpha \leq (\sup_{i\in I} \beta_i) + \alpha$. Z vlastností supréma už potom dostaneme dokazovanú nerovnosť. □

7.3.2 Súčin ordinálnych čísel

{aritmord:SSECTSUCIN}

Definícia 7.3.6. Súčin ordinálnych čísel α a β definujeme ako ordinálny typ množiny $\alpha \times \beta$ usporiadanej antilexikografickým súčinom usporiadaní množín α a β. Označujeme ho $\alpha.\beta$

Pripomeňme, že antilexikografické usporiadanie sme zaviedli v definícii 3.4.6.

Ekvivalentne by sme mohli definovať $\alpha.\beta$ ako ordinálny typ množiny $\beta \times \alpha$ usporiadanej lexikografickým súčinom. V oboch prípadoch ide o usporiadanie dvojíc prvkov, pričom ako dôležitejšiu berieme tú súradnicu, ktorú sme dostali z β.

Intuitívne sa na súčin $\alpha.\beta$ môžeme pozerať tak, že sme postupne za sebou usporiadali β kópií ordinálu α. (Ak si znázorníme ordinál β, tak $\alpha.\beta$ dostaneme tak, že každú bodku predstavujúcu prvok množiny β nahradíme diagramom predstavujúcim ordinál α.)

Príklad 7.3.7. Priamo z definície dostaneme $\omega.2 = \omega + \omega$ a $2.\omega = \omega$.

Súčin ordinálnych čísel teda nie je vo všeobecnosti komutatívny.

Nasledujúce tvrdenie by malo byť pomerne jasné z intuitívnej predstavy o tom, čo znamená súčin a súčet ordinálov, napriek tomu aspoň stručne naznačíme i formálny dôkaz.

Tvrdenie 7.3.8. *Ak α, β, γ sú ľubovoľné ordinály, tak platí*

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

Dôkaz. Na dôkaz prvého tvrdenia chceme porovnať ordinálne typy množín $\alpha \times (\beta \times \gamma)$ a $(\alpha \times \beta) \times \gamma$ usporiadaných antilexikograficky (t.j. vždy podľa poslednej súradnice). Izomorfizmus medzi týmito dvomi množinami je zobrazenie $(a, (b, c)) \mapsto ((a, b), c)$ (kde $a \in \alpha$, $b \in \beta$, $c \in \gamma$).

Podobne druhá rovnosť vlastne hovorí o rovnosti ordinálnych typov množín $\alpha \times (\beta \times \{0\} \cup \gamma \times \{1\})$ a $(\alpha \times \beta) \times \{0\} \cup (\alpha \times \gamma) \times \{1\}$. Izomorfizmus je $(a, (b, \varepsilon)) \mapsto ((a, b), \varepsilon)$, kde $a \in \alpha$ a $(b, \varepsilon) \in \beta \times \{0\} \cup \gamma \times \{1\}$. □

Keďže $(1 + 1).\omega = 2\omega = \omega \neq \omega + \omega$, vidíme, že distributívnosť pre sčitovanie a násobenie ordinálov platí iba z jednej strany.

Tvrdenie 7.3.9. *Nech α, β, γ sú ordinály. Potom*

$$\alpha < \beta \Rightarrow \gamma.\alpha < \gamma.\beta$$
$$\alpha \leq \beta \Rightarrow \alpha.\gamma \leq \beta.\gamma$$

Dôkaz. Ponechávame ako cvičenie pre čitateľa. (Dajú sa využiť tvrdenia 7.2.15 a 7.2.16). □

Druhá časť tvrdenia neplatí, ak neostrú nerovnosť nahradíme ostrou. Stačí si všimnúť, že $1 < 2$ ale $1.\omega = \omega = 2.\omega$.

7.3.3 Limitné ordinály

Definícia 7.3.10. Ordinál α sa nazýva *limitný*, ak $\alpha \neq 0$ a súčasne neexistuje ordinál β taký, že $S(\beta) = \alpha$.

Vidíme teda, že ordinály môžeme rozdeliť na tri skupiny – nulu, limitné ordinály a nasledovníkov.

Príkladmi limitných ordinálov sú ω, $\omega+\omega$. Nelimitné ordinály sú napríklad $\omega+1$ a všetky prirodzené čísla okrem nuly.

Ukážeme si, ako súvisí pojem limitného ordinálu s pojmom supréma:

Tvrdenie 7.3.11. *Ak α je limitný ordinál, tak $\alpha = \sup\{\beta; \beta < \alpha\}$; t.j. α je suprémum všetkých ordinálov menších ako α.*

Podobne ako ste zvyknutí z iných predmetov, namiesto zápisu $\sup\{\beta; \beta < \alpha\}$ budeme často písať $\sup\limits_{\beta<\alpha} \beta$. (Analogicky pre supréma iných množín.)

Dôkaz. Pripomeňme, že $\gamma := \sup\{\beta; \beta < \alpha\} = \bigcup_{\beta<\alpha} \beta$ (definícia 7.2.19).

Inklúzia

$$\gamma = \bigcup_{\beta<\alpha} \beta \subseteq \alpha$$

platí pre ľubovoľný ordinál α.

Predpokladajme, že by neplatilo $\gamma = \beta$, čiže potom musí platiť $\gamma < \beta$. Potom pre ordinál $S(\gamma)$ platí $S(\gamma) < \beta$. (Z $\gamma < \alpha$ vyplýva $S(\gamma) \leq \alpha$ podľa tvrdenia 7.2.13. Keďže ale $S(\gamma) \neq \alpha$, máme ostrú nerovnosť $S(\gamma) < \alpha$.) Z definície γ dostávame potom $S(\gamma) \subseteq \gamma$, čo znamená

$$S(\gamma) \leq \gamma < S(\gamma).$$

Dostali sme spor, teda musí platiť rovnosť $\gamma = \beta$. □

7.4 Transfinitná indukcia

{transf:SECTTRANSF}

Transfinitná indukcia je veľmi užitočná dôkazová technika. Ide vlastne o indukciu na dobre usporiadaných množinách, ktorú už poznáme (veta 3.4.3); keď už však vieme, že každá dobre usporiadaná množina je izomorfná s nejakým ordinálnym číslom, umožní nám to zjednodušenie a sprehľadnenie niektorých dôkazov.

{transf:VTIND}

Veta 7.4.1. *Nech $\varphi(x)$ je formula teórie množín taká, že ak platí $\varphi(\beta)$ pre všetky ordinály menšie ako $\varphi(\alpha)$, tak platí aj $\varphi(\alpha)$.*

Potom je formula $\varphi(\alpha)$ pravdivá pre každý ordinál α.

Dôkaz. Nech α je ľubovoľný ordinál. Potom $(S(\alpha), \leq)$ a $B = \{\beta \in S(\alpha); \varphi(\beta)\}$ spĺňajú predpoklady vety 3.4.3, teda $B = S(\alpha)$. Tým sme ukázali, že $\varphi(\beta)$ platí pre každý ordinál $\beta \in S(\alpha)$, špeciálne ja pre ordinál α. □

Poznámka 7.4.2. Formulácia, ktorú sme uviedli, je vhodná ak chceme ukázať platnosť nejakého tvrdenia pre všetky ordinály. V praxi dosť často nastane situácia, že chceme ukázať platnosť tvrdenie pre všetky ordinály menšie ako nejaký vopred daný ordinál λ. (Tak je to napríklad už v príklade 7.4.3, ktorý je našou prvou ilustráciou transfinitnej indukcie.) Ak chceme dokázať, že $\psi(\alpha)$ platí pre každý ordinál $\alpha < \lambda$, môžeme jednoducho použiť vetu 7.4.1 pre formulu $\varphi(\alpha) = \psi(\alpha) \vee (\alpha \geq \lambda)$ (alebo využiť priamo vetu 3.4.3, podobne ako v dôkaze vety 7.4.1).

Neskôr si ukážeme použitie transfinitnej indukcie aj na dôkaz zaujímavejších tvrdení, na zoznámenie sa s novou dôkazovou technikou je však vhodné začať s jednoduchými dôkazmi. Dokážeme si tvrdenie 7.1.1. Už na dôkaze tohoto tvrdenia budete vidieť jav často sa vyskytujúci v takýchto dôkazoch – dôkaz „indukčného kroku“ obvykle býva rozdielny pre $\alpha = 0$, pre prípad, že α je limitný ordinál a pre prípad, že α je nasledovník nejakého ordinálu.

{transf:PRIKLMONOT}

Príklad 7.4.3. Nech λ je ordinálne číslo a $f\colon \lambda \to \lambda$ je monotónna injekcia (t.j. $\beta < \gamma \Rightarrow f(\beta) < f(\gamma)$). Potom pre každé $\alpha \in \lambda$ platí $f(\alpha) \geq \alpha$.

Tvrdenie 7.1.1 hovorí o dobre usporiadaných množinách, nie o ordináloch. Keď už však vieme, že každá dobre usporiadaná množina je izomorfná s nejakým ordinálom, je zrejmé, že ide o ekvivalentnú formuláciu tohoto tvrdenia.

Dôkaz. 1° Určite platí $0 \leq f(\alpha)$, pretože 0 je najmenší ordinál.

2° Nech $\alpha = \beta + 1$ a tvrdenie platí pre ordinál β. Pretože $\alpha > \beta$, máme $f(\alpha) > f(\beta) \geq \beta$, a teda aj

$$f(\alpha) \geq \beta + 1.$$

3° Nech α je limitný ordinál a tvrdenie platí pre všetky menšie ordinály $\beta < \alpha$, t.j.

$$(\forall \beta < \alpha) f(\beta) \geq \beta.$$

Z toho vyplýva, že

$$(\forall \beta < \alpha) f(\alpha) \geq \beta,$$

a teda

$$f(\alpha) \geq \sup_{\beta < \alpha} \beta = \alpha.$$

□

7.4.1 Definícia transfinitnou indukciou

Už sme spomínali, že transfinitná indukcia je rozšírením matematickej indukcie. Z viacerých predmetov ste zvyknutí na to, že matematickou indukciou nielen dokazujeme tvrdenia, ale niekedy ju používame aj na konštrukciu rôznych objektov. To sa dá robiť aj pomocou transfinitnej indukcie.

Nemusí byť na prvý pohľad jasné, že nasledujúce tvrdenie skutočne formalizuje transfinitnú indukciu, aspoň na jednom prípade si ho aj podrobne vysvetlíme. V mnohých učebniciach nájdete toto tvrdenie sfomulované inak než tu, dôvod prečo sme použili túto formuláciu je ten, že sme nedefinovali pojem triedovej funkcie.

{transf:VTREKUR}

Veta 7.4.4 (O transfinitnej rekurzii)**.** *Nech α je ordinálne číslo a φ je výroková funkcia s vlastnosťou, že pre každé $\beta < \alpha$ a pre každú funkciu f, ktorá má definičný obor $D(f) = \beta$, existuje práve jedno y také, že $\varphi(f, y)$.*

Potom existuje práve jedna funkcia F taká, že $D(F) = \alpha$ a

$$F(\beta) = y \qquad \Leftrightarrow \qquad \varphi(F|_\beta, y).$$

Poznámka 7.4.5. Jednoznačnosť funkcie F v predchádzajúcom tvrdení chápeme v zmysle rovnosti množín, t.j. ako množinu usporiadaných dvojíc. (Vlastne ani veľmi nemáme inú možnosť, keďže sme nepopísali obor hodnôt zobrazenia F.)

Možno sa oplatí vysvetliť v akom zmysle formalizuje predchádzajúce tvrdenie definíciu transfinitnou indukciou. V tomto tvrdení popisujeme, ako transfinitnou indukciou môžeme definovať funkciou F na celom α, pričom formula φ nám popisuje, ako pokračovať, ak už máme zadefinované hodnoty na nejakom počiatočnom úseku (tieto sú popísané funkciou f).

Dôkaz. Existencia. Uvažujme formulu $\psi(\beta)$, ktorá hovorí, že ak $\beta \leq \alpha$, tak existuje funkcia F taká, že $D(F) = \beta$ a pre každé $\gamma < \beta$ platí

$$F(\gamma) = y \qquad \Leftrightarrow \qquad \varphi(F|_\gamma, y).$$

Stačí nám overiť, že pre túto formulu sú splnené predpoklady vety 7.4.1.

Predpokladajme teda, že $\psi(\gamma)$ platí pre každý ordinál menší ako β. Ak $\beta > \alpha$, tak nieto čo dokazovať. Ak $\beta \leq \alpha$, tak rozlíšime tri prípady:

Ak $\beta = 0$, tak stačí položiť $F = \emptyset$.

Ak β je nelimitný ordinál, tak $\beta = S(\gamma) = \gamma \cup \{\gamma\}$ pre nejaké β. Pretože pre γ platí $\psi(\gamma)$, existuje funkcia F definovaná na γ spĺňajúca predpoklady tvrdenia pre ordinál γ. Ak definujeme

$$\overline{F}(\delta) = \begin{cases} F(\delta) & \delta \in \gamma, \\ y & \delta = \gamma \text{a } y \text{ je jediné } y \text{ spĺňajúce } \psi(\overline{F}, y), \end{cases}$$

tak táto funkcia ukazuje platnosť $\psi(\beta)$.

Ak β je limitný ordinál a F_γ označíme funkciu z formuly $\psi(\gamma)$, tak stačí položiť $F = \bigcup_{\gamma<\beta} \overline{F}$ a opäť dostaneme, že platí $\psi(\beta)$.

Z vety 7.4.1 máme, že $\psi(\beta)$ platí pre každý ordinál, špeciálne že platí $\psi(\alpha)$. To ale presne znamená existenciu zobrazenia s uvedenými vlastnosťami.

Jednoznačnosť. Prepokladajme, že by existovali dve rôzne zobrazenia $G \neq F$ s uvedenými vlastnosťami. Nech $\beta < \alpha$ je najmenší ordinál taký, že $F(\beta) \neq G(\beta)$. To znamená, že $F|_\beta = G|_\beta$. Podľa predpokladov vety je $y = F(\beta)$ jednoznačne určené vlastnosťou $\varphi(F|_\beta, y)$, to isté platí aj pre funkciu G. Takže dostávame $F(\beta) = G(\beta)$, čo je spor. □

Ako príklad použitia transfinitnej rekurzie si ukážeme, ako by sme pomocou nej mohli zadefinovať sčitovanie ordinálnych čísel. Podobne ako pri transfinitnej indukcii, aj pri použití transfinitnej rekurzie obvykle budeme uvažovať zvlášť tri prípady: nulu, nasledovník a limitný ordinál.

Príklad 7.4.6. Pomocou transfinitnej rekurzie ukážeme nasledujúce tvrdenie: Nech γ je ordinálne číslo. Potom pre každé ordinálne číslo α existuje jednoznačne určená funkcia F taká, že $D(F) = \alpha$ a platí:

(i) Ak $\alpha = 0$, tak $F(\alpha) = \gamma$.

(ii) Ak $\alpha = S(\alpha')$, tak $F(\alpha) = S(F(\alpha'))$.

(iii) Ak α je limitný ordinál, tak $F(\alpha) = \sup\{F(\alpha'); \alpha' < \alpha\}$.

Dôkaz. Vlastne nám stačí overiť, že formula $\varphi(f, y)$, ktorá pre $\beta < \alpha$ a funkciu f definovanú na β hovorí, že

(i) $y = \gamma$, ak $\beta = 0$;

(ii) $y = S(f(\beta))$, ak $\beta = S(\beta')$;

(iii) $y = \sup\{f(\beta'); \beta' < \beta\}$, ak β je limitný ordinál;

určuje pre každé β a f jediné y. (To stačí na to, aby boli splnené predpoklady vety 7.4.4.)

Pre každé $\beta < \alpha$ však nastane práve jeden z uvedených prípadov a v každom z nich je y určené jednoznačne v závislosti od f a β (pričom $\beta = D(f)$ je jednoznačne určené funkciou f). Teda vlastne niet čo dokazovať. □

V budúcnosti nebudeme pri používaní transfinitnej rekurzie postupovať takto podrobne. Namiesto uvedeného dôkazu by sme jednoducho napísali, že F definujeme transfinitnou rekurziou pomocou uvedených troch vlastností.

Keď tieto vlastnosti porovnáme s tvrdením 7.3.2 a rovnosťami (7.2), (7.3), tak vidíme, že $F(\alpha) = \gamma + \alpha$, čiže takto môžeme transfinitnou rekurziou zadefinovať sčitovanie ordinálnych čísel. Podobný postup použijeme v časti 7.4.2 na definíciu umocňovania ordinálnych čísel.

7.4.2 Umocňovanie ordinálnych čísel

{transf:SSECTEXP}

7.5 Definícia kardinálnych čísel

{defkard:SECTDEFKARD}

Keď už máme v ZFC zadefinovné ordinály, tak sme pomocou nich schopný v jazyku teórie množín definovať i kardinály. (Tým sa vyriešia problémy, o ktorých sme hovoril v poznámke 4.1.3.)

{defkard:TVRDEFKARD}

Tvrdenie 7.5.1. *(AC) Nech A je ľubovoľná množina. Potom existuje práve jeden taký ordinál, že*

{defkard:itbijek}

(i) *existuje bijekcia medzi A a α;*

(ii) *pre každý ordinál β taký, že existuje bijekcia medzi A a β platí $\alpha \leq \beta$ (t.j α je najmenší ordinál spĺňajúci* (i)*).*

Definícia 7.5.2. Ordinál α s vlastnosťami z predchádzajúceho tvrdenia budeme nazývať *kardinálnym číslom* množiny A. Ordinály, ktoré sú kardinálnymi číslami nejakej množiny, budeme nazývať *kardinálmi.*

Dôkaz tvrdenia 7.5.1. Priamo z formulácie tvrdenia je jasné, že ak existuje ordinál s uvedenými vlastnosťami, tak je určený jednoznačne. (Ak by α i α' spĺňali uvedené podmienky, tak máme $\alpha \leq \alpha'$ a $\alpha' \leq \alpha$.)

Na množine A existuje dobré usporiadanie $<$ podľa (WO), podľa vety 7.2.22 existuje ordinál γ taký, že dobre usporiadaná množina $(A, <)$ je izomorfná s $(\gamma, \in)$. Špeciálne to znamená existenciu bijekcie medzi γ a A.

Označme

$$M := \{\delta \in S(\gamma); \text{existuje bijekcia medzi } A \text{ a } \delta\}$$

a položme

$$\alpha = \min M.$$

(Množina M je neprázdna, lebo $\gamma \in M$.)

Zrejme pre takto definovaný ordinál α existuje bijekcia s množinou A, t.j. α spĺňa (i). Zostáva len overiť, či je to najmenší ordinál s touto vlastnosťou. Nech β je ľubovoľný ordinál, pre ktorý platí (i). Môžu nastať dve možnosti.

Ak platí $\beta > \gamma$, tak očividne $\alpha \leq \gamma < \beta$.

Druhá možnosť je, že platí $\beta \leq \gamma$. Potom $\beta \in S(\gamma)$, a teda $\beta \in M$. Pretože α je najmenší prvok množiny M, platí $\alpha \leq \beta$. □

7.6 Aplikácie ordinálnych čísel a transfinitnej indukcie

V tejto časti by sme chceli ukázať niektoré príklady použitia transfinitnej indukcie. Okrem iného ukážeme platnosť vzťahu $a.a = a$, resp. $a.b = \max\{a, b\}$ pre nekonečné kardinálne čísla, ktorý sme doteraz používali bez dôkazu (pozri poznámku 4.2.16).

7.6.1 Kardinálna aritmetika

{aplikord:NTA

Veta 7.6.1. *Pre každý kardinál $a \geq \aleph_0$ platí $a.a = a$.*

Dôkaz. V príklade 4.2.15 sme ukázali, že toto tvrdenie platí pre $a = \aleph_0$. Ukážeme, že ak toto tvrdenie platí pre každý nekonečný kardinál $b < a$, tak platí aj pre a.

Nech teda $a > \aleph_0$. Majme dobré usporiadanie $\leq$ na a, také, že všetky počiatočné úseky tvaru $\{x \in a; x < b\}$ pre $b \in a$ majú kardinalitu menšiu ako a. Pomocou tohoto usporiadania[3] zadefinujeme usporiadanie $\leq^*$ na množine $a \times a$, o ktorom potom ukážeme, že je dobrým usporiadaním.

Definujme $\leq^*$ takto: Nech $m_1 = \max\{a_1, b_1\}$ a $m_2 = \max\{a_2, b_2\}$. Potom

$$(a_1, b_1) \leq^* (a_2, b_2) \Leftrightarrow \begin{cases} (m_1 < m_2) & \vee \\ (m_1 = m_2 \wedge a_1 < a_2) & \vee \\ (m_1 = m_2 \wedge a_1 = a_2 \wedge b_1 < b_2) \end{cases}$$

Nie je ťažké overiť, že ide o lineárne usporiadanie. (Prvky množiny a sme vlastne umiestnili do akýchsi štvorcov a usporiadali najprv podľa toho, na hranici ktorého štvorca ležia a ako sekundárne kritérium sme použili lexikografické usporiadanie.) Je to aj dobré usporiadanie – pre každú podmnožinu $a \times a$ môžeme vybrať najmenšie m, ktoré sa vyskytuje ako maximum nejakej dvojice prvkov tejto podmnožiny. Keď sa už pozeráme iba na prvky s rovnakým maximom, tie sú usporiadané lexikograficky.

Navyše, každý dolný úsek $a \times a_{(a_1,b_1)} = \{(x, y) \in a \times a; (x, y) <^* (a_1, b_1)\}$ má kardinalitu menšiu ako a. (Jeho kardinalita je rovná súčinu kardinalít dolných úsekov pre a_1 a b_1 v usporiadaní. Ak $m_1 = \max\{a_1, b_1\}$, tak ju zhora môžeme odhadnúť $|a_{m_1}|.|a_{m_1}|$. Pretože $|a_{m_1}| < a$ a predpokladáme, že dokazované tvrdenie platí pre všetky kardinály menšie ako a, dostávame $|a_{m_1}|.|a_{m_1}| = |a_{m_1}|$.)

Potom pre každý počiatočný úsek $(a \times a, \leq^*)$ existuje bijekcia na počiatočný úsek dobre usporiadanej množiny $(a, \leq)$. (Vieme, že pre 2 dobre usporiadané existuje buď zobrazenie jednej na počiatočný úsek druhej alebo obrátene. Množinu $(a, \leq)$ však nemožno vnoriť do $(a \times a, \leq^*)$ ako počiatočný úsek, lebo potom by tento počiatočný úsek musel mať kardinalitu a). Navyše, všetky tieto vnorenia na počiatočné úseky sú kompatibilné.

Vďaka tomu ako zjednotenie týchto zobrazení (inak povedané – ako zobrazenie, ktorého hodnota bude spoločná hodnota všetkých vnorení) dostaneme vnorenie $(a \times a, \leq^*)$ na počiatočný úsek $(a, \leq)$. Tým sme našli injekciu z $a \times a$ do a, preto platí

$$a.a \leq a.$$

Opačná nerovnosť je zrejmá, čím dostávame rovnosť $a.a = a$.

Poznamenajme ešte, že argumentovaním pomocou kardinality sme mohli dokonca ukázať, že uvedené vnorenie je v skutočnosti priamo bijekcia. □

{aplikord:DOSSUCMAX}

Dôsledok 7.6.2. *Ak a, b sú nekonečné kardinály, tak*

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

[3] Odkiaľ vieme, že usporiadanie $\leq$ s uvedeným vlastnosťami existuje? Ak kardinály chápeme ako ordinály, tak je to priamo usporiadanie ordinálu a. Môžeme to dostať aj inak: Vezmeme si ľubovoľné dobré usporiadanie množiny A, ktorá má kardinalitu a – nejaké dobré usporiadanie A existuje podľa (WO). V tomto usporiadaní vezmeme najmenší prvok b taký, že $A_b = \{x \in A; x < b\}$ má kardinalitu a. Ak taký prvok neexistuje, tak už pôvodné usporiadanie množiny A má požadovanú vlastnosť. Ak taký prvok existuje, tak pomocou bijekcie medzi A_b a A môžeme preniesť toto usporiadanie na celú množinu A.

Dôkaz. Bez ujmy na všeobecnosti nech $a \leq b$. Potom

$$b \leq a + b \leq b + b = 2b \leq a.b \leq b.b = b.$$

□

7.6.2 Ekvivalenty axiómy výberu

{aplikord:SSECTEKVAC}

Vo vete 6.1.5 sme si povedali, že AC, WO, ZL a PM sú ekvivalentné v ZF. Zatiaľ sme dokázali však len implikácie ZL $\Rightarrow$ WO $\Rightarrow$ AC a ekvivalenciu ZL $\Leftrightarrow$ PM. S využitím transfinitnej indukcie teraz dokončíme dôkaz tejto vety.

Dôkaz implikácie AC $\Rightarrow$ ZL. Nepriamo. Nech $(P, \leq)$ je čiastočne usporiadaná množina, ktorá nemá maximálny prvok. To znamená, že pre každé $p \in P$ je

$$p\uparrow = \{q \in P; q > p\} \neq \emptyset.$$

Nech f je selektor na množine $\mathcal{P}(P) \setminus \{\emptyset\}$. Transfinitnou indukciou definujeme:
$p_0 = f(P)$;
$p_{\beta+1} = f(p_\beta\uparrow)$;
$p_\beta = f(\{q \in P; q$ je horné ohraničenie pre $\{p_\gamma; \gamma < \beta\}\})$, ak β je limitný ordinál a existuje aspoň jedno horné ohraničenie množiny $\{p_\gamma; \gamma < \beta\}$.

Tento proces sa musí raz zastaviť, inak by sme takto dostali bijekciu medzi podmnožinou množiny P a všetkými ordinálmi, čo je spor s tvrdením 7.2.21.

Dostaneme tak, ordinál α pre ktorý

$$\{p_\gamma; \gamma < \alpha\}$$

je reťazec v $(P, \leq)$, ktorý nemá horné ohraničenie. □

Poznámka 7.6.3. Použitie transfinitnej rekurzie v predchádzajúcom dôkaze je odlišné od toho, čo sme dokázali vo vete 7.4.4. Tam sme mali vopred daný ordinál, na ktorom sme definovali α nejaké zobrazenie. V predchádzajúcom dôkaze sme tento ordinál α získali len v priebehu dôkazu – konkrétne ako ten ordinál, pri ktorom sa zastaví induktívny proces, lebo sa vyčerpajú všetky možnosti.

Dôkaz by sme vedeli pomerne ľahko zmodifikovať tak, aby zodpovedal vete 7.4.4. Mohli by sme napríklad zobrať suprémum všetkých ordinálnych typov dobrých usporiadaní na podmnožinách množiny P zväčšené o 1. Pre tento ordinál máme zaručené, že nastane situácia, keď množina $\{p_\gamma; \gamma < \beta\}$ už nemá horné ohraničenie. (Stačí si uvedomiť, že ide o dobre usporiadanú podmnožinu P, čiže ordinálny typ je menší ako zvolený ordinál.) Museli by sme nejako dodefinovať p_β pre prípad, že táto množina je prázdna. Potom by sme pracovali s najmenším ordinálom, pre ktorý tento prípad nastane a zvyšok dôkazu by bol rovnaký.

Aj v ďalšom dôkaze použijeme podobný postup. (Takýto postup sa často využíva i v literatúre.) Pokiaľ čitateľ chce, môže si i pri nasledujúcom dôkaze rozmyslieť, ako by sa tam vyriešil analogický problém.

Hoci implikácia AC $\Rightarrow$ WO vyplýva z už dokázaných tvrdení, ukážeme si, ako na jej dôkaz možno použiť transfinitnú indukciu.

Dôkaz implikácie AC $\Rightarrow$ WO. Nech X je neprázdna množina a f je selektor na $\mathcal{P}(X) \setminus \{\emptyset\}$.

Transfinitnou indukciou definujeme pre ordinál β

$$g(\beta) = f[X \setminus g[\beta]],$$

pričom sa zastavíme pri prvom ordinále pre ktorý je $X \setminus g[\alpha] = \emptyset$, t.j. $g[\beta] = X$.

Takto dostaneme bijekciu $g\colon \alpha \to X$ Na x môžeme potom zadefinovať usporiadanie predpisom

$$g(\beta) \leq g(\gamma) \Leftrightarrow \beta \leq \gamma.$$

Dostaneme tak dobré usporiadanie, ktorého ordinálny typ je α. □

7.6.3 Aplikácie v algebre a analýze

{aplikord:VTSTEINITZ}

Veta 7.6.4 (Steinitz)**.** *Steinitzova veta: Pre každé pole existuje algebraicky uzavreté nadpole, ktoré ho obsahuje.*

Najprv pripomeňme niečo, čo ste sa kedy si učili na algebre. Pre každý polynóm $f(x) \in F[x]$ existuje rozkladové pole tohoto polynómu – je to také nadpole poľa F, v ktorom sa dá polynóm $f(x)$ rozložiť na súčin konštanty a koreňových činiteľov.[4] Pozri napríklad [KGGS, Kapitola 8.3], [CL, Section 2.2], [Sl1].

Dôkaz. Transfinitnou indukciou o chvíľu ukážeme, že pre dané pole F existuje algebraické rozšírenie[5] K, v ktorom sa každý polynóm $f(x) \in F[x]$ dá rozložiť na súčin koreňových činiteľov. Ukážme najprv však, že takéto pole už nutne musí byť algebraicky uzavreté.

Uvažujme ľubovoľný ireducibilný polynóm $p(x) \in K[x]$. Nech koeficienty polynómy $p(x)$ sú $a_0, \ldots, a_n \in K$. Potom p je polynómom už nad menším poľom $L := F(a_0, \ldots, a_n) \subseteq K$. V nadpoli $L[x]/(p(x))$ má polynóm $p(x)$ koreň. Pole L je algebraickým rozšírením poľa F (každý z prvkov $a_0, \ldots, a_n$ je algebraický na F) a v $L[x]/(p(x))$ existuje koreň α polynómu $p(x)$. Tento koreň je teda algebraický nad L, čiže je aj algebraický nad F. Existuje teda minimálny polynóm $q(x)$ tohoto koreňa nad poľom F. Tento minimálny polynóm je v $L[x]$ delí polynóm $p(x)$, čiže $q(x) = p(x).r(x)$. Táto rovnosť platí aj v $K[x]$ (K je nadpole L), ale v K sa navyše polynóm $q(x)$ dá rozložiť na súčin koreňových činiteľov. Z toho vyplýva, že aj $p(x)$ sa dá rozložiť na súčin koreňových činiteľov.

Zostáva teda dokázať, že sa dá zostrojiť pole K s uvedenými vlastnosťami. Toto pole skonštruujeme transfinitnou rekurziou.

Nech $\{f_\beta(x), \beta < \gamma\}$ sú všetky ireducibilné polynómy nad F oindexované ordinálmi menšími ako γ. (Využili sme fakt, že množinu ireducibilných polynómov možno dobre usporiadať.) Pre každé $\alpha \leq \gamma$ zostrojíme algebraické rozšírenie K_α poľa F, v ktorom je každý polynóm $f_\beta(x)$ pre $\beta < \alpha$ rozložiteľný na súčin koreňových činiteľov.

1° Pre $\alpha = 0$ zoberieme priamo pole K.

2° Ak máme zostrojené pole K_α, tak $K_{\alpha+1}$ bude rozkladové pole polynómu f_α nad poľom K_α. Rozkladové pole je algebraické rozšírenie K_α, pretože K_α je algebraické rozšírenie F je aj K_α algebraickým rozšírením F.

3° Ak α je limitný ordinál, tak by sme K_α chceli zadefinovať ako pole, ktoré bude obsahovať K_β pre všetky $\beta < \alpha$ – čosi ako zjednotenie týchto polí. Pretože všetky polia sú také, že polia oindexované nižšími ordinálmi sú vnorené ako podpolia v tých poliach, ktoré majú vyššie indexy, môžeme priamo predpokladať, že sú to polia na podmnožinách tej istej množiny (toto si treba rozmyslieť!) a potom skutočne stačí zobrať priamo zjednotenie týchto polí. □

[4] Navyše sa v definícii rozkladového poľa ešte vyskytuje podmienka, že je to v istom zmysle najmenšie pole s touto vlastnosťou, t.j. je generované množinou $F \cup \{u_1, \ldots, u_n\}$, kde $u_1, \ldots, u_n$ sú korene $f(x)$ v rozkladovom poli. Túto druhú vlastnosť však potrebovať nebudeme. Pripomeňme tiež, pre ireducibilný polynóm $f(x) \in F[x]$ je $F[x]/(f(x))$ nadpole F, v ktorom má $f(x)$ aspoň jeden koreň. Existencia rozkladového poľa sa dokázala induktívne pomocou tejto konštrukcie.

[5] t.j. každý z prvkov K je algebraický nad F

Po príklade z algebry by sa snáď hodil nejaký príklad z analýzy. Ukážeme, ako môžeme zostrojiť použitím transfinitnej rekurzie reálne funkcie, ktoré majú neobvyklé vlastnosti.

Tvrdenie 7.6.5. *Existuje podmnožina $A \subseteq \mathbb{R} \times \mathbb{R}$ taká, že všetky x-ové rezy $A_x = \{y \in \mathbb{R}; (x,y) \in A\}$ sú jednoprvkové a všetky y-ové rezy $A^y = \{x \in \mathbb{R}; (x,y) \in A\}$ sú husté v $\mathbb{R}$.*

Takáto množina je grafom silno darbouxovskej funkcie. Funkcia $f\colon \mathbb{R} \to \mathbb{R}$ sa volá *silno darbouxovská,* ak pre ľubovoľné reálne čísla $a < b$ nadobúda f na intervale (a,b) všetky reálne hodnoty.

Slabšia vlastnosť je *darbouxovská funkcia* – ak nadobúda všetky hodnoty medzi $f(a)$ a $f(b)$. Z analýzy viete, že každá spojitá funkcia je darbouxovská. Príklad silno darbouxovskej funkcie je súčasne príklad darbouxovskej funkcie, ktorá nie je spojitá.

Dôkaz. V dôkaze budeme netradične používať označenie $[a,b]$ pre dvojice reálnych čísel – z toho dôvodu, že tu budeme často pracovať s otvorenými intervalmi na reálnej osi a nechceme, aby sa tieto 2 označenia plietli.

Transfinitnou rekurziou budeme definovať množinu B s podobnými vlastnosťami s tým rozdielom, že x-ové rezy B_x sú najviac jednoprvkové.

Najprv si poriadne uvedomme, že znamená požiadavka na y-vé rezy. Vlastne chceme, aby pre každý interval (a,b) a pre každé $y \in \mathbb{R}$ platilo

$$A \cap (a,b) \times \{y\} \neq \emptyset.$$

Množina všetkých takýchto vodorovných úsečiek v rovine $\{(a,b) \times \{y\}; y,a,b \in \mathbb{R}, a < b\}$ má kardinalitu $\mathfrak{c}$. Môžeme ich teda dobre usporiadať pomocou ordinálu, ktorý zodpovedá kardinálu $\mathfrak{c}$. (Inak povedané, dá sa dobre usporiadať tak, že vlastné počiatočné úseky budú mať kardinalitu menšiu ako $\mathfrak{c}$.)

Majme teda nejaké takéto usporiadanie $\{U_\alpha = (a_\alpha, b_\alpha) \times \{y_\alpha\}; \alpha < \mathfrak{c}\}$.

Transfinitnou rekurziou pomocou neho zostrojíme $B = \{(x_\alpha, y_\alpha); \alpha < \mathfrak{c}\}$. (V tomto prípade nebude potrebné rozdeľovať indukciu podľa typu ordinálu.)

Predpokladajme, že už máme zadefinované x_β pre všetky $\beta < \alpha$. Prvok y_α už máme zadefinovaný usporiadaním úsečiek U_α. Množina $\{x_\beta; \beta < \alpha\}$ má kardinalitu menšiu ako $\mathfrak{c}$, teda množina $(a_\alpha, b_\alpha) \setminus \{x_\beta; \beta < \alpha\}$ je neprázdna. Za x_α zvolíme nejaký jej prvok.

Takto postupne zostrojíme množinu B, ktorá má neprázdny prienik s každou úsečkou U_α, teda spĺňa podmienku pre y-ové rezy. Navyše voľba x_α v indukčnom kroku zabezpečí, že žiadne x sa nevyskytne dvakrát, čiže y-ové rezy B sú najviac jednoprvkové.

Množinu A zostrojíme tak, že pre x-ové súradnice, ktoré sa v B nevyskytli, zvolíme y-ovú súradnicu ľubovoľne. Napríklad ak ju zvolíme ako nulu, tak $A = B \cup \{(x,0); x \in \mathbb{R}, B_x = \emptyset\}$. □

Literatúra

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

[B2] Lev Bukovský. *Štruktúra reálnej osi.* Veda, Bratislava, 1979.

[B3] Lev Bukovský. *Množiny a všeličo okolo nich.* Alfa, Bratislava, 1985.

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

[Č1] Juraj Činčura. Elementárna teória čísel. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/cvicenia/tc/`.

[Č2] Juraj Činčura. Model aritmetiky celých nezáporných čísel v teórii množín. `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/2010/temno/cisla.pdf`.

[Č3] Juraj Činčura. Teoretická aritmetika. `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?jazyk=sk&clen=cincura`.

[CL] Antoine Chambert-Loir. *A Field Guide to Algebra.* Springer, New York, 2005. Undergraduate Texts in Mathematics.

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

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

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

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

[Ha] Paul R. Halmos. *Naive Set Theory.* Springer-Verlag, New York, 1974. Undergraduate Texts in Mathematics.

[He1] Horst Herrlich. Choice principles in elementary topology and analysis. *Comment. Math. Univ. Carolinae*, 38(3):545–552, 1997.

[He2] Horst Herrlich. *The Axiom of Choice.* Springer-Verlag, Berlin, 2006. Lecture Notes in Mathematics 1876.

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

[HR] Paul Howard a Jean E. Rubin. *Consequences of the axiom of choice.* Mathematical Surveys and Monographs. 59. Providence, RI: American Mathematical Society (AMS), 1998.

[J] Thomas J. Jech. *The Axiom of Choice.* North-Holland, Amsterdam, 1973.

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

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

[Lev] Azriel Levy. *Basic set theory.* Courier Dover Publications, 2002.

[Lew] Jonathan Lewin. A simple proof of Zorn's lemma. *Amer. Math. Monthly*, 98:353–354, 1991.

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

[M] Gregory H. Moore. *Zermelo's Axiom of Choice. Its Origins, Development and Influence.* Springer-Verlag, New York, 1982.

[OŠ] Daniel Olejár a Martin Škoviera. *Úvod do teórie diskrétnych matematických štruktúr.* Univerzita Komenského, Bratislava, 2007. `http://www.dcs.fmph.uniba.sk/texty/dsmain.pdf`.

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

[Sl1] Martin Sleziak. 1-INF-155 Algebra 2. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[Sl2] Martin Sleziak. Lineárna algebra. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[So] Antonín Sochor. *Klasická matematická logika.* Karolinum, Praha, 2001.

[Š] Petr Štěpánek. Predikátová logika. `http://kti.ms.mff.cuni.cz/teaching/files/materials/StepanekPetr_PredikatovaLogika.pdf`.

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

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

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

[Wa] Leonard M. Wapner. *The Pea and the Sun.* A. K. Peters, Wellesley, Massachusetts, 2005.

[Wi] Freek Wiedijk. Formal proof–getting started. *Notices of AMS*, 55(11):1408–1414, 2008. `http://www.ams.org/notices/200811/tx081101408p.pdf`.

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

[WR] A. N. Whitehead a B. Russell. *Principia mathematica, vol.1.* Cambridge University Press, Cambridge, 1st edition.

[Z1] Pavol Zlatoš. O dobrom usporiadaní a axióme výberu. `http://thales.doa.fmph.uniba.sk/zlatos/wo/DUAC1w.pdf`.

[Z2] 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