Aplikácie teórie množín

Martin Sleziak

8. februára 2023

Obsah

Kapitola 1

Úvod

Verzia: 8. februára 2023

1.1 Sylaby a literatúra

1.1.1 Literatúra

Pri príprave týchto poznámok som čerpal najmä z kníh [BŠ, Ci, Hal1, Her2, HH, JW1, JW2, KT]. Niektoré cvičenia sú prevzaté z [Li]. Prednáška predpokladá, že už ovládate základné poznatky z teórie množín, ak si ich potrebujete zopakovať, tak vhodné texty sú napríklad [ŠS, Sl3], ale v podstate aj úvodné kapitoly skoro akejkoľvek pokročilejšej učebnice teórie množín. Aspoň zhruba otestovať, či ovládate poznatky z teórie množín potrebné na zvládnutie tejto prednášky, môžete v časti 2.1 nazvanej *vstupný test*.

Táto prednáška zahŕňa aj aplikácie teórie množín v iných oblastiach, tu som okrem kníh venovaných teórii množín čerpal aj z iných textov, ako napríklad [AB, Bu3, CL, Eng, Hal2, Hei, Jo, Kha1, Kha2, Ku, NS, O, Tao, Wil]. Pri príprave prednášok mi pomohli aj mnohé internetové zdroje ako napríklad [MO, MSE, WIK, Ma, TRI].

1.1.2 Sylaby predmetu

Axióma výberu a jej ekvivalentné formulácie. Zornova lema a jej aplikácie. Ordinály, transfinitná indukcia a jej aplikácie. Skoro disjunktné systémy, nekonečné stromy, ultrafiltre.

1.2 Predhovor

Cieľom tohoto predmetu i sprievodného textu je zoznámiť sa s niektorými výsledkami a dôkazovými technikami založenými na teórii množín a ukázať si aj nejaké ich aplikácie. Najdôležitejšie z nich sú zrejme Zornova lema a transfinitná indukcia. Je veľmi pravdepodobné, že s použitím aspoň jednej z týchto dvoch metód ste sa už stretli na iných predmetoch. Tu sa im budeme venovať podrobnejšie a budeme sa snažiť uviesť aj dôkaz, prečo dôkazy založené na týchto postupoch naozaj fungujú.

Od čitateľa sa očakáva ovládanie teórie množín prinajmenšom v rozsahu preberanom na predmete Diskrétna matematika v prvom ročníku. Budeme sa snažiť ukázať si rôzne aplikácia množinovo-teoretických výsledkov v algebre, analýze, kombinatorike. Preto je užitočné mať dobrý základ z viacerých matematických disciplín preberaných v rámci bakalárskeho štúdia.

Zornova lema, transfinitná indukcia ako aj iné výsledky teórie množín našli využitie vo viacerých matematických disciplínach. Výber aplikácií, ktoré sú uvedené v tomto texte je do značnej miery závislý na osobných preferenciách autora (a takisto je podmienený i jeho (ne)vedomosťami). Aj keď je pravda, že typicky sa takéto aplikácie dajú nájsť skôr v oblastiach blízkych algebre, analýze, geometrii a topológii než napríklad v diskrétnej matematike.

Kapitola 2 nazvaná opakovanie by mala obsahovať prehľad vecí, s ktorými by ste sa mali stretnúť už niekedy v nižších ročníkoch. (Aj keď je tam zopár drobných poznámok navyše.) Text podstatný pre tento predmet začína až po nej.

Je veľmi pravdepodobné, že na prednáške nestihneme prebrať úplne všetko, čo je spomenuté v tomto texte. (Osobne za najdôležitejšie považujem aplikácie axiómy výberu a Zornovej lemy a tiež transfinitnú indukciu. Ďalšie veci, ktorým sa tu venujeme, sú tiež zaujímavé a užitočné, ale v matematickej praxi sa vyskytujú rozhodne menej ako Zornova lema a transfinitná indukcia.) Snažil som sa písať tento text tak, aby sa dal použiť aj pri samostatnom štúdiu. Takže ho môžete použiť aj v prípade, že nebude navštevovať prednášku, pre ktorú je určený; ale aj účastníci kurzu si môžu samostatne pozrieť ďalšie témy, na ktoré počas semestra nezvýšil čas.

Niektoré časti uvedené v tomto texte na prednáške vôbec neplánujem preberať. Sú tu uvedené do istej miery pre úplnosť resp. preto, že by mohli čitateľa zaujímať. Takéto „nepovinné“ (možno by bolo lepšie povedať doplňujúce) časti sú vyznačené menším fontom alebo hviezdičkou pri názve príslušnej podkapitoly. (Zhruba povedané, sú to veci, ktoré nejako súvisia s téma preberanými na tomto predmete, ale nie sú jadrom toho, čomu by som sa mal venovať. Stále sa mi však z nejakých dôvodov zdalo užitočné ich spomenúť.)

V dodatkoch sú uvedené tiež niektoré veci, ktoré nebudem preberať, ale sú užitočné pri niektorých aplikáciách uvedených v texte. (Niektoré z týchto vecí by ste mohli poznať z iných predmetov.)

1.2.1 Špecifiká tohoto predmetu

V tomto texte sa stretneme z rôznymi dôkazovými technikami založenými na teórii množín, ktoré sa dajú využiť v rôznych oblastiach matematiky. Stretneme sa napríklad z aplikáciami v algebre, reálnej analýze, teórii miery, funkcionálnej analýze, všeobecnej topológii, atď. Teda okrem teórie množín sa budeme venovať aj rôznym ďalším oblastiam matematiky, aby sme si ilustrovali, ako sa dajú výsledky, ktoré sme sa naučili, použiť. Chceme síce aj vysvetliť, prečo tieto techniky fungujú. Nebolo by rozumné naučiť sa nejaké postupy bez toho, aby sme videli ich použitie v praxi.

V závislosti od toho, aké predmety ste už absolvovali a čo všetko už viete, sa môže stať, že sa tu znovu dozviete niektoré veci, ktoré už poznáte. (Čo nemusí byť nutne na škodu.) Ale takisto sa môže stať, že zablúdime do oblastí, ktoré sú pre vás nové a kde sa budete musieť pokúsiť aspoň trochu zorientovať, aby ste rozumeli uvedeným výsledkom. (Čo tiež nemusí byť na škodu. Pre vás ako budúcich matematikov je určite užitočné nadobudnúť schopnosť získať rýchlo aspoň v hrubých rysoch predstavu o nejakej novej matematickej oblasti.)

Snažil som sa tu v nejakej rozumnej miere uviesť aj veci z iných oblastí matematiky, ktoré potrebujeme. V rozumnej miere znamená to, že by som nemal priveľmi opakovať veci, ktoré by ste mali všetci bez problémov ovládať. Ale takisto, ak to má byť text o teórii množín, asi by nebolo dobre, aby sme v ňom veľa času strávili budovaním teórie patriacej do nejakej úplne inej oblasti.

V texte takejto dĺžky sa nevyhnutne vyskytnú rôzne chyby a preklepy. Budem sa ich snažiť postupne upravovať. Takže v ďalších verziách tohoto textu snáď niektoré z nich odbudnú (a nejaké naopak pribudnú).

1.2.2 Čo je Zornova lema a transfinitná indukcia?

Všetci sme sa už veľakrát stretli s rôznymi použitiami matematickej indukcie. Je to často užitočná dôkazová technika. Matematickú indukciu vieme využiť aj na konštrukciu (resp. dôkaz existencie) rôznych objektov.

Zjednodušene sa dá povedať, že ak si zdôvodnenie nejakého tvrdenia vieme predstaviť ako nejaký proces, ktorý vieme urobiť pre jeden, dva, tri prvky, tak na mieste, kde by sme povedali „a podobným spôsobom postupujeme ďalej" ako formálny dôkaz často použijeme matematickú indukciu.

Istým obmedzením tejto metódy je to, že „podobne postupovať ďalej" môžeme iba pre prirodzené čísla. Matematickou indukciou teda vieme dokázať, že nejaké tvrdenie platí pre každé prirodzené číslo. Mali by sme však problém zdôvodniť takýmto spôsobom nejakú vec pre každé reálne číslo.

Veľmi zjednodušene sa dá povedať, že transfinitná indukcia a Zornova lema nám (za istých podmienok) umožnia induktívne pokračovať aj za hranice prirodzených čísel. Azda nie úplne neprirodzený pohľad na tieto dve dôkazové techniky je brať ich ako dve možné rozšírenia matematickej indukcie. (Táto analógia je asi pomerne nejasné a aj nepresná. Snáď na konci prednášky bude jasnejšie, čo sa chce týmto prirovnaním povedať.)

Ešte sa na chvíľu vrátim k prirovnaniu týchto dvoch techník k matematickej indukcii. Zrejme každý, kto je na dostatočnej matematickej úrovni, aby študoval tento text, bežne používa matematickú indukciu. Asi by ste si vedeli predstaviť, že by ste sa snažili niekoho naučiť matematickú indukciu. Keď si rozmyslíte, ako by ste na to išli, tak si vcelku ľahko uvedomíte dve veci.

To, že niekto ovláda matematickú indukciu, zrejme poviete až vtedy, keď ju vie používať v praxi. Určite je dôležité vysvetliť, prečo vlastne indukcia funguje. Ale pre praktické používanie je asi dosť dôležité odskúšať si veľa príkladov a zvyknúť si na bežné triky, ktoré sa pri indukcii často vyskytujú. Napríklad:

- Niekedy je užitočné dokazovať silnejšie tvrdenie. (Silnejší predpoklad nám poslúži v indukčnom kroku.)
- Často sa stane, že v indukčnom kroku zistíme, že potrebujeme nejaké pomocné tvrdenie. Skúsime teda toto pomocné tvrdenie sformulovať a dokázať indukciou.
- Ak tvrdenie obsahuje viacero premenných, tak môže záležať na tom, ktorú premennú vyberieme. Niekedy môže dôkaz zjednodušiť použitie novej indukčnej premennej, ktorá v dokazovanom tvrdení vôbec nevystupuje. (Napríklad: $N = m+n$ alebo $N = \max\{m, n\}$.)
- Niekedy je vhodné techniku dôkazu matematickou indukciou trochu zmodifikovať (silná indukcia, Cauchyho indukcia).

Podobných trikov je určite ešte oveľa viac. Človek, ktorý má dostatočnú prax a ovláda základné triky, je schopný zvládnuť bežné dôkazy založené na matematickej indukcii bez najmenších problémov.

Aj na tejto prednáške sa chceme zaoberať nejakými dôkazovými technikami. Budeme chcieť povedať niečo o tom, prečo vlastne fungujú. Ale veľmi dôležité bude vidieť dostatočný počet príkladov a naučiť sa ich používať. Ak sa vám na konci prednášky bude zdať, že väčšina dôkazov používajúcich Zornovu lemu alebo transfinitnú indukciu je na jedno kopyto a nebudete mať s nimi žiadne problémy, tak táto prednáška splnila svoj účel.

Ešte raz si skúste predstaviť, že by ste niekoho učili matematickú indukciu. Možno by ste začali tým, že by ste vysvetlili, ako a prečo tento typ dôkazu vlastne funguje. Potom by ste sa už ale pravdepodobne venovali precvičovaniu dôkazovej techniky. Na to by ste vybrali konkrétne príklady (napríklad dôkazy nejakých vzorcov pre sumy, niečo o deliteľnosti, dôkazy nejakých nerovností, rôzne vlastnosti Fibonacciho postupnosti). Určite budú tieto príklady prístupnejšie pri niekoho, kto sa s pojmami vystupujúcimi v zadaniach úloh už niekde stretol. Takisto bude pre takéhoto človek jasnejšie, že sa naučil niečo užitočné. (Aj keď je v princípe vcelku predstaviteľné, že sa niekto spolu s matematickou indukciou naučí aj niektoré nové veci, na ktoré sa dá použiť.) Podobne ak niekomu ukážete dôkaz nerovnosti medzi aritmetickým priemerom pomocou Cauchyho indukcie[1], tak v prípade, že dotyčný túto nerovnosť predtým nikdy v živote nevidel, môžete čakať reakciu ako: „Ok, no tak sme dokázali takúto nerovnosť. Ale nie je jasné, či to je na niečo dobré.“ Ale človek, ktorý túto nerovnosť videl veľakrát použitú a vie teda, že je užitočná, prípadne sa ju pokúšal dokázať sám a nepodarilo sa mu nájsť nejaký jednoduchý dôkaz, si možno povie: „To je super, aký pekný trik. Nečakal som, že AM-GM nerovnosť sa dá dokázať aj takto jednoducho.“ Alebo: „Do kelu, a ja som sa to snažil robiť cez Lagrangeove multiplikátory.“

V podobnej situácii sme aj my, keď sa chceme naučiť niečo o Zornovej leme a transfinitnej indukcii. Sú to dôkazové techniky, ktoré sú užitočné a často používané v rôznych oblastiach matematiky. Je zaujímavé vedieť aj to, prečo fungujú. Ale na to, aby sme boli schopní porozumieť dôkazom, kde sa tieto techniky vyskytujú, a aj ich samostatne používať, je dôležité vyskúšať si na viacerých úlohách ich použitie. Dá sa nájsť zopár aplikácií, ktoré nevyžadujú prakticky žiadne prerekvizity. (Napríklad ak ich aplikujeme na výsledky o čiastočne usporiadaných množinách, ktorým treba rozumieť už len na to, aby človek pochopil formuláciu Zornovej lemy či princíp transfinitnej indukcie. Alebo ak ich používame na dôkaz nejakého tvrdenia o kardinalite, čo je pojem, ktorý by mal mať človek zvládnutý, keď si zapíše pokročilejší kurz z teórie množín.) Ale väčšina aplikácií uvedených v tomto texte (či už ako tvrdenia s dôkazom alebo ako úlohy na precvičenie) predpokladá znalosti z nejakej oblasti matematiky. V princípe sa dá pozrieť sa na základné veci z danej oblasti pri štúdiu tohoto textu. Ale človek majúci aspoň základné znalosti z tej disciplíny, v ktorej chceme množinovo–teoretické výsledky aplikovať, je očividne vo výhode.

1.2.3 Aspoň jeden konkrétny príklad

Síce som toho napísal pomerne dosť, ale z predchádzajúceho textu asi nie je príliš jasné, čo vlastne Zornova lema resp. transfinitná indukcia je. Skúsim teda pridať aspoň jeden príklad, ktorý tu síce nedokončím, ale aspoň by mohol naznačiť, pri akých typoch úvah budú tieto techniky užitočné.[2] Keď sa naučíte viac z vecí, ktorým sa chceme venovať práve ne tomto predmete, tak budete vedieť tento postup dokončiť. Táto úloha je v tomto texte aj ako problém 4.3.3.

Skúsme sa pozrieť na to, či by sme vedeli povedať niečo o funkciách $f\colon \mathbb{R} \to \mathbb{R}$ takých že

{predh:EQCAUCHY}
$$(\forall x, y \in \mathbb{R}) f(x+y) = f(x) + f(y). \tag{1.1}$$

(Možno viete, že tejto rovnici sa hovorí Cauchyho funkcionálna rovnica.) Nie je ťažké zistiť, že každá funkcia tvaru $f(x) = ax$ je riešením – zaujímalo by nás ale, či existujú aj nejaké iné riešenia.

Mali by ste byť schopní prísť na to, že ak f spĺňa podmienku (1.1) tak musí platiť $f(rx) = rf(x)$ pre $r \in \mathbb{Q}$ (a ľubovoľné x).

{predh:EQQLIN}
$$(\forall r \in \mathbb{Q})(\forall x \in \mathbb{R}) f(rx) = rf(x) \tag{1.2}$$

Týmto sme vlastne prišli na to, že ak sa pozeráme na $\mathbb{R}$ ako na vektorový priestor nad $\mathbb{Q}$, tak ide o lineárne zobrazenie – potom už s použitím nejakých, aj keď možno nie úplne

[1] `http://math.stackexchange.com/questions/97350/`

[2] Tento príklad je zvolený preto, že je jednoduchý a netreba naň žiadne prerekvizity – takže by sa mohol hodiť ako úvodný príklad. Je „ukradnutý“ z blogu T. Gowersa: `https://gowers.wordpress.com/2008/08/12/how-to-use-zorns-lemma/`, `http://www.tricki.org/article/How_to_use_Zorns_lemma`. Oplatí sa prečítať – je to tam vysvetlené určite lepšie než sa podarí mne.

triviálnych, faktov z lineárnej algebry by sme vedeli vyriešiť túto úlohu. Konkrétne by nám pomohli veci uvedené v probléme 4.3.1. Skúsme sa ale ešte chvíľu radšej pozrieť na to, či vieme niečo povedať bez odvolávania sa na nejaké pokročilejšie výsledky.

Pozorovanie o racionálnych násobkoch by nám stačilo na to, že ak by sme vedeli vyriešiť trochu modifikovanú úlohu, kde hľadáme iba zobrazenia $\mathbb{Q} \to \mathbb{R}$. V tomto prípade skutočne všetky riešenia majú tvar $f(x) = ax$, kde $a = f(1)$. Otázka je, či sa niečo zmení, ak chceme rozšíriť f na reálne čísla. Začnime pomaly, skúsme aspoň o trochu zväčšiť definičný obor.

Ak poznáme $f(1)$, tak sú na základe (1.2) už jednoznačne určené hodnoty pre všetky racionálne čísla. Táto podmienka nám však nič nehovorí o $f(\sqrt{2})$. Povedzme, že si nejako vyberieme, čomu sa má táto hodnota rovnať. Potom vieme nájsť hodnotu pre všetky čísla z $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$, konkrétne

$$f(a + b\sqrt{2}) = af(1) + bf(\sqrt{2}).$$

Vidíme, že ak si zvolíme $f(1)$ a $f(\sqrt{2})$, tak zadaná funkcionálna rovnica nám vynúti ako sa správa funkcia na množine $\mathbb{Q}(\sqrt{2})$. Podarilo sa nám od $\mathbb{Q}$ pohnúť k väčšej množine, stále máme však ďaleko od toho, aby sme poznali funkciu f na celom $\mathbb{R}$.

Vedeli by sme nejako podobne postupovať ďalej? Ak vieme, že $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, tak vidíme, že si môžeme zvoliť $f(\sqrt{3})$ ľubovoľne. Dostali by sme tak rozšírenie na funkciu definovaná pre všetky čísla tvaru $a + b\sqrt{2} + c\sqrt{3}$, $a, b, c \in \mathbb{Q}$. Stále sme tak nepokryli všetky reálne čísla – vieme napríklad, podobne by sa dalo postupovať pre ľubovoľné odmocniny prvočísel, t.j. pridávať ďalej $\sqrt{5}, \sqrt{7}, \sqrt{11}, \dots$. (Aj keď je asi o čosi ťažšie dokázať pre ľubovoľné prvočíslo p, že $\sqrt{p}$ sa nedá dostať ako racionálna kombinácia jednotky a menších prvočísel, než to bolo pre $\sqrt{3}$ a $\mathbb{Q}(\sqrt{2})$.)

Vôbec by sme však nemuseli pridávať prvky takto explicitne. Ak sme začali s $a_0 = 1$ a $a_1 = \sqrt{2}$, mohli by sme si zvoliť úplne ľubovoľné a_2 také, že nie je racionálnou kombináciou a_0 a a_1. Potom by sme volili a_3, ktoré sa nedá dostať z a_0, a_1, a_2, atď.

Takto indukciou vieme definovať funkcie definované na čoraz väčších množinách – stále nie na celom $\mathbb{R}$. (Stačí si uvedomiť, že takto dostaneme vždy iba spočítateľnú množinu.)

Práve techniky, ktorým sa chceme venovať, nám umožnia pokračovať ďalej. (Ak by sme chceli pokračovať takto, tak sa dá použiť buď Zornova lema. Iná možnosť by bola transfinitná indukcia v kombinácii s princípom usporiadania.) Na tomto mieste končí časť, kde boli veci, ktoré vieme dokázať poriadne a stačia nám na to vedomosti z prvého ročníka. Chcel by som ale aspoň naznačiť, čo sa vlastne myslí pod tým, že vieme „pokračovať ďalej“.

Sme teda v takejto situácii: Máme nejakú rastúcu postupnosť množín $M_0 \subseteq M_1 \subseteq \dots \subseteq M_n \subseteq \dots$ a na každej z nich máme definované zobrazenie $f_n \colon M_n \to \mathbb{R}$, ktoré rozširuje všetky predchádzajúce zobrazenia a vyhovuje rovnici (1.1). Teraz označíme

$$M_\omega = \bigcup_{n=0}^{\infty} M_n$$

a zadefinujeme $f_\omega \colon M_\omega \to \mathbb{R}$ jednoducho tak, že $f_\omega(x)$ je spoločná hodnota všetkých $f_n(x)$ takých, že $x \in M_n$. Dostali sme takto rozšírenie na väčšej množine M_ω. (Ale ešte stále spočítateľnej.)

Môžeme však pokračovať ďalej – nejako dostať čoraz väčšie množiny $M_{\omega+1}, M_{\omega+2}, \dots$ atď. Potom by sme mohli znovu urobiť limitný krok a rozšíriť to na $M_{\omega+\omega}$. Ako uvidíme, dosť podobným spôsobom sa dá pokračovať tak, aby sme pokryli všetky reálne čísla. (Stále je pomerne vágne, čo znamená podobným spôsobom – azda keď sformulujeme Zornovu lemu, bude jasné čo bol kľúčový krok tejto úvahy a kedy sa vlastne dá pokračovať ďalej.) Myslím si však, že tento príklad aspoň dáva nejakú hrubú predstavu o technikách, ktoré sa chceme naučiť používať – azda o trochu lepšiu než sa dala získať z toho, čo je v predchádzajúcej časti.

1.2.4 Je užitočné vedieť, kedy používame axiómu výberu?

1.3 Problémy na precvičovanie techník z tohoto textu

Niekedy však bolo vhodné úlohu uviesť v inej kapitole, než v tej, kde sa preberá príslušná technika. (Napríklad na mieste, kde sa zavádzajú pojmy použité v úlohe alebo kde sa o nich dokazujú nejaké ďalšie veci.)

1.3.1 Úlohy na precvičenie použitia Zornovej lemy a axiómy výberu

- Existencia Hamelovej bázy: Problém 4.3.1.
- Existencia linearizácie čiastočného usporiadania: Problém 4.3.6.
- Voľné ultrafiltre: Problém 4.3.7.
- Maximálne ideály v okruhoch s jednotkou: Problém 4.3.8.
- Maximálny antireťazec: Problém 4.3.9.
- Existencia ortonormálnej bázy: Problém 4.3.10.
- Teichmüller–Tukeyho lema: Problém 4.3.11.
- Maximálne skoro disjunktné systémy: Problém 6.1.1.

1.3.2 Úlohy na transfinitnú indukciu

- Podmnožina roviny, ktorá pretína každú priamku práve v dvoch bodoch: Problém 5.7.1.
- Bernsteinove množiny: Problém 5.7.2.
- Rozklad $\mathbb{R}^3$ na priamky/kružnice: Problém 5.7.3.
- σ-algebra generovaná danou množinou, borelovské funkcie: Problémy 5.7.4 a 5.7.5.
- Mengerova veta a metrická konvexnosť: Problém 5.7.6.
- Sekvenciálne priestory a sekvenciálny uzáver: Problém 5.7.7.

1.3.3 Iné úlohy

- Vlastnosti Hamelovej bázy v lineárnych normovaných priestoroch: Problém 4.3.2.
- Existencia nespojitých riešení Cauchyho funkcionálnej rovnice: Problém 4.3.3.
- Niektoré vlastnosti nespojitých riešení Cauchyho funkcionálnej rovnice: Problém 4.3.4.
- O nemerateľnosti riešení Cauchyho funkcionálnej rovnice: Problém 4.3.5.

Kapitola 2

Opakovanie

{opak:CHAPTEROPAK}

Cieľom tejto kapitoly je pripomenúť nejaké veci, ktoré by ste mali poznať (hlavne z predmetov **Diskrétna matematika 1,2**) a ktoré budeme využívať. Ak by ste zistili, že si potrebujete niektoré z týchto vecí zopakovať, vhodné texty sú napríklad [ŠS, Sl3].

Môže sa tu vyskytnúť aj zopár vecí, ktoré ste možno nespomínali. Napríklad ste možno nehovorili o karteziánskom súčine ľubovoľného systému množín (časť 2.5.1).

Ak ste hovorili o tom, že ľubovoľné dva kardinály sú porovnateľné (poznámka 2.7.7) alebo o tom, že pre nekonečné kardinály platí $a + b = a \cdot b = \max\{a, b\}$ (poznámka 2.7.13), tak ste tieto tvrdenia uviedli len bez dôkazu.

2.1 Vstupný test

{test:SECTVSTUPTEST}

V tejto časti nájdete fiktívny vstupný test – v skutočnosti žiadny takýto test nebudeme na tomto predmete robiť, ale keď si pozriete otázky, môžete aspoň zhruba získať prehľad o tom, či si v niektorých oblastiach potrebujete doplniť vedomosti.

2.1.1 Zadania vstupného testu

Úloha 2.1.1. Ktoré z nasledujúcich tvrdení sú pravdivé? Svoju odpoveď zdôvodnite!
a) Prienik konečného počtu relácií ekvivalencie na množine A je opäť relácia ekvivalencie.
b) Prienik ľubovoľnej množiny relácií ekvivalencie na množine A je opäť relácia ekvivalencie.
c) Zjednotenie konečného počtu relácií ekvivalencie na množine A je opäť relácia ekvivalencie.
d) Zjednotenie ľubovoľnej množiny relácií ekvivalencie na množine A je opäť relácia ekvivalencie.

Úloha 2.1.2. Zadefinujte čiastočne usporiadanú množinu, maximálny prvok a najväčší prvok. Musí byť najväčší prvok maximálny? Platí to obrátene? Čo sa stane, ak ide o lineárne usporiadanie?

Úloha 2.1.3. 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 2.1.4. Je zjednotenie $\bigcup \emptyset$ definované a čomu sa rovná? Svoje tvrdenie vysvetlite! Ako by to bolo s prienikom $\bigcap \emptyset$?

Úloha 2.1.5. Čomu sa rovná množina $\emptyset^\emptyset$? Čomu sa rovná kardinálne číslo 0^0?

Úloha 2.1.6. Ukážte, že pre ľubovoľné kardinálne čísla platí $a^{bc} = (a^b)^c$. (Inými slovami: Pre ľubovoľné množiny A, B, C existuje bijekcia medzi $A^{B\times C}$ a $(A^B)^C$.)

Úloha 2.1.7. Aká je kardinalita množiny všetkých konečných podmnožín $\mathbb{Q}$?

Úloha 2.1.8. a) Aká je kardinalita množiny všetkých postupností racionálnych čísel, ktoré konvergujú k 0?
b) Aká je kardinalita množiny všetkých reálnych postupností, ktoré konvergujú k 0?
c) Aká je kardinalita množiny všetkých konvergentných reálnych postupností?

Úloha 2.1.9. Aká je kardinalita všetkých Lebesguovsky merateľných podmnožín $\mathbb{R}$? (Hint: Poznáte nejakú podmnožinu $\mathbb{R}$, ktorá má mieru 0 a kardinalitu $\mathfrak{c}$?)

2.1.2 Poznámky k niektorým otázkam

2.2 Operácie s množinami

V tejto časti sa budeme venovať niektorým operáciam s množinami a pripomenieme si tvrdenia

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

Tvrdenie 2.2.1(ii) často používame na dôkaz rovnosti množín – môžeme dokazovať to, že množiny A a B sa rovnajú tak, že zvlášť dokážeme inklúzie $A \subseteq B$ a $B \subseteq A$.

Definícia 2.2.2. Ak A je podmnožina B a súčasne $A \neq B$, tak hovoríme, že A je *vlastná podmnožina* množiny B. Označenie $A \subsetneq B$.

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

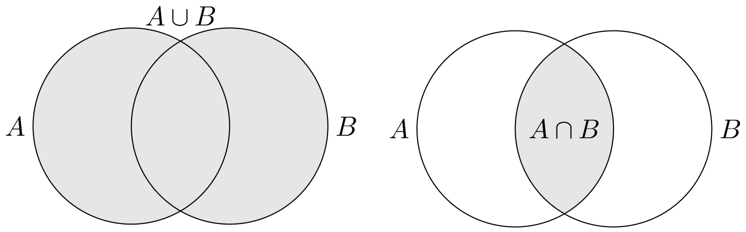
Poznámka 2.2.3. V tomto texte používam $\subseteq$ na označenie podmnožiny a $\subsetneq$ na označenie vlastnej podmnožiny. Toto označenie som zvolil z toho dôvodu, že som sa chcel vyhnúť možným nedorozumeniam. Dosť často sa na označenie inklúzie používa $\subset$, nájdu sa však aj texty (hoci zriedkavejšie), 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.



:FIGZJEDPRIE}

Obr. 2.1: Zjednotenie a prienik dvoch množín

TVRZJEDPRIEN}

Tvrdenie 2.2.4. *Nech A, B, C sú množiny. Potom platí:*

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) $\emptyset \cup A = A$, $\emptyset \cap A = \emptyset$*;*
(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:itDISTRIB}
(v) $A \cap A = A$, $A \cup A = A$ (*idempotentnosť operácií* $\cup$ *a* $\cap$) {oper:itIDEMP}
(vi) $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$ (*zákony absorpcie*). {oper:it6ZJEDPRIEN}

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

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

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

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

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

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

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

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

{oper:TVRDISTRIBSYSTEM}

Tvrdenie 2.2.5. *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) $B \cup \bigcap_{A \in \mathcal{S}} A = \bigcap_{A \in \mathcal{S}} (B \cup A)$.

Pripomeňme aj niektoré vzťahy medzi množinovými operáciami a reláciou inklúzie.

{oper:TVRSUBEKV}
{oper:it1SUBEKV} **Tvrdenie 2.2.6.** *Nech A a B sú množiny. Nasledujúce podmienky sú ekvivalentné:*
{oper:it2SUBEKV} (i) $A \subseteq B$;
{oper:it3SUBEKV} (ii) $A = A \cap B$;
(iii) $B = A \cup B$.

{oper:TVRSUB}
Tvrdenie 2.2.7. *Nech A, B, C sú množiny. Potom platí:*

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

Ako príklad použitia predchádzajúcich tvrdení uvedieme iný dôkaz tvrdenia 2.2.4(vi).

{oper:PRABSORP}
Príklad 2.2.8. $A \cap (A \cup B) \overset{(1)}{=} (A \cap A) \cup (A \cap B) \overset{(2)}{=} A \cup (A \cap B) \overset{(3)}{=} A$, pričom v jednotlivých rovnostiach sme použili:
(1) distributívnosť – tvrdenie 2.2.4(iv)
(2) idempotentnosť – tvrdenie 2.2.4(v)
(3) fakt, že $A \cap B \subseteq A$ – tvrdenie 2.2.7(ii) – a tvrdenie 2.2.6 pre množiny $A \cap B$ a A.

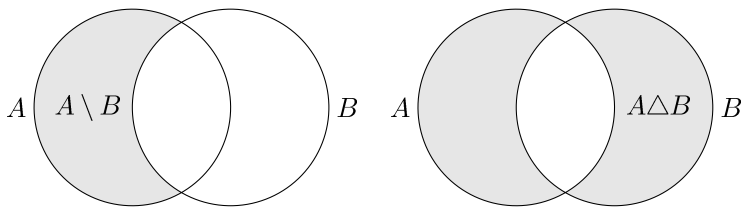
Ďalšie operácie, ktoré budeme niekedy používať, sú rozdiel a symetrická diferencia (symetrický rozdiel) dvoch množín.

Definícia 2.2.9. *Rozdiel množín* A a B je množina

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

Symetrická diferencia množín A a B je množina

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



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

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

{oper:TVRSETMINUS}
Tvrdenie 2.2.10. *Nech A, B, C sú množiny. Potom platí:*

{oper:itDEMORGAN}
(i) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$, $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(ii) $A \setminus (B \cup C) = (A \setminus B) \setminus C$;
(iii) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$;

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

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

{oper:TVRSYMDIF}

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

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

2.3 Usporiadané dvojice a karteziánsky súčin

{kartez:SECTKARTEZ}

Symbolom (a, b) budeme označovať *usporiadanú dvojicu* a, b t.j. dvojicu prvkov, kde prvý prvok je a a druhý prvok je b.

Ako hovorí názov, pri usporiadaných dvojiciach záleží na poradí. Teda dve usporiadané dvojice sa rovnajú, ak sa zhodujú prvky na prvej súradnici a prvky na druhej súradnici:

$$(a, b) = (c, d) \qquad \Leftrightarrow \qquad a = c \wedge b = d. \tag{2.1}$$ {kartez:EQUSPDVOJ}

Pomocou pojmu usporiadanej dvojice definujeme karteziánsky súčin dvoch množín.

Definícia 2.3.1. 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

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

Spomeňme aj niektoré základné vlastnosti karteziánskeho súčinu.

{kartez:TVROPER}

Tvrdenie 2.3.2. *Nech* A, B, C, D *sú množiny. Potom platí*
(i) $A \times \emptyset = \emptyset \times A = \emptyset$;
(ii) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
(iii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;
(iv) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.
(v) *Ak navyše predpokladáme, že* A, B, C, D *sú neprázdne, tak* $A \times B = C \times D$ *platí práve vtedy, keď* $A = C$ *a* $B = D$.

Cvičenia

Úloha 2.3.1. Dokážte (priamo, nie s použitím tvrdenia 2.3.2):
a) Pre $A, B \neq \emptyset$ platí $A \times B = B \times A \Rightarrow A = B$;
b) $A \times B = \emptyset \Leftrightarrow A = \emptyset \vee B = \emptyset$.

{kartezcvic:UI

Úloha 2.3.2. Dokážte, že pre $A \neq \emptyset$ platí $A \times B \subseteq A \times C \Leftrightarrow B \subseteq C$. Platí toto tvrdenie bez predpokladu $A \neq \emptyset$?

Úloha 2.3.3. Dokážte, alebo nájdite kontrapríklad:
a) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$;
b) $(A \times B) \cup (C \times D) \supseteq (A \cup C) \times (B \cup D)$;
c) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$;
d) $(A \times B) \cap (C \times D) \subseteq (A \cap C) \times (B \cap D)$;
e) $(A \times B) \cap (C \times D) \supseteq (A \cap C) \times (B \cap D)$;
f) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Úloha 2.3.4. Dokážte, že množiny A, B sú disjunktné práve vtedy, keď $(A\times B)\cap(B\times A) = \emptyset$.

Úloha 2.3.5. Dokážte, že pre ľubovoľné množiny A, B, C platí $A\times(B\triangle C) = (A\times B)\triangle(A\times C)$.

Úloha 2.3.6. Ukážte, že ak $A \times C \subseteq B \times D$ a $A \times C \neq \emptyset$, tak $A \subseteq B$ a $C \subseteq D$. Ukážte na príklade, že bez predpokladu $A \times C \neq \emptyset$ už toto tvrdenie neplatí.

2.4 Relácie

Definícia 2.4.1. *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 2.4.2. Ak A je ľubovoľná množina, tak

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

je relácia na množine A.

{rel:PRIKLKRUZNICA}

Príklad 2.4.3. 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 2.4.4. 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 2.4.5. 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 2.4.3 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 zaoberali 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 aj na diskrétnej matematike.)

Definícia 2.4.6. 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 2.4.7. 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 2.4.4). Táto relácia je dokonca lineárnym usporiadaním.

Čiastočnými usporiadaniami sa budeme podrobne zaoberať v časti 2.6. Teraz sa ešte pozrieme na to, ako môžeme relácie skladať.

Definícia 2.4.8. 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 2.4.9. *Ak R je ľubovoľná relácia medzi množinami A, B, tak platí*

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

Definícia 2.4.10. Nech A je množina. Potom reláciu {rel:DEFID}

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

na množine A nazývame *identita* na množine A.

Tvrdenie 2.4.11. *Nech A, B sú množiny, R je relácia medzi množinami A, B a S je relácia medzi množinami B, A. Potom platí*

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

{rel:TVRINVZLOZ} **Tvrdenie 2.4.12.** *Nech R je relácia medzi množinami A a B, S je relácia medzi množinami B a C. Potom platí:*

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

{rel:TVRTRANZSKLAD} **Tvrdenie 2.4.13.** *Nech R je relácia na množine A. Potom platí:*

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

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 aj priamo z definície.

Tvrdenie 2.4.14. *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}.

Tranzitívny uzáver V niektorých aplikáciách býva užitočný pojem tranzitívneho uzáveru, čo je vlastne relácia obsahujúcu danú reláciu R, ktorá aby sa od R priveľmi nelíši a súčasne je tranzitívna. Pod pojmom „priveľmi nelíši“ rozumieme minimalitu vzhľadom na inklúziu.

Definícia 2.4.15. 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 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 2.4.16. *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 2.4.3. Dôkaz, ktorý sme tu uviedli, má však tú výhodu, že od istej miery aj popisuje, ako tranzitívny uzáver danej relácie vyzerá.

{relmat:POZNTOPDOWN}

Poznámka 2.4.17. Tranzitívny uzáver relácie R sme popísali dvoma spôsobmi: ako prienik tranzitívnych relácií ekvivalencií obsahujúcich R a tiež pomocou konštrukcie, kde sme do R postupne pridávali nové dvojice, ktoré boli nevyhnutné, aby mohla byť splnená tranzitívnosť. S podobnou situáciou ste sa už mohli stretnúť vo viacerých kontextoch. Môžeme hovoriť o popise *zhora-nadol* alebo *zdola-nahor*.[1]

Do rovnakej schémy zapadajú viaceré pojmy s ktorými ste sa už stretli:

- Vo vektorových priestoroch: lineárny obal – podpriestor generovaný danou množinou M. Môžeme ho dostať ako množinu všetkých lineárnych kombinácií prvkov z M. Súčasne je to prienik všetkých podpriestorov obsahujúcich množinu M.
- Uzáver množiny A v topologickom priestore je najmenšia uzavretá množina, ktorá ju obsahuje. Dá sa vyjadriť ako prienik všetkých uzavretých množín obsahujúcich A. Súčasne ho vieme dostať tak, že k A pridávame limity sietí. (Ak sme v metrickom priestore prípadne v priestore vyhovujúcom prvej axióme spočítateľnosti, tak stačia aj limity postupností.)
- V grupách: podgrupa generovaná danou množinou. (Špeciálne cyklické podgrupy – generované jediným prvkom.)
- Podokruh generovaný danou množinou.
- Ideál v okruhu generovaný danými prvkami.
- Konvexný obal danej podmnožiny vektorového priestoru..

Obvykle sa hodí mať pre objekty, s ktorými chceme pracovať, popis zhora-nadol aj zdola-nahor. V závislosti od toho, na čo ich chceme použiť, môže byť jeden z nich vhodnejší.

Všetky uvedené príklady sú špeciálnymi prípadmi operátorov uzáveru[2] a uzáverových systémov, pozri napríklad [G, Section 3.12], [KLŠZ, podkapitola 2.4]. S nejakou teóriou okolo uzáverových operátorov sa máte šancu stretnúť na predmete **Univerzálne algebry a zväzy**.

Cvičenia

Úloha 2.4.1.

Úloha 2.4.2. Dokážte tvrdenia, ktoré sme v tejto kapitole uviedli bez dôkazu.

{relcvic:ULOTRANZUZ}

Úloha 2.4.3. Nech A je množina.

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

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

Úloha 2.4.4. 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.)

[1] Pozri aj `http://math.stackexchange.com/a/54334/`.
[2] closure operator

2.5 Funkcie

Definícia 2.5.1. *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.

Namiesto zápisu $(a, b) \in f$ budeme používať zápis $f(a) = b$, tak ako ste boli zvyknutí aj doteraz. Často budeme používať aj zápis $f\colon a \mapsto b$.

Definícia 2.5.2. 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. Ľahko sa však overí, že táto relácia je zobrazením.

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 ešte niektoré ďalšiepojmy, ktoré poznáte už z nižších ročníkov:

Definícia 2.5.3. 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.

Opäť si spomenieme niektoré užitočné fakty o o injekciách, surjekciách a bijekciách.

{fun:TVRINVBIJEK}

Tvrdenie 2.5.4. *Nech $f\colon A \to B$ je zobrazenie. Potom f^{-1} je zobrazenie z B do A práve vtedy, keď f je bijekcia.*

Definíciu inverzného zobrazenie môžeme ekvivalentne preformulovať tak, že je to zobrazenie, pre ktoré platí
$$f^{-1}(b) = a \qquad \Leftrightarrow \qquad f(a) = b.$$
Iná ekvivalentná formulácia je takáto:

Tvrdenie 2.5.5. *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 $f \circ g = id_B$.*

{fun:POZNAXSUBST}

Poznámka 2.5.6. Po zavedení pojmu funkcie vidno, že schéma axióm substitúcie vlastne hovorí to, že pre každú funkciu f definovanú na množine A existuje množina $f[A] = \{f(x); x \in A\}$. [3]

Definícia 2.5.7. Nech $f\colon X \to Y$ je zobrazenie, $A \subseteq X$, $B \subseteq Y$.
Potom množinu
$$f[A] := \{f(a); a \in A\}$$
nazývame *obraz množiny* A v zobrazení f a množinu
$$f^{-1}[B] = \{a; f(a) \in B\}$$
nazývame *vzor množiny* B v zobrazení f.

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

To znamená, že vzor a obraz množiny sú charakterizované týmito podmienkami:
$$x \in f[A] \Leftrightarrow (\exists a \in A) x = f(a)$$
$$x \in f^{-1}[B] \Leftrightarrow f(x) \in B$$

Uvedieme základné vlastnosti vzoru a obrazu množín:

{fun:TVROBRAZVZOR}

Tvrdenie 2.5.8. *Nech $f\colon X \to Y$, $g\colon Y \to Z$ sú zobrazenia, $A, B \subseteq X$, $C, D \subseteq Y$, $E \subseteq Z$, $A_i \subseteq X$ a $B_i \subseteq Y$ pre každé $i \in I$. Potom platí*
(i) $g \circ f[A] = g[f[A]]$;
(ii) $(g \circ f)^{-1}[A] = g^{-1}[f^{-1}[A]]$;
(iii) $A \subseteq f^{-1}[f[A]]$ *a ak f je injektívne, tak* $A = f^{-1}[f[A]]$;
(iv) $f[f^{-1}[C]] \subseteq C$ *a ak f je surjektívne, tak* $f[f^{-1}[C]] = C$;
(v) $f[A \cap B] \subseteq f[A] \cap f[B]$ *a ak f je injektívne, tak* $f[A \cap B] = f[A] \cap f[B]$; {fun:itOBRCAP}
(vi) $f[\bigcap_{i\in I} A_i] \subseteq \bigcap_{i \in I} f[A_i]$ *a ak f je injektívne, tak* $f[\bigcap_{i\in I} A_i] = \bigcap_{i\in I} f[A_i]$; {fun:itOBRBIGCAP}
(vii) $f[A \cup B] = f[A] \cup f[B]$;
(viii) $f[\bigcup_{i\in I} A_i] = \bigcup_{i\in I} f[A_i]$; {fun:itOBRBIGCUP}
(ix) $f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$;
(x) $f^{-1}[\bigcap_{i\in I} A_i] = \bigcap_{i\in I} f^{-1}[A_i]$; {fun:itOBRCAPSYST}
(xi) $f^{-1}[C \cup D] = f^{-1}[C] \cup f^{-1}[D]$;
(xii) $f^{-1}[\bigcup_{i\in I} B_i] = \bigcup_{i\in I} f^{-1}[B_i]$;
(xiii) $A \subseteq B \Rightarrow f[A] \subseteq f[B]$ *a ak f je injekcia, tak platí aj opačná implikácia;*

[3] 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.

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

Nasledujúce tvrdenie už možno poznáte z nižších ročníkov, pozri napríklad [Sl4, 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 4.2.2 ukážeme, že táto časť tvrdenia je dokonca ekvivalentná s axiómou výberu v systéme ZF.)

Odporúčam ale, aby ste sa pokúsili si tvrdenie dokázať sa mi. A keď už navyše viete, že sa v dôkaze niekde využije axióma výberu, skúste dať pozor, či si všimnete kde.

{fun:TVRSURJINV}
{fun:itSURJ} **Tvrdenie 2.5.9.** *Nech $f\colon A \to B$ je zobrazenie. Potom platí:*
{fun:itINJ} (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 je preformulovaná v poznámke 3.1.5) 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 2.5.10. *Ak $A \neq \emptyset$ a existuje injekcia $f\colon A \to B$, tak existuje surjekcia $g\colon B \to A$.*

Dôkaz. Ak f je injekcia, tak podľa druhej časti tvrdenia 2.5.9 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. □

2.5.1 Karteziánsky súčin systému množín

{fun:SSECTKARTEZ}

V časti 2.3 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 2.5.11. 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 prefolrmulovaná podmienka (2.1)).

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

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

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

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

ktoré nazývame *i-ta projekcia.*

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

2.5.2 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 2.5.13. Nech $f \colon A \to C$, $g \colon B \to D$ sú zobrazenia. Potom ich *karteziánsky súčin* je zobrazenie $f \times g \colon A \times B \to C \times D$ určené predpisom

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

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

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

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

{fun:TVRSUCBIJ}

Tvrdenie 2.5.14. *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 4.

Tvrdenie 2.5.15. *Nech $f_i\colon A_i \to B_i$ je zobrazenie pre každé $i \in I$.*
(i) *Ak f_i je injekcia pre každé $i \in I$, tak $\prod\limits_{i\in I} f_i$ je injekcia.*
(ii) *Ak f_i je surjekcia pre každé $i \in I$, tak $\prod\limits_{i\in I} f_i$ je surjekcia.*
(iii) *Ak f_i je bijekcia pre každé $i \in I$, tak $\prod\limits_{i\in I} f_i$ je bijekcia.*

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

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

(ii) Nech každé f_i je surjektívne a nech $f \in \prod\limits_{i\in I} B_i$. Potom pre každé $i \in I$ existuje $a_i \in A_i$ také, že $f_i(a_i) = f(i)$. Inak povedané, $\{a \in A_i; f_i(a) = f(i)\}$ je systém neprázdnych množín. Z ekvivalentnej formulácie axiómy výberu (tvrdenie 4.2.2(iii)) vyplýva existencia zobrazenia h definovaného na I takého, že $h(i) \in \{a \in A_i; f_i(a) = f(i)\}$, čiže $h(i) \in A_i$ a $f_i(h(i)) = f(i)$ pre každé $i \in I$. Posledná rovnosť hovorí presne to, že $g(h) = f$. Ukázali sme, že pre každé $f \in \prod\limits_{i\in I} B_i$ existuje vzor, čiže g je surjektívne zobrazenie.

(iii) Ľahko vyplýva z predchádzajúcich dvoch častí. □

Cvičenia

ULOINVSURINJ}

Úloha 2.5.1. 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 2.5.9, že ak pre množiny X, Y existuje injekcia $f\colon X \to Y$ práve vtedy, keď existuje surjekcia $g\colon Y \to X$.

Úloha 2.5.2. Nech $f\colon X \to Y$ je zobrazenie. Dokážte, že f je injekcia práve vtedy, keď pre ľubovoľné dve podmnožiny $A, B \subseteq X$ platí $f[A \cap B] = f[A] \cap f[B]$.

Úloha 2.5.3. Nech $f\colon X \to Y$ je zobrazenie. Dokážte, že f je injekcia $\Leftrightarrow$ pre ľubovoľné dve podmnožiny $A, B \subseteq X$ platí $f[B \smallsetminus A] = f[B] \smallsetminus f[A]$.

2.6 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 2.6.1. Jednoduchými príkladmi čiastočne usporiadaných množín sú $(\mathbb{R}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{N}, \leq)$ s obvyklým usporiadaním. Vo všetkých spomenutých prípadoch ide o lineárne usporiadanie.

{cum:PRPOMDNCUM}

Príklad 2.6.2. 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 2.6.3. 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 2.2.1.

Podľa príkladu 2.6.2 dostaneme čiastočne usporiadanú množinu aj pre ľubovoľnú podmnožinu množiny $\mathcal{P}(A)$.

Príklad 2.6.4. Ďalším príkladom je relácia „delí“ na množine prirodzených čísel definovaná tak, že

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

Overiť, že ide o čiastočne usporiadanú množinu, je vcelku jednoduché – necháme to ako cvičenie pre čitateľa.

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 2.6.5.** 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 2.3 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 2.4 je 5-rozmerná hyperkocka.

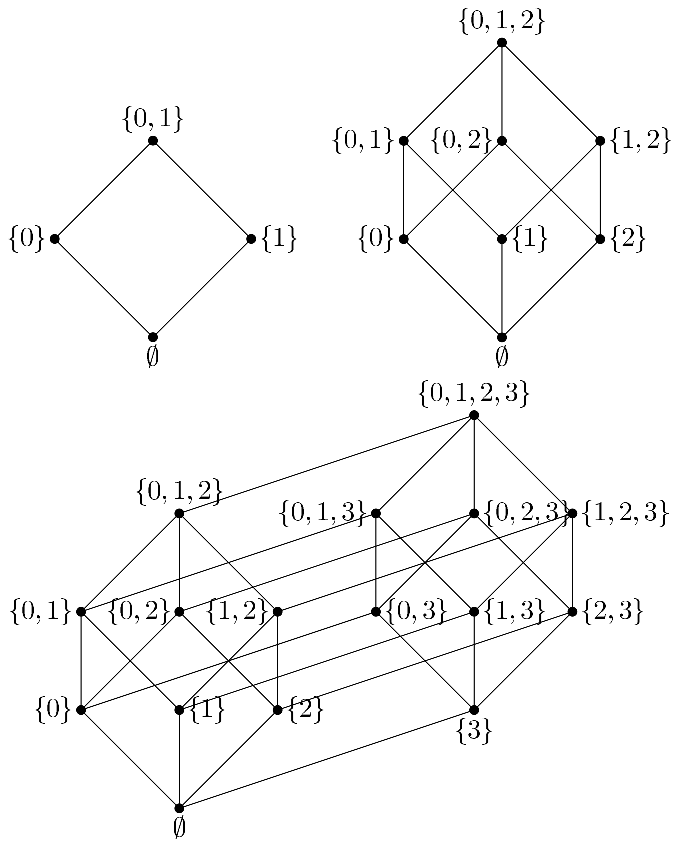
Môžeme si tiež všimnúť, že ak nakreslíme Hasseho diagram pre čiastočne usporiadanú množinu $(\{0, 1, 2, 3, 5, 6, 10, 15\}, |)$, tak dostaneme (pri vhodnom umiestnení vrcholov), presne ten istý obrázok ako pre $(\mathcal{P}(\{0, 1, 2\}), \subseteq)$. Vidíme, že tieto dve čiastočne usporiadané množiny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

Definícia 2.6.6. Nech $(X, \leq)$ a $(Y, \preceq)$ sú čiastočne usporiadané množiny a $f \colon X \to Y$ je zobrazenie. Hovoríme, že zobrazenie f je *monotónne,* ak platí

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

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

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



m:FIGHASSEPX}

Obr. 2.3: Hasseho diagram $(\mathcal{P}(X), \subseteq)$ pre 2-,3- a 4-prvkovú množinu

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

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

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

Definícia 2.6.7. 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 $b \leq a$;

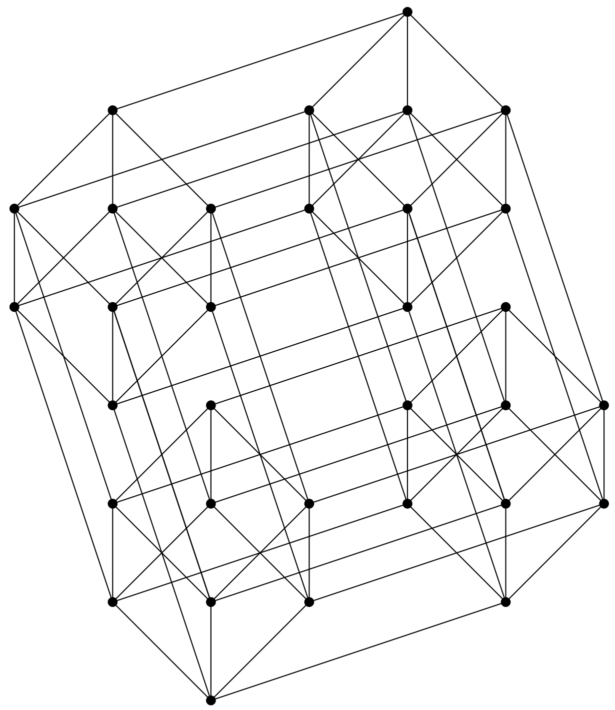
(iii) *minimálny prvok* množiny A, ak pre každé $b \in A$ platí $b \leq a \Rightarrow b = a$;

(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



{cum:FIGCUBE5} Obr. 2.4: 5-rozmerná hyperkocka – Hasseho diagram pre $\mathcal{P}(X)$, kde X je 5-prvková množina

príkladov (môžete si rozmyslieť, ako je to s čiastočne usporiadanými množinami znázornenými na obrázku 2.6); my si ukážeme jeden z nich. Ak uvažujeme ľubovoľnú množinu A, ktorá má aspoň dva prvky, tak relácia id_A je čiastočné usporiadanie na množine A. Pri tomto usporiadaní je každý prvok množiny A minimálny (a súčasne aj maximálny), ale množina A nemá najmenší ani najväčší prvok.

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

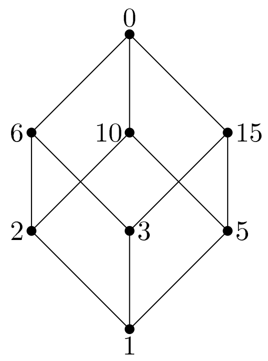
Ostré čiastočné usporiadanie V definícii čiastočného usporiadania sme sa vlastne snažili nájsť spoločné vlastnosti relácií ako sú $\leq$, $\subseteq$. V niektorých textoch nájdete inú definíciu čiastočného usporiadania, ktorú spĺňajú napríklad relácie $<$, $\subsetneq$. (Napríklad v [ŠS], pozri [ŠS,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

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

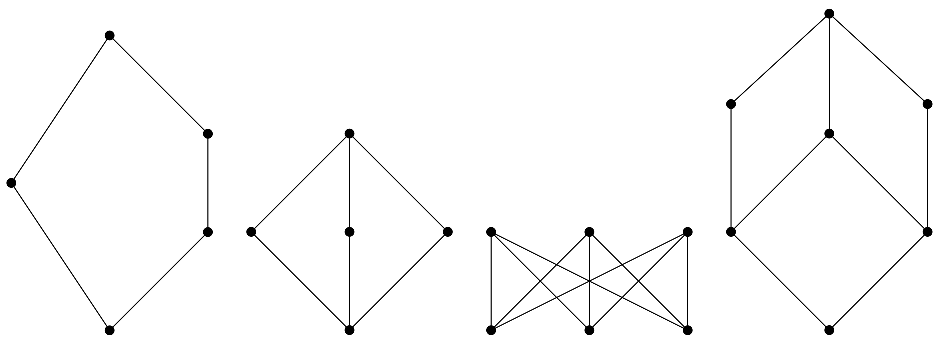
V tomto texte budeme bežne používať ostré i neostré čiastočné usporiadanie, bez toho, že by sme na to špeciálne upozornili. Od čitateľa sa očakáva, že by nemal mať problémy s prekladom akejkoľvek definície či tvrdenia medzi týmito dvoma formalizáciami pojmu usporiadania.

{cum:DEFOSTRE}

Definícia 2.6.8. Reláciu $<$ na množine A nazývame *ostré čiastočné usporiadanie,* ak je



{cum:FIGMID} Obr. 2.5: Hasseho diagram pre čiastočné usporiadanie $|$ na množine $\{0, 1, 2, 3, 5, 6, 10, 15\}$



FIGMOREHASSE} Obr. 2.6: Ďalšie príklady Hasseho diagramov

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 2.6.9. *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 2.4.13 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 2.6.10. *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 2.6.11. *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 2.6.12. 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 2.6.1. Ukážte, že ak $(A, \leq)$ je čiastočne usporiadaná množina, tak A má nanajvýš jeden najväčší prvok a nanajvýš jeden najmenší prvok.

Úloha 2.6.2. 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 2.6.3. Ukážte, že ak A, B sú lineárne usporiadané množiny, tak bijektívne monotónne zobrazenie $f\colon A \to B$ je izomorfizmus.

Úloha 2.6.4. 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 2.6.5. Nájdite pre každý z Hasseho diagramov na obrázku 2.6 podmnožinu $A \subseteq \mathbb{N}$ takú, že čiastočne usporiadaná množina $(A, |)$ má daný Hasseho diagram.

Úloha 2.6.6. Nájdite pre každý z Hasseho diagramov na obrázku 2.6 množinu $A \subseteq \mathcal{P}(\mathbb{N})$ takú, že čiastočne usporiadaná množina $(A, \subseteq)$ má daný Hasseho diagram.

{cumcvic:ULOPRAZDCUM}

Úloha 2.6.7. Nech A je ľubovoľná množina. Sú relácie $A \times A$, id_A a $\emptyset$ čiastočnými usporiadaniami na množine A?

Úloha 2.6.8. Môže byť čiastočné usporiadanie na množine A zobrazením z A do A?

Úloha 2.6.9. Pre aké množiny A je $(\mathcal{P}(A), \subseteq)$ lineárne usporiadaná množina?

Úloha 2.6.10. 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 2.6.11. 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?

2.7 Kardinálne čísla

2.7.1 Porovnávanie mohutností množín

{def:DEFKARD}

Definícia 2.7.1. Hovoríme, že množiny X a Y majú rovnakú *kardinalitu* (*mohutnosť*), ak existuje bijekcia $f\colon X \to Y$. Označujeme $|X| = |Y|$.

Očividne platí $|X| = |X|$ pre každú množinu X. Ďalej z $|X| = |Y|$ a $|Y| = |Z|$ vyplýva $|X| = |Z|$. Teda rovnosť kardinalít má vlastnosti, ktoré by sme od vzťahu „rovná sa" aj očakávali. Táto podmienka nám súčasne dáva nádej definovať rozumným spôsobom kardinálne číslo – ak chceme pre každú množinu mať nejakého reprezentanta, pričom množinám rovnakej kardinality priradíme rovnakého reprezentanta, tak nevyhnutne potrebujeme tranzitívnosť, reflexívnosť a symetriu.

{aritm:DEFKONKARD}

Definícia 2.7.2. Kardinálne číslo množiny prirodzených čísel budeme označovať $\aleph_0$.

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

Definícia 2.7.3. 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 2.7.4. Keďže pre dané kardinálne číslo môžeme nájsť veľa množín rovnakej kardinality, je potrebné (podobne ako pri iných definíciach využívajúcich reprezentanta nejakej triedy ekvivalencie alebo nejakej vlastnosti) skontrolovať, či je nerovnosť kardinálnych čísel dobre definovaná. Znamená to, že si treba rozmyslieť, či z $|X| = |X'|$, $|Y| = |Y'|$ a $|X| \leq |Y|$ vyplýva $|X'| \leq |Y'|$.

Overiť tento fakt je pomerne jednoduché (ponecháme to na čitateľa), je však asi rozumné pripomenúť, že pri definíciach vzťahov medzi kardinálmi a operácií s nimi treba myslieť aj na takéto veci.

{def:VTCANTBE

Veta 2.7.5 (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 $h\colon X \to Y$.

Veta 2.7.6. *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 2.7.7. V tomto kontexte je ďalšou prirodzenou otázkou to, či sú ľubovoľné dve kardinálne čísla porovnateľné. (Presnejšie: Platí pre ľubovoľné dve množiny X, Y, že existuje buď injekcia z X do Y alebo opačným smerom?) 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 5.1.6. Dá sa odvodiť aj použitím Zornovej lemy – úloha 4.3.3.

2.7.2 Kardinálna aritmetika

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

Definícia 2.7.8. Nech a, b sú kardinálne čísla a nech A, B sú množiny také, že $|A| = a$, $|B| = b$. Potom:
(i) Predpokladajme navyše, že množiny A a B sú disjunktné. Potom *súčet kardinálnych čísel* a a b je kardinálne číslo množiny $A \cup B$, t.j.

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

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

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

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

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

Poznámka 2.7.9. Opäť, podobne ako pri nerovnosti medzi kardinálov, aj pri operáciami s kardinálnymi číslami by sme sa mali presvedčiť o tom, že tieto operácie sú dobre definované.

{aritm:VTPX2NAX}

Veta 2.7.10. *Nech X je ľubovoľná množina. Potom platí*

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

Dôsledok 2.7.11.

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

{cantor:VTCANTOR}

Veta 2.7.12 (Cantor)**.** *Pre každú množinu X platí $|X| < |\mathcal{P}(X)|$.*

Ešte uveďme stručný prehľad vlastností operácií s kardinálmi, ktoré by ste mali poznať.

$$
\begin{gathered}
a \leq b \wedge b \leq a \Rightarrow a = b \\
|\mathcal{P}(X)| = 2^{|X|} \\
a + b = b + a \\
a + (b + c) = (a + b) + c \\
b \leq c \Rightarrow a + b \leq a + c \\
ab = ba \\
a(bc) = (ab)c \\
a(b + c) = ab + ac \\
b \leq c \Rightarrow ab \leq ac \\
a^2 = a.a \\
a \leq b \Rightarrow a^c \leq b^c \\
a \leq b \wedge c \neq 0 \Rightarrow c^a \leq c^b \\
a^{b+c} = a^b.a^c \\
(a^b)^c = a^{bc} \\
a^b \leq 2^{ab} \\
a < 2^a
\end{gathered}
$$

{kardm:POZNMAX}

Poznámka 2.7.13. Spomeňme si ešte niečo viac o kardinálnej aritmetike. Už sme v poznámke 2.7.7 spomenuli, že neskôr ukážeme, že ľubovoľné dve množiny možno z hľadiska kardinality „porovnať“. Ďalší fakt, ktorý si ukážeme v rámci tejto prednášky hovorí, že sčitovanie a násobenie kardinálov je „v podstate“ jednoduché. Konkrétne, pre ľubovoľné dva nekonečné kardinály a, b platí

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

(Vďaka tomu, že ľubovoľné dve kardinálne čísla sú porovnateľné, má zmysel hovoriť o ich maxime.) Tento fakt dokážeme neskôr (s využitím axiómy výberu a transfinitnej indukcie) ako dôsledok 5.7.2.

2.7.3 Mohutnosť niektorých v praxi sa vyskytujúcich množín

Tvrdenie 2.7.14.

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

2.7.4 Spočítateľné a nespočítateľné množiny

Cvičenia

Úloha 2.7.1. Ukážte, že nerovnosť medzi kardinálmi, súčet, súčin a mocnina kardinálnych čísel sú dobre definované.

{kardcvic:ULOALOALO}

Úloha 2.7.2. Ukážte, že $\aleph_0 = \aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0$.

Úloha 2.7.3. Ukážte, že $\mathfrak{c} = 2^{\aleph_0} = \aleph_0^{\aleph_0} = \mathfrak{c}^{\aleph_0}$.

{kardcvic:ULO

Úloha 2.7.4. Pripomeňme, že 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.*

Ukážte, že množina všetkých algebraických reálnych čísel je spočítateľná. Z toho vyplýva aj to, že existuje aspoň jedno transcendentné reálne číslo.

Argument uvedený v tejto úlohe je v podstate pôvodný Cantorov dôkaz. V čase, keď Cantor objavil tento dôkaz, boli známe konkrétne príklady transcendentných čísel, napríklad *Liouvilleove čísla.* Nevýhoda Cantorovho dôkazu je, že nie je konštruktívny. Výhoda je, že je jednoduchý a súčasne ukázal to, že transcedentných čísel je v istom zmysle veľa – kardinalita množiny transcendentých čísel je $\mathfrak{c}$.

{kardcvic:ULOKRUZ}

Úloha 2.7.5. Z daných bodov v rovine vieme vytvárať nové body pomocou pravítka a kružidla takto: Môžeme spojiť dva body priamkou. Môžeme zostrojiť kružnicu takú, že stred bude v niektorom zo zadaných bodov a polomer je vzdialenosť niektorých dvoch zadaných bodov. Dostaneme takto nové body na priesečníkoch takýchto priamok a kružníc.

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

Aká je kardinalita množiny všetkých skonštruovateľných bodov? Viete na základe toho zdôvodniť, že existujú body v rovine, ktoré z jednotkovej úsečky nedokážeme zostrojiť pomocou pravítka a kružidla?[4]

{kardcvic:ULOVYPOC}

Úloha 2.7.6. Funkcia $f\colon \mathbb{N} \to \mathbb{N}$ sa nazvime *vypočítateľnou,* ak existuje *algoritmus* [5] ktorý pre vstup n vráti $f(n)$.

Aká je kardinalita množiny všetkých vypočítateľných funkcií? Existujú aj funkcie, ktoré nie sú vypočítateľné?

[4] O tom, že nie všetky konštrukcie sa dajú urobiť pravítkom a kružidlom by ste už mohli vedieť z algebry; dokonca by ste mohli poznať niektoré konkrétne dĺžky, pre ktoré sa nedajú zostrojiť takto dlhé úsečky, ako napríklad $\sqrt[3]{2}$ alebo $\cos\frac{\pi}{9}$. Pozri napríklad [KGGS, Podkapitola 4.1 a 8.2], [DF, Section 13.3], [JMP], [S, Chapter 7], [Sl2].

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

[5] Pod pojmom algoritmus si jednoducho predstavte program vo vašom obľúbenom programovacom jazyku alebo aj neformálny návod v prirodzenom ako funkciou vypočítať. Ak by ste chceli rigoróznejšiu definíciu, tak vhodnou formalizáciou pojmu algoritmu je napríklad pojem Turingovho stroja, s ktorým ste sa niektorí z vás mohli stretnúť na iných predmetoch. Nech už si ho predstavíte akokoľvek, pre účely tejto úlohy je dôležité iba to, že popis algorimu má konečnú dĺžku a používa iba znaky z nejakej konečnej abecedy.

Kapitola 3

Naivná a axiomatická teória množín

{axiom:CHAPTERAXIOM}

Do istej miery by sa dalo povedať, že táto kapitola sa zaoberá tým, čomu sa na tejto prednáške *nechceme* venovať.

Hlavným cieľom je povedať niečo o tom, aký je rozdiel medzi axiomatickou teóriou množín a naivnou teóriou množín. A tiež aby ste získali aspoň hrubú predstavu o tom, čo znamená, keď povieme, že nejaké tvrdenie sa nedá dokázať v ZF alebo že sa nedá dokázať v ZFC.

Niektoré z vecí v tejto kapitole by ste už mohli poznať. S axiómami teórie množín ste sa mohli stretnúť aj na predmetoch **Diskrétna matematika 1,2**, určite by vám však mali byť známe ak ste absolvovali predmety **Teória množín 1,2**. Azda výnimkou je axióma regularity a jej dôsledky. Možné je, že ani axiómou výberu ste sa nezaoberali priveľmi podrobne. (Na tejto prednáške si to vynahradíme.)

3.1 Zermelov-Fraenkelov axiomatický systém

{zfc:SECTZFC}

V axiomatickej teórii množín pracujeme so systémom axióm, z ktorých sa odvodzujú ďalšie tvrdenia. Čiže formalisticky by sa dalo na celú teóriu množín pozerať len na akúsi hru so symbolmi, kde reťazce symbolov máme povolené meniť podľa určitých pravidiel. Na tejto prednáške nás zaujímajú skôr aplikácie teórie množín, takže nebudeme priveľmi formálny. Je však užitočné si uvedomiť, že sa na dôkazy dá pozerať aj z takéhoto hľadiska.

Takisto sa nebudeme venovať *pravidlám*, ktoré sa môžu pri odvodeniach používať – tieto pravidlá predstavuje axiomatizácia logiky druhého rádu. Viac sa o takýchto veciach môžete dozvedieť na predmetoch **Teória množín 1,2** a v mnohých textoch venovaných tejto oblasti, ako napríklad [Bu1, End, So, Š].

Teória množín je založená na dvoch *primitívnych pojmoch* – tak nazývame pojmy, ktoré nedefinujeme.[1] 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.“. Presnejšie povedané: Ak nejaký objekt označíme premennou, budeme o ňom chcieť vysloviť nejaké tvrdenie vo forme formuly jazyka teórie množín, budeme s ním chcieť robiť nejaké operácie, tak automaticky predpokladáme, že tento objekt je množina.

[1] 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.

Jedna množina môže patriť do inej množiny. Tento fakt označíme $a \in b$, jeho negáciu budeme zapisovať $a \notin b$.

Všetky tvrdenia s ktorými budeme v axiomatickom systéme ZFC pracovať (tak axiómy ako aj tvrdenia, ktoré z nich odvodíme) budú formuly jazyka teórie množín. Stručne (a zjednodušene) povedané, sú to formuly, ktoré sa dajú zapísať pomocou konečného počtu kvantifikátorov, logických spojok, premenných a symbolov $\in$ a $=$.

Aby sme videli aspoň jeden príklad takejto formuly, môžeme uviesť napríklad podmienku

$$(\forall z)(z \in A \Rightarrow z \in B),$$

ktorá je vlastne definíciou toho, že A je podmnožina B.

3.1.1 Axiómy systému ZFC

Pripomeňme si základné axiómy, s ktorými sa v axiomatickej teórii množín pracuje. 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 3.1.1. 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 $\{a, b\}$.

Pomocou axiómy dvojice a axiómy zjednotenia sa dá ukázať, že pre ľubovoľné dve množiny A, B existuje ich zjednotenie

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

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

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

Pomocou schémy axióm vymedzenia možno dokázať napríklad existenciu prieniku dvoch množín

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

alebo tiež ďalších množinových operácií.

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 3.1.2. 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 3.1.3. 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

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

Táto schéma axióm hovorí zhruba to, že ak formula $\varphi(x, y)$ „predstavuje funkciu" (=ku každému vzoru existuje práve jeden obraz) a vezmeme si nejakú množinu A, tak aj obrazy vytvoria množinu.

Toto nie je úplne presné, pretože funkcie definujeme ako funkcie medzi dvoma množinami; teda na to, aby sme definovali funkciu, musíme vopred vedieť, že obor hodnôt je funkcia. Správnejšie by bolo povedať, že ide o triedovú funkciu – o triedach ešte budeme hovoriť.

Napriek tomu by to, že $\varphi(x, y)$ sa „správa ako funkcia" mohlo trochu viac objasniť význam tejto axiómy.

Axióma (Axióma regularity)**.**

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

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

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

{zfc:TVRREGXINX}

Tvrdenie 3.1.4. *Pre ľubovoľnú množinu platí $x \notin x$.*

Dôkaz. Ak x je množina, tak môžeme vytvoriť množinu $A := \{x\}$ (použijeme axiómu dvojice pre x 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 3.1.4 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.

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 4. 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.

{fun:POZNACFUN}

Poznámka 3.1.5. 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 4.2.2.

Veľmi dobre napísané poznámky o motivácii a význame jednotlivých axióm si môžete prečítať napríklad v [Z, s.79–83][2]. (Môžete si tam prečítať aj o axiómach, ktorými sa v tomto texte podrobne nezaoberáme, ako je axióma regularity.)

{zfc:POZNHRA}

Poznámka 3.1.6. 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 daným pravidlám, tak kontrola dôkazu je už iba algoritmický proces. Viac o použití počítačov pri verifikácii formálnych dôkazov sa môžete dočítať napríklad v článku [Wie].

3.1.2 Triedy*

{triedy:SSECTTRIEDY}

TODO

[2]Táto kniha je voľne dostupná na internete

3.2 Axiomatická vs. naivná teória množín

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

Možno by sme sa mohli trochu zastaviť pri otázke, či vôbec je na niečo dobrá axiomatická teória množín a v akých kontextoch je užitočná.

Z prvého ročníka už viete, že vznik teórie množín bol spojený s istou kontroverziou.

Na jednej strane sa zdala byť užitočná, dali sa pomocou nej dokázať pomerne jednoducho niektoré zaujímavé výsledky. Z iných predmetov zrejme poznáte dôkaz existencie transcendentných čísel, kde argument je založený na tom, že reálne čísla majú väčšiu kardinalitu ako algebraické reálne čísla, takže musí existovať aspoň jedno číslo, ktoré leží v rozdiele týchto dvoch množín. (Tento dôkaz je naznačený v úlohe 2.7.4. Vedeli by sme dostať veľa iných výsledkov založených na podobnom princípe, pozri napríklad úlohy 2.7.5, 2.7.6.)

Potom sa však začali objavovať rôzne paradoxy, ako napríklad dobre známy *Russelov paradox*. Tu uvažujeme množinu

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

takých množín, ktoré nie sú svojimi vlastnými prvkami. 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.

Jeden z dôvodov prečo by mohla byť užitočná axiomatická teória množín je ten, že by nám mohla pomôcť vyhnúť sa takýmto problémom. (V rámci axiomatickej teórie ZFC sa práve načrtnutý argument stane dôkazom, že neexistuje množina všetkých množín.)

Aj ak zistíme, že pri zvolených axiómach sa už nedá zopakovať Russelov paradox, stále sme tým nevylúčili, že sa v rámci nášho axiomatického systému nemôže nejaký spor objaviť nejakým iným spôsobom. Preto by je vcelku lákavá predstava, že detailná formulácia toho, s akými axiómami robíme a čo presne považujeme za dôkazy, by nám azda mohla aj pomôcť dokázať bezospornosť axiomatického systému v ZFC. Potom by sme mali istotu, že keď budeme pracovať iba v rámci tohoto systému, tak sa môžeme cítiť pomerne bezpečne – vedeli by sme, že sa nám nepodarí dokázať dve navzájom si odporujúce tvrdenia.

Dnes už však vieme, že bezospornosť systému ZFC sa dokázať nedá. Vyplýva to z výsledkov Kurta Gödla. Viac o nich sa môžete dočítať napríklad v [Z] alebo tiež v [Smi, Smu].

Aj napriek tomu môže byť v rôznych situáciách užitočný axiomatický prístup. Jedna z vecí, ktoré budeme viackrát spomínať, sú výsledky hovoriace o tom, že nejaké tvrdenie sa nedá dokázať z axióm systému ZFC. (A ak ste teda ochotný prijať na chvíľu pohľad, že tento axiomatický systém berieme ako štandardný základ, na ktorom sa buduje zvyšok matematiky, tak by sa dalo povedať, že sa takéto tvrdenie nedá dokázať v „bežnej“ matematike – bez toho, aby sme pridali nejaké ďalšie axiómy.)

Je snáď vcelku uveriteľné, že keď chceme hovoriť o tom, či nejaké tvrdenie je alebo nie je dokázateľné, tak sa nám asi bude hodiť mať presnú formálnu definíciu toho, čo je *tvrdenie* a čo je *dôkaz*. Práve tieto veci nám poskytuje axiomatický prístup.

K problematike tvrdení, ktoré sú nedokázateľné v rámci ZFC, sa ešte vrátime v časti 3.4.

3.3 Čo sa dá vybudovať v rámci ZFC

V tomto okamihu by sa mohlo zdať, že sme síce zaviedli nejakú peknú axiomatickú teóriu v rámci ktorej vieme nejaké veci dokazovať, ale je veľmi málo vecí, čo v nej vieme vyjadriť. V tejto axiomatickej teórii vieme sformulovať (a dokázať) iba tvrdenia, ktoré majú tvar formuly jazyka teórie množín, t.j., máme povolené používať iba logické spojky, kvantifikátory, premenné. V matematike by sme chceli hovoriť aj o tvrdeniach zaoberajúcich sa reálnymi číslami, vektorovými priestormi, spojitými funkciami, diferenciálnymi rovnicami, atď.

V skutočnosti sa prakticky všetko, čo sa študuje v modernej matematike, dá vybudovať v rámci ZFC. Nie je to však úplne jednoduché a asi by ani nebolo účelné snažiť sa pracovať s komplikovanejšími objektami tak, že by sme sa všetko snažili prefomulovať v takomto jazyku. Pre naše účely ale úplne postačí vedieť, že sa to v princípe dá urobiť. Aspoň stručne si tu aj načrtneme ako.

3.3.1 Usporiadaná dvojica

Skúsme začať s veľmi jednoduchým príkladom. Zadefinujeme v rámci ZFC pojem usporiadanej dvojice. Rozmyslime si najprv, čo vlastne chceme urobiť – pre ľubovoľné množiny a, b by sme chceli mať nejaký objekt, ktorý označíme (a,b), pričom:

- Dvojica (a,b) by mala byť prvkami a, b jednoznačne určená.
- Aj (a,b) by mala byť množina (lebo s inými objektami ani v ZFC nepracujeme).
- Z axióm ZFC by sa malo dať dokázať, že pre ľubovoľné a, b existuje aj (a,b).

Jedna z možných definícií usporiadanej dvojice je nasledovná:

{oboryzfc:DEFPAIR}

Definícia 3.3.1. Nech a, b sú množiny. Potom množinu

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

nazývame *usporiadanou dvojicou* množín a a b.

Všimnime si, že ak existujú množiny a, b, tak viacnásobným použitím axiómy dvojice vieme zdôvodniť aj existenciu množiny, ktorú sme označili ako (a,b).

Okrem toho je podstatné aj to, že pre ľubovoľné množiny a, b, c, d platí

$$(a,b)=(c,d) \qquad \Leftrightarrow \qquad a=c \wedge b=d. \tag{3.1}$$ {oboryzfc:EQUSPDVOJ}

(Overenie tohoto faktu ponechávame ako cvičenie pre čitateľa.)

Skúsme aspoň trochu okomentovať, čo sme vlastne dosiahli. Chceli sme v ZFC vybudovať nejaký objekt – usporiadanú dvojicu. Dôležité je, že sme vedeli, aké vlastnosti od tohoto objektu požadujeme – konkrétne chceme, aby platila podmienka (3.1). A podarilo sa nám naozaj nájsť nejakú definíciu, ktorá zaručuje existenciu usporiadanej dvojice v ZFC a takto definovaná usporiadaná dvojica má požadované vlastnosti.

V podstate od tohoto okamihu môžeme pokojne zabudnúť na definíciu usporiadanej dvojice – podstatné je, že sa vybudovať v rámci ZFC a spĺňa (3.1). Ak budeme využívať iba túto vlastnosť, tak pre nás nie je podstatné, ako presne vyzerá naša definícia usporiadané dvojice.

Hocijaká iná definícia vyhovujúca tejto podmienke by nám poslúžila rovnako dobre. A skutočne existujú aj iné definície usporiadanej dvojice.

Ak sme si nejakú konkrétnu definíciu vybrali, dostali sme možno nejaké vlastnosti navyše. Napríklad pre takto definovanú usporiadanú dvojicu platí $(a,a)=\{\{a\}\}$. Alebo tiež pre každú usporiadanú dvojicu máme $\{a\}\subseteq(a,b)$. Tieto fakty však zrejme nebudeme potrebovať a používať, nebudú nám však ani nijako priveľmi prekážať.

V podobnej situácii sme aj keď chceme v rámci ZFC budovať iné objekty – napríklad prirodzené čísla. Mali by sme si uvedomiť, čo by sme vlastne od prirodzených čísel očakávali. (V tomto prípade to bude asi trochu komplikovanejšie než pri usporiadanej dvojici, kde sme vlastne iba chceli aby bola splnená jedna jednoduchá podmienka.) A potom sa pokúsiť zadefinovať prirodzené čísla v rámci ZFC tak, aby naozaj spĺňali tieto požiadavky.

3.3.2 Číselné obory

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
(*Dobrotivý Boh nám dal celé čísla, všetko ostatné je už dielom človeka.*)
Leopold Kronecker

Vlastne úplne stačí, ak sa nám nejako podarí zaviesť reálne čísla. (Z nich potom viete dostať aj komplexné čísla, napríklad spôsobom, aký ste videli už v prvom ročníku na predmete **Lineárna algebra a geometria.** [3]) Keď už máme k dispozícii reálne čísla tak môžeme robiť reálnu, či komplexnú analýzu jednej aj viac premenných, zaviesť rôzne priestory, s ktorými pracujeme vo funkcionálnej analýze atď. Sme už v situácii, že môžeme začať robiť nejakú serióznu matematiku. (Vlastne v prvom ročníku ste začínali tak, že reálne čísla ste brali ako štruktúru, ktorá je daná, a na nej ste budovali ďalšie veci.)

Dá sa povedať, že na zavedenie celých a racionálnych čísel sa skoro vždy používajú spôsoby spomenuté nižšie. Pre reálne čísla spomenieme dva často používané spôsoby. Existuje aj veľa ďalších – každý z nich má svoje výhody aj nevýhody.

Prirodzené čísla

TODO

Celé čísla

Jedna možnosť ako dostať z prirodzených čísel celé čísla je zaviesť nasledovnú reláciu ekvivalencie na $\mathbb{N} \times \mathbb{N}$:

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

Bolo by treba overiť, že ide skutočne o reláciu ekvivalencie. Triedy ekvivalencie by sme nazvali celými číslami. Zaviedli by sme potom na nich sčitovanie, násobenie, nerovnosť.

Základná idea je, že chceme vedieť prirodzené čísla odčitovať. Aby dvojice (a, b) a (c, d) dali ten istý rozdiel, t.j. aby $a - b = c - d$, tak by sme od nich očakávali, že bude platiť $a + d = b + c$.

Podobá sa to na konštrukciu, ktorú ste videli na **Algebre 2**, keď ste v podstate rovnakým spôsobom ukázali, že každú komutatívnu pologrupu s krátením možno vnoriť do grupy. (Pozri napríklad [N, Theorem 3.10].) Tam ste však pracovali s jedinou operáciou, t.j. z pologrupy $(\mathbb{N}, +)$ uvedenou konštrukciou dostanete grupu $(\mathbb{Z}, +)$. Tu chceme mať na celých číslach aj operáciu $\cdot$ a reláciu $\leq$.

Racionálne čísla

Takisto postup na konštrukciu racionálnych čísel poznáte z nižších ročníkov. Z oboru integrity $(\mathbb{Z}, +, \cdot)$ vieme dostať $(\mathbb{Q}, +, \cdot)$ ako podielové pole. Nie je príliš ťažké zaviesť aj usporiadanie tak, aby sme dostali usporiadané pole. Pozri napríklad [KGGS, Kapitola 4.5].

[3] V priebehu doterajšieho štúdia ste mohli stretnúť viacero spôsobov, ako zaviesť komplexné čísla. Ako usporiadané dvojice s vhodne definovanými operáciami. Ako matice tvaru $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ s operáciami sčitovania a násobenia matíc. Komplexné čísla tiež môžeme chápať ako faktorový okruh $\mathbb{R}[x]/(x^2 - 1)$; toto je špeciálny prípad konštrukcie, ktorou ste k nejakému poľu pridali koreň ireducibilného polynómu.

Reálne čísla

Dve najčastejšie používané konštrukcie reálnych čísel sú zúplnenie a Dedekindove rezy. Viacero spôsobov zavedenia reálnych čísel môžete nájsť napríklad v knihách [A, Blo, Š].

Z analýzy poznáte pojem zúplnenia metrického priestoru. Išlo o konštrukciu, pri ktorej zoberieme všetky Cauchyovské postupnosti daného metrického priestoru X a zavedieme na nich vhodnú reláciu ekvivalencie. Takto dostaneme úplný metrický priestor, ktorý obsahuje X. Zúplnenie metrického priestoru je až na izometriu jednoznačne určené.

Ak urobíme takúto konštrukciu s racionálnymi číslami, na ktorých uvažujeme obvyklú euklidovskú metriku $d(x, y) = |x - y|$, tak dostaneme reálne čísla. Pri tomto prístupe máme „zadarmo" metrickú štruktúru. Nie je však ťažké pre triedy ekvivalencie cauchyovských postupností zaviesť i sčitovanie, násobenie, nerovnosť a overiť, že sú dobre definované a že takto dostaneme usporiadané pole.

Iná často používaná konštrukcia je 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 $A = \{x \in \mathbb{Q}; x < q\}$ a $B = \{x \in \mathbb{Q}; x \geq q\}$.

Často sa Dedekindove rezy zavádzajú takým spôsobom, že sa pokúsime sformulovať ekvivalentné podmienky iba pre jednu z uvedených množín A, B, aby sme nemuseli pracovať s dvojicami množín.

Pretože už samotná definícia Dedekindových rezov je postavená na štruktúre usporiadanej množiny $(\mathbb{Q}, \leq)$, dá sa očakávať, že vlastnosti usporiadanej množiny $(\mathbb{R}, \leq)$ dostaneme pri tomto prístupe pomerne ľahko. Trochu viac sa potrápime s operáciami sčitovania a násobenia.

Táto konštrukcia sa dá zovšobecniť na ľubovoľnú čiastočne usporiadanú množinu. Dostaneme tak Dedekind–MacNeillove zúplnenie, ktorým sa z čiastočne usporiadanej množiny dá zostrojiť úplný zväz. Pozri napríklad [G, Exercises 3.70–3.74], [KLŠZ, podkapitola C.2.9, s.320].

3.3.3 Ešte niečo o kardinálnych číslach

Ďalší objekt, ktorý často používame, sú kardinálne čísla. Hlavne chcem na tomto mieste zdôrazniť, že pojem kardinálneho čísla máme zadefinovaný zatiaľ iba naivne, nie axiomaticky. Pre čokoľvek, čo sa v praxi vyskytne s kardinálnymi číslami, takýto pohľad úplne stačí. Konštrukciu kardinálnych čísel v ZFC by sme potrebovali asi hlavne pri štúdiu teórie množín. Aj tak sa však môžeme aspoň zamyslieť nad tým, či by sme nejako jednoducho vedeli zaviesť kardinálne čísla v rámci ZFC.

{def:POZNDEFKARD}

Poznámka 3.3.2. Znak = zvykneme písať medzi nejaké dva objekty v prípade, že sú totožné. V definícii 2.7.1 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. Použitie symbolu = možno do istej miery obhájiť tým, že vzťah „mať rovnakú mohutnosť" má skutočne podobné vlastnosti ako rovnosť; konkrétne reflexívnosť, symetriu a transzitívnosť. (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 5.6.)

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 3.1.2 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, táto „trieda ekvivalencie“ nie je množinou, je to vlastná trieda. (Je to tak dokonca už pre jednoprvkové množiny.) 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], [Moo, 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 [Fo, 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).

3.4 Relatívna konzistentnosť a nezávislosť

{konz:SECTKONZ}

TODO

Kapitola 4

Axióma výberu

{CHCHOICE}

4.1 Dobre usporiadané množiny

{dum:SECTDUM}

V tejto časti sa ešte nedostaneme k axióme výberu, budeme sa najprv zaoberať dobre usporiadanými množinami. Budeme ich potrebovať v súvislosti s jednou z ekvivalentých formulácií axiómy výberu. Okrem toho budú veľmi dôležité v súvislosti s ordinálmi a transfinitnou indukciou. Vysvetlíme si, ako dobre usporiadané množiny zovšeobecňujú matematickú indukciu a ukážeme si niekoľko konštrukcií dobre usporiadaných množín.

{dum:DEFDUM}

Definícia 4.1.1. 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 4.1.2.)

Tiež je ľahké ukázať, že podmnožina dobre usporiadanej množiny je tiež dobre usporiadaná (úloha 4.1.1).

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

Definícia 4.1.2. 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 4.1.3 (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 4.1.3 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. □

Príklad 4.1.4. 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 4.1.5. *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.[1] Takto môžeme získať veľké množstvo ďalších príkladov.

{dum:DEFLEXIKO}{dum:DEFANTILEXIKO}

Definícia 4.1.6. Nech $(A, \leq_A)$, $(B, \leq_B)$ sú čiastočne usporiadané množiny. Potom reláciu $\leq$ na množine $A \times B$ definovanú ako

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

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

Antilexikografické usporiadanie na $A \times B$ definujeme ako

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

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

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

Antilexikografické usporiadanie je veľmi podobné, len ako najdôležitejšiu sme zobrali druhú (poslednú) pozíciu namiesto prvej. Tvrdenia, ktoré tu uvedieme, budeme dokazovať len pre lexikografické usporiadanie; dôkazy pre antilexikografické usporiadanie by boli takmer totožné (pozri aj poznámku 4.1.8).

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.

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

{dum:TVRLEXI}

Tvrdenie 4.1.7. *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 $p_A[C]$.

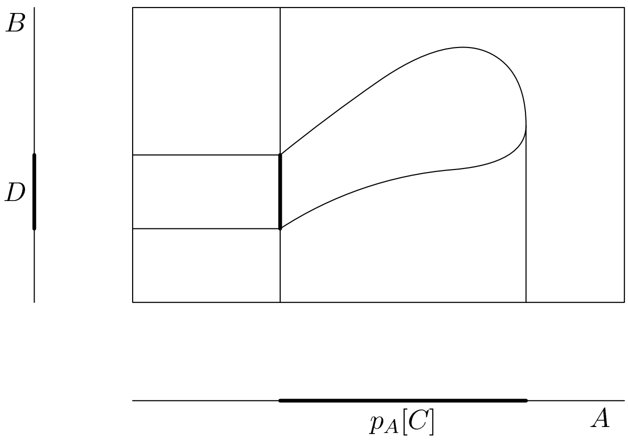
Označme $D:=\{b\in B;(a_0,b)\in C\}$. Množina D je neprázdna, keďže $a_0\in p_A[C]$, t.j. existuje aspoň jedna dvojica $(a,b)\in C$, kde prvá súradnica je $a=a_0$. Pretože $(B,\leq)$ je dobre usporiadaná množina, existuje najmenší prvok množiny D, označme ho b_0.

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 4.1.8. 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 4.1.7 skutočne stačilo dokázať jednotlivé časti pre jedno z týchto dvoch usporiadaní.)



{dum:FIGLEXI} Obr. 4.1: Ilustrácia k dôkazu tvrdenia 4.1.7

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

{dum:PRSUCET}

Príklad 4.1.9. 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.

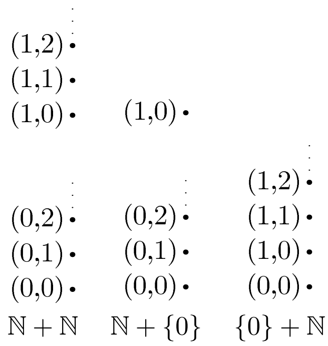
Ak obe množiny sú lineárne (dobre) usporiadané, platí to aj o výslednej množine – overenie tohoto faktu ponecháme ako cvičenie pre čitateľa. (Zovšeobecnenie tohoto faktu môžete nájsť v úlohe 4.1.5.)

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 4.2 môžete vidieť, čo dostaneme, ak za B resp. C zvolíme $\mathbb{N}$ (s obvyklým usporiadaním) alebo jednoprvkovú množinu. Môžete si napríklad všimnúť, že dobre usporiadaná množina $\{0\} + \mathbb{N}$ je izomorfná s dobre usporiadanou množinou $\mathbb{N}$, zatiaľčo $\mathbb{N} + \{0\}$ nie je. Neskôr uvidíme, že takto definovaný súčet a antilexikografický súčin dobre usporiadaných množín sa dajú použiť na zavedenie súčtu a súčinu ordinálnych čísel.

{dum:POZNDISJZJED}

Poznámka 4.1.10. 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. My ho síce budeme potrebovať iba pre dobre



Obr. 4.2: Príklady na súčet dobre usporiadaných množín {dum:FIGSUCET}

usporiadané množiny, ale môžeme tento pojem zaviesť všeobecnejšie pre ľubovoľné čiastočné usporiadanie.

Definícia 4.1.11. *Počiatočný úsek* čiastočne 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 4.1.12. *Nech $(X,\leq)$ je lineárne usporiadaná množina a nech $X'=\{X_a; a\in X\}$. 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 $X_a\subseteq X_b$.)[2]

Iná možnosť – namiesto overovania monotónnosti f^{-1} – je použiť výsledok z úlohy 2.6.3. □

Nasledujúce tvrdenie je do istej miery odbočkou od hlavnej témy – nás na tomto mieste zaujímajú dobre usporiadané množiny. Azda však stojí za zmienku, keďže dôkaz je takmer rovnaký ako v predchádzajúcom tvrdení. A dozvieme sa z neho zaujímavý fakt, že každá čiastočne usporiadaná množina X sa dá vnoriť do $(\mathcal{P}(X),\subseteq)$. Pozri napríklad aj [R, Theorem 1.11].

[2]Všimnime si, že na tomto mieste sme použili linearitu usporiadania. Veľmi podobné tvrdenie, ktoré platí aj pre čiastočné usporiadania, je tvrdenie 4.1.13.

Na tento výsledok sa dá pozerať ako na vetu o reprezentácii. Napríklad z Cayleyho vety vieme, že každá grupa je izomorfná s nejakou grupou permutácií. Podobne každý konečnorozmerný vektorový priestor je izomorfný s priestorom F^n. Tento výsledok má podobný charakter – istý spôsobom môžeme reprezentovať všetky čiastočne usporiadané množiny. Konkrétne každú čiastočne usporiadanú množinu môžeme chápať ako nejakú množinu množín, kde čiastočné usporiadanie je inklúzia.

{dum:TVRIZOMPOCUSEKCUM}

Tvrdenie 4.1.13. *Nech $(X, \leq)$ je čiastočne usporiadaná množina a nech $X' = \{X_a \cup \{a\}; a \in X\}$. Potom zobrazenie $f\colon X \to X'$ určené predpisom*

$$f(a) = X_a \cup \{a\}$$

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

Dôkaz. Pre potreby tohoto dôkazu zaveďme označenie

$$a \downarrow = X_a \cup \{a\} = \{x \in X; x \leq a\},$$

keďže tieto množiny budeme často používať. Máme teda $f(a) = a \downarrow$ a $X' = \{a \downarrow; a \in X\}$.

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

Nech $a, b \in X$ a $a \neq b$. Uvažujme dve možnosti, ktoré môžu nastať.

Ak $a \leq b$, tak platí $b \in b \downarrow$, súčasne však $b \notin a \downarrow$. Teda mám $a \downarrow \neq b \downarrow$, t.j. $f(a) \neq f(b)$.

Ak neplatí $a \leq b$, tak $a \notin b \downarrow$ a súčasne $a \in a \downarrow$. Opäť dostávame $a \downarrow \neq b \downarrow$ a $f(a) \neq f(b)$.

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

Ešte treba overiť, že aj f^{-1} je monotónne. Na to si stačí všimnúť, že ak $a \downarrow \subseteq b \downarrow$, tak $a \leq b$ (To vidno priamo z toho, že $a \in b \downarrow$.) $\square$

Cvičenia

{dumcvic:ULOSUB}

Úloha 4.1.1. Ukážte, že každá podmnožina dobre usporiadanej množiny (so zdedeným usporiadaním) je dobre usporiadaná.

{dumcvic:ULODUMLUM}

Úloha 4.1.2. 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 4.1.1: Namiesto čiastočného usporiadania požadujeme lineárne usporiadanie a existenciu najmenšieho prvku sme nahradili existenciou minimálneho prvku.)

Úloha 4.1.3. Nech $(X, \leq)$ je lineárne usporiadaná množina. Ukážte, že $a \in X$ je minimálny prvok množiny X práve vtedy, keď $X_a = \emptyset$.

{dumcvic:ULOKLESPOST}

Úloha 4.1.4. Nech $(X, \leq)$ je lineárne usporiadaná množina. Ukážte, že $(X, \leq)$ je dobre usporiadaná práve vtedy, keď neexistuje postupnosť $(x_n)_{n=0}^{\infty}$ prvkov X taká, že $x_0 > x_1 > \dots > x_n > x_{n+1} > \dots$

{dumcvic:SUMSYST}

Úloha 4.1.5. V tejto úlohe zadefinujeme isté zovšeobecnenie lexikografického súčinu.
Nech $(A, \leq_A)$ je čiastočne usporiadaná množina a pre každé $a \in A$ je $(B_a, \leq_a)$ čiastočne usporiadaná množina. Na množine $\bigcup_{a \in A} \{a\} \times B_a$ definujeme reláciu $\leq$ predpisom:

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

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

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

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

c) Ak $A = \{0, 1\}$ (s obvyklým usporiadaním, t.j. $0 < 1$), $B_0 = B$ a $B_1 = C$, tak dostaneme čiastočne usporiadanú množinu z príkladu 4.1.9.

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

Úloha 4.1.6. 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) $\sum_{n\in\mathbb{N}}(\{1, 2, \dots, n\}, \leq)$
i) $\sum_{n\in\mathbb{N}}(\mathbb{N}, \leq)$

{dumcvic:ULOHSPOCR}

Úloha 4.1.7*. Dokážte, že:
a) Každá podmnožina $\mathbb{R}$, ktorá je dobre usporiadaná (pri obvyklom usporiadaní reálnych čísel) je spočítateľná.
b) Každá dobre usporiadaná podmnožina $\mathbb{R}$ je izomorfná s podmnožinou $\mathbb{Q}$ (s obvyklým usporiadaním racionálnych čísel).
c) 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. Tu nás zaujímajú dobre usporiadané množiny, aj tak však poznamenajme, že sa dá v skutočnosti dokázať o niečo viac, než tvrdíme v časti c). Platí, že každá spočítateľná lineárne usporiadaná množina sa dá vnoriť do reálnych čísel s obvyklým usporiadaním.)

4.2 Ekvivalentné formy axiómy výberu

Základnú formu axiómy výberu, ktorú sme uviedli v časti 3.1, 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 3.1:

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 i časti (ii) a (iii) tvrdenia 4.2.2 používať pod pomenovaním axióma výberu.

Definícia 4.2.1. 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}

Tvrdenie 4.2.2 (ZF)**.** *Nasledujúce podmienky sú ekvivalentné* (*ako tvrdenia ZF*)*:* {ekviv:itAC}
(i) *axióma výberu;* {ekviv:itSELDISJ}
(ii) *pre každý systém neprázdnych po dvoch disjunktných množín existuje selektor;* {ekviv:itSEL}
(iii) *pre každý systém neprázdnych množín existuje selektor;* {ekviv:itPROD}
(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 2.5.9.

(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 sformulovaním týchto podmienok dokážeme lemu, ktorá sa nám bude viackrát hodiť v niektorých dôkazoch.

Definícia 4.2.3. Podmnožinu čiastočne usporiadanej množiny $(P, \leq)$, ktorá je usporiadaním $\leq$ lineárne usporiadaná, budeme nazývať *reťazec* v P.

{ekviv:LMCHAINOFPOSETS}

Lema 4.2.4. *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.*

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 $(a, c) \in R$. □

{ekviv:VTEKVACWO}

Veta 4.2.5 (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 4.2.6. 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.

{ekviv:POZNZLNEPR}

Poznámka 4.2.7. Zornovu lemu budeme často využívať na to, aby sme ukázali existenciu nejakého objektu, ktorý dostaneme, ako maximálny prvok vo vhodne zvolenej čiastočne usporiadanej množine $(P, \leq)$. Vidíme, že ak chceme Zornovou lemou existenciu niečoho dokázať, tak potrebujeme vedieť, že $P \neq \emptyset$. Preto je dôležité pri aplikáciách Zornovej lemy nezabudnúť skontrolovať aj to, že čiastočne usporiadaná množina, s ktorou pracujeme, je neprázdna.

Jednotlivé implikácie v dôkaze vety 4.2.5 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 $(\bigcup \mathcal{S}, \leq)$.) $\square$

Dôkaz implikácie ZL $\Rightarrow$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. Všimnime si, že $P \neq \emptyset$, lebo $(\emptyset, \emptyset) \in P$.

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 pre ľubovoľné $b \in B$, $b' \in B'$ z $b'R'b$ vyplýva $b' \in B$.

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. Budeme sa snažiť ukázať, že $(\overline{B}, \overline{R})$ patrí do P a že je to horné ohraničenie reťazca $\mathcal{C}$.

Všimnime si najprv, že ak $(B, R), (B', R') \in \mathcal{C}$ a $a, b \in B \cap B'$, tak

$$aRb \qquad \Leftrightarrow \qquad aR'b.$$

Keďže $\mathcal{C}$ je reťazec, tak máme buď $(B,R) \leq (B',R')$ alebo $(B,R) \leq (B',R')$. BUNV nech nastane prvý prípad. Teda $B \subseteq B'$ a relácia R je zúžením relácie R'. Potom hneď máme, že z $aR'b$ vyplýva aRb (lebo R je zúženie relácie R). Ale aj obrátene, ak platí aRb a R sme dostali ako zúženie R', tak musí platiť aj $aR'b$.

Z toho pomerne priamočiaro dostaneme aj to, že pre $(B,R) \in \mathcal{C}$ a $a,b \in B$ platí

$$aRb \qquad \Leftrightarrow \qquad a\overline{R}b.$$

Stačí si uvedomiť, že $a\overline{R}b$ znamená, že $aR'b$ pre nejaké $(B',R') \in \mathcal{C}$.

Overenie, že $(\overline{B},\overline{R}) \in P$. Je zrejmé, že $\overline{B} \subseteq A$, treba overiť, že $\overline{R}$ je dobré usporiadanie na $\overline{B}$. Z lemy 4.2.4 vieme, že $\overline{R}$ je čiastočné usporiadanie.

Ešte ukážme, že $(\overline{B},\overline{R})$ je dobre usporiadaná množina. Nech C je neprázdna podmnožina $\overline{B}$. Z neprázdnosti vyplýva, že existuje $c \in C$ a z definície množiny $\overline{B}$ vyplýva, že existuje $(B,R) \in \mathcal{C}$ tak, že $c \in B$. Položme $m := \min_R(C \cap B)$, 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 $c' \in C$. Potom existuje $(B',R') \in \mathcal{C}$ také, že $c' \in B'$. 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 $c' \in C \cap B$, a teda mRc' (keďže m je najmenší prvok množiny $C \cap B$), čiže aj $m\overline{R}c'$.
Druhý možný prípad je $(B,R) \leq (B',R')$. Ak $c' \in B$, tak môžeme bezo zmeny zopakovať úvahu z predchádzajúceho prípadu. Zostáva teda len prípad $c' \in B' \smallsetminus B$. Potom však nemôže platiť $c'R'm$, lebo B je počiatočný úsek B' a z podmienky $m \in B$ by sme potom dostali aj $c' \in B$. Keďže R' je lineárne usporiadanie, zostáva len druhá možnosť $mR'c$. To ale znamená, že $m\overline{R}c'$.

$(\overline{B},\overline{R})$ *je horné ohraničenie reťazca* $\mathcal{C}$. Chceme ukázať, že pre každé $(B,R) \in \mathcal{C}$ platí $(B,R) \leq (\overline{B},\overline{R})$. Očividne $B \subseteq \overline{B}$. Takisto vieme, že R je zúžením relácie $\overline{R}$ na B, lebo sme už skontrolovali, že podmienky aRb a $a\overline{R}b$ sú ekvivalentné (pre $a,b \in B$).

Treba už len overiť, že B je dolným úsekom $\overline{B}$. Predpokladajme teda, že $b'\overline{R}b$ pre nejaké $b' \in \overline{B}$. Potom $b' \in B'$ pre nejaké $(B',R') \in \mathcal{C}$. Ak $(B',R') \leq (B,R)$ a $B' \subseteq B$, tak aj $b' \in B$. Zostáva sa pozrieť na prípad $(B,R) \subseteq (B',R')$. Lenže už vieme, že z $b'\overline{R}b$ vyplýva aj $b'R'b$. Pretože (B,R) je počiatočný úsek (B',R'), dostávame $b' \in B$.

Maximálny prvok dáva dobré usporiadanie na 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 $A \smallsetminus B_0 \neq \emptyset$. Potom existuje $a \in A \smallsetminus B_0$. 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. Súčasne je neprázdna, keďže $\emptyset \in P$.

Všimnime si, že ak pre zobrazenia $f\colon A_1 \to B$, $g\colon A_2 \to B$ platí $f \subseteq g$, tak aj $A_1 \subseteq A_2$.

Overme, že táto množina spĺňa predpoklady Zornovej lemy. Nech $\mathcal{C}$ je reťazec v $(P, \subseteq)$. 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 zobrazenie.

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 $A' \subsetneqq A$. 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 $f \subsetneqq \overline{f}$. 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 princíp 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 $\mathcal{E} \supseteq \mathcal{C}$. Ďalej ak si vezmeme ľubovoľné dva prvky $a, b \in \mathcal{E}$, tak musí existovať $\mathcal{D} \in \mathcal{R}$, ktoré obsahuje oba tieto prvky. (Tu využívame, že $\mathcal{R}$ je reťazec.) To znamená, že ľubovoľné dva prvky z $\mathcal{E}$ sú porovnateľné. Teda aj $\mathcal{E}$ je reťazec a patrí do U.

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 $\Rightarrow$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. □

4.2.1 Dôkaz Zornovej lemy

Aby sme mali dokázanú ekvivalenciu všetkých podmienok uvedených vo vete 4.2.5, stačí nám už len dokázať napríklad AC $\Rightarrow$ ZL. Tento dôkaz sa dá urobiť pomocou transfinitnej indukcie, takýto dôkaz je uvedený v časti 5.7.2. Na tomto mieste spomenieme základnú ideu dôkazu – a potom si ukážeme aj to, ako sa dá dôkaz naozaj poriadne formálne zapísať.

Idea dôkazu Zornovej lemy. Nech by $(P,\leq)$ bola čiastočne usporiadaná množina, kde každý reťazec má horné ohraničenie, ale súčasne v P neexistuje maximálny prvok.

Vyberme si ľubovoľné $a_0 \in P$. Pretože $\{a_0\}$ je reťazec v P a súčasne a_0 nie je maximálny prvok, vieme vybrať $a_1 > a_0$.

Podobne indukciou môžeme každý reťazec $a_0 < a_1 < \cdots < a_n$ rozšíriť o nový prvok a_{n+1} ostro väčší od $a_0, \dots, a_n$.

Tento argument však funguje aj pre nekonečné reťazce – ak máme reťazec R, tak určite existuje jeho horné ohraničenie h. Pretože h nie je maximálny prvok, existuje $\widehat{h} > h$. Takýto prvok $\widehat{h}$ je teda ostro väčší od všetkých prvkov reťazca R.

Teda v takomto induktívnom procese vieme pokračovať ďalej. Ak sme už zadefinovali a_k pre všetky prirodzené čísla, tak vieme pridať horné ohraničenie a_ω. Ďalej vieme už vytvorený reťazec rozšíriť o $a_{\omega+1}, a_{\omega+2}, \dots, a_{\omega+\omega}, \dots$ atď.

Týmto spôsobom dostávame čoraz dlhší a dlhší reťazec, až časom dospejeme k reťazcu, ktorý má kardinalitu ostro väčšiu ako P, čo je spor. □

Uvedený argument samozrejme nie je dôkaz. Potrebujeme poriadne sformalizovať miesto, na ktorom sme povedali „a tak ďalej“ – čiže potrebujeme induktívny argument, ktorý funguje aj pre ľubovoľne veľké množiny. Už sme videli, že nejaký takýto typ indukcie nám dávajú dobre usporiadané množiny.

Ako sme už spomenuli, v časti 5.7.2 uvedieme dôkaz pomocou transfinitnej indukcie – tento dôkaz je do značnej miery prepisom náčrtu naznačeného vyššie. A pre človeka, ktorý už dobre pozná ordinály a transfinitnú indukciu, je to veľmi prirodzený prístup ako tento náčrt sformalizovať. Uvedieme tu aj iný dôkaz, ktorý má tiež podobný charakter, t.j. do istej miery sa dá považovať za formalizáciu vyššie naznačeného postupu – ale nevyžaduje znalosť ordinálnych čísel.

Uviesť dôkaz bez transfinitnej indukcie môže mať viacero výhod:

- Je možné, že čitateľ sa rozhodne, že ho z tohto textu nezaujíma časť venovaná ordinálnym číslam a transfinitnej indukcii – v takom prípade by tu zostal veľmi dôležitý výsledok bez dôkazu.
- Súčasne sa vyhneme tomu, že by sme vzbudili dojem, že dôkaz Zornovej lemy je ťažký a vyžaduje dlhú prípravu. (Na druhej strane, dôkaz uvedený tu môže niekomu pripadať trochu umelý – najmä človeku, ktorý sa už oboznámil s transfinitnou indukciou. Má však výhodu, že sa mu dá porozumieť už so znalosťou faktov, ktoré sme o dobre usporiadaných množinách uviedli doteraz a nevyžaduje si najprv vybudovať pojem ordinálnych čísel a zaviesť transfinitnú indukciu.)

Dôkaz, ktorý uvádzame, je dôkaz z článku [Lew]. Dôkaz uvedený v [We] má do istej miery podobný charakter.

Dôkaz Zornovej lemy. Sporom. Nech $(P,\leq)$ je čiastočne usporiadaná množina, v ktorej každý reťazec má horné ohraničenie. Predpokladajme súčasne, že P nemá maximálny prvok.

Z toho vyplýva, že pre každý reťaze $R\subseteq P$ máme *ostré* horné ohraničenie. Potom pre každý reťazec R v P existuje ostré horné ohraničenie a na základe AC máme funkciu f, ktorá reťazcu R priradí niektoré jeho ostré horné ohraničenie $f(R)$.

Reťazec R volajme f-reťazec, ak platí:

- $(R,\leq)$ je dobre usporiadaná množina.
- Pre každé $x\in R$ platí[3]

$$x=f(R_x)=f(\{a\in R; a<x\}).$$

O f-reťazcoch nižšie ukážeme nasledujúce dve pozorovania:

- Ak máme dva f-reťazce, tak jeden z nich je počiatočným úsekom druhého.
- Zjednotenie všetkých f-reťazcov v P opäť tvorí f-reťazec.

Ak platia tieto dva fakty, tak už pomerne ľahko dostávame spor. Ak položíme

$$\overline{R}=\bigcup\{R; R \text{ je } f\text{-reťazec v } P\}.$$

Množina $\overline{R}$ je f-reťazec. Takisto je f-reťazcom aj $R'=\overline{R}\cup\{f(\overline{R})\}$. Máme teda

$$R'\subseteq\overline{R}\subsetneq R',$$

čo je spor. Zostáva nám teda ešte zdôvodniť obe pozorovania spomenuté vyššie.

Kompatibilita f-reťazcov. Nech $A,B\subseteq P$ sú f-reťazce a $A\neq B$. Bez ujmy na všeobecnosti predpokladajme, že $A\setminus B\neq\emptyset$. Množina A je dobre usporiadaná, teda existuje najmenší prvok x neprázdnej množiny $A\setminus B$.

$$x=\min(A\setminus B) \qquad A_x\subseteq B$$

Ak platí $A_x=B$, tak sme dokázali to, čo sme chceli. Ak by to tak nebolo, tak množina $B\setminus A_x$ je neprázdna, jej najmenší prvok označme y. Evidentne platí $B_y\subseteq A_x$.

$$y=\min(B\setminus A_x) \qquad B_y\subseteq A_x$$

[3] Práve táto podmienka zodpovedá tomu, že ak máme nejaký začiatok reťazca, ktorý vytvárame, tak ďalší prvok priradíme pomocou funkcie f. T.j. pridáme nejaké ostré horné ohraničenie pre doteraz vytvorené prvky a teda predĺžime reťazec. Oproti dôkazu transfinitnou indukciou tento dôkaz o čosi menej vyzerá ako „proces“, pri ktorom postupne reťazec vytvárame – v podstate v dôkaze už pracujeme so systémom všetkých f-reťazcov a zjednotením tohto systému.

Označme z najmenší prvok množiny $A \setminus B_y$.

$$z = \min(A \setminus B_y) \qquad A_z \subseteq B_y$$

Zatiaľ teda pre tieto prvky máme

$$A_z \subseteq B_y \subseteq A_x \subseteq B.$$

Poďme ukázať, že v skutočnosti platí $A_z = B_y$.

Všimnime si, že $z \leq x$. Ak $x = z$, tak máme $A_z \subseteq B_y \subseteq A_z$, čiže dostávame rovnosť $A_z = B_y$.

Zostáva sa pozrieť na možnosť $z < x$. Z toho, že $z \in A_x$ dostávame $z \in B$. Nemôže platiť $z = y$; to by totiž znamenalo, že $y \in A_x$. Nemôže platiť ani $z < y$; dostali by sme $z \in B_y$. Máme teda $y \leq z$, z čoho už vyplýva $B_y \subseteq A_z$.

V oboch prípadoch sme dostali

$$A_z = B_y,$$

a teda aj

$$z = f(A_z) = f(B_y) = y.$$

Nemôže teda platiť $z = x$. (V takom prípade by sme totiž dostali $x = f(A_x) = y \in B$.) Máme teda ostrú nerovnosť $z < x$. To znamená, že $y = z \in A_x$, čo je spor s tým, že $y \in B \setminus A_x$.

Zjednotenie všetkých f-reťazcov je f-reťazec. Využitím kompatibility dostávame nasledujúcu vlastnosť: Nech $x \in A$ pre nejaký f-reťazec A a súčasne $y \leq x$. Potom buď $y \in A$ alebo y nepatrí do žiadneho f-reťazca.

Označme ako $\overline{R}$ zjednotenie všetkých f-reťazcov v P. Zoberme si ľubovoľné $x \in \overline{R}$. Potom $x \in A$ pre nejaký f-reťazec A. Z pozorovania, ktoré sme práve spomenuli, vidíme, že

$$\{y \in \overline{R}; y \leq x\} = \{y \in A; y \leq x\}$$
$$\overline{R}_x = \{y \in \overline{R}; y < x\} = \{y \in A; y < x\} = A_x$$

Z prvej rovnosti vidíme, že $(\overline{R}, \leq)$ je dobre usporiadaná množina. (Relácia $\leq$ dáva dobré usporiadanie na každom dolnom úseku množiny $\mathbb{R}$.) A súčasne máme

$$x = f(A_x) = f(\overline{R}_x).$$

Teda $\overline{R}$ je skutočne f-reťazec. □

4.3 Aplikácie axiómy výberu a Zornovej lemy

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 2.5.9(i). Dokonca sme v tvrdení 4.2.2(vi) ukázali, že v ZF je toto tvrdenie s axiómou výberu ekvivalentné. Ďalším príkladom takéhoto tvrdenia je ekvivalencia Cauchyho a Heineho definícia spojitosti.

4.3.1 Cauchyho a Heineho definícia spojitosti

Na úvod si pripomeňme definíciu spojitosti reálnej funkcie v bode:

Definícia 4.3.1 (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 4.3.2 (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 4.3.3. *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 [Her2, 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. [4]

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) [Her1, Theorem 1.1], [Her2, Theorem 4.54].

[4]Pozri aj `http://thales.doa.fmph.uniba.sk/sleziak/texty/rozne/AC/cont.pdf`

4.3.2 Alexandrova veta o subbáze

{alex:SSECTAL

V tejto časti si ukážeme užitočnú vetu týkajúcu sa kompaktných priestorov. Kompaktnosť je jeden z najdôležitejších pojmov vo všeobecnej topológii.

Pripomeňme, že ak $(X, \mathcal{T})$ je topologický priestor, tak systém otvorených množín $\mathcal{B}$ sa nazýva *báza* topológie $\mathcal{T}$, ak pre každé $x \in X$ a otvorené okolie $U \ni x$ existuje $B \in \mathcal{B}$ také, že $x \in B \subseteq U$. Ekvivalentne: Každá otvorená množina sa dá napísať ako zjednotenie množín z $\mathcal{B}$.

Systém otvorených množín $\mathcal{S}$ je *subbáza* pre $(X, \mathcal{T})$, ak konečné prieniky množín z $\mathcal{S}$ vytvoria bázu $(X, \mathcal{T})$.

Ako jednoduchý príklad bázy môžeme spomenúť množinu otvorených intervalov s racionálnymi koncovými bodmi $\mathcal{B} = \{(a, b); a, b \in \mathbb{Q}\}$, ktorá tvorá bázu obvyklej topológie na $\mathbb{R}$. Ako subbázu by sme mohli zobrať $\mathcal{S} = \{(-\infty, b), (a, \infty); a, b \in \mathbb{Q}\}$.

Topologický priestor X je *kompaktný,* ak pre každé otvorené pokrytie existuje konečné podpokrytie.

Azda najzákladnejším príkladom kompaktného priestoru je jednotkový interval $\langle 0, 1\rangle$. V tejto kapitole ukážeme, že súčin kompaktných priestorov je opäť kompaktný. Pomerne ľahko sa dá ukázať, že uzavretý podpriestor kompaktného priestoru musí byť kompakt. Z toho napríklad vidíme, že každý uzavretý podpriestor priestoru $\langle 0, 1\rangle^A$ je kompaktný. V skutočnosti vieme povedať o čosi viac – takéto priestory sú vlastne (až na homeomorfizmus) presne všetky hausdorffovské kompaktné priestory.

Nie je ťažké ukázať, že ak si zvolíme nejakú bázu $\mathcal{B}$, tak požiadavka aby existovalo konečné podpokrytie pre každé otvorené pokrytie pozostávajúce z bázových množín, je ekvivalentná s kompaktnosťou. (Čiže kompaktnosť stačí overovať pre pokrytia tvorené bázovými množinami. Úloha 4.3.4.) Zaujímavé je, že rovnaké tvrdenie platí i pre subbázu. Tento výsledok sa nazýva Alexandrova veta o subbáze. Pozri napríklad [Eng, Problem 3.2.12], [Ci, Lemma 4.4.4], [KT, Problem 14.9], [Tao, Theorem 1.8.9].

Veta 4.3.4 (Alexander subbase theorem)**.** *Nech X je topologický priestor a $\mathcal{S}$ je jeho subbáza. Ak každé pokrytie $\mathcal{U} \subseteq \mathcal{S}$ má konečné podpokrytie, tak X je kompaktný.*

Dôkaz. Sporom. Nech X spĺňa uvedenú vlastnosť pre subbázu $\mathcal{S}$ a pritom nie je kompaktný.

To znamená, že existuje otvorené pokrytie, ktoré nemá konečné podpokrytie. Z Zornovej lemy vyplýva, že existuje aj maximálne pokrytie s touto vlastnosťou. Overme predpoklady Zornovej lemy. Nech $\mathcal{R}$ je reťazec takýchto pokrytí. Potom evidentne $\bigcup \mathcal{R}$ je tiež pokrytie. Ak by malo konečné podpokrytie, tak toto podpokrytie je už podpokrytím niektorého prvku z $\mathcal{R}$. (Vďaka konečnosti a tomu, že $\mathcal{R}$ je reťazec.)

Nech teda $\mathcal{C}$ je maximálne otvorené pokrytie, ktoré nemá konečné podpokrytie. Špeciálne to znamená, že ak pridáme ľubovoľnú otvorenú množinu U, tak $\mathcal{C} \cup \{U\}$ už bude mať konečné podpokrytie.

Uvažujme teraz systém $\mathcal{C} \cap \mathcal{S}$, t.j. zoberme len tie množiny z $\mathcal{C}$, ktoré patria do subbázy. Tento systém už nie je pokrytím – inak by mal konečné podpokrytie, ktoré by bolo súčasne podpokrytím pokrytia $\mathcal{C}$. Teda existuje $x \in X$, ktoré nie je pokryté žiadnou množinou z $\mathcal{C} \cap \mathcal{S}$.

Keďže $\mathcal{C}$ je pokrytie, bod x musí byť pokrytý nejakou množinou z $\mathcal{C}$, teda máme $x \in U \in \mathcal{C}$. Ďalej existujú $S_1, \dots, S_n$ také, že $x \in S_1 \cap \dots \cap S_n \subseteq U$.

Pretože bod x nie je pokrytý žiadnou množinou z $\mathcal{C} \cap \mathcal{S}$, máme $S_i \notin \mathcal{C}$ (pre $i = 1, \dots, n$). Z maximality $\mathcal{C}$ ale vieme, že $\mathcal{C} \cup \{S_i\}$ už má nejaké konečné podpokrytie, čiže existuje konečný podsystém $\mathcal{C}_i \subseteq \mathcal{C}$ taký, že $\mathcal{C}_i \cup \{S_i\}$ pokrýva celé X. Posledná podmienka je ekvivalentná s tým, že $X \setminus S_i \subseteq \bigcup \mathcal{C}_i$.

Potom ale dostaneme

$$X \setminus U \subseteq X \setminus \bigcap_{i=1}^{n} S_i = \bigcup_{i=1}^{n} (X \setminus S_i) \subseteq \bigcup_{i=1}^{n} \bigcup \mathcal{C}_i.$$

Teda

$$\mathcal{F} = \{U\} \cup \bigcup_{i=1}^{n} \mathcal{C}_i$$

je konečné podpokrytie pokrytia $\mathcal{C}$. □

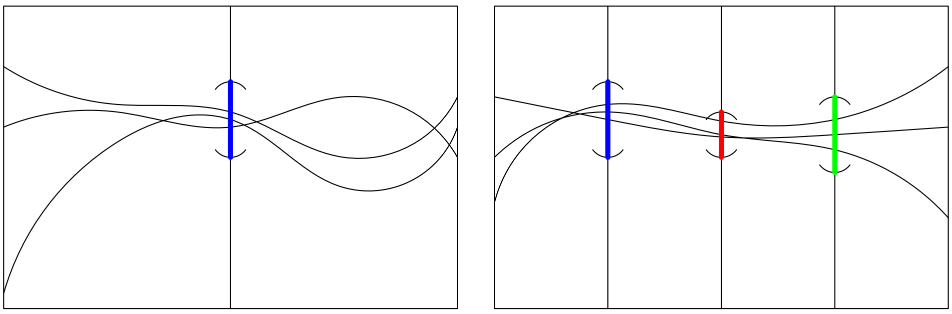
Z Alexandrovej vety o subbáze vieme ľahko dostať Tichonovovu vetu. Opäť s pokojným svedomím môžeme povedať, že ide o jeden z najdôležitejších výsledkov vo všeobecnej topológii. [5]

Pred sformulovaním tejto vety sa oplatí pripomenúť definíciu topologického súčinu. Ak máme topologické priestory X_i, $i \in I$, tak na množine $\prod\limits_{i\in I} X_i$ môžeme definovať topológiu takým spôsobom, že vezmeme za subbázu množiny $p_i^{-1}[U]$ pre ľubovoľné $i \in I$ a ľubovoľnú otvorenú množinu U v X_i, kde $p_i \colon X \to X_i$ označuje projekciu na i-tu zložku.

$$\mathcal{S} = \{p_i^{-1}[U]; i \in I; U \text{ je otvorená podmnožina } X_i\}$$

Topologický priestor na množine $\prod\limits_{i\in I} X_i$ s topológiou určenou touto subbázou sa nazýva *topologický súčin* priestorov X_i.

Typická (sub)bázová množina je znázornená na obrázku 4.3.



Obr. 4.3: Obrázok znázorňuje typickú množinu zo subbázy (resp. bázy) spolu s niektorými funkciami patriacimi do tejto množiny {alex:FIGPROD}

Veta 4.3.5 (Tichonovova veta)**.** *Topologický súčin kompaktných priestorov je kompaktný. T.j. ak X_i je kompaktný topologický priestor pre každé $i \in I$, tak aj $\prod\limits_{i\in I} X_i$ je kompaktný priestor.*

Dôkaz. Nech $\{X_i, i \in I\}$ je systém kompaktných priestorov. V priestore $X = \prod\limits_{i\in I} X_i$ máme subbázu tvorenú množinami tvaru $p_i^{-1}[U]$. Chceme ukázať, že každé pokrytie množinami z tejto subbázy má konečné podpokrytie.

[5] Pravdepodobne sa stretnete s touto vetou aj na iných predmetoch a možno budete vidieť iné dôkazy. Keďže ide o pomerne dôležitý výsledok, nezaškodí poznať viacero dôkazov tejto vety; navyše si pri ich môžete osvojiť užitočné koncepty a rôzne dôkazové techniky.

Nech teda $\mathcal{C}$ je ľubovoľné pokrytie subbázovými množinami. Označme

$$\mathcal{C}_i = \{U \subseteq X_i; p_i^{-1}[U] \in \mathcal{C}\}.$$

Ak pre niektoré $i \in I$ tvorí $\mathcal{C}_i$ pokrytie kompaktného priestoru X_i, tak má konečné podpokrytie $\mathcal{F}_i$ a

$$\{p_i^{-1}[U]; U \in \mathcal{F}_i\}$$

je konečné podpokrytie pokrytia $\mathcal{C}$.

Zostáva teda možnosť, že pre žiadne $i \in I$ systém $\mathcal{C}_i$ nepokrýva X_i, čo znamená, že existuje $x_i \in X_i$, ktoré nie je pokryté systémom $\mathcal{C}_i$, t.j.

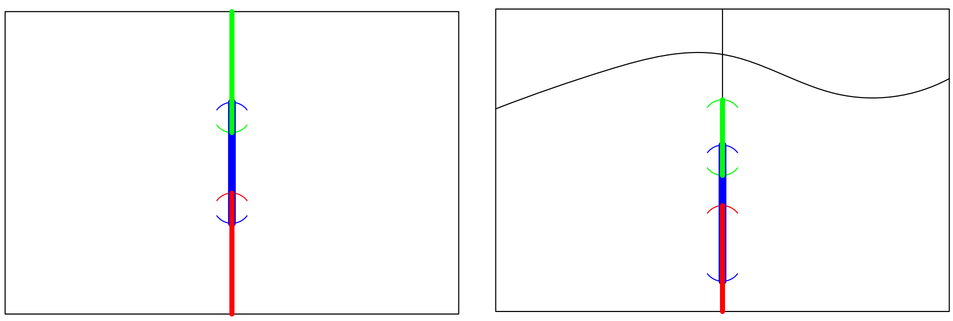
$$x_i \notin \bigcup \mathcal{C}_i.$$

Ukážeme, že táto možnosť vedie k sporu.

Definujme prvok $f \in X$ predpisom [6]

$$f(i) = x_i.$$

Potom $f \notin \bigcup \mathcal{C}$, čo znamená, že $\mathcal{C}$ nie je pokrytie. Skutočne, ak by f patrilo do nejakej množiny $p_i^{-1}[U]$ z $\mathcal{C}$, znamenalo by to, že $f(i) = x_i \in U$, čo je v spore s výberom x_i. $\square$



Obr. 4.4: Dve možné situácie, ktorými sa zaoberáme v dôkaze Tichonovovej vety: Buď máme na niektorej súradnici pokrytie celého X_i, alebo vieme nájsť funkciu, ktorá nepatrí do žiadnej množiny z pokrytia

{alex:FIGPALEX}

Poznámka 4.3.6. Poznamenajme, že Tichonovova veta sa nedá dokázať v ZF. (Ak ste na iných predmetoch videli nejaké dôkazy Tichonovovej vety, môžete sa skúsiť zamyslieť nad tým, kde konkrétne sa v dôkaze použila nejaká forma axiómy výberu.)

Platí dokonca, že v ZF z platnosti Tichonovovej vety (pre ľubovoľné kompaktné priestory) už vyplýva AC. (Ak by sme predpokladali platnosť Tichonovovej vety iba pre kompaktné Hausdorffovské priestory, dostaneme slabší výsledok než AC. Stále je to však výsledok, ktorý nie je dokázateľný v ZF. Viac sa dá nájsť v [Her2, Theorem 4.68, 4.70].)

[6] Využívame AC – pre každé $i \in I$ sme vybrali jedno x_i. Ekvivalentne by sme mohli funkciu f zadefinovať pomocou selektora na systéme neprázdnych množín $\{X_i \setminus \bigcup \mathcal{C}_i; i \in I\}$.

4.3.3 Hahnova-Banachova veta

Jedným z veľmi dôležitých tvrdení vo funkcionálnej analýze, je Hahn-Banachova veta. Pred jej vyslovením zadefinujme niektoré pojmy:

Definícia 4.3.7. Nech X je vektorový priestor a $f\colon X \to \mathbb{R}$ je funkcia.

(i) Funkcia f je *konvexná* ak pre ľubovoľné $x, y \in X$ a $\alpha \in (0,1)$ platí

$$f(\alpha x + (1-\alpha)y) \leq \alpha f(x) + (1-\alpha)f(y).$$

(ii) Funkcia f je *subaditívna,* ak pre ľubovoľné $x, y \in X$ platí

$$f(x+y) \leq f(x) + f(y).$$

(iii) Funkcia f je *pozitívne homogénna,* ak pre ľubovoľné $\alpha > 0$ a $x \in X$ platí $f(\alpha x) = \alpha f(x)$.

(iv) Funkcia f je *sublineárna,* ak je subaditívna a pozitívne homogénna

(v) Funkcia f je *polonorma,* ak je subaditívna a pre ľubovoľné $\alpha \in \mathbb{R}$, $x \in X$ platí $f(\alpha x) = |\alpha| f(x)$.

Môžeme si všimnúť, že definícia polonormy sa podobá na definíciu normy, iba sme z nej vynechali podmienku, že $f(x) = 0$ iba pre $x = 0$. Takisto je ľahko vidieť, že každá polonorma je sublineárna a každá sublineárna funkcia je konvexná (úloha 4.3.7).

Poznámka 4.3.8. Hahn-Banachovu vetu často nájdete sformulovanú pre polonormy alebo pre sublineárne funkcie. Tu uvedená formulácia s konvexnou funkciou je o čosi všeobecnejšia; v aplikáciach aj tak prakticky vždy budete pracovať s polonormou. Táto formulácia je možno o trochu ľahšie zapamätateľná, keďže s pojmom konvexnej funkcie sa stretnete už v prváckej analýze alebo možno aj na strednej škole; ak sa však bude trochu viac zaoberať funkcionálnou analýzou, tak určite dosť často narazíte na pojem polonormy.

Takisto sa obvykle neuvádza rozsah možných hodnôt takéhoto rozšírenia, hoci implicitne sa v dôkaze nachádza. Keďže občas môže užitočné poznať možný rozsah hodnôt rozšírení v Hahn-Banachovej vete, doplnil som ho sem. (Využijete ho napríklad v úlohe 6.3.5.)

Definícia 4.3.9. Nech $f, p\colon X \to \mathbb{R}$ a $M \subseteq X$. Hovoríme, že funkcia f je *majorizovaná funkciou p na množine M,* ak

$$(\forall x \in M) f(x) \leq p(x).$$

{HBT:VTHBT}

Veta 4.3.10 (Hahn-Banach)**.** *Nech X je vektorový priestor a $p\colon X \to \mathbb{R}$ je konvexná funkcia. Nech M je podpriestor X a nech $f\colon M \to \mathbb{R}$ je lineárny funkcionál, ktorý je na M majorizovaný funkciou p. Potom existuje lineárna funkcia $\widehat{f}$, ktorá je rozšírením f na celé X a je majorizovaná funkciou p na celom X.*

Navyše pre $x \in X$ existuje rozšírenie nadobúdajúce hodnotu $\widehat{f}(x) = c$ práve vtedy, keď

$$\sup_{m \in M, \lambda > 0} \frac{f(m) - p(m - \lambda x)}{\lambda} \leq c \leq \inf_{m \in M, \mu > 0} \frac{p(m + \mu x) - f(m)}{\mu}. \tag{4.1}$$ {HBT:EQRANGE}

V prípade, že p je kladne homogénna, možno vyjadrenie tohoto intervalu zjednodušiť na

$$\sup_{m \in M} [f(m) - p(m - x)] \leq c \leq \inf_{m \in M} [p(m + v) - f(m)].$$

Ak funkcie p a f navyše spĺňajú podmienku

$$(\forall x \in X)(\forall y \in M) p(x+y) = p(x) + f(y),$$

tak sa tento interval dá zjednodušiť na tvar

$$-p(-x) \leq c \leq p(x).$$

Plán dôkazu je takýto: Najprv ukážeme, že je možné dimenziu podpriestoru, na ktorom určite existuje hľadané rozšírenie, vždy zväčšiť o jedna. Pomocou tohoto faktu a ZL potom rozšírime daný funkcionál na celý priestor. Rozšírenie o jeden rozmer dokážme a sformulujme ako samostatnú lemu.

Lema 4.3.11. *Nech X je vektorový priestor a $p\colon X \to \mathbb{R}$ je konvexná funkcia. Nech M je podpriestor X a nech $f\colon M \to \mathbb{R}$ je lineárny funkcionál, ktorý je na M majorizovaný funkciou p. Nech ďalej $x \in X$.*

Potom existuje lineárne zobrazenie $\overline{f}\colon [M \cup \{x\}] \to \mathbb{R}$, ktoré rozširuje f je na podpriestore $[M \cup \{x\}]$ majorizované funkciou p.

Možné hodnoty, ktoré môže takéto rozšírenie nadobúdať v bode x, sú presne hodnoty z intervalu uvedeného v (4.1)*.*

Dôkaz. Máme danú lineárnu funkciu $f\colon M \to \mathbb{R}$, ktorú chceme rozšíriť na podpriestor

$$[M \cup \{x\}] = \{m + ax; m \in M, a \in \mathbb{R}\}.$$

Akonáhle si zvolíme hodnotu $\overline{f}(x) = c$, tak už je hodnota funkcie $\overline{f}$ jednoznačne určená pre všetky body z $[M \cup \{x\}]$, pre ľubovoľné $a \in \mathbb{R}$ totiž máme

$$f(m + ax) = f(m) + ac.$$

Zostáva nám zistiť, či existuje taká voľba c, aby bol funkcionál $\overline{f}$ majorizovaný funkciou p na celom podpriestore $[M \cup \{x\}]$.

Chceme teda, aby pre ľubovoľné $m \in M$, $a \in \mathbb{R}$ platilo

$$f(m + ax) = f(m) + ac \leq p(m + ax).$$

Ak a je kladné, tak uvedená nerovnosť je ekvivalentná s

$$c \leq \frac{p(m+ax) - f(m)}{a}.$$

Pre záporné a naopak dostávame

$$c \geq \frac{p(m+ax) - f(m)}{a}.$$

Zistili sme teda, že hodnota c musí nutne vyhovovať týmto nerovnostiam

{HBT:EQLMRANGE}
$$\sup_{m \in M, \lambda > 0} \frac{f(m) - p(m - \lambda x)}{\lambda} \leq c \leq \inf_{m \in M, \mu > 0} \frac{p(m + \mu x) - f(m)}{\mu}. \tag{4.2}$$

Pomerne ľahko vidno, že voľba c vyhovujúceho nerovnostiam (4.2) už zabezpečí, že $\overline{f}$ bude majorizované funkciou p. Ak $a > 0$, tak

$$f(m + ax) = f(m) + ac \leq f(m) + a\frac{p(m+ax) - f(m)}{a} = p(m + ax).$$

Podobne pre $a < 0$ máme

$$f(m+ax) = f(m) + ac \leq f(m) + a\frac{p(m+ax) - f(m)}{a} = p(m+ax).$$

Zostáva nám teda len overiť, či je takáto voľba možná (či existuje aspoň jedno c v uvedenom intervale). Pýtame sa teda vlastne, či pre ľubovoľné $m, m' \in M$, $\lambda, \mu > 0$ platí

$$\frac{f(m) - p(m-\lambda x)}{\lambda} \leq \frac{p(m'+\mu x) - f(m')}{\mu}.$$

Táto nerovnosť je ekvivalentná s

$$f\left(\frac{1}{\mu}m' + \frac{1}{\lambda}m\right) = \frac{1}{\mu}f(m') + \frac{1}{\lambda}f(m) \leq \frac{p(m'+\mu x)}{\mu} + \frac{p(m-\lambda x)}{\lambda}.$$

Po vydelení tejto rovnosti kladným výrazom $\frac{1}{\mu} + \frac{1}{\lambda} = \frac{\mu+\lambda}{\mu\lambda}$ máme ekvivalentnú nerovnosť

$$\frac{f(\frac{1}{\mu}m' + \frac{1}{\lambda}m)}{\frac{1}{\mu} + \frac{1}{\lambda}} = \frac{f(\frac{1}{\mu}(m'+\mu x)) + \frac{1}{\lambda}(m - \lambda x)}{\frac{1}{\mu} + \frac{1}{\lambda}} \leq \frac{\frac{p(m'+\mu x)}{\mu} + \frac{p(m-\lambda x)}{\lambda}}{\frac{1}{\mu} + \frac{1}{\lambda}}$$

Ak označíme $\alpha = \frac{\frac{1}{\mu}}{\frac{1}{\mu}+\frac{1}{\lambda}} = \frac{\lambda}{\mu+\lambda}$, tak predošlá nerovnosť je ekvivalentná s nerovnosťou

$$f(\alpha(m'+\mu x) + (1-\alpha)(m-\lambda x)) \leq \alpha p(m'+\mu x) + (1-\alpha)p(m-\lambda x). \tag{4.3}$$ {EQTREBA}

Pretože

$$\alpha(m'+\mu x) + (1-\alpha)(m-\lambda x) = \frac{\lambda(m'+\mu x) + \mu(m-\lambda x)}{\mu+\lambda} = \frac{\lambda m' + \mu m}{\mu+\lambda}$$

je prvok z M, máme nerovnosť

$$f(\alpha(m'+\mu x) + (1-\alpha)(m-\lambda x)) \leq p(\alpha(m'+\mu x) + (1-\alpha)(m-\lambda x))$$

na základe predpokladu, že na podpriestore M je funkcia f majorizovaná funkciou p. Z konvexnosti funkcie p máme

$$p(\alpha(m'+\mu x) + (1-\alpha)(m-\lambda x)) \leq \alpha p(m'+\mu x) + (1-\alpha)p(m-\lambda x).$$

Z predošlých dvoch nerovností už vyplýva nerovnosť (4.3), ktorú sme chceli dokázať. □

Dôkaz Hahn-Banachovej vety. Budeme pracovať s množinou všetkých lineárnych rozšírení funkcie f, ktoré sú majorizované funkciou p. Čiastočné usporiadanie je

$$g \preceq h \Leftrightarrow h \text{ je rozšírením } g.$$

Ľahko sa overí, že ak systém funkcií $\{f_i; i \in I\}$ je reťazec v tejto čiastočne usporiadanej množine, tak

$$\widehat{f} := \bigcup_{i\in I} f_i$$

je jeho horným ohraničením a patrí do našej čiastočne usporiadanej množiny. Teda množina s ktorou pracujeme má maximálny prvok (podľa ZL).

Zistili sme teda, že existuje nejaké maximálne rozšírenie $\widehat{f}$ zobrazenia f. Predchádzajúca lema zaručuje, že maximálne rozšírenie zobrazenia f už musí byť definované na celom X, inak by sa dalo rozšíriť na podpriestor dimenzie väčšej o 1.

Ak navyše chceme ukázať aj tvrdenie o možných hodnotách rozšírení, tak začneme s funkciou definovanou na $[M \cup \{x\}]$ s predpísanou hodnotou v bode x, ktorej existenciu nám zaručí predchádzajúca lema. □

Z Hahn-Banachovej vety pomerne ľahko dostaneme tento často používaný dôsledok:

{HBT:DOSHBTNO

Dôsledok 4.3.12. *Nech X je lineárny normovaný priestor, M je podpriestor priestoru X a nech $f\colon M \to \mathbb{R}$ je ohraničený lineárny funkcionál. Potom existuje lineárny funkcionál $\widehat{f}\colon X \to \mathbb{R}$ rozširujúci f, pre ktorý platí $\|\widehat{f}\| = \|f\|$.*

Dôkaz. Ak označíme $C = \|f\|$, tak pre $x \in M$ máme $f(x) \leq C\|x\|$. Stačí teraz použiť Hahn-Banachovu vetu 4.3.10 pre $p(x) = C\|x\|$. □

4.3.4 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 4.3.13. Množina $\mathcal{S} \subseteq \mathcal{P}(X)$ sa nazýva *σ-algebra* na množine X, ak platí
(i) $X \in \mathcal{S}$;
(ii) $A \in \mathcal{S} \Rightarrow X \smallsetminus A \in \mathcal{S}$; (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 $m\colon \mathcal{S} \to \langle 0, \infty \rangle$ je *miera na $\mathcal{S}$* ak platí $m(\emptyset) = 0$ a

$$m\left(\bigcup_{n\in\mathbb{N}} A_n\right) = \sum_{n\in\mathbb{N}} m(A_n)$$

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 4.3.14. 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.

VREXISTNEMER}

Tvrdenie 4.3.15. *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 $\mathbb{Q}$. (T.j. rozklad určený reláciu ekvivalencie na $\mathbb{R}$ definovanou ako $x\sim y \Leftrightarrow x-y\in\mathbb{Q}$.) 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 $\langle 0,1\rangle \subseteq \bigcup\limits_{q\in\mathbb{Q}\cap\langle -1,1\rangle} q+V$.

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 $\bigcup\limits_{q\in\mathbb{Q}\cap\langle -1,1\rangle} q+V\subseteq\langle -1,2\rangle$.

Čo vieme povedať o množine $B:=\bigcup\limits_{q\in\mathbb{Q}\cap\langle -1,1\rangle} q+V$? 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

$$1=m(\langle 0,1\rangle)\le m(B)\le m(\langle -1,2\rangle)=3,$$

čím dostávame spor. □

Dôsledok 4.3.16. *Existuje lebesguovsky nemerateľná podmnožina* $\mathbb{R}$.

{aplik:POZNNEMERZF}

Poznámka 4.3.17. Existencia lebesguovsky nemerateľnej podmnožiny $\mathbb{R}$ sa nedá dokázať v ZF.

Banach-Tarskiho paradox

Ešte spomenieme bez dôkazu jeden veľmi známy a veľmi kontraintuitívny dôsledok axiómy výberu.

Veta 4.3.18 (Banach-Tarski). *Pre ľubovoľné dve ohraničené množiny $A, B \subseteq \mathbb{R}^n$, $n \geq 3$, ktoré majú neprázdne vnútro, existujú rozklady $A = A_1 \cup \dots \cup A_k$ a $B = B_1 \cup \dots \cup B_k$ 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 [Wap] 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. Ďalšia známe kniha venovaná Banach-Tarskiho paradoxu je [Wag].

Problémy

Hamelova báza

Z prvého ročníka poznáte bázy v konečnorozmerných vektorových priestoroch. Dá sa ukázať, že podobne sa dá definovať báza pre ľubovoľný (aj nekonečnorozmerný) priestor a viaceré základné vlastnosti bázy platia aj v nekonečnorozmerných priestoroch.

Definícia 4.3.19. 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

$$c_1\vec{\alpha}_1 + \dots + c_n\vec{\alpha}_n = \vec{0} \qquad \Rightarrow \qquad c_1 = \dots = c_n = 0.$$

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

$$\vec{\alpha} = c_1\vec{\alpha}_1 + \dots + c_n\vec{\alpha}_n.$$

Označujeme $[A] = V$.

Podmnožina A sa nazýva *Hamelova báza* (alebo stručne báza) priestoru V, ak je lineárne nezávislá a $[A] = V$.

{aplikprob:PROBHAMEL}

Problém 4.3.1.

a) Porovnajte definíciu lineárnej množiny, generujúcej množiny a bázy s pojmami, ktoré ste sa učili pre konečnorozmerné vektorové priestory.
b) Nájdite Hamelovu bázu v priestore c_{00} pozostávajúcom z postupností reálnych čísel, ktoré majú iba konečne veľa nenulových hodnôt.
c) Ukážte, že ak V je vektorový priestor nad poľom F a A je lineárne nezávislá podmnožina V, tak existuje Hamelova báza B taká, že $A \subseteq B$. (Návod: Pomocou Zornovej lemy ukážte, že existuje maximálna lineárne nezávislá množina s vlastnosťou $B \supseteq A$. O nej ukážte, že je to báza.)

d) Ukážte, že ľubovoľné dve bázy majú rovnakú kardinalitu. (Návod: Najprv sa pozrite na prípad keď jedna z báz je konečná. Ak máme dve nekonečné bázy B_1 a B_2, tak pre každé $\vec{\alpha} \in B_1$ existuje jednoznačne určená konečná množina $B_2(\vec{\alpha})$ vektorov z B_2, ktorých lineárnou kombináciou je $\vec{\alpha}$. Pokúste sa ukázať $B_2 = \bigcup\limits_{\vec{\alpha}\in B_1} B_2(\vec{\alpha})$.) Z tohoto výsledku vyplýva, že aj pre nekonečnorozmerné vektorové priestory má zmysel hovoriť o dimenzii, bude to však teraz už kardinálne číslo. Ak budeme chcieť zdôrazniť, že máme na mysli kardinalitu Hamelovej bázy, použijeme názov *Hamelova dimenzia.* (V dôkaze môžete použiť to, že pre ľubovľný nekonečný kardinál a platí $a \cdot \aleph_0 = a$; hoci tento fakt sme ešte nedokázali; pozri poznámku 2.7.13.)

e) Nech B je Hamelova báza vektorového priestoru V a $f\colon B \to W$ je zobrazenie, pričom W je vektorový priestor. Potom existuje práve jedno lineárne zobrazenie $g\colon V \to W$ také, že $g|_B = f$.

f) Vektorové priestory V a W sú izomorfné práve vtedy, keď majú rovnakú Hamelovu dimenziu.

Poznámka 4.3.20. Existenciu Hamelovej bázy sa nám nepodarí dokázať bez použitia axiómy výberu. V ZF sa totiž dá ukázať, že z existencie bázy pre *každý vektorový priestor* už vyplýva axióma výberu, pozri [Bla], [Hal1, Theorem 5.4], [Her2, Theorem 4.44], [HR, Form 1A].

Ako sme však videli napríklad pre konečnorozmerné priestory ale aj pre priestor c_{00} v probléme 4.3.1, v niektorých konkrétnych príkladoch vieme bázu explicitne popísať a nepotrebujeme používať AC.

Napríklad otázka, či AC vyplýva z existencie bázy pre každý vektorový priestor nad poľom $\mathbb{R}$, je stále otvorená, pozri [P, 7.5.18, p.586] alebo [Her2, p.68].

K tejto téme sa neskôr ešte vrátime – Hamelovými bázami v Banachových priestoroch sa budeme zaoberať v časti 6.1.1. Ale už aj na tomto mieste spomenieme niečo viac o tom, ako je to s bázami v lineárnom normovanom, či Banachovom priestore.

{aplikprob:PROBHAMELLNP}

Problém 4.3.2.

a) Nech X je nekonečnorozmerný lineárny normovaný priestor. Ukážte, že existuje lineárne zobrazenie $f\colon X \to \mathbb{R}$, ktoré nie je spojité.[7]

b) Ak X je vektorový priestor a B je jeho báza, tak rovnosť

$$x = \sum_{b\in B} f_b(x),$$

kde pre každé x je iba konečne veľa z hodnôt $f_b(x)$ nenulových, jednoznačne definuje pre každé $b \in B$ zobrazenie $f_b\colon X \to \mathbb{R}$. (Prečo?) Ukážte, že pre každé $b \in B$ je zobrazenie f_b lineárne.

c) Nech X je Banachov priestor. Ukážte, že iba konečne veľa z lineárnych funkcionálov $f_b\colon X \to \mathbb{R}$ môže byť spojitých. (Návod 1: Skúste zvoliť bázu tak, že jej prvky majú veľkosť jedna a pozrieť sa na prvok $x := \sum\limits_{i=1}^{\infty} \frac{1}{2^i} b_i$. Návod 2: Skúste najprv pomocou Banach-Steinhausovej vety ukázať $\sup\{\|f_b\|; b \in C\} < \infty$, kde $C = \{b \in B; f_b \text{ je spojité zobrazenie}\}$.)

d) Ukážte, že ak X je nekonečnorozmerný priestor, tak ľubovoľný konečný počet funkcionálov f_b môže byť spojitý.

[7] Azda sa oplatí pripomenúť, že ak X je konečnorozmerný lineárny normovaný priestor, tak každý lineárny funkcionál na X je spojitý.

e) Ukážte, že ak X je lineárny normovaný priestor, tak môžu byť (pre vhodnú bázu B) spojité všetky funkcionály f_b. (Samozrejme, z predchádzajúcich častí vyplýva, že takýto priestor nemôže byť úplný.)

Poznámka 4.3.21. TODO Schauderova báza

Cauchyho funkcionálna rovnica

Cauchyho funkcionálnou rovnicou nazývame rovnicu

{aplik:EQCAUCHY}
$$(\forall x, y \in \mathbb{R}) f(x+y) = f(x) + f(y), \tag{4.4}$$

kde f je funkcia z $\mathbb{R}$ do $\mathbb{R}$.

Funkcie $f\colon \mathbb{R} \to \mathbb{R}$ vyhovujúce tejto rovnici sa často nazývajú aj *aditívne funkcie.*

Môžeme si tiež všimnúť, že riešenia tejto funkcionálnej rovnice sú vlastne presne grupové homomorfizmy $(\mathbb{R}, +) \to (\mathbb{R}, +)$.

Ukážeme si, že ak pridáme niektoré dodatočné podmienky (napríklad spojitosť), tak sú všetky riešenia rovnice (4.4) veľmi jednoduché; ale s pomocou axiómy výberu sa dá ukázať aj existencia nespojitých riešení.

{aplikprob:PROBCAUCHY}

Problém 4.3.3.

a) Ak f je riešenie (4.4), tak pre ľubovoľné $r \in \mathbb{Q}$, $x \in \mathbb{R}$ platí $f(rx) = rf(x)$.
b) Ak f je spojité riešenie (4.4), tak $f(x) = ax$ pre nejaké $a \in \mathbb{R}$.
c) Ukážte, že existujú aj nespojité riešenia rovnice (4.4). (Návod: Skúste sa pozrieť na $\mathbb{R}$ ako vektorový priestor nad $\mathbb{Q}$ a využiť to, čo vieme o Hamelovej báze a lineárnych zobrazeniach z problému 4.3.1.)

Našli sme všetky spojité riešenia Cauchyho rovnice, dokázali sme však aj existenciu nespojitých riešení. Ukážeme si, že nespojité riešenia majú neobvyklé vlastnosti. Takáto funkcia napríklad nie je spojitá v žiadnom bode a jej graf je hustá podmnožina roviny.

ikprob:PROBCAUCHYDIVOKE}

Problém 4.3.4.

a) Ak nejaká funkcia $f\colon \mathbb{R} \to \mathbb{R}$ spĺňa (4.4) a je spojitá v jednom bode $x_0 \in \mathbb{R}$, tak je spojitá na celom $\mathbb{R}$.
b) Ak nejaká funkcia $f\colon \mathbb{R} \to \mathbb{R}$ spĺňa (4.4) a je ohraničená na nejakom netriviálnom intervale I, tak f je spojitá.
c) Ak nejaká funkcia $f\colon \mathbb{R} \to \mathbb{R}$ spĺňa (4.4) a je navyše monotónna na nejakom netriviálnom intervale I, tak f je spojitá.
d) Ak $f\colon \mathbb{R} \to \mathbb{R}$ je nespojité riešenie (4.4), tak graf tejto funkcie
$$G(f) = \{(x, f(x)); x \in \mathbb{R}\}$$
je hustá podmnožina $\mathbb{R}^2$.

Ďalším zaujímavým faktom je to, že dokonca každé merateľné riešenie je spojité. (Inak povedané: Nespojité riešenia Cauchyho funkcionálnej rovnice sú nemerateľné.)

Pri dôkaze sa môže hodiť nasledujúci výsledok:

Veta 4.3.22 (Steinhaus)**.** *Nech $A \subseteq \mathbb{R}$ je Lebesguovsky merateľná množina s kladnou mierou. Potom množina*
$$A - A = \{x - y; x, y \in A\}$$
je okolie nuly, t.j. existuje $\varepsilon > 0$ také, že $(-\varepsilon, \varepsilon) \subseteq A - A$.

Analogický výsledok platí aj v $\mathbb{R}^n$. Dôkaz tejto vety sa dá nájsť napríklad v [AE, Theorem 5.18], [Ku, Section 3.7], [O, Theorem 4.8].[8]

BCAUCHYNEMER}

Problém 4.3.5. Dokážte, že ak funkcia spĺňa (4.4) a je merateľná, tak je spojitá.
(Návod 1: Stačí nám ukázať, že pre každé okolie nuly je jeho vzor opäť okolím nuly. Ak U je okolie nuly, tak existuje otvorená množina V taká, že $0 \in V \subseteq U$ a aj $V - V \subseteq U$. Ak $\mathbb{Q} = \{q_n; n \in \mathbb{N}\}$, tak dostaneme $\mathbb{R} = \bigcup_{n\in\mathbb{N}} f^{-1}[q_n + V]$. Pokúste sa nejako aplikovať Steinhausovu vetu.
Návod 2: B.u.n.v predpokladajme, že $f(a) = 1$, $f(b) = 0$ pre nejaké reálne čísla $a, b \neq 0$. Položme $A_n = f^{-1}\langle n, n+1)$ a zvoľme $q_n \in \mathbb{Q}$ tak, že $|na - q_n b| < \frac{1}{2}$. Ďalej pre $n \in \mathbb{Z}$ položme $B_0 := A_0 \cap \langle -\frac{1}{2}, \frac{3}{2}\rangle$ a $B_n := B_0 + na - q_n b$. Pre takto zvolené množiny by ste mali byť schopní ukázať $A_n \cap \langle 0, 1) \subseteq B_n \subseteq \langle -1, 2\rangle$, z čoho vyplýva

$$\langle 0, 1) \subseteq \bigcup_{n\in\mathbb{Z}} B_n \subseteq \langle -1, 2\rangle.$$

Z tohoto by sa už mal dať odvodiť spor.)

Poznámka 4.3.23. Videli sme, že s pomocou axiómy výberu vieme ukázať existenciu nemerateľných riešení (4.4). Existencia nemerateľnej funkcie samozrejme už implikuje aj existenciu nemerateľnej množiny – tú sme už predtým dokázali v tvrdení 4.3.15.

Z toho hneď vidíme aj to, že existencia nespojitých riešení (4.4) sa nedá dokázať v ZF, pretože v ZF nie je možné dokázať existenciu nemerateľných množín (poznámka 4.3.17).

Linearizácia čiastočne usporiadanej množiny

Všetky pojmy potrebné v tejto úlohe by ste mali poznať z predmetov **Diskrétna matematika 1,2** (prvý ročník).

Problém 4.3.6. {aplikprob:PROBLINEARIZ}

a) Ukážte, že 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

$$a \leq b \qquad \Rightarrow \qquad a \preceq b.$$

(Preferované riešenie je pomocou Zornovej lemy.) Tento výsledok sa zvykne volať aj Szpilrajnova veta.

b) Ukážte, že pre dva prvky a, b čiastočne usporiadanej množiny $(A, \leq)$ platí $a \leq b$ práve vtedy, keď $a \preceq b$ platí pre každú jej linearizáciu $(A, \preceq)$.

c) Nájdite príklad konečnej čiastočne usporiadanej množiny, ktorá nie je lineárne usporiadaná. Ako vyzerá linearizácia množiny, ktorú ste si vybrali?

d) Ukážte na príklade, že linearizácia čiastočne usporiadanej množiny nemusí byť jednoznačne určená.

Existencia voľných ultrafiltrov

S pojmom ultrafiltra a centrovaného systému sa môžete stretnúť napríklad na predmetoch **Všeobecná topológia** a **Teória množín a matematická logika**. Potrebné definície sú uvedené aj v časti 6.3.

Problém 4.3.7. {aplikprob:PROBULTRA}

[8] Pozri aj `https://en.wikipedia.org/wiki/Steinhaus_theorem` a `http://math.stackexchange.com/questions/38902/the-set-of-differences-for-a-set-of-positive-lebesgue-measure`.

a) Nech $\mathcal{F}$ je filter na množine M. Ukážte, že $\mathcal{F}$ je ultrafilter práve vtedy, keď $\mathcal{F}$ je maximálny (vzhľadom na inklúziu) filter na M (t.j. je to maximálny prvok v množine filtrov na M, ak za čiastočné usporiadanie berieme $\subseteq$).
b) Ukážte, že pre každý centrovaný systém $\mathcal{S}$ existuje ultrafilter $\mathcal{F}$, ktorý ho obsahuje. (Návod: Zornova lema.)
c) Ukážte, že každý voľný ultrafilter $\mathcal{F}$ na množine $\mathbb{N}$ má kardinalitu $\mathfrak{c}$. (Môžete využívať, že pre nekonečný kardinál a platí $a + a = a$; hoci tento fakt sme ešte nedokázali; pozri poznámku 2.7.13.)

Existencia maximálnych ideálov v okruhoch s jednotkou

Všetky pojmy, ktoré sú potrebné v tejto úlohe by ste mali poznať z predmetov **Algebra 1,2** (druhý ročník).

{aplikprob:PROBMAXID}

Problém 4.3.8.
a) Pripomeňte definíciu ideálu a maximálneho ideálu.
b) Ukážte, že ak R je okruh s jednotkou a I je vlastný ideál v R, tak existuje maximálny ideál J v okruhu R taký, že $I \subseteq J$.
c) Ako dôsledok dostaneme, že každý okruh s jednotkou má maximálny ideál. (Prečo?) Kedy je v okruhu s jednotkou jediný maximálny ideál?
d) Nájdite príklad okruhu, ktorý nemá žiadne maximálne ideály. (Riešení je určite veľa, ale jeden možných hintov by bol: Keď si vezmeme ľubovoľnú grupu $(G, +)$, tak dodefinovaním $a \cdot b = 0$ dostaneme okruh, ktorý nemá jednotku. Treba skúsiť sformulovať, aké podmienky by mala spĺňať naša grupa, aby sme dostali kontrapríklad a potom sa pokúsiť takú grupu nájsť.) Keďže táto časť úlohy nie je (podľa môjho názoru) jednoduchá, pokojne môžete slovo „nájdite“ chápať ako „nájdite v literatúre alebo na internete“. Keď už budete mať nejaký vhodný príklad – či už ste ho vymysleli sami, niekto vám ho poradil, alebo ste ho niekde našli – zdôvodnenie, že ide skutočne o kontrapríklad, sa pokúste vymyslieť samostatne.

Maximálny antireťazec

{aplikprob:PROBANTICHAIN}

Problém 4.3.9. Pripomeňme, že podmnožina A čiastočne usporiadanej množiny $(P, \leq)$ sa nazýva *antireťazec,* ak žiadne dva rôzne prvky z A nie sú porovnateľné.
a) Ukážte, že v každej čiastočne usporiadanej množine existuje maximálny antireťazec. (Pod „maximálny“ tu rozumieme maximálny *vzhľadom na inklúziu.*)
b) Ukážte, že v každej nekonečnej čiastočne usporiadanej množine existuje nekonečný antireťazec alebo nekonečný reťazec. (Hint: Možno pomôže uvedomiť si, že ak A je maximálny antireťazec v $(P, \leq)$, tak pre každé $p \in P$ existuje $a \in A$ také, že a a p sú porovnateľné; t.j. každý prvok z P leží nad alebo pod niektorým prvkom z antireťazca A.)

Výsledku, že každá čiastočne usporiadaná množina sa niekedy hovorí aj *Kurepov princíp.* Azda stojí za zmienku, že z Kurepovho princípu už vyplýva (v ZF) axióma výberu, pozri napríklad [Hal1, Theorem 5.4].

Ortonormálna báza

V tomto probléme sa vyskytnú sumy, kde budeme sčitovať prvky systému indexované množinou, ktorá nemusí byť spočítateľná. Základné veci o takýchto sumách si môžete zopakovať prečitaním dodatku B. Všetky sumy vyskytujúce sa v tomto probléme budeme chápať v zmysle definície B.1.1.

PROBORTOBAZA}

Problém 4.3.10.

a) Nech X je priestor so skalárnym súčinom. Ukážte, že v ňom existuje ortonormálny systém $\{x_i; i \in I\}$, ktorý je maximálny vzhľadom na inklúziu. (*Ortornomálny systém* znamená, že $\|x_i\|^2 = 1$ pre každé i a $\langle x_i, x_j\rangle = 0$ pre $i \neq j$.)

b) Ukážte, že ak $\{x_i; i \in I\}$ je maximálny ortonormálny systém, tak jeho lineárny obal $[x_i; i \in I]$ je hustý v X.

c) Ukážte, že ak x_i je ortornormálny systém a $x = \sum\limits_{i\in I} c_i x_i$, $y = \sum\limits_{i\in I} d_i x_i$, tak existuje suma $\sum\limits_{i\in I} c_i d_i$ a platí

$$\langle x, y\rangle = \sum_{i\in I} c_i d_i.$$

Špeciálne dostaneme $\|x\|^2 = \sum\limits_{i\in I} c_i^2 {x_i}^2$.

d) Predpokladajme teraz navyše, že X je Hilbertov priestor. Ak existuje suma $\sum\limits_{i\in I} c_i^2$, tak konverguje aj $\sum\limits_{i\in I} c_i x_i$.

e) Nech M je ľubovoľná množina. Definujme

$$\ell_2(M) = \{x\colon M \to \mathbb{R}; \sum_{i\in M} x_i^2 < \infty\}.$$

Dokážte, že $\ell_2(M)$ je vektorový priestor. Ak ďalej definujeme

$$\langle x, y\rangle = \sum_{i\in M} x_i y_i,$$

tak tento predpis definuje skalárny súčin na $\ell_2(M)$ a takýmto spôsobom dostaneme Hilbertov priestor. (Hint: Pri dôkaze, že priestor $\ell_2(M)$ je uzavretý na sčitovanie, môže pomôcť dokázať najprv Cauchy-Schwarzovu nerovnosť $\sum\limits_{i\in M} x_i y_i \leq \left(\sum\limits_{i\in M} x_i\right)\left(\sum\limits_{i\in M} y_i\right)$. Pri dôkaze úplnosti sa pokúste zopakovať obvyklý dôkaz pre ℓ_2.) Môžeme si všimnúť, že pre $M = \mathbb{N}$ dostávame obvyklý priestor ℓ_2.

f) Ukážte, že každý Hilbertov priestor X je izomorfný[9] s priestorom $\ell_2(M)$ pre nejakú množinu M.

Všimnime si, že sme vlastne ukázali takýto výsledok: Nech $\{x_i, i \in M\}$ je maximálny ortonormálny systém v Hilbertovom priestore X. Každý prvok $x \in X$ sa dá jednoznačne vyjadriť v tvare $\sum\limits_{i\in M} c_i x_i$. (Konkrétne máme $c_i = \langle x, x_i\rangle$.)

Poznamenajme ešte, že ak je Hilbertov priestor X separabilný, tak je izomorfný s priestorom ℓ_2.

Môžeme si uvedomiť, že sme vlastne v istom zmysle klasifikovali všetky Hilbertove priestory: Vieme, že ich môžeme dostať ako $\ell_2(M)$ pre vhodnú množinu M. (Kardinalita tejto množiny je rovnaká ako kardinalita maximálneho ortogonálneho systému. Je daný priestorom jednoznačne určená a hovorí sa jej *Hilbertova dimenzia.*)

Do istej miery je to analógia toho, ako ste v prvom ročníku klasifikovali všetky konečnorozmerné vektorové priestory – až na izomorfizmus sú to priestory tvaru F^n. (Resp. teraz, keď už vieme aj o Hamelovej báze, máme podobnú klasifikáciu už pre všetky vektorové priestory.)

[9]Pod izomorfizmom Hilbertových priestorov rozumieme lineárny izomorfizmus, ktorý zachováva aj skalárny súčin.

A veľmi podobné tvrdenie ste videli aj pre priestory so skalárnym súčinom: Ak máme vektorový priestor nad poľom $\mathbb{R}$ taký, že $\dim(V) = n$ a na ňom nejaký skalárny súčin, tak je izomorfný s $\mathbb{R}^n$ so štandardným skalárnym súčinom (ako euklidovský vektorový priestor). Pozri napríklad [Ko, Veta 7.9.2], [KG, Veta 10.12].

Teichmüller–Tukeyho lemma

Definícia 4.3.24. Nech $\mathcal{A} \subseteq \mathcal{P}(X)$. Systém množín $\mathcal{A}$ má *konečný charakter,* ak pre ľubovoľné $A \subseteq X$ platí $A \in \mathcal{A}$ práve vtedy, keď všetky konečné podmnožiny množiny A patria do $\mathcal{A}$.

Podobne by sme mohli hovoriť o *vlastnosti konečného charakteru.*

{aplikprob:VTTUKEY} Pre takéto systémy platí nasledovný výsledok:

Veta 4.3.25 (Teichmüller–Tukeyho lema)**.** *Ak $\mathcal{A} \subseteq \mathcal{P}(X)$ je systém konečného charakteru, tak $\mathcal{A}$ má maximálny prvok (vzhľadom na inklúziu).*

{aplikprob:PROBTUKEY}

Problém 4.3.11. a) Nájdite nejaké systémy (vlastnosti) konečného charakteru, s ktorými ste sa niekde stretli. (Napríklad v kontexte vektorových priestorov, čiastočne usporiadaných množín, ...)
b) Dokážte v ZF (t.j. bez použitia axiómy výberu) ekvivalenciu medzi Zornovou lemou a Teichmüller–Tukeyho lemou.
c) Vyberte si niektoré výsledky, ktoré sme dokázali pomocou Zornovej lemy, a dokážte ich pomocou Teichmüller–Tukeyho lemy.[10]

Cvičenia

Úloha 4.3.1. a) Nájdite všetky spojité riešenia funkcionálnej rovnice $f(x+y) = f(x) \cdot f(y)$; $f\colon \mathbb{R} \to \mathbb{R}$. 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 $f(xy) = f(x) \cdot f(y)$; $f\colon \langle 0,\infty) \to \mathbb{R}$. Existujú aj nespojité riešenia?

Úloha 4.3.2. Použitím Hamelovej bázy ukážte, že grupy $(\mathbb{R},+)$ a $(\mathbb{C},+)$ sú izomorfné.

{aplikcvic:ULOPOROV}

Úloha 4.3.3. Ukážte pomocou Zornovej lemy, že pre ľubovoľné dve množiny A, B existuje injekcia z A do B alebo injekcia z B do A. (Tento výsledok pomocou (WO) a vlastností dobre usporiadaných množín ukážeme v dôsledku 5.1.7.)

{aplikcvic:ULOKOMPBAZA}

Úloha 4.3.4. Nech X je topologický priestor a $\mathcal{B}$ je báza jeho topológie. Ukážte, že X je kompaktný práve vtedy, keď pre každé pokrytie priestoru X množinami z $\mathcal{B}$ existuje konečné podpokrytie.

Úloha 4.3.5. Ukážte pomocou Alexandrovej vety o subbáze, že jednotkový interval $\langle 0,1\rangle$ s obvyklou topológiou je kompaktný.

Úloha 4.3.6. Aká je kardinalita Hamelovej bázy $\mathbb{R}$ ako vektorového priestoru nad $\mathbb{Q}$? (Môžete, využívať, že pre nekonečné kardinály a, b platí $a + b = ab = \max\{a,b\}$; hoci tento fakt sme ešte nedokázali; pozri poznámku 2.7.13.)

{aplikcvic:ULOSUBLIN}

Úloha 4.3.7. Nech X je vektorový priestor a $f\colon X \to \mathbb{R}$ je funkcia. Ukážte, že:
a) Ak f je polonorma, tak f je sublineárna funkcia.
b) Ak f je sublineárna funkcia, tak f je konvexná.
c) Ak f je pozitívne homogénna a konvexná, tak f je sublineárna.

[10] Ak tento problém odovzdávate ako súčasť hodnotenia predmetu, tak si vyberte dva také výsledky.

Kapitola 5

Ordinálne čísla

5.1 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 5.1.1. *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 5.1.2. *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 5.1.1, raz pre zobrazenie f a raz pre f^{-1}.) □

Dôsledok 5.1.3. *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 5.1.2 znamená, že $g^{-1} \circ f = id_A$, a teda $g = f$. □

{dum2:DOSNEEXIZOMPOCUSEK

Dôsledok 5.1.4. *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 5.1.1 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 5.1.2 to znamená, že $f = id_A$. □

Nasledujúci výsledok bude pre nás pomerne dôležitý:

{dum2:VTZAKL}

Veta 5.1.5 (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. □

S využitím vety 5.1.5 už vieme ukázať (s použitím AC, presnejšie WO), že ľubovoľné dve kardinálne čísla sú porovnateľné.

{dum2:DOSPOROVKARD}

Dôsledok 5.1.6. *Pre ľubovoľné dve kardinálne čísla a, b platí $a \leq b$ alebo $b \leq a$.*

Dôsledok 5.1.6 môžeme ekvivalentne preformulovať aj takýmto spôsobom:

{dum2:DOSPOROVINJ}

Dôsledok 5.1.7 (AC)**.** *Pre ľubovoľné množiny X, Y existuje injekcia z X do Y alebo existuje injekcia z Y do X.*

Na základe úlohy 2.5.1 by sme mohli druhú časť v predchádzajúcej formulácii nahradiť existenciou surjekcie z X do Y. T.j. pre dve množiny X, Y v smere $X \to Y$ vždy existuje injekcia alebo surjekcia $X \to Y$.

Dôkaz. Nech X, Y sú ľubovoľné dobre usporiadané množiny. Podľa vety 4.2.5 existuje na množine X dobré usporiadanie $\leq_X$ a na množine Y dobré usporiadanie $\leq_Y$. Z vety 5.1.5 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. □

Dôsledok 5.1.7 sa dá pomerne ľahko dokázať aj pomocou Zornovej lemy – úloha 4.3.3.

5.2 „Naivný“ prístup k ordinálom

{ordnaiv:SECTDEFORDNAIV}

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 nimi.

V časti 5.3 uvidíme, ako sa ordinálne čísla dajú zaviesť i v rámci ZFC. Ak však netrváme na axiomatickom prístupe a uspokojíme sa s naivnou teóriou množín, tak by nám mala stačiť aj menej formálna definícia ordinálov. Napriek tomu nezaškodí vedieť aspoň niečo aj o obvyklej konštrukcii ordinálov používanej v axiomatickej teórii množín – najmä preto, aby sme rozumeli dôkazom transfintnou indukciou, ak narazíme na nejaký text využívajúci túto konštrukciu.

Ešte poznamenajme, že čitateľ, ktorý uprednostní axiomatický prístup, môže namiesto tejto podkapitoly čítať nasledujúcu. Resp. ak sa rozhodne prečítať si obe, tak ich môže čítať v ľubovoľnom poradí.

5.2.1 Kardinály ako iniciálne ordinály

:POZNKARDMIN}

Poznámka 5.2.1. Priamo z toho, ako sme definovali kardinály, dostaneme, že každá množina kardinálov má najmenší prvok.

Kardinály sú podtriedou ordinálov. Teda ľubovoľná množina kardinálov je súčasne ordinálov a teda je dobre usporiadaná. Nerovnosť medzi kardinálnymi číslami je rovnaká bez ohľadu na to, či ich porovnávame v zmysle nerovnosti kardinálnych čísel – existencia injekcie – alebo v zmysle nerovnosti ordinálnych čísel – existencia vnorenia na počiatočný úsek.

{defordnaiv:DEFKARDNASL}

Definícia 5.2.2. Pre ľubovoľné kardinálne číslo $\varkappa$ nazývame najmenšie kardinálne číslo, ktoré je ostro väčšie ako $\varkappa$, *kardinálnym nasledovníkom* čísla $\varkappa$ a označujeme ho $\varkappa^+$.

Špeciálne kardinálny nasledovník čísla $\aleph_0$ označujeme $\aleph_1$.

5.3 Von Neumanova konštrukcia ordinálnych čísel*

{defordnew:DEFVONNEU}

Poznámka 5.3.1. Ordinálne čísla chceme zaviesť už v tejto kapitole 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, 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.)

5.3.1 Tranzitívne množiny

Najprv zavedieme pojem tranzitívnej množiny a ukážeme si niektoré základné vlastnosti tranzitívnych množín.

Definícia 5.3.2. Množina X je *tranzitívna,* ak pre každé $x \in X$ platí $x \subseteq X$.

Definíciu tranzitívnej množiny môžeme ekvivalentne preformulovať tak, že platí

$$(\forall x, y) y \in x \in X \Rightarrow y \in X \tag{5.1}$$ {defordnew:EQTRANZ}

alebo tiež $y \in x \wedge x \in X \Rightarrow y \in X$. (Z (5.1) a z podmienky (iii) v leme 5.3.3 vidno, odkiaľ sa vzalo pomenovanie tranzitívna množina.)

Jednoduché príklady tranzitívnych množín sú napríklad $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$.

{defordnew:LMTRANZSUBSET

Lema 5.3.3.

(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.* (*V časti hovoriacej o $\bigcap \mathcal{S}$ navyše predpokladáme $\mathcal{S} \neq \emptyset$, aby sme mali zaručenú existenciu prieniku.*)

{defordnew:it

(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:it

(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 (5.1) 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 (5.1) 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 5.3.4. 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.)

Napokon presne rovnaká námietka by sa dala vzniesť proti používaniu symbolu $\subseteq$ ako relácie. Napriek tomu sme na jeho používanie zvyknutí, priam by sa dalo povedať, že $(\mathcal{P}(X), \subseteq)$ a podmnožiny takýchto množín sú patria medzi príklady čiastočne usporiadaných množín, s ktorými sme sa najviac zoznámili, keď sme sa prvýkrát učili o čiastočných usporiadaniach.

5.3.2 Ordinálne čísla ako tranzitívne množiny

Definícia 5.3.5. 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 2.6. 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.

Všimnime si, že antireflexívnosť máme zadarmo – vyplýva z axiómy regularity (tvrdenie 3.1.4). Ale ak sa z nejakých dôvodov radšej chceme axióme regularity vyhnúť, tak by sme to tiež vedeli urobiť – nasledujúci dôkaz nikde axiómu regularity nepoužíva:

{defordnew:TVRNOTIN}

Tvrdenie 5.3.6. *Pre ľubovoľný ordinál α platí $\alpha \notin \alpha$.*

Dôkaz. Pretože $\in$ je *ostré* dobré usporiadanie na α, pre každé $\beta \in \alpha$ platí

$$\beta \notin \beta.$$

Teda ak by platilo $\alpha \in \alpha$ dostali by sme súčasne, že $\alpha \notin \alpha$, čo je spor. □

Zadefinovali sme pojem ordinálu, zatiaľ však nevieme ani to, či nejaké ordinály vôbec existujú. Pomocou nasledujúceho tvrdenia vieme nájsť viacero konkrétnych príkladov ordinálov.

TVRNASLJEORD}

Tvrdenie 5.3.7.

(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 5.3.3 (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 4.1.9 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 tvrdením 5.3.6.) Takže jediný rozdiel oproti relácii definovanej v príklade 4.1.9 je ten, že tu používame ostré usporiadanie. $\square$

{defordnew:PRIKLKONORD}

Príklad 5.3.8. Množina $\emptyset$ je očividne ordinálne číslo. Keď sa budeme na túto množinu pozerať ako na ordinál, tak budeme veľmi často používať označenie 0. T.j. ako prvý príklad ordinálu máme $0 = \emptyset$. Ďalšie príklady môžeme dostať z tvrdenia 5.3.7: $1 = S(0) = 0 \cup \{0\} = \{\emptyset\}$
$2 = S(1) = 1 \cup \{1\} = \{0, 1\} = \{\emptyset, \{\{\emptyset\}\}\}$
$3 = S(2) = 2 \cup \{2\} = \{0, 1, 2\} = \{\emptyset, \{\{\emptyset\}\}, \{\emptyset, \{\{\emptyset\}\}\}\}$

Nasledujúce tvrdenie ukazuje, že všetky prvky ordinálu sú opäť ordinály. Dokonca dostaneme, že každý ordinál je presne množina obsahujúca všetky menšie ordinály.

Tvrdenie 5.3.9. *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 5.3.3 (iii) vyplýva, že β je tranzitívna množina. $\square$

{defordnew:TVRINLRASUB}

Tvrdenie 5.3.10. *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.

$\boxed{\Leftarrow}$ Najprv si skúsme uvedomiť, že ak $\alpha \subseteq \beta$ a α, β sú ordinály, tak α musí byť počiatočný úsek dobre usporiadanej množiny $(\beta, \in)$. Zoberme si ľubovoľné $\gamma \in \alpha$. Ak $\gamma' \in \gamma$ (t.j. γ' je menšia ako γ v usporiadaní $\in$), tak z $\gamma' \in \gamma \in \alpha$ a z tranzitívnosti množiny α máme $\gamma' \in \alpha$.

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 $\alpha = \gamma$.

$\boxed{\alpha \subseteq \gamma}$ Pretože α je počiatočným úsekom β, tak najmenší prvok množiny $\beta \setminus \alpha$ je súčasne horným ohraničením α vzhľadom na ostré lineárne usporiadanie $\in$. To znamená, že ak $\delta \in \alpha$, tak $\delta \in \gamma$.

$\boxed{\gamma \subseteq \alpha}$ 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 $\delta \in \alpha$. $\square$

Definícia 5.3.11. Nech α, β sú ordinálne čísla. Hovoríme, že α je menšie ako β, ak $\alpha \in \beta$. Používame označenie $\alpha < \beta$.

Ďalej definujeme
$$\alpha \leq \beta \overset{\text{def}}{\Leftrightarrow} \alpha < \beta \vee \alpha = \beta.$$

{defordnew:POZNEKVPODM}

Poznámka 5.3.12. Vidíme teda, že 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 5.3.13. Keďže už vieme, že podmienky $\alpha < \beta$, $\alpha \in \beta$ a $\alpha \subsetneqq \beta$ 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 môže 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 5.3.14. *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 5.3.12 už vieme ukázať, že $S(\alpha)$ sa vzhľadom na nerovnosť ordinálov správa rovnako ako nasledovník v dobre usporiadanej množine.

defordnew:TVRSAJENASLED}

Tvrdenie 5.3.15. *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 5.3.14 a vety 5.1.5 okamžite dostaneme:

{defordnew:DOSTRICHO}

Dôsledok 5.3.16. *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.)

ew:TVRLEUSEK}

Tvrdenie 5.3.17. *Nech α, β sú ordinálne čísla. Potom:*
$\alpha \le \beta$ práve vtedy, keď α je izomorfné s nejakým počiatočným úsekom dobre usporiadanej mmožiny $(\beta, \in)$;
$\alpha < \beta$ práve vtedy, keď α je izomorfné s nejakým vlastným počiatočným úsekom $(\beta, \in)$.

Dôkaz. Budeme dokazovať prvú časť tvrdenia; druhá časť sa z nej dá pomerne ľahko odvodiť.

$\boxed{\Rightarrow}$ Ak $\alpha < \beta$, tak $\alpha = \beta_\alpha$. Ak $\alpha = \beta$, tak tvrdenie takisto platí, lebo ordinál β je počiatočným úsekom samého seba.

$\boxed{\Leftarrow}$ 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. To je spor s dôsledkom 5.1.4. ☐

{defordnew:TVRSUBSETLE}

Tvrdenie 5.3.18. *Nech α je ordinál a $B \subseteq \alpha$. Nech β je ordinálny typ množiny B. Potom $\beta \le \alpha$.*

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 5.3.17.) ☐

{defordnew:LMZJEDSYS}

Lema 5.3.19. *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 5.3.3 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 3.1.4).

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 5.3.16). 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:DOSMNOZORDJEDU}

Dôsledok 5.3.20. *Ľubovoľná množina $\mathcal{S}$ ordinálnych čísel je dobre usporiadaná reláciou $\in$.*

Dôkaz. Je to podmnožina dobre usporiadanej množiny $\bigcup S$. □

{defordnew:DEFSUPINF}

Definícia 5.3.21. 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 5.3.22. *Nech $\mathcal{S}$ je množina ordinálov a β je ordinál. Potom $\beta = \sup \mathcal{S}$ práve vtedy, keď β spĺňa nasledujúce podmienky:*

{defornew:itSUP1} (i) *je horným ohraničením – pre každé $\alpha \in \mathcal{S}$ platí $\alpha \leq \beta$;*

{defornew:itSUP2} (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:TVRORDJETRIEDA}

Tvrdenie 5.3.23. *Neexistuje množina všetkých ordinálnych čísel.*

Predchádzajúce tvrdenie vlastne hovorí, že systém všetkých ordinálnych čísel tvorí vlastnú triedu – pozri časť 3.1.2.

Dôkaz. Predpokladajme, že

$$\mathrm{On} = \{\alpha; \alpha \text{ je ordinál}\}$$

by bola množina. Podľa lemy 5.3.19 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.

new:VTORDTYP}

Veta 5.3.24. *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 5.1.5 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 5.3.14), 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 5.1.1.

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 5.3.23. □

{defordnew:DEFORDTYP}

Definícia 5.3.25. (Jednoznačne určený) ordinál, ktorý je izomorfný s dobre usporiadanou množinou X nazývame *ordinálny typ* množiny X.

5.3.3 Konečné ordinály a ordinál ω

Zatiaľ sme videli len zopár príkladov konečných ordinálnych čísel, ako napríklad $0, 1, 2, \dots,$ v príklade 5.3.8. Keď už vieme, že každá dobre usporiadaná množina má svoj ordinálny typ, tak by sme mohli nejaký nekonečný ordinál dostať tak, že ho zadefinujeme ako ordinálny typ dobre usporiadanej množiny $(\mathbb{N}, \leq)$. Tento ordinál sa zvykne označovať ω.

Ak by sme sa chceli poctivo držať toho, že veci odvodzujeme naozaj iba z axióm ZFC, tak to nemôžeme urobiť takto – lebo prirodzené čísla zatiaľ nemáme skonštruované v rámci ZFC. Ak chceme skonštruovať prirodzené čísla resp. ordinál ω naozaj axiomaticky, využijeme na to axiómu nekonečnej množiny.

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

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

[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 2.5.9(ii) s tým rozdielom, že opäť nemôžeme hovoriť o zobrazeniach, keďže ordinálne čísla netvoria množinu.

Definícia 5.3.26. 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], [Č].)

Definícia 5.3.27. *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.

{defordnew:LMPRIENINDUK}

Lema 5.3.28. *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 $x \cup \{x\} \in \bigcap \mathcal{S}$. ☐

Teraz by sme chceli ukázať, že množina $\mathbb{N}$, ktorú sme definovali ako najmenšiu induktívnu množinu, je v skutočnosti ordinálne číslo.

Tvrdenie 5.3.29. *Množina* $\mathbb{N}$ *je ordinálne číslo.*

Poznámka 5.3.30. V kontexte ordinálnych čísel zvyčajne namiesto $\mathbb{N}$ používame označenie ω. (Hoci ide o tú istú množinu.) V niektorých textoch, najmä v oblastiach blízkych teórii množín, sa stretnete s tým, že ω označuje množinu prirodzených čísel. Aj v tomto texte budeme tieto dve označenia odteraz používať ako vzájomne zameniteľné.

Dôkaz. Označme

$$\omega = \{\alpha \in \mathbb{N}; \alpha \text{ je ordinál}\}.$$

Priamo z definície tejto množiny je jasné, že $\omega \subseteq \mathbb{N}$.

Aby sme ukázali, že $\mathbb{N} \subseteq \omega$, stačí nám ukázať, že ω je induktívna. Zrejme $\emptyset \in \omega$. Súčasne ak nejaké $n \in \omega$, tak $S(n)$ patrí do $\mathbb{N}$ (lebo $\mathbb{N}$ je induktívna) a $S(n)$ je ordinál (tvrdenie 5.3.7).

Zistili sme teda, že platí rovnosť $\omega = \mathbb{N}$. Vedeli by sme nejako zdôvodniť to, že ω je ordinálne číslo? Na to by nám stačilo ukázať, že

$$\omega = \bigcup_{n \in \omega} n,$$

pretože potom ω je zjednotenie ordinálov, čiže je to opäť ordinál (tvrdenie 5.3.19).

Všimnime si, že ak $n \in \omega$, tak $n \subseteq \omega$ (podľa tvrdenia 5.3.10). Teda $\bigcup\limits_{n \in \omega} n \subseteq \omega$.

Obrátene, ak $k \in \omega$, tak aj $S(k) \in \omega$ (lebo je to induktívna množina). Súčasne máme $k \in S(k)$, z čoho vyplýva $k \in \bigcup\limits_{n \in \omega} n$. ☐

5.3.4 Zhrnutie

TODO

Cvičenia

{defordcvic:ULOTRANZNEORD

Úloha 5.3.1. Nájdite príklad tranzitívnej množiny, ktorá nie je ordinálom.

5.4 Ordinálna aritmetika*

{aritmord:SECTORDARIT}

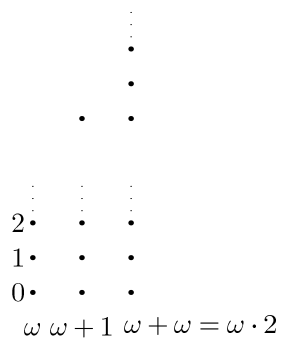
Už sme sa naučili ordinálne čísla porovnávať. V tejto podkapitole zavedieme súčet a súčin ordinálov a budeme sa zaoberať základnými vlastnosťami týchto operácií, podobne ako sme to predtým urobili pre kardinálne čísla. (Neskôr zadefinujeme aj umocňovanie ordinálov, jeho definícia je však o dosť komplikovanejšia.) 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).

5.4.1 Súčet ordinálnych čísel

{aritmord:SSECTSUCET}

Definícia 5.4.1. 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 4.1.9, kde sme sa venovali aj tomu, že takto dostaneme (z dobre usporiadaných množín) dobré usporiadanie. Niektoré príklady sú znázornené na obrázku 5.1.



Obr. 5.1: 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:TVI

Tvrdenie 5.4.2. *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.

{aritmord1:EQPLUSNASL}

$$\alpha + S(\beta) = S(\alpha + \beta). \tag{5.2}$$

Podobne ako pri kardinálnych číslach, aj tu nás bude zaujímať, či sčitovanie ordinálov zachováva nerovnosti.

{aritmord1:TVRSUCNEROV}

Tvrdenie 5.4.3. *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 $f: \beta \to \gamma$, $f(\delta) = \delta$ je vnorenie β na vlastný počiatočný úsek dobre usporiadanej množiny $(\gamma, \in)$. Pomocou neho môžeme zadefinovať zobrazenie $g: \alpha \times \{0\} \cup \beta \times \{1\} \to \alpha \times \{0\} \cup \gamma \times \{1\}$ 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 $f: \alpha \to \beta$, $f(\delta) = \delta$, ordinálu α na počiatočný úsek ordinálu β. Potom zobrazenie $g: \alpha \times \{0\} \cup \gamma \times \{1\} \to \beta \times \{0\} \cup \gamma \times \{1\}$ 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 5.3.18 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 5.4.4. *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 5.4.3 potom máme $\beta = \alpha + \gamma \geq \alpha + 0 = \alpha$.

$\boxed{\Rightarrow}$ Stačí za γ zvoliť ordinálny typ množiny $\beta \setminus \alpha$. □

1:TVRSUCSPOJ}

Tvrdenie 5.4.5. *Nech α je ordinál a $\{\beta_i; i\in I\}$ je množina ordinálov. Potom*

d1:EQSUCSPOJ}
$$\alpha+\sup_{i\in I}\beta_i=\sup_{i\in I}(\alpha+\beta_i) \tag{5.3}$$

tmord1:EQSUP}
$$(\sup_{i\in I}\beta_i)+\alpha\geq\sup_{i\in I}(\beta_i+\alpha) \tag{5.4}$$

Dôkaz. Rovnosť (5.3): 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 5.4.3 $\alpha+\beta_i>\alpha+\gamma=\rho$, 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 (5.4): 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. □

5.4.2 Súčin ordinálnych čísel {aritmord:SSECTSUCIN}

Definícia 5.4.6. Súčin ordinálnych čísel α a β definujeme ako ordinálny typ množiny $\alpha\times\beta$ usporiadanej antilexikografickým súčinom usporiadaní množín α a β. Označujeme ho $\alpha\cdot\beta$.

Pripomeňme, že antilexikografické usporiadanie sme zaviedli v definícii 4.1.6.

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 5.4.7. 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 5.4.8. *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 5.4.9. *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 5.3.17 a 5.3.18). □

Druhá časť tvrdenia neplatí, ak neostrú nerovnosť nahradíme ostrou. Stačí si všimnúť, že $1 < 2$ ale $1.\omega = \omega = 2.\omega$.

5.5 Transfinitná indukcia

{transf:SECTTRANSF}

Vo vete 4.1.3 sme videli, že na dobre usporiadaných množinách funguje indukcia. Vlastne nič viac nepotrebujeme – na aplikácia transfinitnej indukcie by nám úplne stačila táto veta. Prečo sa teda vlastne venujeme ordinálom? Nekomplikujeme tým zbytočne celú situáciu?

Do istej miery je to pravda. Na druhej strane by však bolo pomerne nešťastné zavádzať iné označenia pre veci, ktoré sa nejako označujú štandardne. Výrazne by sme sťažili situáciu iným ľuďom, ktorý by chceli čítať naše dôkazy. A takisto by sme mohli mi mať problémy čítať dôkazy iných ľudí, kde sa využívajú ordinálne čísla.

Okrem toho, že naše dôkazy budú mať štandardný a bežne používaný zápis, dosiahneme aj to, že budú zapísané prehľadnejšie a stručnejšie.

Opäť si môžeme trochu pomôcť prirovnaním k obvyklej matematickej indukcii. Aj pri nej existujú isté štandardné postupy a označenia. Používanie transfinitnej indukcie bez použitia ordinálnych čísel by sa do istej miery podobalo na to, keby sme pri matematickej indukcie nepoužívali množinu $\mathbb{N}$, ale v každom dôkaze nejakú inú, pričom by sme vysvetlili ako a prečo vlastne funguje indukcia na tejto množine.

5.5.1 Limitné ordinály

Ešte predtým, než sa dostaneme k transfintnej indukcii, si povieme, čo sú limitné ordinály.

Definícia 5.5.1. 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 5.5.2. *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 5.3.21).

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 5.3.15. 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 $\gamma = \beta$. □

5.5.2 Veta o transfinitnej indukcii

Transfinitná indukcia je veľmi užitočná dôkazová technika. Ide vlastne o indukciu na dobre usporiadaných množinách, ktorú už poznáme (veta 4.1.3); 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 5.5.3. *Nech $\varphi(x)$ je formula teórie množín taká, že ak platí $\varphi(\beta)$ pre všetky ordinály menšie ako α, 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 4.1.3, teda $B = S(\alpha)$. Tým sme ukázali, že $\varphi(\beta)$ platí pre každý ordinál $\beta \in S(\alpha)$, špeciálne aj pre ordinál α. □

Poznámka 5.5.4. 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 5.5.5, ktorý je našou prvou ilustráciou transfinitnej indukcie.) Ak chceme dokázať, že $\psi(\alpha)$ platí pre každý ordinál $\alpha < \lambda$, môžeme jednoducho použiť vetu 5.5.3 pre formulu $\varphi(\alpha) = \psi(\alpha) \vee (\alpha \geq \lambda)$ (alebo využiť priamo vetu 4.1.3, podobne ako v dôkaze vety 5.5.3).

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 5.1.1. 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 5.5.5. 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 5.1.1 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

$$f(\alpha) \geq \sup_{\beta < \alpha} \beta = \alpha.$$

□

5.5.3 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 5.5.6 (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 5.5.7. 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. (Doteraz zadefinované hodnoty sú popísané funkciou f.)

Dôkaz. 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.

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 5.5.3.

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

$$\overline{F}(\delta) = \begin{cases} F(\delta) & \delta \in \gamma, \\ y & \delta = \gamma \text{ a } y \text{ je jediné } y \text{ spĺňajúce } \varphi(F, y), \end{cases}$$

tak táto funkcia ukazuje platnosť $\psi(\beta)$.

Ak β je limitný ordinál a F_γ označíme funkciu z formuly $\psi(\gamma)$, tak stačí položiť $F = \bigcup_{\gamma<\beta} F_\gamma$ a opäť dostaneme, že platí $\psi(\beta)$. (Z rovnakého argumentu, aký sme použili pri dôkaze jednoznačnosti, vidíme že tieto zobrazenia sú navzájom kompatibilné.)

Z vety 5.5.3 máme, že $\psi(\beta)$ platí pre každý ordinál, špeciálne že platí $\psi(\alpha)$. To ale presne znamená existenciu zobrazenia s uvedenými vlastnosťami. □

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 5.5.8. 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 5.5.6.)

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 5.4.2 a rovnosťami (5.2), (5.3), tak vidíme, že $F(\alpha) = \gamma + \alpha$, čiže takto môžeme transfinitnou rekurziou zadefinovať sčitovanie ordinálnych čísel. Podobný postup použijeme v časti 5.5.4 na definíciu umocňovania ordinálnych čísel.

5.5.4 Umocňovanie ordinálnych čísel*

{transf:SSECTI

5.6 Definícia kardinálnych čísel

{defkard:SECTI

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 3.3.2.)

{defkard:TVRDI

Tvrdenie 5.6.1. *(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 5.6.2. 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 5.6.1. 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 5.3.24 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 $\alpha \leq \beta$. □

5.7 Aplikácie ordinálnych čísel a transfinitnej indukcie

V tejto časti by sme chceli ukázať niektoré príklady použitia transfinitnej indukcie. Okrem iného ukážeme platnosť vzťahu $a \cdot a = a$, resp. $a \cdot b = \max\{a, b\}$ pre nekonečné kardinálne čísla, ktorý sme doteraz používali bez dôkazu (pozri poznámku 2.7.13).

5.7.1 Kardinálna aritmetika

Veta 5.7.1. *Pre každý kardinál $a \geq \aleph_0$ platí $a \cdot a = a$.*

Dôkaz. Vieme, že toto tvrdenie platí pre $a = \aleph_0$ (úloha 2.7.2). 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

$$(a_1, b_1) \leq^* (a_2, b_2) \Leftrightarrow \begin{cases} (m_1 < m_2) \qquad \vee \\ (m_1 = m_2 \wedge a_1 < a_2) \qquad \vee \\ (m_1 = m_2 \wedge a_1 = a_2 \wedge b_1 < b_2) \end{cases}$$

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 neprázdnu podmnožinu množiny $a \times a$ 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

$$a \cdot a \leq a.$$

Opačná nerovnosť je zrejmá, čím dostávame rovnosť $a \cdot a = a$.

Poznamenajme ešte, že argumentovaním pomocou kardinality sme mohli dokonca ukázať, že uvedené vnorenie je v skutočnosti priamo bijekcia. □

{aplikord:DOSSUCMAX}

Dôsledok 5.7.2. *Ak a, b sú nekonečné kardinály, tak*

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

Dôkaz. Bez ujmy na všeobecnosti nech $a \leq b$. Potom

$$b \leq a + b \leq b + b = 2b \leq a \cdot b \leq b \cdot b = b.$$

□

[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.

Všimnime si, že vetu 5.7.1 môžeme preformulovať aj tak, že nepoužijeme pojem kardinálneho čísla:

{aplikord:DOS

Dôsledok 5.7.3. *Pre ľubovoľnú nekonečnú množinu A platí*

$$|A| = |A \times A|.$$

Uvedený dôkaz tohoto výsledku používal axiómu výberu. Využili sme totiž dobré usporiadanie na množine A resp. to, že existuje ordinálne číslo $a = |A|$, ktoré je v bijekcii s množinou A.

Výsledok pochádzajúci od Alfreda Tarskiho [Tar] hovorí, že v ZF z platnosti dôsledku 5.7.3 už vyplýva AC. Pozri napríklad [Hal1, Theorem 5.5], [Her2, Theorem 4.24].

5.7.2 Ekvivalenty axiómy výberu

{aplikord:SSECTEKVAC}

Vo vete 4.2.5 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:
$p_0 = f(P)$;
$p_{\beta+1} = f(p_\beta \uparrow)$;
$p_\beta = f(\{q \in P; q \text{ je horné ohraničenie pre } \{p_\gamma; \gamma < \beta\}\})$, 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 5.3.23.

Dostaneme tak, ordinál α pre ktorý

$$\{p_\gamma; \gamma < \alpha\}$$

je reťazec v $(P, \leq)$, ktorý nemá horné ohraničenie. □

Poznámka 5.7.4. Použitie transfinitnej rekurzie v predchádzajúcom dôkaze je odlišné od toho, čo sme dokázali vo vete 5.5.6. 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 5.5.6. 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 ⇒ WO vyplýva z už dokázaných tvrdení, ukážeme si, ako na jej dôkaz možno použiť transfinitnú indukciu.

Dôkaz implikácie AC ⇒ 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

$$g(\beta) \le g(\gamma) \Leftrightarrow \beta \le \gamma.$$

Dostaneme tak dobré usporiadanie, ktorého ordinálny typ je α. □

5.7.3 Aplikácie v algebre a analýze

{aplikord:VTSTEINITZ}

Veta 5.7.5 (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 $a_0, \dots, a_n \in K$. Potom p je polynómom už nad menším poľom $L := F(a_0, \dots, a_n) \subseteq K$. V nadpoli $L[x]/(p(x))$ má polynóm $p(x)$ koreň. Pole L je algebraickým rozšírením poľa F (každý z prvkov $a_0, \dots, a_n$ 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 $q(x) = p(x) \cdot r(x)$. 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 $\alpha \le \gamma$ 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.

[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 $F \cup \{u_1, \dots, u_n\}$, kde $u_1, \dots, u_n$ 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

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. □

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.

{aplikord:TVRDARBOUX}

Tvrdenie 5.7.6. *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. (Ale určite by ste našli aj jednoduchší príklad takejto funkcie.)

Názov darbouxovská funkcia pochádza z Darbouxovej vety, ktorá hovorí, že ak nejaká funkcia je deriváciou, tak je darbouxovská. Vzájomný vzťah týchto tried funkcií môžeme teda zhrnúť tak, že každá spojitá funkcia je deriváciou, každá derivácia je darbouxovská funkcia. Ani v jednom z týchto dvoch prípadov však neplatí opačná implikácia.

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 $A = B \cup \{(x,0); x \in \mathbb{R}, B_x = \emptyset\}$. □

Poznámka 5.7.7. Dalo by sa nájsť aj veľa iných možností ako ukázať existenciu silno darbouxovskej funkcie, dokonca aj explicitne napísať predpis takejto funkcie. (Uvedený dôkaz využíva AC na dvoch miestach. Využívame, že množina kardinality $\mathfrak{c}$ sa dá dobre usporiadať. A v indukčnom kroku vyberáme z neprázdnych množín $(a_\alpha, b_\alpha) \setminus \{x_\beta; \beta < \alpha\}$.) Dôkaz existencie takejto funkcie alebo jej explicitnú konštrukciu môžete nájsť napríklad v [KN, Problem 1.3.29], [vRS, Example 9.M]. [6]

Dôkaz transfinitnou indukciou má však tú výhodu, že je pomerne jednoduchý a priamočiary. Rovnaký princíp sa dá použiť pre veľa úloh podobného typu: Máme $\varkappa$ objektov, pre každý z nich chceme mať splnenú nejakú podmienku. Navyše táto podmienka je taká, že ak ju máme splnenú pre niektoré z týchto objektov, vieme vždy pridať nový, tak aby sme ju nepokazili pre tie z nich, ktoré naším požiadavkám už vyhovujú. V našom prípade sme mali $\mathfrak{c}$ vodorovných úsečiek a chceli sme dosiahnuť, aby skonštruovaná množina pretínala každú z nich. (A súčasne aby neobsahovala dva body na žiadnej zvislej priamke.)

Iné príklady založené na podobnom princípe sú existencia Mazurkiewiczovej množiny (problém 5.7.1), existencia Bernsteinovej množiny (problém 5.7.2).

5.7.4 Vzťah transfinitnej indukcie a axiómy výberu

Azda sa oplatí povedať niečo o tom v akom vzťahu je axióma výberu (prípadne Zornova lema) a transfinitná indukcia.

V prvom rade si uvedomme, že výsledky hovoriace o transfinitnej indukcii (vety 5.5.3 a 5.5.6, prípadne sem môžeme zarátať aj vetu 4.1.3) boli dokázané bez akéhokoľvek použitia axiómy výberu. Na používanie transfinitnej indukcie teda a priori nepotrebujeme AC.

Je však pravdou, že v praxi sa často v dôkaze založenom na transfinitnej indukcii niekde vyskytne aj použitie AC. Napríklad na to, aby sme použili transfinitnú indukciu, potrebujeme často dobré usporiadanie na nejakej množine, na ktorej dobré usporiadanie nevieme nejakým prirodzeným spôsobom zadefinovať. Vtedy často použijeme axiómu výberu vo forme WO na to, aby sme mali k dispozícii nejaké dobré usporiadanie. (Konkrétne napríklad v dôkaze tvrdenia 5.7.6 sme využívali dobré usporiadanie na množine kardinality $\mathfrak{c}$.) Takisto v indukčnom kroku často potrebujeme vybrať nejaký prvok z nejakej neprázdnej množiny. (Opäť sa môžete pozrieť na dôkaz tvrdenia 5.7.6, resp. na poznámku nasledujúcu tesne za ním.)

Ďalšie do istej miery užitočné pozorovanie je to, že často (hoci nie vždy) sa dôkaz transfinitnou indukciou dá pomerne priamočiaro pretransformovať na dôkaz založený na Zornovej leme a obrátene. Napokon sme videli, ako pomocou transfinitnej indukcie môžeme ukázať, že z AC vyplýva ZL.

Problémy

Mazurkiewiczova množina

{ordprob:PROBPRIAMKA2BOD

Problém 5.7.1. Ukážte, že existuje podmnožina $A \subseteq \mathbb{R}^2$, ktorá každú priamku pretína práve v dvoch bodoch.

Uvedený výsledok pochádza od S. Mazurkiewicza, takýmto množinám sa niekedy hovorí aj Mazurkiewiczove množiny. Dá sa dokázať aj silnejší výsledok – pre každú priamku L môžeme predpísať kardinálne číslo $2 \leq m_L \leq \mathfrak{c}$, pozri [Ba, BE] alebo tiež [Si, p. 450].

[6] Alebo tiež online, napríklad `http://mathoverflow.net/q/32126/`, `http://math.stackexchange.com/q/186427/`, `http://math.stackexchange.com/q/21812/`

Bernsteinova množina

Definícia 5.7.8. Pozmnožinu $B \subseteq \mathbb{R}^n$ nazveme *Bernsteinova množina,* ak pre každú nespočítateľnú uzavretú vlastnú podmnožinu $C \subsetneq \mathbb{R}^n$ platí $B \cap C \neq \emptyset$ aj $C \setminus B \neq \emptyset$. (T.j. C pretína množinu B i jej doplnok.)

V dôkaze existencie Bernsteinovej množiny sa nám bude hodiť fakt, že každá nespočítateľná uzavretá podmnožina $\mathbb{R}^n$ už má kardinalitu $\mathfrak{c}$ (veta 6.2.5).

{ordprob:PROBBERNSTEIN}

Problém 5.7.2.
a) Aká je kardinalita množiny všetkých uzavretých podmnožín $\mathbb{R}^n$? (Má rovnakú kardinalitu systém všetkých nespočítateľných uzavretých podmnožín?)
b) Ukážte, že existuje Bernsteinova podmnožina $\mathbb{R}^n$.
c) Ukážte, že Bernsteinova množina nie je Lebesguovsky merateľná. (Môžete využiť napríklad regularitu Lebesguovej miery.[7])
d) Kde sme v dôkaze použili axiómu výberu? (Vieme, že v ZF sa nedá dokázať existencia nemerateľnej množiny. Teda buď v dôkaze existencie Bernsteinovej množiny alebo v dôkaze, že táto množina je nemerateľná, musí byť použitá AC.)

Zaujímavé rozklady $\mathbb{R}^n$

{ordprob:PROBROZKLR3}

Problém 5.7.3.
a) Dokážte, že $\mathbb{R}^3$ sa dá rozložiť na disjunktné kružnice polomeru 1. Akú kardinalitu bude mať takýto systém kružníc?
b) Dokážte, že $\mathbb{R}^3$ sa dá napísať ako disjunktné zjednotenie priamok takých, že žiadne dve z nich nie sú rovnobežné. Akú kardinalitu bude mať takýto systém priamok?
c) Dá sa rozložiť $\mathbb{R}^2$ na kružnice s polomerom 1? Dá sa rozložiť $\mathbb{R}^2$ na priamky tak, aby žiadne z nich neboli rovnobežné? Dá sa rozložiť $\mathbb{R}^3$ na *roviny* také, že žiadne z nich neboli rovnobežné?

σ-algebry, Borelovské množiny, Bairove triedy funkcií

Pripomeňme definíciu σ-algebry:

Definícia 5.7.9. 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).

Je zrejmé, že ekvivalentnú definíciu dostaneme, ak namiesto uzavretosti na spočítateľné zjednotenia

Ľahko sa ukáže, že prienik ľubovoľného systému σ-algebier je opäť σ-algebra. Teda pre $\mathcal{A} \subseteq \mathcal{P}(X)$ máme najmenšiu σ-algebru na X obsahujúcu $\mathcal{A}$. (Dostaneme ju jednoducho ako prienik všetkých σ-algebier obsahujúcich $\mathcal{A}$. Všimnime si, že $\mathcal{P}(X)$ je tiež σ-algebra, teda robíme prienik z neprázdneho systému.) Označme túto σ-algebru ako $\sigma(\mathcal{A})$.

Tento prístup nám dáva popis $\sigma(\mathcal{A})$ zhora–nadol (pozri poznámku 2.4.17). Pomocou transfinitnej indukcie ju môžeme popísať aj zdola–nahor. Ukážeme si, že aj takýto popis môže byť užitočný.

{ordprob:PROBSIGMAALG}

Problém 5.7.4.

[7] Vieme, že pre Lebesguovu mieru platí: $m(B) = \sup\{m(C); C \subseteq B; C \text{ je kompaktná}\} = \inf\{m(U); U \supseteq B; U \text{ je otvorená}\}$.

a) Nech $\mathcal{A} \subseteq \mathcal{P}(X)$. Transfinitnou indukciou definujme:
$\mathcal{A}_0 = \mathcal{A}$;
$\mathcal{A}_{\alpha+1}$ je množina, ktorú dostaneme z $\mathcal{A}_\alpha$, ak pridáme všetky doplnky, spočítateľné zjednotenia a spočítateľné prieniky;
Ak α je limitný ordinál, tak $A_\alpha = \bigcup\limits_{\beta<\alpha} A_\beta$.
Ukážte, že $\sigma(\mathcal{A}) = \bigcup\limits_{\alpha<\omega_1} A_\alpha$.

b) *Borelova algebra* je σ-algebra generovaná všetkými otvorenými podmnožinami daného topologického priestoru X a jej prvky sa nazývajú *borelovské množiny.* Ukážte, že v $\mathbb{R}$ dostaneme tú istú algebru, ak ju generujeme otvorenými intervalmi (alebo tiež uzavretými intervalmi resp. polouzavretými intervalmi).

c) Aká je kardinalita Borelovej algebry priestoru $\mathbb{R}$? (Všeobecnejšie: Aká je kardinalita $\sigma(\mathcal{A})$, ak $|\mathcal{A}| \leq \mathfrak{c}$.) Existuje podmnožina $\mathbb{R}$, ktorá nie je borelovská?

{ordprob:PROBBAIRE}

Problém 5.7.5. V tejto úlohe budeme pracovať s funkciami z $\mathbb{R}$ do $\mathbb{R}$.

a) Transfinitnou indukciou definujme:
$\mathcal{B}_0 = C(\mathbb{R})$, t.j. $\mathcal{B}_0$ je množina všetkých spojitých funkcií z $\mathbb{R}$ do $\mathbb{R}$;
$\mathcal{B}_{\alpha+1}$ je množina všetkých bodových limít postupností funkcií z $\mathcal{B}_\alpha$;
Ak β je limitný ordinál, tak $\mathcal{B}_\beta = \bigcup\limits_{\alpha<\beta} \mathcal{B}_\alpha$.
Funkcie patriace do $\mathcal{B}_\alpha$ nazývame funkcie *α-tej Baireovej triedy.*
Ukážte, že $\mathcal{B} = \bigcup\limits_{\alpha<\omega_1} \mathcal{B}_\alpha$ je najmenšia množina funkcií, ktorá obsahuje všetky spojité funkcie a je uzavretá na bodové limity postupností. (T.j. ak $f_n \in \mathcal{B}$ a $f_n \to f$ bodovo, tak aj $f \in \mathcal{B}$.)

b) Funkciu f nazveme *borelovsky merateľnou,* ak pre každú otvorenú množinu $U \subseteq \mathbb{R}$ patrí $f^{-1}[U]$ do Borelovej σ-algebry. Podobne pre ľubovoľnú σ-algebru $\mathcal{S}$ môžeme hovoriť o *$\mathcal{S}$-merateľnej funkcii.* Ukážte, že nasledujúce podmienky pre zobrazenie $f\colon \mathbb{R} \to \mathbb{R}$ a σ-algebru $\mathcal{S}$ sú ekvivalentné:
   (a) Funkcia f je $\mathcal{S}$-merateľná.
   (b) Pre každé $a \in \mathbb{R}$ platí $f^{-1}[(a,\infty)] \in \mathcal{S}$.
   (c) Pre každé $a \in \mathbb{R}$ platí $f^{-1}[\langle a,\infty)] \in \mathcal{S}$.

c) Ukážte, že $\mathcal{B}$ je presne množina Borelovsky merateľných funkcií.

Poznamenajme, že uvedená charakterizácia by sa dala ešte zjemniť. Vieme, že spojité funkcie (t.j. funkcie nultej Bairovej triedy) sú presne tie funkcie, kde vzor každej otvorenej množiny je otvorená. Ekvivalentne, vzor každej uzavretej množiny je uzavretá.

Pojem F_σ-množiny definujeme ako množinu, ktorá je zjednotením spočítateľne veľa uzavretých množín. Podobne G_δ-množiny sú spočítateľné prieniky otvorených množín. Funkcie prvej Bairovej triedy sú presne tie funkcie, kde vzory otvorených množín sú F_σ-množiny. Ekvivalentná podmienka je, že vzory uzavretých množín sú G_δ.

V uvedenej konštrukcii by sme mohli veľmi prirodzeným spôsobom postupovať ďalej a dostať $F_{\sigma\delta}$-množiny, $G_{\delta\sigma}$-množiny atď. Táto hierarchia sa dá rozšíriť nielen na konečne veľa úrovní, ale dala by sa rozšíriť transfinitnou indukciou aj na ľubovoľné ordinály. (Opäť však reálne vystačíme s ordinálmi po ω_1.) Pomocou takýchto množín sa dajú ocharakterizovať funkcie patriace do α-tej Bairovej triedy. Podrobnosti môžete nájsť napríklad v [Ke, Chapter 24].

Mengerova veta a metrická konvexnosť

Pojem konvexnosti poznáme z vektorových priestorov. Istý typ konvexnosti sa dá zadefinovať aj v metrických priestoroch:

Definícia 5.7.10. Metrický priestor (X, d) nazveme *konvexný* (alebo *konvexný v Mengerovom zmysle* alebo tiež *metricky konvexný*), ak pre ľubovoľné x, y také, že $x \neq y$ existuje $z \neq x, y$ také, že

{EQMENG}

$$d(x, y) = d(x, z) + d(z, y). \tag{5.5}$$

{ordprob:PROBMENGER}

Problém 5.7.6.

a) Dokážte, že v ľubovoľnom metrickom priestore platí: Ak $d(x, y) = d(x, z) + d(z, y)$ a $d(x, z) = d(x, t) + d(t, z)$, tak aj $d(x, y) = d(x, t) + d(t, y)$.

b) Dokážte Mengerovu vetu: Ak (X, d) je úplný konvexný metrický priestor a $x \neq y$ sú nejaké body v X, tak pre ľubovoľné $t \in (0, 1)$ existuje bod $w \in X$ taký, že $d(x, w) = td(x, y)$ a $d(w, y) = (1 - t)d(x, y)$. (Návod: Transfinitnou indukciou sa pokúste zostrojiť postupnosti $x_\alpha, x'_\alpha \in X$ a $t_\alpha, t'_\alpha \in (0.1)$ také, že $t_\alpha < t < t'_\alpha$ a súčasne

$$\begin{array}{ccc} d(x, x_\alpha) = t_\alpha d(x, y) & \text{a} & d(x_\alpha, y) = (1 - t_\alpha)d(x, y); \\ d(x, x'_\alpha) = t'_\alpha d(x, y) & \text{a} & d(x'_\alpha, y) = (1 - t'_\alpha)d(x, y); \\ & d(x_\alpha, x'_\alpha) = (t'_\alpha - t_\alpha)d(x, y). & \end{array}$$

Skúste ich voliť vhodným spôsobom, aby ste sa nejako vedeli priblížiť k hodnote t.) [8]

c) Ukážte, že bez predpokladu o úplnosti už Mengerova veta nemusí platiť.

d) Predpokladajme, že máme dané $t \in (0, 1)$ a dva body x, y v nejakom metrickom priestore. Predpokladajme ďalej, že existuje bod z taký, že

$$d(x, z) = td(x, y) \qquad \text{a} \qquad d(z, y) = (1 - t)d(x, y).$$

Je bod z predchádzajúcou podmienkou jednoznačne určený? (T.j. môže pre dané x, y, t existovať aj viacero bodov z vyhovujúcich uvedenej podmienke?)

e) Ak pracujeme v lineárnom normovanom priestore, je pojem metrickej konvexnosti totožný s obvyklým pojmom konvexnosti?

Sekvenciálne priestory, sekvenciálny uzáver

Nech X je ľubovoľný topologický priestor a $A \subseteq X$. Označme A^* množinu všetkých limít postupností prvkov z A. Ako $\widehat{A}$ označme najmenšiu množinu obsahujúcu A, ktorá je uzavretá vzhľadom na limity postupností.[9] (Pretože aj množinu A^* aj množinu $\hat{A}$ by bolo pomerne prirodzené nazvať sekvenciálnym uzáverom množiny A, nebudeme v tomto texte používať uvedenú terminológiu ani pre jednu z týchto množín; namiesto toho budeme jednoducho používať iba uvedené označenie.)

Topologický priestor nazveme *sekvenciálny,* ak pre každú podmnožinu $A \subseteq X$ platí $\overline{A} = \widehat{A}$.

Podmnožinu A nazvime *sekvenciálne uzavretou,* ak $A = \widehat{A}$, t.j. ak A je uzavretá vzhľadom na limity postupností. Ekvivalentne môžeme sekvenciálny priestor definovať ako priestor, v ktorom sú uzavreté práve sekvenciálne uzavreté množiny.

[8] Keďže je úloha zaradená v tejto kapitole, preferujem dôkaz pomocou transfinitnej indukcie. Dôkaz využívajúci Zornovu lemu môžete nájsť napríklad v [C].

[9] Fakt, že najmenšia množina s takouto vlastnosťou existuje, ľahko vyplynie z toho, že prienik ľubovoľného systému takýchto množín má uvedenú vlastnosť.

Každý priestor vyhovujúci prvej axióme spočítateľnosti (a teda špeciálne každý metrický priestor) je aj sekvenciálny priestor. Existujú však aj priestory, ktoré nie sú sekvenciálne. Dokonca aj medzi priestormi, ktoré sa pomerne bežne vyskytujú v praxi – napríklad niektoré priestory so slabou alebo slabou* topológiou.

Z nasledujúcich úloh sú prvé dve zamerané na transfinitnú indukciu; tretia a štvrtá sú skôr cvičenia na prácu s pojmom sekvenciálneho priestoru.

{ordprob:PROBSEKVEN}

Problém 5.7.7.

a) Pre každý ordinál α definujeme A_α nasledovne:
$A_0 = A$;
$A_{\alpha+1} = (A_\alpha)^*$;
ak α je limitný ordinál, tak $A_\alpha = \bigcup_{\beta<\alpha} A_\beta$.
Ukážte, že $\widehat{A} = A_{\omega_1} = \bigcup\limits_{\alpha<\omega_1} A_\alpha$. (Poznamenajme, že sa dá zostrojiť príklad priestoru, kde skutočne treba až ω_1 iterácií [AF].)

b) Ukážte, že ak A je podmnožina Hausdorffovského sekvenciálneho priestoru taká, že $|A| \le \mathfrak{c}$, tak aj $|\overline{A}| \le \mathfrak{c}$, t.j. kardinalita jej uzáveru je nanajvýš $\mathfrak{c}$.

c) Nech X je sekvenciálny priestor, Y je topologický priestor a $f\colon X \to Y$ je zobrazenie. Dokážte, že f je spojité práve vtedy, keď pre každú konvergentnú postupnosť (x_n) v X platí, že ak $\lim\limits_{n\to\infty} x_n = a$, tak aj $\lim\limits_{n\to\infty} f(x_n) = f(a)$. (Návod: Skúste ukázať, že vzor každej uzavretej množiny je uzavretý)

d) Nech X je ľubovoľný topologický priestor. Na tej istej množine definujeme topologický priestor sX tak, že uzavreté množiny v sX sú práve tie množiny, ktoré sú sekvenciálne uzavreté v X. (Dostaneme takto skutočne topologický priestor?) Ukážte, že tento topologický priestor má navyše tú vlastnosť, že pre každý sekvenciálny priestor Y a spojité zobrazenie $f\colon Y \to X$ je aj zobrazenie $f\colon Y \to sX$ spojité. Priestor sX sa zvykne nazývať *sekvenciálna koreflexia* priestoru X.

Viac o sekvenciálnych priestoroch sa môžete dočítať napríklad v [AP, Section 1.8], [Eng, Section 1.6], [Fr1, Fr2]. Ďalšia súvisiaca trieda topologických priestorov sú *Fréchetove-Urysohnove priestory.* To sú priestory, v ktorých platí pre každú podmnožinu $\overline{A} = A^*$.

Doplním ešte aj drobnú poznámku k odhadu na kardinalitu priestoru. Ak by sme vynechali požiadavku, že daný priestor je sekvenciálny, tak už uvedený odhad pre kardinalitu neplatí. Vedeli by sme dokázať, že v Hausdorfovskom priestore má uzáver danej množiny kardinalitu najviac $2^{2^{|A|}}$. Pozri napríklad [Eng, Theorem 1.5.3], [Ju, 2.4].[10] Tento horný odhad sa nedá zlepšiť. Dá sa nájsť príklad Hausdorffovského priestoru kardinality 2^{2^a}, ktorý obsahuje hustú množinu kardinality a. Príkladom takého priestoru je *Stone-Čechova kompaktifikácia* diskrétneho priestoru kardinality a. So Stone-Čechovou kompaktifikáciou ste sa mohli stretnúť na predmetoch **Všeobecná topológia 1,2**.

Vlastnosť priestoru sX, ktorú sme dostali v poslednej úlohe, môžeme sformulovať aj takto. Vieme, že $id_X\colon sX \to X$ je spojité zobrazenie. (To je len inými slovami povedané, že topológia sX je hrubšia než pôvodná topológia.) A pre ľubovoľné spojité zobrazenie $f\colon Y \to X$, kde Y je sekvenciálny, existuje práve jedno spojité zobrazenie $\overline{f}$ také, že nasledujúci diagram komutuje:

$$\begin{tikzcd} X & sX \arrow[l, "id_X"'] \\ & Y \arrow[ul, "f"] \arrow[u, dashed, "\overline{f}"'] \end{tikzcd}$$

[10]Alebo aj http://math.stackexchange.com/q/430747 http://math.stackexchange.com/q/45429

Toto je špeciálny prípad pojmu *koreflexie* a *koreflektívnej podkategórie.* Duálny pojem (pri obrátení všetkých šípok) by bola *reflexia* a *reflektívna podkategória.* Na reflexiu a koreflexiu sa dá pozerať ako na špeciálny prípad *adjungovaného funktora.* S uvedenými pojmami sa máte možnosť zoznámiť na predmetoch **Teória kategórií 1,2**.

Ale aj v prípade, že neviete nič o kategóriách, by vám uvedená formulácia mohla pripomenúť niektoré objekty, ktoré boli definované nejakou *univerzálnou vlastnosťou.* (Napríklad voľná grupa, rôzne typy súčinov či zúplnení, podielové pole a mnohé ďalšie dôležité konštrukcie.)

Kapitola 6

Niektoré ďalšie aplikácie teórie množín

6.1 Skoro disjunktné systémy

V tejto kapitole sa budeme zaoberať systémami skoro disjunktných množín. Takéto systémy môžu byť občas užitočné.

Definícia 6.1.1. Nech M je ľubovoľná nekonečná spočítateľná množina, t.j. $|M| = \aleph_0$. Množiny $A, B \subseteq M$ nazveme *skoro disjunktné,* ak ich prienik $A \cap B$ je konečný.

Ak $\mathcal{A} \subseteq \mathcal{P}(M)$ je systém nekonečných podmnožín M taký, že ľubovoľné dve množiny z $\mathcal{A}$ sú skoro disjunktné, tak $\mathcal{A}$ voláme *systém skoro disjunktných množín* alebo tiež *AD-systém*[1] na množine M. Nekonečný AD-systém, ktorý je maximálny vzhľadom na inklúziu, budeme volať *maximálny AD-systém* alebo stručne *MAD-systém.*

Požiadavka, že MAD systém má byť nekonečný je užitočná na to, aby sme vylúčili niektoré triviálne prípady. Napríklad ak $\omega = A \cup B$, kde A, B sú nekonečné disjunktné množiny (mohli by sme zobrať napríklad párne a nepárne čísla), tak $\mathcal{A} = \{A, B\}$ je AD-systém, ktorý je maximálny vzhľadom na inklúziu. Ale obsahuje iba konečne veľa množín, takže ho nepovažujeme za MAD-systém.

Ľahko nájdeme AD-systém na množine $\mathbb{N}$ kardinality $\aleph_0$; množinu $\mathbb{N}$ dokonca vieme rozložiť na $\aleph_0$ disjunktných množín (cvičenie 6.1.4), disjunktné množiny sú očividne aj skoro disjunktné.

Štandardnou aplikáciou Zornovej lemy sa dokáže, že každý nekonečný AD-systém je obsiahnutý v nejakom maximálnom AD-systéme.

Tvrdenie 6.1.2. *Ak $\mathcal{A}$ je nekonečný AD-systém na množine M, tak existuje MAD-systém $\mathcal{A}'$ na množine M taký, že $\mathcal{A}' \supseteq \mathcal{A}$.*

Dôkaz. Problém 6.1.1. $\square$

Budeme sa zaoberať hlavne AD-systémami na nekonečných spočítateľných množinách.

Tvrdenie 6.1.3. *Nech M je nekonečná spočítateľná množina a $\mathcal{A}$ je MAD-systém na M. Potom $|\mathcal{A}| \geq \aleph_1$.*

[1] z anglického *almost disjoint*

Dôkaz. Problém 6.1.1. □

{mad:TVRADC}

Tvrdenie 6.1.4. *Pre každú nekonečnú spočítateľnú množinu M existuje AD-systém $\mathcal{A} \subseteq \mathcal{P}(M)$ taký, že $|\mathcal{A}| = \mathfrak{c}$.*

Dôkaz. Tvrdenie budeme dokazovať pre $M = \mathbb{Q}$. (Dokazovaná vlastnosť sa evidentne prenáša cez bijekcie, takže ak ho dokážeme pre tento prípad, tak platí aj pre ostatné nekonečné spočítateľné množiny.)

Pre každé reálne číslo $r \in \mathbb{R}$ zoberme prostú postupnosť $x^{(r)} = (x_n^{(r)})_{n=0}^{\infty}$ racionálnych čísel, ktorá konverguje k r. Ďalej uvažujme množiny členov týchto postupností, teda $A_r = \{x_n^{(r)}; n \in \omega\}$ a systém $\mathcal{A} = \{A_r; r \in \mathbb{R}\}$.

Každá z množín A_r je nekonečná, lebo sme použili prosté postupnosti. Z toho, že pre $r_1 \neq r_2$ majú postupnosti $x^{(r_1)}$ a $x^{(r_2)}$ rôzne limity vyplýva, že priradenie $r \mapsto A_r$ je prosté (a teda $|\mathcal{A}| = \mathfrak{c}$) a tiež to, že tieto dve postupnosti majú nanajvýš konečne veľa spoločných členov – čo znamená, že $\mathcal{A}$ je systém skoro disjunktných množín. □

V predošlom dôkaze sme použili AC (na výber prostej postupnosti $x^{(r)}$). Axióme výberu sa môžeme vyhnúť, ak explicitne popíšeme konštrukciu postupnosti $x^{(r)}$ pre dané reálne číslo r. Ponechávame ako cvičenia pre čitateľa, aby si rozmyslel ako sa to dá urobiť (úloha 6.1.3).

{mad:POZNBIJEK}

Poznámka 6.1.5. Hoci trik použitý v dôkaze tvrdenia 6.1.4 bol veľmi jednoduchý, zaslúži si podľa mňa stručný komentár. Využívali sme to, že dokazovaná vlastnosť sa zachováva bijekciou a namiesto toho, aby sme tvrdenie dokazovali pre ľubovoľnú množinu kardinality $\aleph_0$, použili sme množinu $\mathbb{Q}$. Výhodné to bolo z toho dôvodu, že vďaka tomu sme na tejto množine mali dodatočnú štruktúru (mohli sme ju chápať ako podmnožinu $\mathbb{R}$) a tú sme mohli v dôkaze využiť.

Takýto trik vlastne nevyužíva nič zložité – mal by byť jasný každému, kto pochopil ideu bijekcie a kardinality v prvom ročníku. Napriek tomu naň nie je vždy celkom jednoduché prísť; asi by to bolo ľahšie, keby nám niekto priamo povedal, že to máme skúsiť dokazovať pre $\mathbb{Q}$. Niekoľko úloh, kde sa dá použiť takýto princíp som pridal do cvičení za touto kapitolou; úlohy 6.1.1, 6.1.2, 6.1.4.

Ešte sa azda oplatí uvedomiť, že to je vlastne najjednoduchší prípad princípu, ktorý ste sa pri prechode k abstraktnej matematike naučili. Spomeňme si napríklad na lineárnu algebru. Definovali ste vektorový priestor tak, že tam boli veci popisujúce lineárnu štruktúru. Dva vektorové priestory, ktoré sú izomorfné, sú „v podstate“ rovnaké. Myslí sa tým, že ak sa pýtame na tvrdenie, ktoré sa dá vyjadriť v jazyku vektorových priestorov, tak ak platí v jednom z nich, musí platiť aj v druhom. Napríklad ak dokážeme tvrdenie takéhoto typu pre všetky priestory $\mathbb{R}^n$, tak platí aj v každom konečnorozmernom priestore nad $\mathbb{R}$. Rovnako to funguje s izomorfizmom grúp, izomorfizmom čiastočne usporiadaných množín, homeomorfizmom topologických priestorov, izometriou medzi dvoma metrickými priestormi atď. V tomto prípade sme sa vlastne zaoberali množinou bez akejkoľvek ďalšej štruktúry, a preto nám stačila existencia bijekcie.

Poznámka 6.1.6. Povedzme si ešte niečo o možnej kardinalite AD-systémov a MAD-systémov na množine $\mathbb{N}$. Je jasné, že existujú AD-systémy na $\mathbb{N}$, ktoré majú malú kardinalitu – ľahko nájdeme napríklad konečné alebo spočítateľné AD-systémy. (Ak nám ich stačí spočítateľne veľa, vieme dokonca nájsť systém nekonečných množín, ktoré sú disjunktné; nie iba skoro disjunktné – úloha 6.1.4.)

Už sme ukázali, že na $\mathbb{N}$ existuje AD-systém kardinality $\mathfrak{c}$. Ten sa dá rozšíriť na MAD-systém, ktorý tiež nutne musí mať kardinalitu $\mathfrak{c}$.

Takisto vieme, že každý MAD-systém musí mať kardinalitu aspoň $\aleph_1$.

Možno by človek na prvý pohľad očakával, že všetky MAD-systémy budú mať kardinalitu $\mathfrak{c}$. (Prečo by sa niektoré z nich mali správať inak?) Je snáď aspoň trochu prekvapivým faktom, že to tak byť nemusí.

Aby sa nám ľahšie formulovali výsledky, o ktorých chceme hovoriť, zadefinujme

$$\mathfrak{a} = \min\{|\mathcal{A}|; \mathcal{A} \text{ je MAD-systém na množine } \mathbb{N}\}.$$

(Vieme, že každá množina kardinálnych čísel má najmenší prvok – poznámka 5.2.1. Vďaka tomu táto definícia má zmysel.)

Zatiaľ vlastne vieme, že

$$\aleph_1 \leq \mathfrak{a} \leq \mathfrak{c}.$$

Z toho vyplýva, že ak platí hypotéza kontinua, tak $\mathfrak{a} = \mathfrak{c}$. Keďže hypotéza kontinua je relatívne konzistentná (pozri podkapitolu 3.4), aj tvrdenie, že $\mathfrak{a} = \mathfrak{c}$ je konzistentné vzhľadom na ZFC.

Dá sa však ukázať, že aj tvrdenie $\mathfrak{a} < \mathfrak{c}$ je relatívne konzistentné; existujú modely ZFC, v ktorých platí ostrá nerovnosť (pozri napríklad [Hal1, Chapter 8]). Z axióm ZFC sa teda nedá rovnosť $\mathfrak{a} = \mathfrak{c}$ ani dokázať, ani vyvrátiť.

6.1.1 Hamelova dimenzia v Banachových priestoroch

{mad:SSECTHAMEL}

V probléme 4.3.1 sme sa dozvedeli, že ľubovoľné dve Hamelove bázy vektorového priestoru majú rovnakú kardinalitu, teda aj v prípade nekonečnorozmerných priestorov má zmysel hovoriť o dimenzii. Ideme sa zamyslieť nad tým, či sú nejaké obmedzenia na dimenziu v prípade Banachových priestorov. Najprv ukážeme, že dimenzia nekonečnorozmerného Banachovho priestoru musí byť aspoň $\aleph_1$. (Dôkaz je založený na Bairovej vete o kategórii. Takýto dôkaz sa dá nájsť napríklad v [AB, Corollary 5.23], [Ca, p.25], [FHH$^+$, Exercise 1.81]. Iný dôkaz, nevyužívajúci Baireovu vetu, sa dá nájsť v [Ts] a [Mor, Proposition 5.1].)

Podarí sa nám však ukázať aj o niečo silnejší výsledok – že dimenzia nekonečnorozmerného Banachovho priestoru musí byť aspoň $\mathfrak{c}$. Dôkaz, ktorý uvedieme, pochádza z článku [La] a využíva existenciu AD-systému na $\mathbb{N}$ kardinality $\mathfrak{c}$.

Pre istotu si pripomeňme pojem množiny prvej kategórie a Bairovu vetu o kategórii.

Definícia 6.1.7. Podmnožina A topologického priestoru sa nazýva *riedka* ak $\operatorname{Int}\overline{A} = \emptyset$. Podmnožina topologického priestoru je množinou *prvej kategórie,* ak je spočítateľným zjednotením riedkych množín. Podmnožina, ktorá nie je množinou prvej kategórie, sa nazýva množinou *druhej kategórie.*

Možno sa oplatí pripomenúť aj ekvivalentnú definíciu riedkej množiny: Množina A je riedkou podmnožinou topologického priestoru X, ak pre každú neprázdnu otvorenú množinu $U \subseteq X$ existuje neprázdna otvorená podmnožina $V \subseteq U$ taká, že $V \cap A = \emptyset$. Ak v tejto formulácii hovoríme iba o množinách z nejakej bázy, tak opäť dostaneme ekvivalentnú podmienku. Napríklad v metrickom priestore by sme mohli zobrať iba otvorené gule. (Čiže podmnožina A v metrickom priestore X je riedka, ak v každej otvorenej guli $B(x, r)$ vieme nájsť menšiu otvorenú guľu $B(x', r') \subseteq B(x, r)$, ktorá sa „vyhne" množine A, t.j. $B(x', r') \cap A = \emptyset$.)

Veta 6.1.8 (Bairova veta o kategórii, Baire Category Theorem, BCT)**.** *Ak X je úplný metrický priestor, tak X je množina druhej kategórie.*

Analogické tvrdenie platí napríklad aj pre lokálne kompaktné Hausdorffovské priestory.

Dôkaz tejto vety môžete nájsť napríklad v [AB, Theorem 3.74], [Ke, Theorem 8.4], [Me, Theorem 1.5.4], [Wil, Chapter 25]. Pretože v tomto texte zvykneme uviesť, ktoré výsledky využívajú axiómu výberu, patrí sa spomenúť, že dôkaz Bairovej vety sa tiež opiera o AC.

Bairova veta má často aplikácie pri dôkaze existencie nejakých objektov – ak na množine objektov, ktorými sa zaoberáme, máme vhodnú metriku (takú že dostaneme úplný metrický priestor) a o nejakej podmnožine sa nám podarí ukázať, že je to množina prvej kategórie, tak nutne musí existovať aj objekt mimo tejto podmnožiny. Táto veta sa často využíva aj vo funkcionálnej analýze; napríklad pri dôkaze princípu rovnomernej ohraničenosti (známeho tiež ako Banach-Steinhausova veta).[2]

Ukážeme si, ako pomocou Bairovej vety o kategórii ukázať, že Hamelova báza Banachovho priestoru nemôže byť nekonečná spočítateľná.

{mad:VTDIMBPNESP}

Veta 6.1.9. *Nech X je Banachov priestor. Potom jeho dimenzia nemôže byť $\aleph_0$.*

Dôkaz. Sporom. Predpokladajme, že X je Banachov priestor (t.j. úplný lineárny normovaný priestor) a súčasne má spočítateľnú bázu $\{x_i; i \in \mathbb{N}\}$.

Pre každé $i \in \mathbb{N}$ definujeme konečnorozmerný podpriestor $V_i = [x_0, x_1, \dots, x_i]$. Každý z priestorov V_i je uzavretý podpriestor X. (Každý konečnorozmerný lineárny normovaný priestor je úplný. Úplný podpriestor Banachovho priestoru je uzavretý.) Keďže ide o vlastný uzavretý podpriestor, je to teda riedka podmnožina X (úloha 6.1.5).

Súčasne vcelku ľahko vidno, že $\bigcup\limits_{i=0}^{\infty} V_i = X$. (Každý prvok priestoru X je lineárnou kombináciou konečne veľa prvkov bázy $\{x_i; i \in \mathbb{N}\}$, z čoho vyplýva, že musí patriť do V_i pre niektoré $i \in \mathbb{N}$.)

Zistili sme, že X je spočítateľné zjednotenie riedkych množín, je to teda množina prvej kategórie. Keďže X je úplný priestor, dostávame spor s Bairovou vetou. $\square$

V podstate rovnaký dôkaz, aký sme tu uviedli, by sa dal použiť pre dôkaz podobného tvrdenia pre úplne metrizovateľné topologické vektorové priestory, pozri [AB, Corollary 5.23].

Ako sme spomínali, predchádzajúci výsledok možno o niečo zosilniť:

{mad:VTDIMBPC}

Veta 6.1.10. *Nech X je nekonečnorozmerný Banachov priestor. Potom jeho Hamelova dimenzia je aspoň $\mathfrak{c}$.*

Dôkaz. Nech X nekonečnorozmerný Banachov priestor.

Najprv indukciou skonštruujeme $\{x_i; i \in \mathbb{N}\} \subseteq X$ a $\{x_i^*; i \in \mathbb{N}\} \subseteq X^*$ také, že

$$x_i^*(x_j) = \delta_{ij}$$

a $\|x_i\| = 1$.

Vysvetlime si detailnejšie indukčný krok. Predpokladajme, že už máme skonštruované $x_1, \dots, x_k$ a $x_1^*, \dots, x_k^*$ vyhovujúce uvedeným podmienkam. Potom môžeme priestor X zapísať ako $X = [x_1, \dots, x_k] \oplus X'$, pričom[3] $X' = \bigcap\limits_{i=1}^{k} \operatorname{Ker}(x_i^*)$. Priestor X' je opäť nekonečnorozmerný. T.j. máme

$$X = [x_1, \dots, x_k] \oplus \bigcap_{i=1}^{k} \operatorname{Ker}(x_i^*) = [x_1, \dots, x_k] \oplus X'$$

Potom môžeme zvoliť ľubovoľné $x_{k+1} \in X'$ také, že $\|x_{k+1}\| = 1$. Zobrazenie $x_{k+1}^* \colon [x_1, \dots, x_{k+1}] \to \mathbb{R}$ určené predpisom $x_{k+1}^*(x_i) = \delta_{ij}$ je lineárne zobrazenie na konečnorozmernom podpriestore, teda je spojité. Podľa Hahn-Banachovej vety sa potom dá rozšíriť na spojité lineárne zobrazenie z X do $\mathbb{R}$ (pozri dôsledok 4.3.12).

[2]Viacero aplikácií Bairovej vety môžete nájsť tu: `http://math.stackexchange.com/questions/165696/your-favourite-application-of-the-baire-category-theorem/`

[3]Toto môžeme dostať viacnásobným použitím faktu, že ak $f \in X^*$ and $f(x) \neq 0$, tak $X = \operatorname{Ker} f \oplus [x]$; pozri úlohu 6.1.6.

Z týchto podmienok vyplýva $x_k \notin \overline{[\{x_j; j \in \mathbb{N}, j \neq k\}]}$, pretože $x_k \notin (x_k^*)^{-1}[0]$ a $(x_k^*)^{-1}[0]$ je uzavretý podpriestor priestoru X obsahujúci $\{x_j; j \in \mathbb{N}, j \neq k\}$.

Nech teraz $\mathcal{A} = \{A_i; i \in \mathbb{R}\}$ je AD-systém na $\mathbb{N}$. Pre každé $i \in \mathbb{R}$ definujeme

$$a_i = \sum_{j\in A_i} \frac{1}{2^j} x_j.$$

(Pretože $\|\frac{1}{2^j}x_j\| \leq \frac{1}{2^j}$, tento rad je cauchyovský, a teda konvergentný.)

Ukážeme, že množina $\{a_i; i \in \mathbb{R}\}$ je lineárne nezávislá. Pretože každá lineárne nezávislá množina je obsiahnutá v báze (pozri problém 4.3.1), z toho už vyplynie, že Hamelova dimenzia priestoru X je aspoň $\mathfrak{c}$.

Predpokladajme, že by platilo $\sum\limits_{i\in F} c_i a_i = 0$ pre nejakú konečnú množinu F, pričom všetky c_i sú nenulové. Nech

$$P := \bigcup_{\substack{i,j\in F\\ i\neq j}} (A_i \cap A_j).$$

Táto množina je konečná, lebo $\mathcal{A}$ je AD-systém. Uvedenú konečnú sumu môžeme prepísať ako

$$\sum_{j=1}^{\infty} d_j x_j = 0,$$

kde $d_j = \frac{c_i}{2^j}$ pre $i \in F$ a $j \in A_i \setminus P$. Pretože všetky množiny $A_i \setminus P$ sú nekonečné, vystupuje v tejto sume nekonečne veľa nenulových koeficientov. Teda poslednú rovnosť môžeme prepísať do tvaru

$$x_k = \sum_{i\neq k} f_i x_i$$

pre nejaké k a $f_i \in \mathbb{R}$, čo je v spore s predpokladom, že $x_k \notin \overline{\{x_j; j \neq k\}}$. □

6.1.2 Mrówkov-Isbellov priestor

Táto časť je pripravená najmä podľa [Ma][4]. Tento priestor bol definovaný v [Mr]. Ďalšia literatúra, kde sa môžete o ňom dočítať: [Eng, Exercise 3.6.I, Exercise 3.10.G], [GJ, Problem 5I].

Definícia 6.1.11. Nech $\mathcal{A}$ je AD-systém na množine ω. Priestor $\Psi(\mathcal{A})$ definujeme ako topologický priestor na množine $\mathcal{A} \cup \omega$ taký, že body množiny ω sú izolované a báza okolí v bode $A \in \mathcal{A}$ je tvorená množinami tvaru $\{A\} \cup (A \setminus F)$, kde $F \subseteq \omega$ je konečná podmnožina. Tento priestor budeme volať *Mrówkov-Isbellov priestor.*

Poznamenajme, že terminológia v literatúre nie je úplne jednotná. Niektorí autori používajú názov Mrówkov-Isbellov priestor iba v prípade, že $\mathcal{A}$ je MAD-systém. My budeme používať túto definíciu, pri výsledkoch, kde je potrebná maximalita, to explicitne uvedieme.

Skontrolujme, že keď vezmeme uvedené okolia bodov $A \in \mathcal{A}$ a jednobodové množiny ako okolia bodov $n \in \omega$, tak skutočne dostaneme bázu $\mathcal{B}$ nejakej topológie. Na to treba iba overiť, že pre ľubovoľný bod $x \in \Psi(\mathcal{A})$ a $B_{1,2} \in \mathcal{B}$ také, že $x \in B_1 \cap B_2$ existuje množina $B \in \mathcal{B}$, pre ktorú platí $x \in B \subseteq B_1 \cap B_2$.

- Pre body $x \in \omega$ je uvedená podmienka očividne splnená; stačí zobrať $B = \{x\}$.
- $(\{A\} \cup (A \setminus F_1)) \cap (\{A\} \cup (A \setminus F_2)) = \{A\} \cup (A \setminus (F_1 \cup F_2))$ a $F_1 \cup F_2$ je opäť konečná množina.

[4] `http://dantopology.wordpress.com/tag/mrowka-space/`

- Ak $A \neq B$, tak $(\{A\} \cup (A \setminus F_1)) \cap (\{B\} \cup (B \setminus F_2)) \subseteq \omega$, teda prienik obsahuje iba izolované body.

Môžeme si všimnúť, niektoré základné vlastnosti priestoru $\Psi(\mathcal{A})$. Je vcelku ľahké overiť, že tento priestor je *Hausdorffovský* – úloha 6.1.7. Pre každý bod sme priamo pri definícii uviedli spočítateľnú bázu okolí, teda tento priestor vyhovuje *prvej axióme spočítateľnosti.*

Všimnime si ešte, že tento priestor je lokálne kompaktný. Pripomeňme, že Hausdorffovský priestor je *lokálne kompaktný,* ak každý bod má kompaktné okolie.[5]

Pre bod $n \in \omega$ máme kompaktné okolie $n \in \omega$. Pre $A \in \mathcal{A}$ skúsme overiť, že priamo $\{A\} \cup A$ je kompaktný podpodpriestor. Ak máme nejaké pokrytie množiny $A \cup \{A\}$ otvorenými množinami, tak niektorá z nich musí obsahovať bod A, teda v pokrytí sa musí vyskytovať množina obsahujúca bázové okolie tvaru $\{A\} \cup A \setminus F$, kde $F \subseteq \omega$ je konečná množina. Ak vyberieme takúto množinu, tak zostáva v $\{A\} \cup A$ už len konečne veľa nepokrytých bodov; takže pomocou tejto množiny a konečne veľa ďalších množín vieme dostať konečné podpokrytie.

Vieme, že každý Hausdorffovský lokálne kompaktný priestor je úplne regulárny [Eng, Theorem 3.3.1], [Wil, Theorem 19.3]. Zistili sme teda, že priestor $\Psi(\mathcal{A})$ je *úplne regulárny.*

Budeme sa teraz zaoberať Mrówkovým-Isbellovým priestorom, už len v prípade, že $\mathcal{A}$ je MAD-systém. Pozrieme sa konkrétne na dve vlastnosti príbuzné s kompaktnosťou – pseudokompaktnosť a spočítateľnú kompaktnosť.

Definícia 6.1.12. Topologický priestor X sa nazýva *pseudokompaktný,* ak je Tichonovovský a pre každú funkciu $f\colon X \to \mathbb{R}$ je $f[X]$ ohraničená množina.

Je zrejmé, že každý kompaktný T_2-priestor je pseudokompaktný. Pre priestor $\Psi(\mathcal{A})$ platí:

Tvrdenie 6.1.13. *Ak $\mathcal{A}$ je MAD-systém, tak priestor $\Psi(\mathcal{A})$ je psedokompaktný.*

Dôkaz. Nech by funkcia $f\colon \Psi(\mathcal{A}) \to \mathbb{R}$ bola spojitá a neohraničená. Potom aj zúženie $f|_\omega$ musí byť neohraničená funkcia, pretože podmnožina ω je hustá v $\Psi(\mathcal{A})$. Zoberme si množinu $B \subseteq \omega$ takú, že $f|_B$ je neohraničená a navyše $|f(b_1) - f(b_2)| \geq 1$ pre ľubovoľné $b_{1,2} \in B$. (Takúto množinu môžeme zostrojiť indukciou.)

Potom prienik $B \cap A$ je konečný pre každé $A \in \mathcal{A}$. (Keďže $\{A\} \cup A$ je kompaktný podpriestor a teda funkcia f je na tejto podmnožine ohraničená.)

Našli sme teda nekonečnú množina, ktorá má konečný prienik s každou množinou $A \in \mathcal{A}$. To je spor s maximalitou MAD-systému $\mathcal{A}$. □

Nasledujúci pojem je vcelku prirodzeným zovšeobecnením kompaktnosti.

Definícia 6.1.14. Topologický priestor X je *spočítateľne kompaktný,* ak pre každé spočítateľné otvorené pokrytie priestoru X existuje konečné podpokrytie.

{mad:TVRSPOCKOMPUZAV}

Tvrdenie 6.1.15. *Nech X je topologický priestor. Nasledujúce podmienky sú ekvivalentné:*

(i) *X je spočítateľne kompaktný.*

(ii) *Ak $\{F_n; n \in \mathbb{N}\}$ je centrovaný systém uzavretých množín, tak $\bigcap F_n \neq \emptyset$.*

(iii) *Ak $\{F_n; n \in \mathbb{N}\}$ je nerastúci systém uzavretých množín, t.j. $F_n \supseteq F_{n+1}$ pre každé $n \in \mathbb{N}$, tak $\bigcap F_n \neq \emptyset$.*

Dôkaz prenecháme čitateľovi (úloha 6.1.8) – je pomerne jednoduchý a navyše dôkaz ekvivalencie prvých dvoch podmienok je takmer identický s dôkazom charakterizácie kompaktných priestorov pomocou centrovaných systémov uzavretých množín, ktorú by ste mali poznať z predmetov venovaných všeobecnej topológii.

TODO spojitý obraz, uzavretý podpriestor

[5] V literatúre sa vyskytuje viacero neekvivalentných definícií lokálne kompaktného priestoru, v prípade Hausdorffovských priestorov sú však všetky tieto definície ekvivalentné.

Tvrdenie 6.1.16. *Nech X je T_1-priestor. Nasledujúce podmienky sú ekvivalentné* {mad:itNEKHROM} {mad:itNEKSPOCHROM} {mad:itSPOCK}

(i) *Každá nekonečná podmnožina priestoru X má hromadný bod.* [6]

(ii) *Každá nekonečná spočítateľná podmnožina priestoru X má hromadný bod.*

(iii) *Priestor X je spočítateľne kompaktný.*

Pripomeňme, že *hromadný bod* množiny M je taký bod x, že každé jeho okolie obsahuje nejaký bod z M rôzny od x. Stručne: Ak U je okolie x, tak $U \cap (M \setminus \{x\}) \neq \emptyset$. Ekvivalentne môžeme túto podmienku vyjadriť ako

$$x \in \overline{M \setminus \{x\}}.$$

Dôkaz. Implikácia (i) ⇒ (ii) je zrejmá. Obrátene, ľubovoľná nekonečná množina musí obsahovať nekonečnú spočítateľnú podmnožinu. Táto podmnožina má hromadný bod, ktorý je aj hromadným bodom celej množiny. Teda platí aj (ii) ⇒ (i).

(iii) ⇒ (ii) Nech X je spočítateľne kompaktný priestor a x_n, $n \in \mathbb{N}$, sú navzájom rôzne body tohoto priestoru. Chceme ukázať, že množina $M = \{x_n; n \in \mathbb{N}\}$ má hromadný bod. Označme $F_n = \overline{\{x_k; k > n\}}$. Podľa tvrdenia 6.1.15 existuje $x \in \bigcap F_n$. Ak $x \notin M$, tak máme $x \in \overline{M} = \overline{M \setminus \{x\}}$. Ak $x = x_n$ pre nejaké n, tak $x \in F_n = \overline{F_n} \subseteq \overline{M \setminus \{x\}}$. Teda x je hromadný bod množiny M.

(ii) ⇒ (iii) Nech $M = \{x_n; n \in \mathbb{N}\}$ je množina, ktorá nemá hromadný bod. Potom M je uzavretá a navyše pre každé $n \in \mathbb{N}$ existuje okolie U_n bodu x_n také, že $U_n \cap M = \{x_n\}$. Systém $\{X \setminus M\} \cup \{U_n; n \in \mathbb{N}\}$ tvorí spočítateľné otvorené pokrytie priestoru X, ktoré nemá konečné podpokrytie. □

TODO Nie všade bolo treba T_1, nám to stačí takto.

Tvrdenie 6.1.17. *Nech X je normálny priestor. Ak X je pseudokompaktný, tak X je aj spočítateľne kompaktný.*

Dôkaz. Nech X je normálny a nie je spočítateľné kompaktný. Potom existuje nekonečná podmnožina $A = \{x_n; n \in \omega\}$ priestoru X, ktorá nemá v X hromadný bod. To znamená, že A je ako podpriestor priestoru X je uzavretý diskrétny podpriestor. Zobrazenie $f\colon A \to X$, $f\colon x_n \mapsto n$ je spojité a podľa Tietzeho vety sa dá rozšíriť na spojitú funkciu $F\colon X \to \mathbb{R}$. Potom F je neohraničená spojitá funkcia z X do $\mathbb{R}$, čo znamená, že X nie je pseudokompaktný. □

Mrówkov-Isbellov priestor je teda príkladom, ktorý ukazuje, že uvedená implikácia pre ľubovoľné topologické priestory už nemusí platiť. Súčasne dostávame:

Dôsledok 6.1.18. *Mrówkov-Isbellov priestor nie je normálny.*

Teda je to aj príklad úplne regulárneho priestoru, ktorý nie je normálny.

Cvičenia

{matcvic:ULORETPN}

Úloha 6.1.1. Nech $|A| = \aleph_0$. Ukážte, že v $(\mathcal{P}(A), \subseteq)$ existuje reťazec kardinality $\mathfrak{c}$.

{madcvic:ULOQxQ}

Úloha 6.1.2. 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.)

[6] Uvedená podmienka sa niekedy zvykne nazývať aj *Bolzanova-Weierstrassova vlastnosť* (Bolzano-Weierstrass property) alebo tiež *limit point compactness.*

{madcvic:ULOAI

Úloha 6.1.3. Nájdite predpis, ktorý pre dané reálne číslo $r \in \mathbb{R}$ explicitne popisuje prostú postupnosť racionálnych čísel konvergujúcu k r. (Takýmto spôsobom sa môžeme vyhnúť použitiu axiómy výberu v dôkaze tvrdenia 6.1.4.)

{madcvic:ULORC

Úloha 6.1.4. Ukážte, že $\mathbb{N}$ sa dá zapísať ako zjednotenie spočítateľne veľa disjunktných nekonečných množín. (Túto úlohu som sem síce pridal ako jednu z ilustrácií prenosu cez bijekciu, o ktorom sme hovorili v poznámke 6.1.5, pomerne ľahko sa dajú nájsť aj riešenia, ktoré tento prístup nepoužívajú.)

{madcvic:ULOPPRRIED}

Úloha 6.1.5. Ukážte, že uzavretý vlastný podpriestor v lineárnom normovanom priestore je riedkou množinou.

{madcvic:ULOKER}

Úloha 6.1.6. Ukážte, že ak $f\colon V \to \mathbb{R}$ je lineárne zobrazenie na vektorovom priestore V a $f(x) \neq 0$, tak $V = [x] \oplus \operatorname{Ker} f$.

{madcvic:ULOMROT2}

Úloha 6.1.7. Ukážte, že pre ľubovoľný AD-systém na množine ω je priestor $\Psi(\mathcal{A})$ Hausdorffovský.

madcvic:ULOSPOCKOMPUZAV}

Úloha 6.1.8. Ukážte ekvivalenciu podmienok pre spočítateľnú kompaktnosť z tvrdenia 6.1.15.

Problémy Doteraz sme pracovali iba s AD-systémami na množine, ktorá má kardinalitu $\aleph_0$. Tento pojem sa dá zadefinovať aj pre množiny väčšej kardinality.

AD-systém a MAD-systém na množine M definujeme tak, že je to systém $\mathcal{A} \subseteq \mathcal{P}(M)$ taký, že všetky množiny z $\mathcal{A}$ majú rovnakú kardinalitu, ako množina M a pre $A \neq B$, $A, B \in \mathcal{A}$, platí $|A \cap B| < |M|$.

{madprob:PROBMAD}

Problém 6.1.1.

a) Ukážte pomocou Zornovej lemy, že každý nekonečný skoro disjunktný systém je obsiahnutý v nejakom maximálnom skoro disjunktnom systéme.
b) Ukážte, že MAD-systém na spočítateľnej množine musí mať kardinalitu aspoň $\aleph_1$. (Ekvivalentná formulácia: Ak je AD-systém nekonečný spočítateľný, tak nemôže byť maximálny.)
c) Ukážte, že MAD-systém na množine kardinality $\varkappa$ musí mať kardinalitu väčšiu ako $\varkappa$. (T.j. musí mať kardinalitu aspoň $\varkappa^+$, kde $\varkappa^+$ označuje kardinálny nasledovník čísla $\varkappa$; pozri definíciu 5.2.2.)
d) Existuje na každej nekonečnej množine M nejaký AD-systém kardinality $|M|$?

Problém 6.1.2. Aká je Hamelova dimenzia vektorového priestoru $\mathbb{R}^{\mathbb{N}}$ pozostávajúceho zo všetkých reálnych postupností? (Operácie na tomto vektorovom priestore sú definované obvyklým spôsobom.) Svoje tvrdenie zdôvodnite! (Návod 1: Skúste nejako vhodne využiť AD-systém kardinality $\mathfrak{c}$ na množine $\mathbb{N}$. Návod 2: Skúste sa pozrieť na prvky tvaru $(1, x, x^2, x^3, \dots)$ pre $x \in \mathbb{R}$. Návod 3: Máme nejaký Banachov priestor X, ktorý je vektorovým podpriestorom $\mathbb{R}^{\mathbb{N}}$?)

6.2 Nekonečné stromy

6.2.1 Základné definície a označenia

Nekonečné stromy sú vcelku dobre predstaviteľné matematické objekty. Snáď sa mi podarí vás v tejto kapitole presvedčiť, že sú občas aj užitočné.

Aby sme však o nich vedeli hovoriť, musíme si najprv zaviesť nejaké označenia a definície. A pokúsime sa popísať aj intuitívnu predstavu, ktorá je za nimi.

Budem sa v tejto kapitole viac-menej pridržiavať označenia z [Ke, Chapter 2].

Zoberme si nejakú množinu $A \neq \emptyset$. Potom pre každé prirodzené číslo[7] $n \in \omega$ môžeme množinu A^n chápať ako množinu postupností dĺžky n obsahujúcich iba prvky A. Takéto konečné postupnosti sú indexované prvkami množiny $n = \{0, 1, \dots, n-1\}$. Budeme ich preto aj zapisovať ako $s = (s(0), s(1), \dots, s(n-1)) = (s_0, s_1, \dots, s_{n-1})$ – presne tak, ako sme pri postupnostiach zvyknutí.

Dĺžku konečnej postupnosti s budeme označovať $l(s)$.

Ešte je azda užitočné si všimnúť, že $A^0 = A^\emptyset = \{\emptyset\}$ obsahuje ako jediný prvok $\emptyset$. Takúto funkciu môžeme chápať ako *prázdnu postupnosť;* a prípadne ju môžeme zapísať aj takto: $\emptyset = ()$.

Množinu všetkých konečných postupností prvkov z A budeme označovať ako

$$A^{<\omega} = \bigcup_{n\in\omega} A^n.$$

Dve konečné postupnosti sa dajú spojiť a z konečnej postupnosti sa dá vyrezať nejaká jej časť – nám sa bude hlavne hodiť prípad, keď vyberieme začiatok danej konečnej postupnosti.

Definícia 6.2.1. Ak $s \in A^n$ je postupnosť dĺžky n a $t \in A^k$ je postupnosť dĺžky k, tak postupnosť $s\hat{\ }t = (s_0, \dots, s_{n-1}, t_0, \dots, t_{k-1})$ dĺžky $n + k$ nazývame *zreťazenie* postupností s a t.

Ak $s \in A^n$ je postupnosť dĺžky n a $k \leq n$, tak postupnosť $s|_k = (s_0, \dots, s_{k-1})$ dĺžky k voláme *počiatočný úsek* postupnosti s. Ak $t = s|_k$ pre nejaké $k \leq n$, t.j. t je počiatočný úsek postupnosti s, tak túto skutočnosť budeme označovať aj $t \subseteq s$.

Môžeme si všimnúť, že označenie $s|_k$ je konzistentné s označením, ktoré používame pre zúženie funkcie. (Keď sa na dané postupnosti pozeráme ako na funkcie, tak ide skutočne o zúženie.) Takisto použitie označenia $t \subseteq s$ je oprávnené, pretože ak sa na prvky $A^{<\omega}$ pozrieme ako na množiny usporiadaných dvojíc, tak podmienky „byť podmnožinou" a „byť počiatočný úsekom" sú ekvivalentné. (Podmnožiny funkcie sú presne zúženia funkcie na podmnožiny definičného oboru.)

Definícia 6.2.2. Nech $A \neq \emptyset$

Množinu $T \subseteq A^{<\omega}$ nazývame *strom,* ak je uzavretá na počiatočné úseky. (T.j. ak $t \in T$ a $s \subseteq t$, tak $s \in T$).

Prvky množiny T nazývame *vrcholy*, prázdnu postupnosť $\emptyset$ nazývame *koreň* stromu.

Nekonečná vetva stromu T je taká postupnosť $x \in A^{\mathbb{N}}$, že pre každé $n \in \mathbb{N}$ platí $x|_n \in T$.

6.2.2 Königova lema

Definícia 6.2.3. Strom T na množine A voláme *konečne-vetviaci*, ak pre každé $s \in T$ existuje iba konečne veľa $a \in A$ takých, že $s\hat{\ }a \in T$.

Názov v podstate hovorí, o čo v tejto definícii ide – v každom vrchole sa strom T rozvetvuje iba na konečne veľa častí.

{stromy:VTKONIG}

Veta 6.2.4 (Königova lema)**.** *Nech T je konečne-vetviaci strom na množine A. Aj T má nekonečne veľa vrcholov, tak obsahuje aspoň jednu nekonečnú vetvu.*

[7]Pripomeňme že prirodzené čísla chápeme ako konečné ordinály, a teda každé prirodzené číslo je rovné množine prvkov od neho menších. Pre praktické účely nie je vôbec dôležité, ako konštruujeme prirodzené čísla; ale keďže to zostruční niektoré označenia, budeme sa držať tejto konvencie.

Dôkaz. Nech T je konečne vetviaci strom na množine A. Indukciou zostrojíme postupnosť $s = (s_0, s_1, \dots, s_n, \dots)$ takú, že pre každé $n \in \omega$ platí

- $s|_n \in T$;
- množina $V_n = \{t \in T; t|_n = s|_n\}$ je nekonečná.

Prvá podmienka zabezpečí to, že s je nekonečná vetva stromu T. Druhá podmienka v podstate hovorí to, že „podstrom" zavesený na vrchole $s|_n$ je nekonečný.

1° Pre $n = 0$ obe podmienky platia, lebo $s|_\emptyset = \emptyset$ a T je nekonečná množina.

2° Množina $V_n = \{t \in T; t|_n = s|_n\}$ obsahuje jedinú postupnosť dĺžky n (konkrétne $s|_n$). Musí teda obsahovať aj nejakú postupnosť väčšej dĺžky.

Vieme, že množina $N = \{a \in A; s|_n \hat{} a \in T\}$ nasledovníkov je konečná a navyše platí

$$V_n = \{s|_n\} \cup \left(\bigcup_{a \in N} \{t \in T; t|_{n+1} = s|_n \hat{} a\} \right).$$

Ak by bola pre každé $a \in N$ uvedená množina konečná, dostali aj V_n by bola konečná množina. (Zjednotenie konečne veľa konečných množín.)

Teda existuje aspoň jedno a, pre ktoré je takáto množina nekonečná. Jedno takéto a vyberieme a položíme $s_{n+1} = a$. □

6.2.3 Cantor-Bendixsonova veta

V tejto časti si ukážeme zaujímavé tvrdenie o separabilných metrických priestoroch. Tento výsledok je zaradený v tejto kapitole najmä preto, že stromy nám dávajú vhodný jazyk na vysvetlenie konštrukcie použitej v dôkaze.

{stromy:VTUZAVNESPOC}

Veta 6.2.5. *Nech (X, d) je úplný separabilný metrický priestor. Potom každá nespočítateľná uzavretá podmnožina X má kardinalitu $\mathfrak{c}$.*

Dôkaz. Najprv pripomeňme, že separabilný metrický priestor má spočítateľnú bázu topológie. Topológiu priestoru X označme $\mathcal{T}$.

To, že X je separabilný, znamená, že existuje hustá podmnožina $D \subseteq X$. Potom pre každé $x \in X$ existuje postupnosť prvkov z D, ktorá konverguje k x. Teda prvkov X je nanajvýš toľko, koľko môžeme vytvoriť postupností z prvkov spočítateľnej množiny D. Máme teda $|X| \le \aleph_0^{\aleph_0} = \mathfrak{c}$.

Nech F je nespočítateľná uzavretá podmnožina X. Budeme sa snažiť ukázať existenciu injekcie z množiny vetiev úplného binárneho stromu $T = \{0,1\}^{<\omega}$ do F.

Definujme

$$H := \{x \in F; \text{existuje okolie } U \text{ bodu } X \text{ také, že } |U \cap F| \le \aleph_0\}.$$

Všimnime si, že pre každé $x \in F \setminus H$ a pre každú otvorenú podmnožinu U priestoru X platí

$$|(F \setminus H) \cap U| > \aleph_0.$$

Množina H je spočítateľná. Je to totiž zjednotenie množín tvaru $U \cap F$, ktorých je spočítateľne veľa – máme totiž spočítateľnú bázu topológie – a každá z nich má iba spočítateľne veľa prvkov.

Zadefinujeme najprv funkcie $f\colon T \to F \setminus H$ a $g\colon T \to \mathcal{T} \setminus \{\emptyset\}$ nasledovne: Funkčné hodnoty $f(s)$ aj $g(s)$ budeme definovať indukciou vzhľadom na dĺžku s.

Nech $f(\emptyset)$ je ľubovoľný bod z $F \setminus H$ a $g(\emptyset)$ je jeho okolie s priemerom nanajvýš 1.

Ak už máme definované $f(s)$ a $g(s)$, tak $f(s\hat{}i)$, $i \in \{0,1\}$, zvolíme tak, aby platilo:

- $f(s\hat{}i) \in g(s\hat{}i) \subseteq g(s)$;
- priemer $\overline{g(s\hat{}i)}$ je nanajvýš $2^{-l(s)}$;
- $\overline{g(s\hat{}0)} \cap \overline{g(s\hat{}1)} = \emptyset$.

Vieme, že množina $(F \setminus H) \cap g(s)$ je nespočítateľná, čo nám umožňuje v indukčnom kroku zvoliť dva rôzne body $f(s\hat{}0), f(s\hat{}1) \in g(s)$. (Vieme, že $F \cap g(s)$ je nespočítateľná. Keďže H je spočítateľná množina, tak aj $(F \cap g(s)) \setminus H$ je nespočítateľná.)

Pre každú vetvu $x \in [T]$ potom máme postupnosť do seba zapadajúcich otvorených množín $g(x|n)$ s klesajúcim polomerom. Z úplnosti vyplýva, že prienik je neprázdny. Navyše, keďže polomery konvergujú k nule, musí byť jednobodový. Dostávame teda pre každú vetvu jediný bod, ktorý označíme $G(x)$.

Ďalej vidíme, že $d(G(x), f(x|n)) \leq 2^{-n}$, lebo oba body ležia v množine $g(x|n)$ polomeru nanajvýš 2^{-n}. To znamená, že postupnosť $f(x|n)$ konverguje k $G(x)$. Z uzavretosti množiny F teda potom dostaneme, že aj $G(x) \in F$.

Zobrazenie G je aj injektívne. Ak totiž $x, y \in T$, $x \neq y$ tak pre nejaké n platí $x|n \neq y|n$. Body $G(x)$ a $G(y)$ potom patria do disjunktných množín $\overline{g(x|n)}$ a $\overline{g(y|n)}$. □

Spôsobom použitým v predchádzajúcom dôkaze by sa dalo dokázať dokonca o čosi silnejšie tvrdenie: Nespočítateľná uzavretá podmnožina separabilného metrického priestoru obsahuje podpriestor homeomorfný s Cantorovou množinou. Pozri napríklad [Ke, Theorem 6.2].

Ďalší súvisiaci výsledok je Cantor-Bendixsonova veta, ktorá hovorí, že každý úplný separabilný metrický priestor X sa dá napísať ako $X = P \cup C$, kde P je perfektná[8] podmnožina a C je spočítateľná otvorená podmnožina. Pozri napríklad [Ke, Theorem 6.4].

Poznámka 6.2.6. Na výsledok uvedený vo vete 6.2.5 sa dá pozerať aj tak, že pre uzavreté podmnožiny $\mathbb{R}$ „platí hypotéza kontinua“; t.j. ak sú nekonečné, môžu nadobúdať iba kardinality $\aleph_0$ a $\mathfrak{c}$.

Ak by sme navyše vedeli, že úplne metrizovateľné podmnožiny $\mathbb{R}$ sú práve G_δ množiny, tak takýmto spôsobom môžeme rozšíriť platnosť hypotézy kontinua aj na tieto množiny. (Toto je dôsledok Lavrentieovej vety, [Ke, Theorem 3.11]).

V skutočnosti sa dá ukázať aj o niečo viac. Pre každú nekonečnú borelovskú podmnožinu $\mathbb{R}$ platí, že jej kardinalita je buď $\aleph_0$ alebo $\mathfrak{c}$.

6.2.4 Veta o kompaktnosti

Ako prvú ukážku použitia Königovej lemy dokážeme vetu o kompaktnosti pre výrokovú logiku.

Pripomeňme si niektoré základné pojmy.

Pracujeme teraz s jazykom, v ktorom sa používajú iba logické spojky a premenné; prípadne pomocné znaky – zátvorky. (Premenné zastupujú výroky, ktorým je možné prisudzovať pravdivostnú hodnotu.) Nepoužívame teda kvantifikátory ani symbol rovnosti. Na predmete **Teória množín a matematická logika** sa stretnete aj s vetou o kompaktnosti pre logiku prvého rádu; pre účely ilustrácie použitia výsledku, ktorý sme sa práve naučili, je však azda výhodnejšie ukázať si ho na niečom čo najjednoduchšom. (Okrem iného aj preto, aby sme nemuseli opakovať priveľa pojmov.)

Pomocou logických spojok a premenných vieme zostavovať *výrokové formy* nad danou množinou premenných. Ak si navyše zvolíme nejakú množinu premenných, môžeme si zvoliť aké im priradíme pravdivostné hodnoty. Z nich vieme dostať aj pravdivostnú hodnotu

[8] Podmnožinu topologického priestoru voláme *perfektná*, ak je to uzavretá množina bez izolovaných bodov

ľubovoľnej výrokovej formy obsahujúcej iba tieto premenné. Takéto priradenie sa nazýva *interpretácia.* (Keby sme chceli definovať tieto pojmy poriadne, postupovali by sme indukciou na dĺžku formúl, resp. *štrukturálnou indukciou.*[9])

Definícia 6.2.7. Majme danú množinu premenných P a označme ako $VF(P)$ množinu všetkých výrokových foriem nad množinou premenných P.

Ľubovoľnú podmnožinu $T \subseteq VF(P)$ budeme nazývať *teóriou.*

Teória T sa nazýva *splniteľná,* ak existuje interpretácia $I\colon VF(P) \to \{0,1\}$, pri ktorej majú všetky výrokové formuly z T pravdivostnú hodnotu 1.

Príklad 6.2.8. Uvažujeme premenné $P = \{a, b, c\}$.

Potom napríklad teória $T = \{a \wedge b \wedge c\}$ je splniteľná, pretože môžeme zvoliť interpretáciu takú, že $I(a) = I(b) = I(c) = 1$.

Jednoduchý príklad teórie, ktorá nie je splniteľná, je $T = \{a, \neg a\}$, keďže výroky a a $\neg a$ majú pri každej interpretácii opačné pravdivostné hodnoty. Podobným príkladom je teória $T = \{a \wedge \neg a\}$.

Ukázali sme si iba veľmi jednoduché príklady, kde okamžite vidíme ako je to so splniteľnosťou danej teórie. Uvedomme si však, že množiny P aj T môžu byť aj nekonečné a v takých situáciách situácia môže byť komplikovanejšia.

Veta o kompaktnosti vlastne hovorí to, že keď nás zaujíma splniteľnosť nejakej teórie, stačí sa pozerať iba na konečné časti tejto teórie.

Veta 6.2.9 (Veta o kompaktnosti)**.** *Nech P je* spočítateľná *množina premenných a $T \subseteq VF(P)$ je nejaká teória.*

Ak je každá konečná podmnožina $T_0 \subseteq T$ splniteľná, tak je splniteľná aj teória T.

Inými slovami môžeme túto vetu sformulovať tak, že ak pre každú konečnú množinu výrokových foriem $T_0 \subseteq T$ patriacich do teórie, ktorou sa zaoberáme, máme interpretáciu, pre ktorú sú všetky formuly z T_0 pravdivé, tak existuje taká interpretácia pre T. Čiže táto veta nám dáva prostriedok pomocou ktorého z vhodných interpretácii pre konečné podteórie teórie T vieme „pozošívať“ dokopy jednu interpretáciu pre celú teóriu (ktorá už môže byť aj nekonečná).

Dôkaz. □

6.2.5 Ramseyova veta

V tejto časti dokážeme s použitím stromov Ramseyovu vetu. Táto veta sa týka ofarbovania objektov rôznymi farbami. Spomenieme viacero verzií tejto vety – budú sa líšiť tým, či ofarbujeme konečne alebo nekonečne veľa objektov a tiež počtom použitých farieb.

Začnime najprv s verziou, kde budeme dvoma farbami ofarbovať hrany medzi prirodzenými číslami.

[9] Množina výrokových foriem je definovaná tak, že začneme so základných formúl – obsahujúcich iba jedinú premennú – a indukciou z nich vytvárame nové formuly. Ak chceme definovať nejakú funkciou na všetkých výrokových formulách, tiež môžeme postupovať od najjednoduchších k zložitejším. Potrebujeme na to vedieť, ako je táto funkcia definovaná pre premenné a ako ju definujeme pre formulu odvodenú z jednoduchších formúl pomocou nejakej logickej spojky. Podobný prístup sa dá použiť ak dokazujeme nejaké tvrdenie o všetkých výrokových formulách. Veci takéhoto typu – kde máme nejaké objekty definované indukciou od najjednoduchších po zložitejšie – sa vyskytujú v matematike častejšie. Definície, konštrukcie, či dôkazy takéhoto charakteru – kde induktívne postupujeme od jednoduchších štruktúr k zložitejším – sa zvyknú označovať ako štrukturálna indukcia.

Pre ľubovoľnú množinu A budeme označovať ako $[A]^2$ množinu všetkých dvojprvkových podmnožín množiny A. Podobne $[A]^n$ označuje systém všetkých n-prvkových podmnožín A.

Ramseyovu vetu môžeme vysloviť napríklad v takejto podobe:

Veta 6.2.10 (Ramseyova veta – nekonečná verzia)**.** *Majme ľubovoľné zobrazenie $\pi\colon [\mathbb{N}]^2 \to \{0,1\}$. Potom existuje nekonečná podmnožina A množiny $\mathbb{N}$ taká, že zobrazenie π je na množine H konštantné.*

Pokúsme sa ešte túto vetu preformulovať o čosi názornejšie – snáď bude potom jasnejšie, čo táto veta hovorí. Zobrazenie π priradí každej neusporiadanej dvojici prirodzených čísel nulu alebo jednotku. Môžeme si to predstaviť tak, že sme všetky prirodzené čísla pospájali hranami (každá dvojprvková množina predstavuje jednu hranu) a hrany tohoto nekonečného kompletného grafu sme očíslovali číslami 0 a 1. Samozrejme, namiesto čísel nula a jedna si môžeme prestaviť, že sme ich ofarbili dvoma farbami, napríklad bielou a čiernou.

Uvedená veta potom hovorí, že pri každom ofarbení existuje nekonečná jednofarebná množina. (Teda buď nekonečná množina vrcholov a taká, že každá hrana medzi nimi je tej istej farby.)

Veta 6.2.11 (Ramseyova veta – nekonečná verzia)**.** *Ak máme všetky dvojprvkové podmnožiny $\mathbb{N}$ ofarbené dvoma farbami, tak existuje nekonečná monochromatická podmnožina.*

Dôkaz, ktorý uvedieme, bude spočívať v tom, že vytvoríme vhodný podstrom stromu $\{0,1\}^{<\omega}$ a keď sa v ňom podarí nájsť nekonečnú vetvu, tak z nej budeme nejako vedieť dostať hľadanú jednofarebnú podmnožinu. Podobný dôkaz môžete nájsť napríklad v [Bu2, Problém 1Fc].

Dôkaz. Predpokladajme, že máme zobrazenie $c\colon [\mathbb{N}]^2 \to \{0,1\}$. (Môžeme si predstaviť hrany medzi prirodzenými číslami ofarbené dvomi farbami, nech napríklad 0 predstavuje červenú a 1 modrú farbu.)

Označme $T = \{0,1\}^{<\omega}$; t.j. T je nekonečný binárny strom.

Indukciou budeme postupne konštruovať zobrazenie $f\colon \mathbb{N} \to T$ a prirodzené čísla a_s pre všetky $s \in f[\mathbb{N}]$. Aby bola jasnejšia myšlienka dôkazu, prv než budeme robiť indukčný krok, pozrieme sa

1° Položme $a_\varepsilon = 0$ a $f(a_\varepsilon) = f(0) = \varepsilon$, t.j. nulu zobrazíme na koreň stromu.

Označme ako A_0 množinu tých prirodzených čísel, do ktorých ide z 0 červená hrana a ako A_1 množinu tých vrcholov, do ktorých ide z 0 modrá hrana. Očividne $A_0 \cup A_1$ je presne množina všetkých; pre ktoré ešte nie je definovaná hodnota f. Tiež vidíme, že aspoň jedna z týchto dvoch množín je neprázdna.

Ak je A_0 neprázdna, tak zvolíme $a_0 = \min A_0$ a $f(a_0) = (0)$, podobne $a_1 = \min A_1$ a $f(a_1) = (1)$. (Aspoň jedna z týchto množín je neprázdna, čiže sme zadefinovali hodnotu funkcie f aspoň pre jedno ďalšie prirodzené číslo. Niektorý z prvkov a_0, a_1 mohol zostať nezadefinovaný.)

Teraz budeme definovať, ktoré prvky sa zobrazia na vrcholy stromu v druhej úrovni. Opäť si vezmeme množiny:

$A_{00} =$tie prvky z A_0, ktoré sú s a_0 spojené hranou červenej farby

$A_{01} =$tie prvky z A_1, do ktorých ide z a_0 modrá hrana

A_{10} a A_{11} sú prvky z A_1 rozdelené podľa farby hrany idúcej z a_1. (Ak niektorý z prvkov a_0, a_1 bol nedefinovaný, zostala príslušná množina prázdna.)

Všimnime si, čo vieme povedať napríklad o prvkoch množiny A_{10}. Pretože $A_{10} \subseteq A_1$, do každého prvku v A_1 ide z a_ε hrana farby 1 (červená). Do každého takého prvku ide z a_1 hrana farby 1 (modrá).

Opäť položíme $a_{ij} = \min A_{ij}$ (ak je táto množina neprázdna) a $f(a_{ij}) = (ij)$.

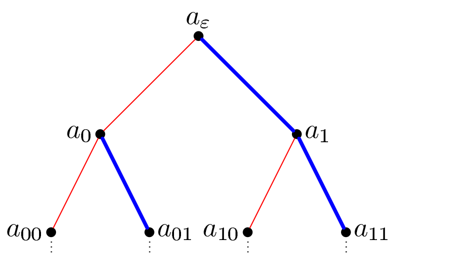
2° Keď sme si ukázali ako začneme konštruovať našu funkciu f, tak indukčný krok by mohol byť pomerne jasný.

Predpokladáme, že už máme zadefinované A_s pre všetky postupnosti $s \in \{0,1\}^n$, t.j. pre postupnosti núl a jednotiek dĺžky n. Pomocou nich máme zadefinované a_s v prípade, že $A_s \neq \emptyset$ a máme aj zadefinovanú hodnotu $f(a_s) = s$.

Pomocou nich definujeme $A_{s\hat{}0}$ a $A_{s\hat{}1}$ tak, že $A_{s\hat{}0}$ sú čísla, pre ktoré ide do a_s hrana farby 0 a $A_{s\hat{}1}$ budú tie, ktoré sú s a_s spojené hranou farby 1. (Definujeme ich iba pre tie s, pre ktoré $A_s \neq \emptyset$, teda iba ak a_s bolo definované.) Položíme $a_{s\hat{}i} = \min A_{s\hat{}i}$ a $f(a_{s\hat{}i}) = s\hat{}i$.

Pomerne ľahko sa dá skontrolovať, že pri takejto indukcii budú v n-tom kroku (t.j. keď pracujeme s postupnosťami dĺžky najviac n) splnené tieto podmienky:

- Hodnoty funkcie f sú zadefinované pre všetky čísla z $\{1, 2, \dots, n\}$.
- Množiny A_s pre postupnosti dĺžky n obsahujú presne tie čísla, pre ktoré sme zatiaľ nezadefinovali funkčnú hodnotu.
- Všetky doteraz zadefinované funkčné hodnoty sú postupnosti dĺžky najviac n.
- Ak máme postupnosť dĺžky n tvaru $s = u\hat{}0\hat{}v$, tak z a_u do a_s ide hrana farby 0. Podobne ak $s = u\hat{}1\hat{}v$, tak z a_u ide do a_s hrana farby 1.



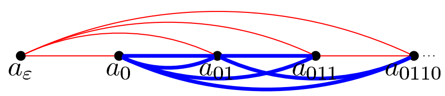
{stromy:FIGRAMSTROM} Obr. 6.1: Strom skonštruovaný v dôkaze Ramseyovej vety

Dostali sme takto nejakú injektívnu funkciu $f\colon \mathbb{N} \to T$, pričom z konštrukcie je jasné, že $f[\mathbb{N}]$ je strom. (Je to množina uzavretá na počiatočné úseky.) Obrázok 6.1 ilustruje, ako by mohol tento strom vyzerať.

Z injektívnosti f vyplýva, že $f[\mathbb{N}]$ musí mať kardinalitu aspoň $\aleph_0$, je to teda nekonečný strom.

Königova lema nám potom hovorí, že tento strom má nejakú nekonečnú vetvu. T.j. existuje taká nekonečná postupnosť $s \in \{0,1\}^\omega$, že $s|_n \in T$ pre každé n.

Táto postupnosť obsahuje nekonečne veľa núl alebo nekonečne veľa jednotiek. Bez ujmy na všeobecnosti nech nastane prvá možnosť.



{stromy:FIGRAMVETVA} Obr. 6.2: Vrcholy v nekonečnej vetve

Zoberme si tie konečné podpostupnosti, ktoré končia nulou. T.j. máme nekonečne veľa podpostupností s tvaru $u\hat{}0$, kde u je nejaká konečná postupnosť. Z našej induktívnej konštrukcie vyplýva, že pre ľubovoľné takéto u a v sú čísla a_u a a_v spojené hranou farby 0. Teda množina

$$\{a_u; u\hat{}0 = s|_n \text{ pre nejaké } n \in \omega\}$$

je hľadaná monochromatická podmnožina $\mathbb{N}$. (Pozri aj obrázok 6.2.) $\square$

Ak ste sa už s Ramseyovou vetou, pravdepodobne ste videli trochu inú verziu. (Mohli ste sa ju učiť napríklad na predmete **Kombinatorika**.)

Veta 6.2.12 (Ramseyova veta – konečná verzia)**.** *Pre ľubovoľné čísla r, s existuje prirodzené číslo N také, že pri ľubovoľnom ofarbení kompletného grafu K_N červenou a modrou farbou buď existuje kompletný červený podgraf na r vrcholoch alebo existuje kompletný modrý podgraf na s vrcholoch.*

Najmenšie N s touto vlastnosťou sa nazýva Ramseyove číslo *a označuje sa $R(r, s)$.*

Výpočet presnej hodnoty $R(r, s)$ pre väčšie čísla je pomerne ťažká úloha. V tomto okamihu nás zaujíma iba existencia týchto čísel, takže pre naše účely bude rovnako vhodná nasledujúca verzia Ramseyovej vety. (Nie je ťažké si uvedomiť, že obe konečné verzie, ktoré uvádzame, sú ekvivalentné.)

Veta 6.2.13. *Pre ľubovoľné prirodzené číslo n existuje prirodzené číslo N také, že pri ľubovoľnom ofarbení kompletného grafu K_N dvoma farbami existuje monochromatická n-prvková podmnožina.*

Už sme si dokázali nekonečnú verziu Ramseyovej vety. Teraz si ukážeme ako z nej vyplýva konečná verzia. Opäť bude pri tom užitočná Königova lema.

Dôkaz. Ukážeme, ako z nekonečnej verzie Ramseyovej vety vyplýva konečná. Budeme postupovať nepriamo, teda budeme predpokladať, že neplatí konečná verzia Ramseyovej vety a budeme sa snažiť dokázať, že neplatí ani nekonečná verzia.

Ak neplatí konečná verzia, znamená to, že existuje číslo n také, že pre každé N existuje ofarbenie množiny $\{1, 2, \dots, N\}$, pri ktorom nemáme n-prvkovú monochromatickú množinu.

Skonštruujeme strom $T \subseteq \omega^{<\omega}$ zodpovedajúci „vhodným“ ofarbeniam konečných úsekov $\{0, 1, 2, \dots, N\}$.

Pre každé prirodzené číslo N máme N dvojprvkových množín obsahujúcich N a nejaké menšie prirodzené číslo. Teda pre každé ofarbenie hrán medzi prvkami $\{0, 1, \dots, N-1\}$ máme práve 2^N možností, ako môžeme rozšíriť toto ofarbenie na ofarbenie množiny $\{0, 1, \dots, N\}$. Môžeme si ho nejako očíslovať a potom máme ofarbenia hrán medzi číslami $0, 1, \dots, N$ zakódované konečnými postupnosťami prirodzených čísel. Všimnime si, že na N-tom mieste sa nevyskytne číslo väčšie ako 2^N.

TODO – dokončiť dôkaz (vytvárame strom obsahujúci ofarbenia, kde nemáme n-prvkovú monochromatickú množinu) $\square$

Na prvý pohľad by sa mohlo zdať, že uvedený dôkaz je zbytočne zložitý – veď predsa ak vieme o existencii nekonečnej monochromatickej množiny, tak musí existovať aj monochromatická množina veľkosti n, či nie? Necháme na čitateľa, aby si rozmyslel, prečo takáto jednoduchá úvaha neprejde (úloha 6.2.2).

TODO Prechod k viacerým farbám

Cvičenia

Úloha 6.2.1. Ukážte, že obe konečné verzie Ramseyovej vety, ktoré sme uviedli, sú skutočne ekvivalentné.

{stromycvic:ULONETRIV}

Úloha 6.2.2. Vysvetlite, prečo nie je implikácia hovoriaca, že z nekonečnej verzie Ramseyovej vety vyplýva konečná, jasná na prvý pohľad.

Problémy

6.3 Ultrafiltre

{ultra:SECTUL

V tejto časti sa chceme venovať ultrafiltrom. Ultrafiltre majú veľa užitočných aplikácií, s niektorými ste sa mohli strenúť na predmetoch **Teória množín a matematická logika** a **Všeobecná topológia**.

Najprv si poviem niekoľko základných faktov o filtroch a ultrafiltroch, potom si ukážeme aj nejaké aplikácie.

6.3.1 Základné definície

{ultra:DEFFILTER}

Definícia 6.3.1. Nech M je ľubovoľná množina. Neprázdny systém $\mathcal{F} \subseteq \mathcal{P}(M)$ sa nazýva *filter* na množine M, ak

(i) $A, B \in \mathcal{F} \Rightarrow A \cap B \in \mathcal{F}$;
(ii) $A \in \mathcal{F}$, $A \subseteq B \Rightarrow B \in \mathcal{F}$;
(iii) $\emptyset \notin \mathcal{F}$.

Filter $\mathcal{F}$ nazveme *voľný,* ak $\bigcap \mathcal{F} \neq \emptyset$.

Stručne povedané; filter je taká podmnožina $\mathcal{P}(M)$, ktorá je uzavretá vzhľadom na prieniky a nadmnožiny. Navyše sa ešte chceme vyhnúť triviálnym prípadom, preto požadujeme, aby množina $\mathcal{F}$ obsahovala aspoň jednu množinu (ekvivalentne by sme mohli požadovať $M \in \mathcal{F}$) a tiež aby neobsahovala prázdnu množinu (čím vylúčime prípad $\mathcal{F} = \mathcal{P}(M)$).

Príklad 6.3.2. *Fréchetov filter* na nekonečnej množine M je filter pozostávajúci z kofinitných množín, t.j.

$$\mathcal{F}_0(M) = \{A \subseteq M; M \setminus A \text{ je konečná množina.}\}$$

V prípade $M = \omega$ ho označujeme $\mathcal{F}_0$. Tento filter je voľný.

Pre ľubovoľnú neprázdnu množinu $A \subseteq M$ môžeme definovať

$$\mathcal{F} = \{B \subseteq M; B \supseteq A\}.$$

Ľahko sa overí, že $\mathcal{F}$ je filter, ktorý nie je voľný, keďže $\bigcap \mathcal{F} = A$.

Často filter zadefinujeme tak, že povieme, akými množinami je generovaný.

{ultra:DEFBAZA}

Definícia 6.3.3. Nech M je ľubovoľná množina a $\mathcal{B} \subseteq \mathcal{P}(M)$ je nejaký neprázdny systém jej podmnožín. Množina $\mathcal{B}$ sa nazýva *báza filtra* ak

(i) $\emptyset \notin \mathcal{B}$.
(ii) Pre ľubovoľné $A, B \in \mathcal{B}$ existuje $C \in \mathcal{B}$ také, že $C \subseteq A \cap B \in$.

Ľahko vidno, že ak $\mathcal{B}$ je báza filtra na množine M, tak z nej môžeme dostať filter tak, že vezmeme všetky nadmnožiny.

$$\mathcal{F} = \{A \subseteq M; (\exists B \in \mathcal{B}) B \subseteq A\}$$

{ultra:DEFULTRA}

Definícia 6.3.4. Filter $\mathcal{F}$ na množine M sa nazýva *ultrafilter,* ak pre ľubovoľné $A \subseteq M$ patrí do $\mathcal{F}$ množina A alebo jej doplnok $M \setminus A$.

$$(\forall A \subseteq M) A \in \mathcal{F} \vee M \setminus A \in \mathcal{F}$$

Ultrafiltre sú presne maximálne filtre vzhľadom na inklúziu (problém 4.3.7). Ekvivalentne sa ultrafiltre dajú charakterizovať ešte aj tak, že pre ľubovoľné dve množiny ktorých zjednotenie je celé M platí, že niektorá z nich patrí od $\mathcal{F}$ (cvičenie 6.3.1).

Príklad 6.3.5. Ako jednoduché príklady ultrafiltrov spomeňme *hlavné ultrafiltre.* Ak M je ľubovoľná množina a $a \in M$, tak

$$\mathcal{F}_a = \{A \subseteq M; a \in A\}$$

je ultrafilter na množine M. Ľahko sa tiež overí, že každý ultrafilter na M, ktorý nie je voľný, musí mať takýto tvar.

Síce nevieme explicitne popísať príklad voľného ultrafiltra; s využitím axiómy výberu však vieme dokázať, že existujú aj voľné ultrafiltre.

{ultra:DEFCENTRO}

Definícia 6.3.6. Systém množín $\mathcal{S}$ sa nazýva *centrovaný systém*[10] množín ak každý konečný podsystém $\mathcal{S}$ má neprázdny prienik.

Príklad 6.3.7. Každý filter je centrovaný systém množín. Takisto je centrovaným systémom aj každá báza filtra.

Veta 6.3.8. *Pre každý centrovaný systém $\mathcal{S} \subseteq \mathcal{P}(M)$ existuje ultrafilter na množine M, ktorý ho obsahuje.*

Dôkaz. Pomocou Zornovej lemy (problém 4.3.7). □

Ak použijeme predchádzajúcu vetu na Fréchetov filter $\mathcal{F}_0(M)$, tak dostaneme:

Dôsledok 6.3.9. *Pre každú nekonečnú množinu M existuje voľný ultrafilter na množine M.*

Poznámka 6.3.10.

6.3.2 $\mathcal{F}$-limity

{ultra:DEFFLIM}

Definícia 6.3.11. Nech $\mathcal{F}$ je filter množine M a X je topologický priestor. Hovoríme, že funkcia $f\colon M \to X$ je *$\mathcal{F}$-konvergentná k $x \in X$,* alebo že x je *$\mathcal{F}$-limita* funkcie f, ak

$$f^{-1}[U] = \{s \in S; f(s) \in U\} \in \mathcal{F}$$

platí pre každé okolie U bodu x.

Označujeme

$$\mathcal{F}\text{-}\lim f = x.$$

Definíciu $\mathcal{F}$-limity môžeme prepísať ako

$$(\forall U \in \mathcal{N}(x)) f^{-1}[U] \in \mathcal{F},$$

kde $\mathcal{N}(x)$ označuje množinu všetkých okolí bodu x; môžeme si všimnúť, že $\mathcal{N}(x)$ je tiež filter.

V tejto prednáške budeme potrebovať iba $\mathcal{F}$-limity (ohraničených) reálnych postupností, t.j. prípad $M = \mathbb{N}$ a $X = \mathbb{R}$ alebo X je ohraničený uzavretý interval v $\mathbb{R}$. Napriek tomu som uviedol všeobecnejšiu definíciu z viacerých dôvodov. Jeden dôvod je zjednodušenie označenia; napríklad zápis $f^{-1}[U]$ sa zdá byť prirodzenejší pre funkciu než pre postupnosť (aj keď postupnosť chápeme ako zobrazenie z množiny $\mathbb{N}$). Tiež si myslím, že ak sa nejaké tvrdenie dá sformulovať všeobecnejšie a nevyžiada si to zmenu dôkazu ani zavedenie nových pojmov, treba ho sformulovať všeobecnejšie. Ďalší dôvod je, že takto dostaneme spoločné zovšeobecnenie dvoch veľmi dôležitých typov konvergencie, o ktorých by ste sa mali dozvedieť na predmetoch **Všeobecná topológia 1, 2**.

[10] V angličtine: *finite intersection property.*

{POZNFLIMNETS}

Poznámka 6.3.12. Jeden z dôležitých pojmov vo všeobecnej topológii je konvergencia sietí. Sieť je zobrazenie $x\colon D \to X$, kde D je nahor usmernená množina a X je topologický priestor. Vcelku ľahko sa overí, že množiny tvaru

$$D_a = \{d \in D; d \geq a\}$$

(horné úseky) tvoria bázu filtra na D. Konvergencia sietí je presne konvergencia z definície 6.3.11.

Ďalší typ konvergencie, ktorý sa často používa, môžeme dostať tak, že v definícii 6.3.11 vezmeme $M = X$. (T.j. filter $\mathcal{F}$ je priamo filter na topologickom priestore, s ktorým pracujeme.)

Je známe, že oba tieto typy konvergencie úplne popisujú štruktúru topologického priestoru a dajú sa pomocou nich charakterizovať mnohé dôležité vlastnosti topologických priestorov.

Viac o $\mathcal{F}$-limitách v takejto všeobecnosti sa môžete dozvedieť napríklad v [Sl5]. Limita vzhľadom na bázu filtra je používaná ako základný typ konvergencie v učebnici [D].

Pre nás bude dôležitý hlavne špeciálny prípad reálnych postupností.

{ultra:DEFFLIMR}

Definícia 6.3.13. Nech $(x_n)_{n=0}^{\infty}$ je postupnosť reálnych čísel a $\mathcal{F}$ je filter na množine $\mathbb{N}$. Potom $L \in \mathbb{R}$ je *$\mathcal{F}$-limita* postupnosti x_n, ak pre každé $\varepsilon > 0$ platí

$$x^{-1}[(L-\varepsilon, L+\varepsilon)] = \{n \in \mathbb{N}; |x_n - L| < \varepsilon\} \in \mathcal{F}$$

Keď porovnáme uvedenú definíciu s obvyklou definíciou limity postupnosti, tak vidíme, že je tu istá podobnosť. Pri obvyklej definícii limity požadujeme, aby množina indexov, pre ktoré sú členy postupnosti blízko k L, obsahovala všetky prirodzené čísla až na konečne veľa výnimiek. Definícia $\mathcal{F}$-limity tiež žiada, aby táto množina bola v nejakom zmysle veľká – v tomto prípade je podmienka, že ide o „veľkú“ množinu, vyjadrená tým, že musí patriť do $\mathcal{F}$.

Vcelku prirodzeným spôsobom by sme pre reálne postupnosti vedeli definovať aj kedy $\mathcal{F}\text{-}\lim x_n = \infty$ a $\mathcal{F}\text{-}\lim x_n = -\infty$.

Pozrime sa zatiaľ na dva veľmi jednoduché špeciálne prípady.

Príklad 6.3.14. Pre Fréchetov filter $\mathcal{F}_0$ dotaneme presne obvyklú konvergenciu, t.j.

$$\mathcal{F}_0\text{-}\lim x_n = \lim x_n.$$

(Táto rovnosť je uvedená v zmysle: Limita na ľavej strane existuje práve vtedy, keď existuje limita na pravej strane rovnosti. V takom prípade sa obe limity rovnajú.)

Ak $a \in \mathbb{N}$, tak pre hlavný ultrafilter $\mathcal{F}_a$ máme

$$\mathcal{F}_\text{a}\text{-}\lim x_n = x_a.$$

{ultra:TVRZAKLD}

Tvrdenie 6.3.15. *Nech $(x_n)_{n=0}^{\infty}$, $(y_n)_{n=0}^{\infty}$ sú reálne postupnosti $c \in \mathbb{R}$ and $\mathcal{F}$ je filter na množine $\mathbb{N}$.*

(i) *Ak $\mathcal{F}\text{-}\lim x_n$ a $\mathcal{F}\text{-}\lim y_n$ existujú, tak existuje aj $\mathcal{F}$-limita postupnosti $(x_n+y_n)_{n=0}^{\infty}$ a platí*
$$\mathcal{F}\text{-}\lim(x_n+y_n) = \mathcal{F}\text{-}\lim x_n + \mathcal{F}\text{-}\lim y_n.$$

(ii) *Ak existuje $\mathcal{F}\text{-}\lim x_n$, tak existuje aj $\mathcal{F}$-limita postupnosti $(cx_n)_{n=0}^{\infty}$ a platí*

$$\mathcal{F}\text{-}\lim(cx_n) = c\,\mathcal{F}\text{-}\lim x_n.$$

(iii) *Ak existujú* $\mathcal{F}\text{-}\lim x_n$ *a* $\mathcal{F}\text{-}\lim y_n$*, tak existuje aj* $\mathcal{F}$*-limita postupnosti* $(x_n y_n)_{n=0}^{\infty}$ *a platí*

$$\mathcal{F}\text{-}\lim(x_n y_n) = \mathcal{F}\text{-}\lim x_n \cdot \mathcal{F}\text{-}\lim y_n.$$

(iv) *Ak* $A \in \mathcal{F}$ *je nekonečná množina a* $\lim\limits_{n\in A} x_n = L$ *existuje, tak* $\mathcal{F}$*-limita tiež existuje a má rovnakú hodnotu*

$$\mathcal{F}\text{-}\lim x_n = \lim_{n\in A} x_n.$$

(v) *Ak* $\mathcal{F}$ *je voľný filter a* $(x_n)_{n=0}^{\infty}$ *je konvergentná postupnosť, tak*

$$\mathcal{F}\text{-}\lim x_n = \lim_{n\to\infty} x_n.$$

(vi) *Nech* $\mathcal{F}$ *je voľný filter a* $\mathcal{F}\text{-}\lim x_n$ *existuje. Potom* $\mathcal{F}\text{-}\lim x_n$ *je hromadným bodom postupnosti* $(x_n)_{n=0}^{\infty}$*. Obrátene, pre každý hromadný bod* L *postupnosti* $(x_n)_{n=0}^{\infty}$ *existuje voľný ultrafilter taký, že* $\mathcal{F}\text{-}\lim x_n = L$*.*

(vii) *Ak* $x_n \geq y_n$ *pre každé* n *a obe postupnosti sú* $\mathcal{F}$*-konvergentné, tak* $\mathcal{F}\text{-}\lim x_n \geq \mathcal{F}\text{-}\lim y_n$*. Špeciálne,* $\mathcal{F}\text{-}\lim x_n \geq 0$ *pre každú postupnosť takú, že* $x_n \geq 0$*.*

Dôkaz. □

{ultra:VTKOMPAKT}

Veta 6.3.16. *Nech* $\mathcal{F}$ *je ultrafilter na množine* M*,* X *je kompaktný priestor* $f\colon M \to X$ *je zobrazenie. Potom* $\mathcal{F}\text{-}\lim f$ *existuje. (Presenejšie povedané, existuje aspoň jedna* $\mathcal{F}$*-limita.)*

Formulácia, že existuje aspoň jedna limita, je uvedená v predošlej vete preto, že $\mathcal{F}$-limita nemusí byť vo všeobecnosti určená jednoznačne. Ak je však priestor X Hausdorffovský, tak funkcia $f\colon M \to X$ môže mať najviac jednu $\mathcal{F}$-limitu – úloha 6.3.3. Čiže v situáciách, ktoré tu budeme potrebovať, máme jednoznačnosť $\mathcal{F}$-limity zaručenú.

Dôkaz. Sporom. Predpokladajme, že by žiadny bod $x \in X$ nebol $\mathcal{F}$-limitou funkcie f. Teda pre každé x existuje okolie U_x také, že

$$f^{-1}[U_x] \notin \mathcal{F}.$$

Z kompaktnosti vyplýva existencia konečného podpokrytia pokrytia $\{U_x; x \in X\}$.

Označme množiny patriace do tohoto konečného podpokrytia ako $U_1, \dots, U_n$. Pre každé $i = 1, \dots, n$ platí $f^{-1}[U_i] \notin \mathcal{F}$. Pretože $\mathcal{F}$ je ultrafilter, znamená to, že $f^{-1}[X \setminus U_i] \in \mathcal{F}$.

Platí $\bigcap_{i=1}^{n}(X \setminus U_i) = \emptyset$, pretože $U_1, \dots, U_n$ je pokrytie. Z toho dostaneme

$$\bigcap_{i=1}^{n} f^{-1}[X \setminus U_i] = f^{-1}[\bigcap_{i=1}^{n} X \setminus U_i] = \emptyset.$$

Potom ale $\emptyset \in \mathcal{F}$, čo je spor. □

Ako dôsledok dostaneme prípad, ktorý budeme potrebovať my.

{ultra:DOSFLIM}

Dôsledok 6.3.17. *Nech* $(x_n)_{n=0}^{\infty}$ *je reálna ohraničená postupnosť a* $\mathcal{F}$ *je ultrafilter na množine* $\mathbb{N}$*. Potom existuje (jednoznačne určená)* $\mathcal{F}$*-limita* $\mathcal{F}\text{-}\lim x_n$*.*

Dôkaz. Ak $(x_n)_{n=0}^{\infty}$ je ohraničená postupnosť, tak existuje $M \in \mathbb{R}$ také, že $|x_n| \leq M$ pre všetky n. Stačí teda použiť vetu 6.3.16 pre $X = \langle -M, M\rangle$. □

Pokiaľ použijeme rozšírenú definíciu $\mathcal{F}$-limity, kde pripúšťame aj možnosti $\mathcal{F}\text{-}\lim x_n = \infty$ a $\mathcal{F}\text{-}\lim x_n = -\infty$, tak každá reálna postupnosť má $\mathcal{F}$-limity. (Stačí si uvedomiť, že priestor $\mathbb{R} \cup \{\pm\infty\}$ je homeomorfný s $\langle 0, 1\rangle$.)

Ako si ukážeme na niekoľkých príkladoch, $\mathcal{F}$-limity sa často dajú použiť na dôkaz existencie rôznych objektov. Hodia sa v situáciách, keď by sme v dôkaze potrebovali urobiť nejaký limitný proces, nemáme však zaručenú existenciu limity. Poznamenajme, že v niektorých prípadoch by sa v podobných argumentoch namiesto $\mathcal{F}$-limít dala použiť konvergencia sietí.[11]

$\mathcal{F}$-limity patria do ℓ_∞^*

Pozrime sa najprv na to, čo vieme povedať o priestoroch ℓ_1 a ℓ_∞ na základe existencie $\mathcal{F}$-limít.

Pripomeňme, že $\ell_1 = \{x = (x_n)_{n=0}^\infty; \sum\limits_{n=0}^\infty |x_n| < \infty\}$ s normou $\|x\|_1 = \sum\limits_{n=0}^\infty |x_n|$ a $\ell_\infty = \{x = (x_n)_{n=0}^\infty; \sup\limits_{n\in\mathbb{N}} |x_n| < \infty\}$ s normou $\|x\|_\infty = \sup\limits_{n\in\mathbb{N}} |x_n|$ sú Banachove priestory. Tiež je dobre známe $\ell_1^* \cong \ell_\infty$, konkrétne každý funkcionál $f \in \ell_1^*$ sa dá reprezentovať ako

$$x \mapsto \sum_{n=0}^\infty c_n x_n$$

pre nejakú postupnosť $(c_n)_{n=0}^\infty \in \ell_\infty$.

Takisto je pomerne ľahké ukázať, že pre každú postupnosť $(c_n)_{n=0}^\infty \in \ell_1$ zobrazenie

{ultra:EQDUAL}

$$x \mapsto \sum_{n=0}^\infty c_n x_n \tag{6.1}$$

nám dáva prvok z ℓ_∞^*.

Toto je vlastne iba obvyklé vnorenie $X \hookrightarrow X^{**}$ pre $X = \ell_1$. Môžeme sa pýtať, či existujú aj funkcionály patriace do ℓ_∞^*, ktoré majú iný tvar. (Inak povedané, či ℓ_1 je reflexívny priestor.) Existenciu takých funkcionálov môžeme ukázať pomocou napríklad pomocou $\mathcal{F}$-limít. (Inou možnosťou, ktorá sa dá použiť, je Hahn-Banachova veta, úloha 6.3.4.)

{ultra:TVRDUAL}

Tvrdenie 6.3.18. *Existujú funkcionály patriace do ℓ_∞^*, ktoré nemajú tvar uvedený v* (6.1). *Teda priestor ℓ_1 nie je reflexívny.*

Dôkaz. Z dôsledku 6.3.17 vieme, že ak $\mathcal{F}$ je ultrafilter na množine $\mathbb{N}$, tak pre každú ohraničenú postupnosť $x = (x_n)_{n=0}^\infty$ existuje $\mathcal{F}\text{-}\lim x_n$, teda zobrazenie

$$f_\mathcal{F}\colon x \mapsto \mathcal{F}\text{-}\lim x_n$$

je definované pre všetky prvky $x \in \ell_\infty$. Prvé dve podmienky z tvrdenia 6.3.15 nám hovoria, že toto zobrazenie je lineárne. Súčasne, opäť na základe tvrdenia 6.3.15, máme $|\mathcal{F}\text{-}\lim x_n| \leq \|x\|_\infty$; teda toto zobrazenie je spojité s normou 1.

Zistili sme teda, že $f_\mathcal{F} \in \ell_\infty^*$. Zostáva nám ukázať, že tento funkcionál sa nedá reprezentovať pomocou žiadnej postupnosti z ℓ_1 spôsobom uvedeným v (6.1). Vezmime postupnosť $e^{(n)}$ takú, že $e_k^{(n)} = \delta_{nk}$, t.j. postupnosť, ktorá má na n-tom mieste jednotku a na všetkých ostatných nuly. Takáto postupnosť konverguje k nule, preto $f_\mathcal{F}(e^{(n)}) = 0$. Súčasne funkcionál tvaru (6.1) priradí takejto postupnosti číslo c_n, čiže ak by sa $f_\mathcal{F}$ dal reprezentovať takýmto spôsobom, zodpovedala by mu nulová postupnosť a bol by to nulový funkcionál. Keďže $f_\mathcal{F}$ priradí konštantnej postupnosti $\overline{c}$ číslo c, nie je to nulový funkcionál. $\square$

[11] Viacero dôkazov, kde je existencia nejakého objektu ukázaná pomocou $\mathcal{F}$-limít aj pomocou sietí, môžete nájsť tu: `http://thales.doa.fmph.uniba.sk/sleziak/texty/rozne/topo/comparg.pdf`.

tra:POZNDUAL}

Poznámka 6.3.19. Tvrdenie 6.3.18 neplatí v ZF, pozri napríklad [V]. [12] Existujú modely ZF, v ktorých $\ell_1^* = \ell_\infty$.

Toto je podľa mňa pomerne dobrý príklad toho, že aj keď človek pracuje v ZFC, môže byť užitočné vedieť o tom, či tvrdenie platí v ZF alebo používa AC (alebo aspoň nejakú slabšiu formu axiómy výberu). Duálne priestory sú užitočné a keď sa človek chce o nich niečo naučiť, asi sa na ne bude pozerať na nejakých pomerne jednoduchých a pochopiteľných priestoroch, ako sú napríklad ℓ_1 a ℓ_∞. Keď sa dozvie, že existujú funkcionály patriace do $\ell_\infty^* \setminus \ell_1$ (či už je zdôvodnenie pomocou $\mathcal{F}$-limít, pomocou Hahn-Banachovej vety alebo nejaké iné), tak ho možno bude zaujímať, či by vedel napísať aj nejaký konkrétny príklad takého funkcionálu. Fakt, že existencia takýchto funkcionálov sa nedá dokázať v ZF, nám hovorí; že ak sa nejako budeme snažiť dokázať ich existenciu, tak na niektorom mieste v dôkaze budeme potrebovať nejaký nekonštruktívny krok, využiť nejaké existenčné tvrdenie.

Banachove limity

{ultra:SSECTBANLIM}

V tejto časti by sme si chceli povedať niečo o Banachových limitách, ktoré sú iným typom rozšírenia pojmu limity než sú $\mathcal{F}$-limity. Limita vzhľadom na ultrafilter bude však práve nástrojom, ktorý využijeme na dôkaz existencie Banachovej limity. Viac o nich si môžete prečítať napríklad aj v diplomovej práci [Š].

Definujme $S\colon \ell_\infty \to \ell_\infty$ ako $S\colon (x_n)_{n=0}^\infty \mapsto (x_{n+1})_{n=0}^\infty$, t.j. S je operátor posunutia, ktorý postupnosti $(x_0, x_1, x_2, \dots)$ priradí postupnosť $(x_1, x_2, x_3, \dots)$. Jednou zo základných vlastností obvyklej limity postupností je platnosť rovnosti $\lim S(x) = \lim x$ pre každú konvergentnú postupnosť $x = (x_n)_{n=0}^\infty$. Nie všetky postupnosti však majú limitu. Skúsime sa pozrieť na to, či existujú rozšírenia limity, ktoré by spĺňali viaceré prirodzené vlastnosti obvyklej limity, vrátane tejto, ale boli by definované pre všetky ohraničené postupnosti.

{ultra:DEFBANLIM}

Definícia 6.3.20. Hovoríme, že $L \in \ell_\infty^*$ je *Banachova limita*, ak platí
(i) $L(x) \geq 0$ pre každú postupnosť takú, že $x \geq 0$;
(ii) $L(Sx) = L(x)$ pre všetky $x \in \ell_\infty$;
(iii) ak $x = (x_n)_{n=0}^\infty$ je konvergentná postupnosť, tak $L(x) = \lim\limits_{n\to\infty} x_n$.

Stručne môžeme túto definíciu zhrnúť tak, že L je Banachova limita, ak je to lineárny spojitý funkcionál definovaný na ℓ_∞, ktorý je nezáporný, invariantný vzhľadom na posunutie a rozširujúci limitu.

Už vieme, že s výnimkou invariantnosti na posun spĺňala $\mathcal{F}$-limita (kde $\mathcal{F}$ je ultrafilter) všetky vlastnosti z definície Banachovej limity. Limita vzhľadom na ultrafilter však nie je Banachovou limitou. Ak by totiž nejaký funkcionál $L\colon \ell_\infty \to \mathbb{R}$ bol Banachovou limitou a súčasne by bol multiplikatívny, t.j.

$$L(x \cdot y) = L(x) \cdot L(y)$$

pre ľubovoľné $x, y \in \ell_\infty$, tak by sme pre postupnosť $x = (0, 1, 0, 1, \dots)$ dostali $L(x^2) = L(x)$, z čoho vyplýva $x \in \{0, 1\}$; a súčasne $2L(x) = L(x) + L(Sx) = L(\overline{1})$, z čoho dostaneme $L(x) = \frac{1}{2}$.

Vidíme teda, že ak chceme nejako rozšíriť limitu na všetky ohraničené postupnosti, tak funkcionál, ktorý dostaneme, nemôže mať všetky uvedené vlastnosti.

Tvrdenie 6.3.21. *Existuje Banachova limita.*

[12] Pozri aj `http://math.stackexchange.com/questions/55651/nonnegative-linear-functionals-over-l-infty`, `http://mathoverflow.net/questions/22661/explicit-element-of-ell-infty-ell1`

Dôkaz. Nech $\mathcal{F}$ je ľubovoľný ultrafilter na množine $\mathbb{N}$. Definujme $L\colon \ell_\infty \to \mathbb{R}$ ako

$$L(x) = \mathcal{F}\text{-lim}\,\frac{x_0 + \cdots + x_{n-1}}{n}.$$

Ak $x = (x_n)_{n=1}^\infty$ je ohraničená postupnosť, tak aj postupnosť $(\frac{x_0+\cdots+x_{n-1}}{n})_{n=0}^\infty$ jej aritmetických priemerov je ohraničená, preto podľa dôsledku 6.3.17 existuje $\mathcal{F}$-limita. Čiže takto skutočne dostaneme nejaké zobrazenie z ℓ_∞ do $\mathbb{R}$. Potrebujeme už len skontrolovať, či spĺňa podmienky z definície Banachovej limity.

Linearita a spojitosť. Na zobrazenie L sa môžeme pozerať ako na zloženie $\mathcal{F}$-limity (chápanej ako funkcionál z ℓ_∞ do $\mathbb{R}$) a zobrazenia $C\colon \ell_\infty \to \ell_\infty$ definovaného ako

$$C\colon (x_n)_{n=0}^\infty \mapsto \left(\frac{x_0 + \cdots + x_{n-1}}{n}\right)_{n=0}^\infty.$$

Zobrazenie C je očividne lineárne. Z nerovnosti

$$\sup_{n\in\mathbb{N}}\left|\frac{x_0 + \cdots + x_{n-1}}{n}\right| \le \sup_{n\in\mathbb{N}}|x_n|$$

máme $\|Cx\| \le \|x\|$, čo znamená, že C je spojité. V dôkaze tvrdenia 6.3.18 sme už ukázali, že $\mathcal{F}$-limita je lineárny spojitý funkcionál pretože. Preto aj L, ako zloženie dvoch lineárnych a spojitých zobrazení, je lineárne a spojité.

Nezápornosť. TODO

Invariantnosť na posun.

L rozširuje limitu.

□

Poznámka 6.3.22. Na základe rovnakého argumentu ako sme použili v dôkaze tvrdenia 6.3.18 môžeme vidieť, že aj ľubovoľná Banachova limita patrí do $\ell_\infty^* \setminus \ell_1$.

Všimnime si teraz napríklad postupnosť $x = (0, 1, 0, 1, 0, 1, \dots)$, v ktorej sa striedajú nuly a jednotky. Čo by sme vedeli povedať o hodnote $L(x)$, kde L je (ľubovoľná) Banachova limita?

Všimnime si, že $x + Sx = \overline{1}$, t.j., súčet postupnosti x a posunutej postupnosti nám dá konštantnú postupnosť pozostávajúcu zo samých jednotiek. Dostávame preto

$$2L(x) = L(x) + L(Sx) = L(x + Sx) = L(\overline{1}) = 1,$$

a teda

$$L(x) = \frac{1}{2}.$$

Teda pre uvedenú postupnosť platí, že každá Banachova limita nadobúda na tejto postupnosti tú istú hodnotu, v tomto prípade $\frac{1}{2}$.

Podobnú vlastnosť majú samozrejme aj všetky konvergentné postupnosti.

Definícia 6.3.23. Ohraničená postupnosť $x \in \ell_\infty$ sa nazýva *skoro konvergentná* k číslu a, ak pre každú Banachovu limitu L platí $L(x) = a$.

Nasledujúci výsledok, pochádzajúci od G. G. Lorentza [Lo], charakterizuje skoro konvergentné postupnosti:

Tvrdenie 6.3.24. *Nech $x = (x_n)_{n=1}^{\infty}$ je ohraničená postupnosť. Potom existuje Banachova limita L taká, že $L(x) = a$ práve vtedy, keď*

$$\lim_{n\to\infty} \inf_p \frac{x_{n+1} + \cdots + x_{n+p}}{n} \leq a \leq \lim_{n\to\infty} \sup_p \frac{x_{n+1} + \cdots + x_{n+p}}{n}$$

Teda postupnosť x skoro konverguje k číslu $a \in \mathbb{R}$ práve vtedy, keď

$$\lim_{n\to\infty} \frac{x_{n+1} + \cdots + x_{n+p}}{n} = a$$

rovnomerne vzhľadom na p.

Miery rozširujúce asymptotickú hustotu

Ultrafilter ako nemerateľná množina

Cvičenia

{ultracvic:ULOEKVZJED}

Úloha 6.3.1. Ukážte, že pre filter $\mathcal{F}$ na množine M platí: $\mathcal{F}$ je ultrafilter práve vtedy, keď pre ľubovoľné $A, B \subseteq M$ také, že $A \cup B = M$ platí $A \in \mathcal{F}$ alebo $B \in \mathcal{F}$.

$$A \cup B = M \qquad \Longrightarrow \qquad (A \in FF) \vee (B \in \mathcal{F})$$

{ultracvic:ULOBAZA}

Úloha 6.3.2. Ukážte, že ak $\mathcal{B}$ je báza filtra na množine M, tak $\mathcal{F} = \{A \subseteq M; (\exists B \in \mathcal{B}) B \subseteq A\}$ je filter na M.

Obrátene, ak $\mathcal{B} \subseteq \mathcal{P}(M)$ je systém množín taký, že $\mathcal{F} = \{A \subseteq M; (\exists B \in \mathcal{B}) B \subseteq A\}$ je filter, tak $\mathcal{B}$ je báza filtra, t.j. spĺňa obe podmienky z definície 6.3.3.

{ultracvic:ULOHAUS}

Úloha 6.3.3. Ukážte, že ak X je Hausdorffovský priestor, tak $\mathcal{F}$-limita zobrazenia $f \colon M \to X$ je určená jednoznačne.

{ultracvic:ULODUAL}

Úloha 6.3.4. Ukážte pomocou Hahn-Banachovej vety, že existuje funkcionál $f \in \ell_\infty^*$, ktorý nie je tvaru

$$f \colon x \mapsto \sum_{n=0}^{\infty} c_n x_n$$

pre žiadnu postupnosť $(c_n)_{n=1}^{\infty} \in \ell_1$.

{aplikcvic:ULOBANLIMHBT}

Úloha 6.3.5. Dokážte existenciu Banachovej limity pomocou Hahn-Banachovej vety. Aký bude možný rozsah hodnôt pre vami zvolenú polonormu? Vedeli by ste zvoliť polonormu tak, aby ste dostali maximálny možný rozsah hodnôt (a teda aj charakterizáciu skoro konvergentných postupností)? (O Banachových limitách a skoro konvergentných postupnostiach sa môžete dočítať v časti 6.3.2; definícia 6.3.20)

Úloha 6.3.6. Nech $\mathcal{U}$ je voľný ultrafilter. Na množine $\mathbb{N}^{\mathbb{N}}$ všetkých zobrazení z $\mathbb{N}$ do $\mathbb{N}$ zaveďme reláciu:

$$f \sim g \qquad \Leftrightarrow \qquad \{n \in \mathbb{N}; f(n) = g(n)\} \in \mathcal{U}.$$

a) Ukážte, že ide skutočne o reláciu ekvivalencie.
b) Aká je kardinalita množiny všetkých tried ekvivalencie. (Hint: Dajú sa využiť skoro disjunktné systémy – tvrdenie 6.1.4.)

6.4 Viac o kardinálnej aritmetike

6.4.1 Kofinalita

6.4.2 Königova veta

6.4.3 Eastonova veta

Cvičenia

Dodatok A

Topologické vektorové priestory

V tejto kapitole spomenieme niektoré fakty o topologických vektorových priestoroch, ktoré využívame v niektorých častiach tohoto textu. Viaceré z tvrdení uvedených v tejto kapitole by ste mohli poznať z niektorých analytických predmetov, napríklad by sa mohli vyskytnúť v pokročilejších kurzoch funkcionálnej analýzy.

V celej kapitole budeme pracovať s vektorovými priestormi nad poľom $\mathbb{K}$, kde $\mathbb{K} = \mathbb{R}$ alebo $\mathbb{K} = \mathbb{C}$. Na $\mathbb{K}$ budeme uvažovať obvyklú (euklidovskú) topológiu reálnej osi resp. komplexnej roviny.

A.1 Topologické vektorové priestory

S topologickými vektorovými priestormi sa často stretnete vo funkcionálnej analýze. Preto asi nebude prekvapivé, že v mnohých textoch z tejto oblasti nájdete aj kapitolu venovanú topologickým vektorovým priestorom: [AB, Chapter 5], [FHH$^+$, Section 3.2], [Me, Section 2.2].

Stručne sa dá povedať, že X je topologický vektorový priestor, ak máme na X štruktúru vektorového priestoru a súčasne topológiu, pričom tieto dve štruktúry sú „kompatibilné“.

Definícia A.1.1. Nech X je topologický vektorový priestor nad poľom $\mathbb{K}$, ktorý je súčasne Hausdorffovským topologickým priestorom. Ak sú zobrazenia $+\colon X\times X \to X$ a $\cdot\colon \mathbb{K}\times X \to X$ spojité, tak X voláme *topologický vektorový priestor.*

Asi by bolo na mieste spomenúť zopár príkladov TVP, ktoré by vám mali byť dobre známe. Začnime s veľmi triviálnym príkladom:

Príklad A.1.2. Ak uvažujeme $\mathbb{K}$ ako vektorový priestor nad $\mathbb{K}$ s obvyklou topológiou, tak dostaneme topologický vektorový priestor. (Stačí si uvedomiť, že sčitovanie a násobenie na $\mathbb{K}$ sú spojité vzhľadom na obvyklú topológiu.)

Väčšina priestorov, s ktorými sa stretnete vo funkcionálnej analýze, sú topologické vektorové priestory. Ak máme lineárny normovaný priestor X, tak tento priestor s topológiou odvodenou od normy je topologický vektorový priestor. Ďalej si ukážeme, že aj ak na ňom uvažujeme slabú topológiu, tak dostaneme TVP. Podobne aj X^* so slabou* topológiou je TVP.

Príklad A.1.3. Každý lineárny normovaný priestor je súčasne topologickým vektorovým priestorom (ak vezmeme topológiu odvodenú od normy).

Na zobrazenie $+\colon X\times X\to X$ sa môžeme pozerať aj ako na zobrazenia medzi lineárnymi normovanými priestormi. Toto zobrazenie je očividne lineárne. Trojuholníková nerovnosť $\|x+y\|\leq\|x\|+\|y\|$ znamená, že sčitovanie je spojité zobrazenie.

Ešte treba overiť spojitosť zobrazenia $\cdot\colon \mathbb{K}\times X\to X$. Pre ľubovoľné $c,c_0\in\mathbb{K}$, $x,x_0\in X$ máme z definície normy a z trojuholníkovej nerovnosti

$$\|cx-c_0x_0\|\leq\|c(x-x_0)\|+\|(c-c_0)x_0\|=|c|\cdot\|x-x_0\|+|c-c_0|\cdot\|x_0\|.$$

Pre dané $\varepsilon>0$ chceme zvoliť $\delta>0$ tak, aby z $|c-c_0|<\delta$ a $\|x-x_0\|<\delta$ vyplývalo, že pravá strana nerovnosti je menšia ako ε. Pre takéto c, x máme

$$|c|\cdot\|x-x_0\|+|c-c_0|\cdot\|x_0\|\leq(|c_0|+\delta)\delta+\delta\|x_0\|=\delta^2+(|c_0|+\|x_0\|)\delta.$$

Stačí teda zvoliť $\delta<1$ také, že $\delta<\frac{\varepsilon}{2}$ a navyše, ak $|c_0|+\|x_0\|\neq0$, tak $\delta<\dfrac{\varepsilon}{2(|c_0|+\|x_0\|)}$.

Predtým, než sa dostaneme k ďalším príkladom topologických vektorových priestorov, je užitočné všimnúť si dva spôsoby ako môžeme z nejakých TVS dostať nové TVS. Konkrétne nás budú zaujímať dve konštrukcie: podpriestory a súčiny.

{tvs:LMTVSPODPR}

Lema A.1.4. *Nech X je topologický vektorový priestor a Y je vektorový podpriestor X. Potom Y s indukovanou topológiou je tiež topologický vektorový priestor.*

Dôkaz. Úloha A.1.1. □

{tvs:LMTVSSUCIN}

Lema A.1.5. *Nech pre každé $i\in I$ je X_i topologický vektorový priestor. Potom aj $\prod\limits_{i\in I}X_i$ so súčinovou topológiou je topologický vektorový priestor.*

Ak si čitateľ potrebuje pripomenúť definíciu súčinovej topológie, nájde ju napríklad v časti 4.3.2.

Dôkaz. Označme $X=\prod\limits_{i\in I}X_i$. Chceme ukázať, že zobrazenia $+\colon X\times X\to X$ a $\cdot\mathbb{K}\times XX$ sú spojité. Na to stačí overiť, či vzor každej množiny zo subbázy je otvorená množina.

Nech $f+g=h$, kde $f,g\in X$. Zoberme nejaké okolie $p_i^{-1}[U]$ bodu h. Potom špeciálne máme, že $f(i)+g(i)=h(i)$ a U je okolie bodu $h(i)$ v priestore X_i. Zo spojitosti sčitovania na X_i máme existenciu otvorených množín $V\ni f(i)$, $W\ni g(i)$ takých, že $V+W\subseteq U$. Potom dostaneme aj $p_i^{-1}[V]+p_i^{-1}[W]\subseteq p_i^{-1}[U]$.

Podobne ak $c\cdot f=g$ a $p_i^{-1}[U]$ je subbázové okolie bodu g, tak máme okolie $U\ni g(i)=c\cdot f(i)$ v priestore X_i. Zo spojitosti násobenia vieme, že existujú okolie $V\ni c$ a $W\ni f(i)$ také, že v priestore X_i platí $V\cdot W\subseteq U$. Potom v X máme $V\cdot p_i^{-1}[W]\subseteq p_i^{-1}[U]$. □

Môžeme si všimnúť, že predchádzajúci dôkaz by sme mohli o čosi zjednodušiť využitím faktu, že okolia bodu 0 už jednoznačne popisujú topológiu celého priestoru – úloha A.1.2.

Uveďme aspoň jeden príklad vektorového priestoru, ktorý nie topologický vektorový priestor.

Príklad A.1.6. Uvažujme ľubovoľný nenulový vektorový priestor nad $\mathbb{K}$ s diskrétnou topológiou. S touto topológiou nedostaneme topologický vektorový priestor.

Zvoľme si nejaký nenulový vektor $\vec{\alpha}\in X$. Ak by išlo o topologický vektorový priestor, tak zobrazenie $c\mapsto c\vec{\alpha}$ z $\mathbb{K}$ do $[\vec{\alpha}]$ by bolo spojité. Ide však o bijekciu z $\mathbb{K}$ do diskrétneho topologického priestoru. Takéto zobrazenie by bolo spojité iba vzhľadom na diskrétnu topológiu na $\mathbb{K}$, nie však vzhľadom na obvyklú topológiu na $\mathbb{K}$.

Cvičenia

:ULOTVSPODPR}

Úloha A.1.1. Ukážte, že podpriestor topologického vektorového priestoru (s indukovanou topológiou) je opäť TVP. (Lema A.1.4.)

{tvscvic:ULOHOMOG}

Úloha A.1.2. Dokážte, že ak X je topologický vektorový priestor a $a \in X$, tak zobrazenie $f_a \colon x \mapsto a + x$ je homeomorfizmus z X do X. Z toho špeciálne vyplýva, že ak $\mathcal{B}$ je báza okolí nuly, tak $\{a + V; V \in \mathcal{B}\}$ je báza okolí bodu a. Inak povedané, ak poznáme okolia nuly, tak už je nimi jednoznačne určená topológia priestoru X.

A.2 Lokálne kompaktné topologické vektorové priestory

Cvičenia

Dodatok B

Sumy nespočítateľne veľa prvkov

{APNESPSUMY}

B.1 Definícia, základné vlastnosti, Cauchyho kritérium

V niektorých situáciách sa nám hodí sčitovať aj systémy, ktoré majú viac než spočítateľne veľa prvkov. (V tomto texte ich potrebujeme napríklad v probléme 4.3.10.) V tomto dodatku si povieme, ako sa dajú takéto sumy definovať, a spomenieme niektoré ich základné vlastnosti.

Viac o takýchto sumách si môžete prečítať napríklad aj v [D, Chapter 9].

{nespsumy:DEFSUMNESPOC}

Definícia B.1.1. Majme nejaký systém prvkov x_i, $i \in I$ topologického vektorového priestoru.[1] Pre každú konečnú množinu $F \subseteq I$ máme definovaný súčet $x_F = \sum\limits_{i\in F} x_i$.

Potom povieme, že x je súčtom tohoto systému a označíme

$$x = \sum_{i\in I} x_i,$$

ak pre každé okolie U bodu x existuje konečná množina F_0 taká, že pre ľubovoľnú konečnú množinu $F \supseteq F_0$ prvok

$$x_F = \sum_{i\in F} x_i$$

patrí do U.

V prípade lineárnych normovaných priestorov to môžeme zapísať tak, že

$$(\forall\varepsilon > 0)(\exists F_0 \in [I]^{<\omega})(\forall F \in [I]^{<\omega})(F \supseteq F_0 \Rightarrow \left\| x - \sum_{i\in F} x_i \right\| < \varepsilon).$$

(Symbol $[I]^{<\omega}$ označuje systém všetkých konečných podmnožín množiny I.)

{nespsumy:POZNSIETE}

Poznámka B.1.2. Ak poznáte pojem konvergencie siete (napríklad z predmetu **Všeobecná topológia**), tak sa na práve zadefinovanú sumáciu dá pozerať ako na konvergenciu sietí. Zobrali sme usmernenú množinu $([I]^{<\omega}, \subseteq)$ všetkých konečných podmnožín I usporiadanú

[1] Topologický vektorový priestor je vektorový priestor V nad poľom $\mathbb{K} = \mathbb{R}$ alebo $\mathbb{K} = \mathbb{C}$, na ktorom máme topológiu takú, že zobrazenia $+\colon V \times V \to V$ aj $\cdot\colon \mathbb{K} \times V \to V$ sú spojité. Napríklad každý lineárny normovaný priestor je topologickým vektorovým priestorom. Obvykle budeme takéto sumy využívať v lineárnych normovaných priestoroch, čiže ak nie ste zvyknutí robiť s topologickými vektorovými priestormi, môžete si všade predstaviť lineárne normované priestory. V niektorých prípadoch nám dokonca bude stačiť pracovať s takýmito sumami v $\mathbb{R}$ či v $\mathbb{R}^n$.

inklúziou. Na nej sme definovali sieť „čiastočných súčtov“ predpisom $x_F = \sum_{i\in F} x_i$. Definícia B.1.1 hovorí, že x je súčtom daného systému práve vtedy, keď uvedená sieť konverguje k x.

Všimnime si, že takto definovaný súčet nezávisí od toho, ako sú prvky usporiadané ani nepoužíva žiadne usporiadanie na množine I. Priamo z definície dostávame nasledovné pozorovanie:

{nespsumy:TVRBIJEK}

Tvrdenie B.1.3. *Nech V je topologický vektorový priestor a $x_i \in V$ pre každé $i \in I$. Nech $\sigma\colon J \to I$ je bijekcia. Ak existuje $\sum_{i\in I} x_i$, tak existuje aj $\sum_{j\in J} x_{\sigma(j)}$ a tieto súčty sa rovnajú.*

$$\sum_{i\in I} x_i = \sum_{j\in J} x_{\sigma(j)}$$

Toto tvrdenie vlastne vyjadruje spomínanú nezávislosť od usporiadania. Tiež sa naň dá pozerať ako na vyjadrenie komutatívnosti takéhoto sčitovania.

Dôkaz. Zrejmé. □

Poznámka B.1.4. Asi je vcelku prirodzené porovnať tento nový pojem s obvyklou konvergenciou radov, t.j. pozrieť sa na to, čo hovorí predošlá definície v prípade $I = \mathbb{N}$.

Očividný rozdiel je, že obvyklá konvergencia závisí aj na usporiadaní prirodzených čísel. Pojem konvergencie, ktorý sme zaviedli tu, nevyužíva žiadne usporiadanie na množine I.

Vcelku ľahko sa overí (úloha B.1.1), že $\sum_{n\in\mathbb{N}} x_n = x$ v zmysle definície B.1.1 platí práve vtedy, keď ku x konverguje každé preusporiadanie tohoto radu. (T.j. pre každú bijekciu $\sigma\colon \mathbb{N} \to \mathbb{N}$ platí $\sum_{i=1}^{\infty} x_{\sigma(n)} = x$.)

Poznamenajme, že tento typ konvergencie radov sa niekedy nazýva *bezpodmienečná konvergencia.* V lineárnych normovaných priestoroch má zmysel hovoriť aj o *absolútnej konvergencii* – ak konverguje rad $\sum_{i=1}^{n} \|x_n\|$.

Z prváckej analýzy viete, že pre reálne čísla sú absolútna a bezpodmienečná konvergencia ekvivalentné. V nekonečnorozmerných priestoroch je situácia o trochu komplikovanejšia: Dá sa ukázať, že v Banachových priestoroch z absolútnej konvergencie vyplýva bezpodmienečná konvergencia, opačná implikácia však platiť nemusí. Pozri napríklad [Hei, Section 3.1], [KK, Chapter 1], [Wo, Section II.D].

Ak pracujeme v Banachovom priestore, tak platí Cauchyho kritérium:

{nespsumy:TVRCAUCHY}

Tvrdenie B.1.5. *Nech V je Banachov priestor a $x_i \in V$ pre každé $i \in I$. Nasledujúce podmienky sú ekvivalentné:*

(i) *Súčet $\sum_{i\in I} x_i$ existuje.*

(ii) *Pre každé $\varepsilon > 0$ existuje konečná podmnožina $F_0 \subseteq I$ taká, že pre každú konečnú podmnožinu F s vlastnosťou $F \subseteq I \setminus F_0$ platí*

$$\left\| \sum_{i\in F} x_i \right\| < \varepsilon.$$

Dôkaz. $\boxed{(i) \Rightarrow (ii)}$ Zrejmé.

$\boxed{(ii) \Rightarrow (i)}$ Ak platí Cauchyho podmienka, tak existujú konečné podmnožiny $F_n \subseteq I$ také, že $F_n \subseteq F_{n+1}$ (t.j. ide o neklesajúcu postupnosť podmnožín) a

$$\left\| \sum_{i \in F} x_i \right\| < \frac{1}{n}$$

pre každú konečnú podmnožinu

$$F \subseteq I \setminus F_n.$$

Označme

$$s_n := \sum_{i \in F_n} x_i.$$

Pre $n < m$ máme

$$\|s_m - s_n\| = \left\| \sum_{i \in F_m \setminus F_n} x_i \right\| < \frac{1}{n}$$

To znamená, že postupnosť s_n je cauchyovská. Nech x je limita tejto postupnosti.

Ukážeme, že

$$x = \sum_{i \in I} x_i.$$

Pre dané $\varepsilon > 0$ existuje $k \in \mathbb{N}$ tak, že

$$\|s_k - x\| < \frac{\varepsilon}{2}$$

a súčasne pre každú konečnú podmnožinu $F \subseteq I \setminus F_k$ máme

$$\left\| \sum_{i \in F} x_i \right\| < \frac{\varepsilon}{2}.$$

Potom pre každú konečnú podmnožinu $F \supseteq F_k$ máme

$$\left\| x - \sum_{i \in F} x_i \right\| \leq \left\| x - \sum_{i \in F_k} x_i \right\| + \left\| \sum_{i \in F \setminus F_k} x_i \right\| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

□

Priamo z definície môžeme vidieť, že platia niektoré vzťahy, na ktoré sme zvyknutí z práce s obvyklou konvergenciou radov.

{nespsumy:TVRSUCET}

Tvrdenie B.1.6. *Nech V je topologický vektorový priestor. Nech $x_i, y_i \in V$ pre každé $i \in I$.*

(i) *Ak $x = \sum\limits_{i \in I} x_i$ a $y = \sum\limits_{i \in I} y_i$, tak $x + y = \sum\limits_{i \in I} (x_i + y_i)$, stručne*

$$\sum_{i \in I} (x_i + y_i) = \sum_{i \in I} x_i + \sum_{i \in I} y_i.$$

(ii) *Ak $x = \sum\limits_{i \in I} x_i$ a $c \in \mathbb{R}$, tak $cx = \sum\limits_{i \in I} (cx_i)$, stručne*

$$\sum_{i \in I} (cx_i) = c \left(\sum_{i \in I} x_i \right).$$

Dôkaz tohoto tvrdenia rozdelíme na dve samostatné lemy.

my:LMSPOJLIN}

Lema B.1.7. *Nech V, W sú topologické vektorové priestory a $f\colon V\to W$ je spojité lineárne zobrazenie. Ak $x=\sum\limits_{i\in I} x_i$, tak $f(x)=\sum\limits_{i\in I} f(x_i)$.*

Tvrdenie lemy môžeme stručne zapísať aj ako

$$f\left(\sum_{i\in I} x_i\right)=\sum_{i\in I} f(x_i),$$

ak túto rovnosť budeme čítať ako: „Ak existuje suma vystupujúca na ľavej strane, tak existuje aj suma na pravej strane a platí uvedená rovnosť.“

Dôkaz z definície B.1.1. Nech U je ľubovoľné okolie bodu $f(x)$. Zo spojitosti funkcie f máme existenciu okolia $V\ni x$ takého, že $f[V]\subseteq U$.

Ďalej vieme, že existuje konečná množina F_0 taká, že ak $F\in[I]^\omega$, $F\supseteq F_0$, tak

$$\sum_{i\in F} x_i\in V.$$

To ale potom znamená, že

$$\sum_{i\in F} f(x_i)=f\left(\sum_{i\in F} x_i\right)\in U.$$

Tým sme overili, že $f(x)=\sum\limits_{i\in I} f(x_i)$. □

Ak ste sa už učili o sieťach, tak vlastne sme len v tomto špeciálnom prípade zopakovali dôkaz toho, že spojité funkcie zachovávajú konvergenciu sietí. T.j. s použitím znalostí o sieťach vieme tento dôkaz zapísať stručnejšie.

Dôkaz pomocou sietí. Pre ľubovoľné $F\in[I]^\omega$ označme

$$x_F:=\sum_{i\in F} x_i$$
$$y_F:=\sum_{i\in F} f(x_i)$$

Z linearity zobrazenia f máme, že

$$y_F=\sum_{i\in F} f(x_i)=f\left(\sum_{i\in F} x_i\right)=f(x_F)$$

pre každú množinu $F\in[I]^{<\omega}$

Ak vieme, že sieť $(x_F;F\in[I]^{<\omega})$ konverguje k x, tak zo spojitosti zobrazenia f dostaneme, že aj sieť $f(x_F;F\in[I]^{<\omega})$ konverguje k $f(x)$. □

{nespsumy:LMSUCPRIES}

Lema B.1.8. *Nech V, W sú topologické vektorové priestory a $x_i\in V$, $y_i\in W$ pre každé $i\in I$. Potom v priestore $V\times W$ platí*

$$\sum_{i\in I}(x_i,y_i)=\left(\sum_{i\in I} x_i,\sum_{i\in I} y_i\right).$$

Dôkaz z definície B.1.1. Ak zoberieme ľubovoľné bázové okolie bodu (x, y), ktoré má tvar $U \times V$, tak vieme, že existujú konečné množiny $F_{1,2}$ také, že pre $F \in [I]^{<\omega}$ platí

$$F \supseteq F_1 \Rightarrow \quad \sum_{i\in F} x_i \in U$$
$$F \supseteq F_2 \Rightarrow \quad \sum_{i\in F} y_i \in V$$

Potom stačí položiť $F_0 = F_1 \cup F_2$ a pre každú konečnú množinu F takú, že $F_0 \subseteq F \subseteq I$ máme

$$\sum_{i\in F}(x_i, y_i) = \left(\sum_{i\in F} x_i, \sum_{i\in F} y_i\right) \in U \times V.$$

□

Opäť vlastne ide o špeciálny prípad jednej pomerne základnej vlastnosti sietí.

Dôkaz pomocou sietí. Ak označíme

$$x_F := \sum_{i\in F} x_i$$
$$y_F := \sum_{i\in F} y_i$$
$$z_F := \sum_{i\in F}(x_i, y_i)$$

tak priamo z definície súčinu topologických priestorov dostaneme

$$z_F = (x_F, y_F).$$

Ak sieť $(x_F; F \in [I]^{<\omega})$ konverguje k x a $(y_F; F \in [I]^{<\omega})$ konverguje k y, tak sieť $((x_F, y_F); F \in [I]^{<\omega})$ konverguje k (x, y). □

Dôkaz tvrdenia B.1.6. (i) Z lemy B.1.8 dostaneme, že v priestore $V \times V$ platí

$$(x, y) = \left(\sum_{i\in I} x_i, \sum_{i\in I} y_i\right).$$

Teraz stačí použiť lemu B.1.7 pre spojité zobrazenie $+\colon V \times V \to V$.

(ii) Stačí použiť lemu B.1.7 pre zobrazenie $x \mapsto cx$. □

Ak sčitujeme reálne čísla, tak ľahko ukážeme, že sčitovanie zachováva nerovnosť:

{nespsumy:TVRINEQ} **Tvrdenie B.1.9.** *Nech $x_i, y_i \in \mathbb{R}$ pre každé $i \in I$. Predpokladajme, že pre každé $i \in I$ platí $x_i \leq y_i$. Ak $x = \sum\limits_{i\in I} x_i$ a $y = \sum\limits_{i\in I} y_i$, tak $x \leq y$.*

T.j. platí nerovnosť

$$\sum_{i\in I} x_i \leq \sum_{i\in I} y_i$$

(*za predpokladu, že uvedené sumy existujú*).

Dôkaz. Úloha B.1.6. □

Cvičenia

ic:ULOPREUSP}

Úloha B.1.1. Ukážte, že $x = \sum\limits_{n\in\mathbb{N}} x_n$ v zmysle definície B.1.1 práve vtedy, keď pre každú bijekciu $\sigma\colon \mathbb{N} \to \mathbb{N}$ platí $x = \sum\limits_{i=1}^{\infty} x_{\sigma(n)}$. (T.j. každé preusporiadanie radu $\sum\limits_{i=1}^{\infty} x_n$ konverguje ku x.) [2]

{nespsumycvic:ULOSUP}

Úloha B.1.2. Ukážte, že ak pre každé $i \in I$ je $x_i \geq 0$ nezáporné reálne číslo, tak

$$\sum_{i\in I} x_i = \sup\{\sum_{i\in F} x_i; F \in [I]^{<\omega}\}.$$

(Zamyslite sa aj nad tým, či sa definícia B.1.1 dá upraviť tak, aby pre reálne čísla dávala zmysel aj ak súčet je $+\infty$. Rovnosť v tejto úlohe treba buď čítať tak, že pripúšťame aj súčet rovný $+\infty$, alebo tak, že uvedený súčet existuje práve vtedy, keď suprémum na pravej strane rovnosti je konečné a v takom prípade sa obe strany rovnajú.)

Úloha B.1.3. Nech pre každé $i \in I$ je x_i reálne číslo a pre každú konečnú podmnožinu $F \in [I]^{\omega}$ platí $\sum\limits_{i\in F} x_i \leq A$. Nech existuje súčet $\sum\limits_{i\in I} x_i$. Potom aj

$$\sum_{i\in I} x_i \leq A.$$

Úloha B.1.4. Ukážte, že ak existuje súčet $\sum_{i\in I} x_i$ prvkov lineárneho normovaného priestoru X, tak pre každé $\varepsilon > 0$ existuje konečná podmnožina $F_0 \subseteq I$ taká, že $\left\|\sum_{i\in F} x_i\right\| < \varepsilon$ pre každú konečnú podmnožinu $F \supseteq F_0$. (Nutná podmienka konvergencie.)

Úloha B.1.5. Nech x_i je reálne číslo pre každé $i \in I$. Ukážte, že ak existuje (konečný) súčet $\sum\limits_{i\in I} x_i$, tak potom množina $\{i \in I; x_i \neq 0\}$ je spočítateľná. (T.j. nenulové prvky sa môžu vyskytnúť len pre spočítateľne veľa indexov.)

{nespsumycvic:ULOINEQ}

Úloha B.1.6. Dokážte tvrdenie B.1.9.

[2] Dokonca platí silnejšie tvrdenie – nemuseli by sme požadovať, že každé prerovnanie konverguje k tomu istému číslu. Z konvergencie všetkých prerovnaní už vyplynie, že všetky prerovnané sumy sa musia rovnať. Dôkaz môžete nájsť napríklad v [Hei, Corollary 3.11], [KK, Theorem 1.3.1], [Wo, Theorem II.D.2]

Literatúra

[A] Benno Artmann. *The Concept of Number: From Quaternions to Monads and Topological Fields.* John Wiley, New York, 1988.

[AB] Charalambos D. Aliprantis a Kim C. Border. *Infinite Dimensional Analysis, A Hitchhiker's Guide.* Springer, Berlin, 3rd edition, 2006.

[AE] Herbert Amann a Joachim Escher. *Analysis III.* Birkhäuser, Basel, 2009. Translated from the German by Silvio Levy and Matthew Cargo.

[AF] A. V. Arhangel'skiĭ a S. P. Franklin. Ordinal invariants for topological spaces. *Michigan Math. J.*, 15:313–320, 1968.

[AP] A. V. Arkhangelskii a V. Ponomarev. *Fundamentals of General Topology. Problems and Exercises.* D. Reidel Publishing Company, Dordrecht, 1983.

[Ba] Frederick Bagemihl. A theorem on intersections of prescribed cardinality. *Ann. Math.*, 55(1):34–37, 1952.

[Bla] Andreas Blass. Existence of bases implies the axiom of choice. *Contemporary Mathematics*, 31:31–33, 1984.

[Blo] Ethan D. Bloch. *The Real Numbers and Real Analysis.* Springer, New York, 2010.

[Bu1] Lev Bukovský. Úvod do matematickej logiky. `http://ics.upjs.sk/~novotnyr/home/skola/logika_a_teoria_mnozin/ltm.pdf`.

[Bu2] Lev Bukovský. *Štruktúra reálnej osi.* Veda, Bratislava, 1979.

[Bu3] Lev Bukovský. *The Structure of Real Line.* Springer, Basel, 2011.

[BE] F. Bagemihl a P. Erdös. Intersections of prescribed power, type, or measure. *Fund. Math.*, 41(1), 1955.

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

[Ca] N. L. Carothers. *A Short Course on Banach Space Theory.* Cambridge University Press, New York, 2004. London Mathematical Society Student Texts 64.

[Ci] Krzysztof Ciesielski. *Set Theory for the Working Mathematician.* Cambridge University Press, Cambridge, 1997. London Mathematical Society Student Texts 39.

[Č] Juraj Činčura. Model aritmetiky celých nezáporných čísel v teórii množín. `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/2010/temno/cisla.pdf`.

[C] Keith Conrad. Zorn's lemma. `http://www.math.uconn.edu/~kconrad/blurbs/`.

[CL] Antoine Chambert-Loir. *A Field Guide to Algebra.* Springer, New York, 2005. Undergraduate Texts in Mathematics.

[D] Jacques Dixmier. *General Topology.* Springer-Verlag, New York, 1984. Undergraduate Texts in Mathematics.

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

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

[Eng] Ryszard Engelking. *General Topology.* Heldermann Verlag, Berlin, 1989. Revised and completed edition, Sigma Series in Pure Mathematics, Vol. 6.

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

[Fr1] S. P. Franklin. Spaces in which sequences suffice. *Fund. Math.*, 57:107–115, 1965.

[Fr2] S. P. Franklin. Spaces in which sequences suffice II. *Fund. Math.*, 61:51–56, 1967.

[FHH$^+$] Marián Fabian, Petr Habala, Petr Hájek, Vicente Montesinos, a Vaclav Zizler. *Banach Space Theory. The Basis for Linear and Nonlinear Analysis.* Springer, New York, 2011. CMS Books in Mathematics.

[G] George Grätzer. *Lattice Theory: Foundation.* Birkhäuser, Basel, 2011.

[GJ] L. Gillman a M. Jerison. *Rings of Continuous Functions.* Van Nostrand, Princeton, 1960.

[Hal1] Lorenz J. Halbeisen. *Combinatorial Set Theory. With a Gentle Introduction to Forcing.* Springer-Verlag, London, 2012. Springer Monographs in Mathematics.

[Hal2] P. Halmos. *Measure Theory.* Springer-Verlag, New York, 1974. Graduate Texts in Mathematics 18.

[Hei] Christopher Heil. *A Basis Theory Primer.* Springer, New York, 2011.

[Her1] Horst Herrlich. Choice principles in elementary topology and analysis. *Comment. Math. Univ. Carolinae*, 38(3):545–552, 1997.

[Her2] Horst Herrlich. *The Axiom of Choice.* Springer-Verlag, Berlin, 2006. Lecture Notes in Mathematics 1876.

[HH] A. Hajnal a P. Hamburger. *Set theory.* Cambridge University Press, Cambridge, 1999.

[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.

[Jo] K. D. Joshi. *Introduction to General Topology.* Wiley Eastern Limited, New Delhi, 1983.

[Ju] I. Juhász. *Cardinal functions in topology - ten years later.* Math. Centre Tracts, Amsterdam, 1980.

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

[JW1] Winfried Just a Martin Weese. *Discovering modern set theory I: The basics.* Amer. Math. Soc., Providence, RI, 1997. Graduate Studies in Mathematics 8.

[JW2] Winfried Just a Martin Weese. *Discovering modern set theory II: Set-theoretic tools for every mathematician.* Amer. Math. Soc., Providence, RI, 1997. Graduate Studies in Mathematics 18.

[Ke] A. S. Kechris. *Classical descriptive set theory.* Springer-Verlag, Berlin, 1995. Graduate Texts in Mathematics 156.

[Kha1] A. B. Kharazishvili. *Strange functions in real analysis.* Taylor & Francis Group, Boca Raton, 2nd edition, 2006.

[Kha2] Alexander B. Kharazishvili. *Set Theoretical Aspects of Real Analysis.* CRC Press, Taylor & Francis Group, Boca Raton, 2015.

[Ko] Július Korbaš. *Lineárna algebra a geometria I.* UK, Bratislava, 2003.

[Ku] Marek Kuczma. *An introduction to the theory of functional equations and inequalities. Cauchy's equation and Jensen's inequality.* Birkhäuser, Basel, 2nd edition, 2009.

[KG] Július Korbaš a Štefan Gyürki. *Prednášky z lineárnej algebra a geometrie.* UK, Bratislava, 2013.

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

[KK] M.I. Kadets a V.M. Kadets. *Series in Banach spaces.* Birkhäuser Verlag, Basel, 1997. Operator Theory; Vol. 94.

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

[KN] W. J. Kaczor a M. T. Nowak. *Problems in Mathematical Analysis II. Continuity and differentiation.* American Mathematical Society, Providence, 2001.

[KT] Péter Komjáth a Vilmos Totik. *Problems and Theorems in Classical Set Theory.* Springer, 2006. Problem Books in Mathematics.

[La] H. Elton Lacey. The Hamel dimension of any infinite dimensional separable Banach space is c. *Amer. Math. Monthly*, 80(3):298, 1973.

[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.

[Lo] G. G. Lorentz. A contribution to the theory of divergent sequences. *Acta Math.*, 80:167–190, 1948.

[Ma] Dan Ma. Dan Ma's Topology Blog. `http://dantopology.wordpress.com/`.

[Me] Robert E. Megginson. *An Introduction to Banach Space Theory*. Springer, New York, 1998. Graduate Texts in Mathematics 193.

[Moo] Gregory H. Moore. *Zermelo's Axiom of Choice. Its Origins, Development and Influence*. Springer-Verlag, New York, 1982.

[Mor] T. J. Morrison. *Functional Analysis: An Introduction to Banach Space Theory*. Wiley, 2000.

[Mr] S. Mrówka. On completely regular spaces. *Fund. Math.*, 11:105–106, 1955.

[MO] MathOverflow. `http://mathoverflow.net/`.

[MSE] Mathematics Stack Exchange. `http://math.stackexchange.com/`.

[N] Attila Nagy. *Special Classes of Semigroups*. Springer-Science+Business Media B.V., Dordrecht, 2001.

[NS] A. Naylor a G. Sell. *Teória lineárnych operátorov v technických a prírodných vedách (Linear Operator Theory in Engineering and Science)*. Alfa, Bratislava.

[O] John C. Oxtoby. *Measure and Category*. Springer-Verlag, New York, 2nd edition, 1980. Graduate Texts in mathematics 2.

[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`.

[P] Albrecht Pietsch. *History of Banach Spaces and Linear Operators*. Birkhäuser, Boston, 2007.

[R] Steven Roman. *Lattices and Ordered Sets*. Springer, New York, 2008.

[Š] Tibor Šalát. *Reálne čísla*. Bratislava, 1981.

[Si] Wacław Sierpiński. *Cardinal and ordinal numbers*. Państwowe Wydawnictwo Naukowe, Warszawa, 1965.

[Sl1] Martin Sleziak. 1-INF-155 Algebra 2. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[Sl2] Martin Sleziak. 1-MAT-260 Algebra 2. Poznámky k prednáške, `https://msleziak.com/vyuka/2011/alg2m/`.

[Sl3] Martin Sleziak. 2-UMA-115 teória množín. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[Sl4] Martin Sleziak. Lineárna algebra. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[Sl5] Martin Sleziak. $\mathcal{F}$-convergence, filters and nets. `http://thales.doa.fmph.uniba.sk/sleziak/texty/rozne/trf/iconv/notions.pdf`.

[Smi] Peter Smith. *An Introduction to Gödel's Theorems.* Cambridge University Press, Cambridge, 2007. Cambridge Intreoductoins to Philosophy.

[Smu] Raymond M. Smullyan. *Gödel's incompleteness theorems.* Oxford University Press, Oxford, 1992. Oxford Logic Guides 22.

[So] Antonín Sochor. *Klasická matematická logika.* Karolinum, Praha, 2001.

[Š] Petr Štěpánek. Predikátová logika. `http://kti.ms.mff.cuni.cz/teaching/files/materials/StepanekPetr_PredikatovaLogika.pdf`.

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

[Š] Jana Štolcová. Banachove limity. Master's thesis, FMFI UK, Bratislava, 2011. In Slovak.

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

[Tao] Terence Tao. *An epsilon of room: pages from year three of a mathematical blog.*

[Tar] Alfred Tarski. Sur quelques theoremes qui equivalent a l'axiome du choix. *Fund. Math.*, 5:147–154, 1924.

[Ts] Nam-Kiu Tsing. Infinite-dimensional Banach spaces must have uncountable basis–an elementary proof. *Amer. Math. Monthly*, 91(8):505–506, 1984.

[TRI] Tricki. `http://tricki.org/`.

[V] Martin Väth. The dual space of L_∞ is L_1. *Indag. Math.*, 9(4):619–625, 1998.

[vRS] A. C. M. van Rooij a W. H. Schikhof. *A Second Course on Real Functions.* Cambridge University Press, Cambridge, 1982.

[Wag] Stan Wagon. *The Banach-Tarski Paradox.* Cambridge University Press, Cambridge, 1985.

[Wap] Leonard M. Wapner. *The Pea and the Sun.* A. K. Peters, Wellesley, Massachusetts, 2005.

[We] J. D. Weston. A short proof of Zorn's lemma. *Archiv der Mathematik*, 8(4):279, 1957.

[Wie] Freek Wiedijk. Formal proof–getting started. *Notices of AMS*, 55(11):1408–1414, 2008. `http://www.ams.org/notices/200811/tx081101408p.pdf`.

[Wil] S. Willard. *General topology.* Addison-Wesley, Massachussets, 1970.

[Wo] P. Wojtaszczyk. *Banach spaces for analysts.* Cambridge University Press, Cambridge, 1991. Cambridge Studies in Advanced Mathmatics 25.

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

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

Register

Zoznam symbolov