Riešené úlohy

Kardinálne čísla

Úloha 1. Ak a, b, c sú kardinálne čísla, tak $a \leq b \Rightarrow a^c \leq b^c$.

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

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

$$\begin{tikzcd} & C \arrow[dl, "g"'] \arrow[dr, "?"] & \\ A \arrow[rr, "f"'] & & B \end{tikzcd}$$

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

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

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

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

Táto rovnosť znamená, že pre každé $x \in C$ platí

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

Pretože f je injektívne, vyplýva z nej rovnosť

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

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

Úloha 2. Ak a, b, c sú kardinálne čísla, tak $a \leq b \Rightarrow c^a \leq c^b$.

Návod: V tomto prípade je situácia o čosi jednoduchšia. Ak máme injekciu $f\colon A \to B$, môžeme predpokladať priamo, že $A \subseteq B$. Ak $C \neq \emptyset$, vedeli by ste nejako rozšíriť každé zobrazenie $A \to C$ na zobrazenie z $B \to C$? (Toto by mohlo pomôcť nájsť injekciu z C^A do C^B.) Čo v prípade, že $C = \emptyset$?

Iná možnosť: Vedeli by ste pomocou zobrazenia $f\colon A \to B$ definovať nejaké zobrazenie $\varphi\colon C^B \to C^A$? Ak f je injekcia, vedeli by ste dokázať, že toto zobrazenie φ je surjekcia? Čo nám o kardinalitách hovorí existencia surjekcie z C^B do C^A? $\square$

Môžete si skúsiť rozmyslieť aj prvú úlohu tak, že budete predpokladať priamo $A \subseteq B$ – možno sa vám bude zdať o niečo jasnejšia.

Úloha 3. Pre ľubovoľné kardinálne čísla platí $a^{b+c} = a^b.a^c$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Úloha 4. Pre ľubovoľné kardinálne čísla platí $(a^b)^c = a^{bc}$.

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

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

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

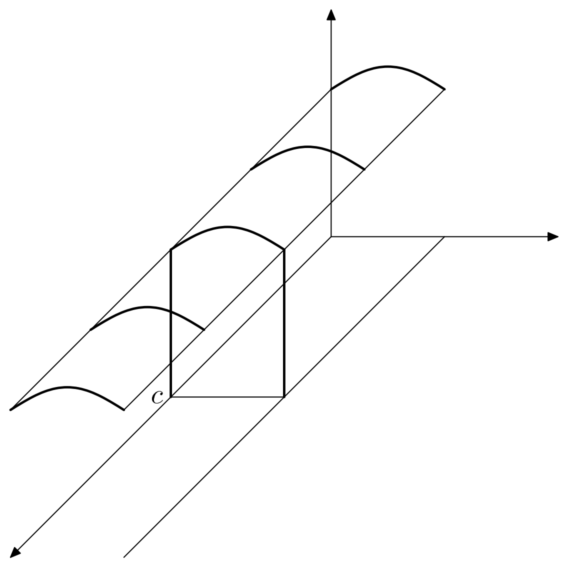
Obrátene, každému zobrazeniu $g\colon B \times C \to A$ by sme chceli priradiť zobrazenie $\psi(g)\colon C \to A^B$, t.j. zobrazenie, ktoré každému prvku z C priradí nejaké zobrazenie z B do A. Ak máme dané zobrazenie z $B\times C$ do A, zafixujeme nejaké $c \in C$ a meníme len prvok $b \in B$ vidíme,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

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

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

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

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



Obr. 1: Obrázok ilustrujúci postup v úlohe 4. (Použitá funkcia je $f(x,y) = \frac{3}{2} + \frac{1}{5}\sin \pi x$.)

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

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

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

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

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

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

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

Dobré usporiadania

Úloha 5. Ak $(A, \leq)$ a $(B, \leq)$ sú dobre usporiadané množiny, tak buď $(A, \leq)$ je izomorfná (podobná) s nejakým počiatočným úsekom množiny B alebo B je izomorfná s nejakým počiatočným úsekom množiny B. (*Počiatočný úsek* lineárne usporiadanej množiny $(X, \leq)$ je podmnožina $U \subseteq X$ s vlastnosťou $x \in U \wedge y \leq x \Rightarrow y \in U$. Počiatočné úseky v $(X, \leq)$ sú X a množiny tvaru $X_a = \{x \in X; x < a\}$ pre $a \in X$.)

Riešenie tejto úlohy môžete nájsť aj v [ŠS, Z]. Sem som sa to snažil napísať zhruba tak, ako sme to robili na cvičení.

Hoci to pre riešenie úlohy priamo nepotrebujeme, všimnime si, že pre ľubovoľnú dobre usporiadanú množinu $(X, \leq)$ má každý počiatočný úseky okrem celého X naozaj iba množiny tvaru $X_a = \{x \in X; x < a\}$. Na to si stačí uvedomiť, že ak U je počiatočný úsek a $a := \min(X \setminus U)$ tak $U = X_a$. (Každý prvok menší ako a musí patriť do U, lebo inak by a nebol najmenší prvok $U \setminus X$. Obrátene, ak by v U bol nejaký prvok, ktorý je väčší alebo rovný a, tak by platilo aj $a \in U$, čo je spor s tým, že $a \in X \setminus U$.)

Riešenie: Budeme sa chvíľu zaoberať bijekciami medzi počiatočnými úsekmi množín A a B. Naším prvým cieľom bude ukázať, že všetky takéto zobrazenia sú v istom zmysle „kompatibilné“ – to neskôr využijeme na dôkaz tvrdenia v zadaní.

Ukážeme najprv nasledujúci fakt: Ak $A_1, A_2 \subseteq A$, $B_1, B_2 \subseteq B$ sú počiatočné úseky a $f_1 \colon A_1 \to B_1$, $f_2 \colon A_2 \to B_2$ sú izomorfizmy medzi príslušnými počiatočnými úsekmi množiny A a nejakými počiatočnými úsekmi B, tak sa tieto zobrazenia na $A_1 \cap A_2$ zhodujú, t.j. $f_1|_{A_1 \cap A_2} = f_2|_{A_1 \cap A_2}$.

Uvažujme ľubovoľné $x \in A_1 \cap A_2$ a označme $f_1(x) = y_1$, $f_2(x) = y_2$. Označme $C := \{a \in A; a \leq x\}$ a $D_1 := \{b \in B; b \leq f_1(x)\}$. Ukážeme, že $f_1|_C$ je bijekcia medzi C a D_1, ktorá zachováva usporiadanie.

Najprv si musíme uvedomiť, že ide skutočne o zobrazenie, teda, že platí $f_1(c) \in D_1$ pre každé $c \in C$. To vyplýva z toho, že f_1 zachováva usporiadanie, preto z $c \in C$ vyplýva $c \leq x \Rightarrow f_1(c) \leq f_1(x) = y_1$, a teda $f_1(c) \in D$.

Keďže $f_1|_C$ je zúženie injekcie zachovávajúcej usporiadanie, aj toto zobrazenie zachováva usporiadanie a je injektívne. (Tieto vlastnosti sa zachovajú pri zúžení.) Zostáva nám ukázať surjektívnosť. Zo surjektívnosti f_1 dostaneme, že pre každé $d \in D_1$ (teda $d \leq y_1$) existuje $c \in A_1$ také, že $f(c) = d$. Súčasne z toho, že f_1 zachováva usporiadanie vidíme, že nemôže platiť $d > x$. Teda sme našli v C vzor pre d, čím sme ukázali, že aj $f_1|_C$ je surjektívne zobrazenie.

Rovnakým spôsobom môžeme ukázať, že $f_2|_C$ je bijekcia medzi C a $D_2 := \{b \in B; b \leq f_2(x)\}$.

Fakt, že máme 2 takéto bijekcie využijeme na dôkaz toho, že $y_1 = y_2$. Bez ujmy na všeobecnosti predpokladajme, že $y_1 \leq y_2$. Máme bijekciu $g := (f_1|_C) \circ (f_2|_C)^{-1} \colon D_2 \to D_1$. Keďže $D_1 \subseteq D_2$ (lebo $y_1 \leq y_2$), môžeme g súčasne chápať ako zobrazenie z D_2 do D_2, z čoho vyplýva nerovnosť[1] $y_2 \leq f(y_2)$. Súčasne $f(y_2) \in D_2$, a teda $f(y_2) \leq y_1$. Spolu máme

$$y_2 \leq f(y_2) \leq y_1,$$

dostali sme teda obe nerovnosti $y_1 \leq y_2$ aj $y_2 \leq y_1$, čo znamená, že $y_1 = y_2$, čiže $f_1(x) = f_2(x)$.

Označme $\mathcal{S} = \{C \subseteq A; C$ je počiatočný úsek množiny A a existuje bijekcia medzi C a nejakým počiatočným úsekom množiny $B\}$. Ak tieto množiny zjednotíme, dostaneme množinu $C_1 = \bigcup \mathcal{S}$, ktorá je opäť počiatočným úsekom A.

[1] Na cvičení sme dokázali, že ak $(A, \leq)$ je dobre usporiadaná množina a $f \colon A \to A$ je injekcia zachovávajúca usporiadanie, tak pre každé $a \in A$ platí $a \leq f(a)$.

Navyše, môžeme definovať zobrazenie $f\colon C_1 \to B$, tak, že $f(x)$ je spoločná hodnota všetkých bijekcií z počiatočných úsekov obsahujúcich x. Takéto zobrazenie opäť zachováva usporiadanie a je to bijekcia na nejaký počiatočný úsek množiny B. (Konkrétne je to počiatočný úsek $\bigcup_{C\in\mathcal{S}} f(C)$.)

Ak $C = A$, našli sme bijekciu medzi A a počiatočným úsekom B. Ak $f(C) = B$, tak máme bijekciu medzi počiatočným úsekom A a celou množinou B. Jediný prípad, ktorý nevyhovuje tvrdeniu v zadaní je ten, že by obe tieto podmnožiny boli vlastné. Ukážeme, že takýto prípad nemôže nastať.

Sporom. Nech $A \setminus C \neq \emptyset$ aj $B \setminus f(C) \neq \emptyset$. Definujme $a := \min(A \setminus C)$, $b := \min(B \setminus f(C))$. Máme bijekciu $f\colon A \to f(A)$. Potom aj zobrazenie $\hat{f}\colon C \cup \{a\} \to f(C) \cup \{b\}$ definované ako

$$\hat{f}(x) = \begin{cases} f(x) & x \in C,\\ b & x = a. \end{cases}$$

je bijekcia medzi počiatočnými úsekmi množín A a B, ktorá zachováva usporiadanie. Potom aj $A \cup \{a\} \in \mathcal{S}$, čo je spor s tým, že $a \notin \bigcup \mathcal{S}$. $\square$

Aplikácie ordinálnych čísel

V tejto časti by sme chceli ukázať použitie ordinálnych čísel na niektorých problémoch z rôznych oblastí matematiky. Pri každej z aplikácií som uviedol aj zdroj, z ktorého som príslušný dôkaz prebral. Preto, že o ordinálnych číslach sme sa ani zďaleka zatiaľ nenaučili úplne všetko, občas uvediem nejaké veci, ktorým bude treba uveriť.

Na pripomenutie z prednášky:

Axióma výberu (AC): Ak $\{A_i; i \in I\}$ je ľubovoľný systém neprázdnych množín. Potom existuje funkcia $f\colon I \to \bigcup\limits_{i\in I} A_i$ taká, že $f(i) \in A_i$.

Princíp dobrého usporiadania (WO): Pre každú množinu existuje nejaké jej dobré usporiadanie.

Axióma výberu a princíp dobrého usporiadania sú ekvivalentné. Axióma výberu je ekvivalentná aj s princípom maximality alebo Zornovou lemou, čo sú ďalšie tvrdenia, ktoré sa v matematike často používajú ako výhodné dôkazové techniky. Na tejto prednáške na ne nezvýšil čas. Viac sa o nich môžete dozvedieť v [ŠS, Z].

Pripomeňme ďalej, že ordinály sa dali chápať jednoducho ako ordinálne typy (typy usporiadania) dobre usporiadaných množín, dali sa však zadefinovať aj formálnym spôsobom (ako tranzitívne množiny dobre usporiadané reláciou $\in$). Ku každej dobre usporiadanej množine existuje práve jeden ordinál, ktorý je s ňou izomorfný.

Hoci sme detailne nedefinovali ako, aspoň zhruba sme videli, že ordinálne čísla sa dajú sčitovať a násobiť (vedeli sme usporiadať viacero dobre usporiadaných množín za sebou a vedeli sme dobre usporiadať $A \times B$ pomocou dobrých usporiadaní na množinách A a B.) Takisto môžeme ordinálne čísla porovnávať.

Ľubovoľná množina ordinálnych čísel je dobre usporiadaná. [2]

Ak už máme zadefinované ordinálne čísla, kardinálne číslo môžeme zadefinovať ako najmenší ordinál danej kardinality (inak povedané, ak máme danú ľubovoľnú množinu A a vezmeme všetky ordinály pre ktoré existuje bijekcia s množinou A, najmenší prvok tejto množiny ordinálnych čísel nazveme kardinálnym číslom množiny A).

Úloha 6. Pre každý kardinál $a \geq \aleph_0$ platí $a.a = a$. (Napríklad [ŠS, Veta 10.2.3], [C, Theorem 5.2.4])

Riešenie: Už sme videli, že toto tvrdenie platí pre $a = \aleph_0$. Ukážeme, že ak toto tvrdenie platí pre každý nekonečný kardinál $b < a$, tak platí aj pre a.

Nech teda $a > \aleph_0$. Majme dobré usporiadanie $\leq$ na a, také, že všetky počiatočné úseky tvaru $\{x \in a; x < b\}$ pre $b \in a$ majú kardinalitu menšiu ako a. Pomocou tohoto usporiadania[3] zadefinujeme usporiadanie $\leq^*$ na množine $a \times a$, o ktorom potom ukážeme, že je dobrým usporiadaním.

Definujme $\leq^*$ takto: Nech $m_1 = \max\{a_1, b_1\}$ a $m_2 = \max\{a_2, b_2\}$. Potom

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

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 podmnožinu $a \times a$ môžeme vybrať najmenšie m, ktoré sa vyskytuje ako maximum nejakej dvojice prvkov tejto podmnožiny. Keď sa už pozeráme iba na prvky s rovnakým maximom, tie sú usporiadané lexikograficky.

Navyše, každý dolný úsek $a \times a_{(a_1,b_1)} = \{(x, y) \in a \times a; (x, y) <^* (a_1, b_1)\}$ má kardinalitu menšiu ako a. (Jeho kardinalita je rovná súčinu kardinalít dolných úsekov pre a_1 a b_1 v usporiadaní. Ak $m_1 = \max\{a_1, b_1\}$, tak ju zhora môžeme odhadnúť $|a_{m_1}|.|a_{m_1}|$. Pretože $|a_{m_1}| < a$ a predpokladáme, že dokazované tvrdenie platí pre všetky kardinály menšie ako a, dostávame $|a_{m_1}|.|a_{m_1}| = |a_{m_1}|$.)

Potom pre každý počiatočný úsek $(a \times a, \leq^*)$ existuje bijekcia na počiatočný úsek dobre usporiadanej množiny $(a, \leq)$. (Vieme, že pre 2 dobre usporiadané existuje buď zobrazenie jednej na počiatočný úsek druhej alebo obrátene. Množinu $(a, \leq)$ však nemožno vnoriť do $(a \times a, \leq^*)$ ako počiatočný úsek, lebo potom

[2] Vidno to napríklad z toho, že ju môžeme vnoriť do nejakého ordinálneho čísla väčšieho od všetkých ordinálnych čísel v tejto množine. Teda je to podmnožina nejakej dobre usporiadanej množiny.

[3] Odkiaľ vieme, že usporiadanie $\leq$ s uvedeným vlastnosťami existuje? Ak kardinály chápeme (pozri vyššie) 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.

by tento počiatočný úsek musel mať kardinalitu a). Navyše, všetky tieto vnorenia na počiatočné úseky sú kompatibilné (pozri predchádzajúcu úlohu).

Vďaka tomu ako zjednotenie týchto zobrazení (inak povedané – ako zobrazenie, ktorého hodnota bude spoločná hodnota všetkých vnorení) dostaneme vnorenie $(a \times a, \leq^*)$ na počiatočný úsek $(a, \leq)$. Tým sme našli injekciu z $a \times a$ do a, preto platí

$$a.a \leq a.$$

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

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

Ordinály využíva dôkazová technika, ktorá sa volá *transfinitná indukcia.* Ak chcem dokázať, že tvrdenie $V(\alpha)$ platí pre všetky ordinály, stačí ukázať

$$(\forall \beta < \alpha) V(\beta) \Rightarrow V(\alpha).$$

(Toto tvrdenie – princíp transfinitnej indukcie – ste na prednáške mali sformulované v trochu inej podobe. Keďže vtedy ste ešte nevedeli o ordináloch, uviedli ste si ho pre ľubovoľné dobre usporiadané množiny.)

Hoci princíp transfinitnej indukcie sme sformulovali ako jedinú implikáciu, z praktických dôvodov sa dôkazy často robia zvlášť pre 3 prípady:

- $\alpha = 0$;
- $\alpha = \beta + 1$, čiže α je nasledovník nejakého ordinálu (nasleduje tesne po ordinále β);
- α nie je nasledovník nijakého ordinálu. Takéto ordinály voláme *limitné.* Ak α je limitný ordinál, tak sa dá vyjadriť ako suprémum všetkých menších ordinálov, čiže $\alpha = \sup_{\beta<\alpha} \beta$. (Suprémum chápeme ako najmenšie horné ohraničenie vzhľadom na usporiadanie ordinálov.) Pri obvyklej reprezentácii ordinálov sú všetky predchádzajúce ordinály priamo podmnožiny α, teda predchádzajúci vzťah znamená rovnosť $\alpha = \bigcup\limits_{\beta<\alpha} \beta$.

Ako prvú ukážku si uveďme dôkaz tvrdenia, ktoré sme už na cvičení dokázali. Na vysvetlenie dôkazu transfinitnou indukciou sa však hodí.

Úloha 7. Nech λ je ordinálne číslo a $f \colon \lambda \to \lambda$ je injekcia zachovávajúca usporiadanie (t.j. $\beta < \gamma \Rightarrow f(\beta) < f(\gamma)$). Potom pre každé $\alpha \in \lambda$ platí $f(\alpha) > \alpha$. [D, Lema 3.5.1]

My sme na cvičení ukázali analogické tvrdenie pre ľubovoľnú dobre usporiadanú množinu. Keďže už vieme, že každá dobre usporiadaná množina je izomorfná s nejakým ordinálom, je to ekvivalentné s týmto tvrdením.

Riešenie: 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

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

□

Ďalšou často používanou technikou je *konštrukcia transfinitnou rekurziou.* Pri transfinitnej indukcie sme na dôkaz nejakého tvrdenia ukázali, že ak platí pre ordinály menšie ako α, tak platí aj pre ordinál α. Ak chceme skonštruovať nejakú množinu pre každý ordinál, tak ukážeme ako z konštrukcie množín s vhodnými vlastnosťami pre ordinály $\beta < \alpha$ môžeme dostať množinu s podobnými vlastnosťami pre ordinál α. (Na dôkaz správnosti takéhoto postupu vás opäť môžem odkázať na [ŠS, Kapitola 9.6] a [Z].)

Úloha 8. Steinitzova veta: Pre každé pole existuje algebraicky uzavreté nadpole, ktoré ho obsahuje. [CL, Theorem 2.3.3]

Riešenie: 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 konštatnty a koreňových činiteľov.[4]

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 na F. Existuje teda minimálny polynóm $q(x)$ tohoto koreňa nad poľom F. Tento minimálny polynóm je v $L[x]$ násobkom polynómu $p(x)$, čiže $q(x) = p(x).r(x)$. Táto rovnosť platí aj v $K[x]$ (K je nadpole L), ale v K sa navyše polynóm $q(x)$ dá rozložiť na súčin koreňových činiteľov. Z toho vyplýva, že aj $p(x)$ sa dá rozložiť na súčin koreňových činiteľov.

Zostáva teda dokázať, že sa dá zostrojiť pole K s uvedenými vlastnosťami. Toto pole skonštruujeme transfinitnou rekurziou.

[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 rozkladovou 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

Nech $\{f_\beta(x), \beta < \gamma\}$ sú všetky ireducibilné polynómy nad F oindexované ordinálmi menšími ako γ. (Využili sme fakt, že množinu ireducibilných polynómov možno dobre usporiadať.) Pre každé $\alpha \leq \gamma$ zostrojíme algebraické rozšírenie K_α poľa F, v ktorom je každý polynóm $f_\beta(x)$ pre $\beta < \alpha$ rozložiteľný na súčin koreňových činiteľov.

1° Pre $\alpha = 0$ zoberieme priamo pole K.

2° Ak máme zostrojené pole K_α, tak $K_{\alpha+1}$ bude rozkladové pole polynómu f_α nad poľom K_α. Rozkladové pole je algebraické rozšírenie K_α, pretože K_α je algebraické rozšírenie F je aj K_α algebraickým rozšírením F.

3° Ak α je limitný ordinál, tak by sme K_α chceli zadefinovať ako pole, ktoré bude obsahovať K_β pre všetky $\beta < \alpha$ – čosi ako zjednotenie týchto polí. Pretože všetky polia sú také, že polia oindexované nižšími ordinálmi sú vnorené ako podpolia v tých poliach, ktoré majú vyššie indexy, môžeme priamo predpokladať, že sú to polia na podmnožinách tej istej množiny (toto si treba rozmyslieť!) a potom skutočne stačí zobrať priamo zjednotenie týchto polí. $\square$

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.

Úloha 9. 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 $A^y = \{y \in \mathbb{R}; (x, y) \in A\}$ sú husté v $\mathbb{R}$. [C, Theorem 6.1.1]

Takáto množina je grafom silno darbouxovskej funkcie. Funkcia $f : \mathbb{R} \to \mathbb{R}$ 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.

Riešenie: 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

$$A \cap \{y\} \times (a, b) \neq \emptyset.$$

Množina všetkých takýchto vodorovných úsečiek v rovine $\{\{y\} \times (a, b); y, a, b \in \mathbb{R}, a < b\}$ 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 $\{U_\alpha = \{y_\alpha\} \times (a_\alpha, b_\alpha); \alpha < \mathfrak{c}\}$.

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

Ako ďalší príklad tvrdenia, ktoré by sa dalo dokazovať použitím princípu dobrého usporiadania a transfinitnej indukcie spomeňme existenciu Hamelovej bázy v ľubovoľnom vektorovom priestore, pozri napríklad [ŠS, Príklad 10.3.1, Cvičenie 10.3.2]. (Štandardný dôkaz je pomocou princípu maximality, ktorý ste však nemali.) Pomocou Hamelovej bázy sa napríklad dá ukázať, že existujú nespojité funkcie $f\colon \mathbb{R} \to \mathbb{R}$ spĺňajúce rovnicu $f(x + y) = f(x) + f(y)$ – [ŠS, Cvičenie 10.3.5]. (Ekvivalentné tvrdenie: Existujú riešenie tejto funkcionálnej rovnice, ktoré nie sú lineárne, t.j. nie sú tvaru $f(x) = kx$, $k \in \mathbb{R}$.)

Literatúra

[C] K. Ciesielski. *Set Theory for the Working Mathematician.* Cambridge University Press, Cambridge, 1997. London Mathematical Society Student Texts 39.

[CL] Antoine Chambert-Loir. *A Field Guide to Algebra.* Springer, New York, 2005. Undergraduate Texts in Mathematics.

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

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

[Z] Pavol Zlatoš. O dobrom usporiadaní a axióme výberu. `http://thales.doa.fmph.uniba.sk/zlatos/wo/DUAC1w.pdf`.