O DOBROM USPORIADANÍ A AXIÓME VÝBERU

Hoci jazyk teórie množín v súčasnej matematike, zdá sa, už nadobro prevládol, v skutočnosti len nepatrný zlomok hlbších výsledkov tejto teórie nachádza širšie uplatnenie v ostatnej matematike. K nim bezosporu patrí najmä axióma výberu, či niektoré jej ekvivalenty – ako napr. rôzne princípy maximality, – dôkazy transfinitnou indukciou či konštrukcia transfinitnou rekurziou. Je preto iróniou a paradoxom, že v súčasnom systéme vzdelávania a výchovy matematikov u nás sa poslucháči s týmito výsledkami nezoznámia, hoci sa považuje za samozrejmé, že ich plody (napr. Hahnova-Banachova veta vo funkcionálnej analýze, alebo Tichonovova veta v topológii) sa bežne využívajú. Ich dôkazy, pokiaľ sa vôbec podávajú, tak spočívajú na nevyjasnených predpokladoch.

Tento príspevok je pokusom zaplniť spomínanú medzeru. Ďalej nepredpokladám u čitateľa nijaké špeciálne znalosti z teórie množín. Používam bežnú množinovú symboliku a pojmy na úrovni absolventov prvého ročníka matematického štúdia. Všetko, čo leží „v hlavnej línii“ a presahuje tento rámec, sa pokúsim aspoň stručne vysvetliť. Na druhej strane text obsahuje rad poznámok určených rôzne zasväteným adresátom, ktoré však nie sú nevyhnutné na sledovanie väčšiny výkladu. Niektoré detaily sú zámerne vynechané a ponechané na doplnenie čitateľovi, ktorého aktívna spolupráca je nevyhnutným predpokladom osvojenia si študovaného materiálu.

Čiastočne usporiadané množiny – základné pojmy

Pod čiastočným usporiadaním budeme vždy rozumieť ostré čiastočné usporiadanie. Zrejme pre ľubovoľnú čiastočne usporiadanú množinu $(X, <)$ je aj $(X, >)$, t. j. X s opačným usporiadaním, čiastočne usporiadaná množina; toto usporiadanie je lineárne práve vtedy, keď pôvodné usporiadanie bolo lineárne.

Každá podmnožina čiastočne usporiadanej množiny $(X, <)$ je zrejme sama čiastočne usporiadaná reláciou $<$. Podmnožina A čiastočne usporiadanej množiny $(X, <)$ sa nazýva *reťazec*, ak $(A, <)$ je lineárne usporiadaná. Hovoríme, že podmnožina A čiastočne usporiadanej množiny $(X, <)$ je *usmernená*, ak pre ľubovoľné $x, y \in A$ existuje $z \in A$ také, že $x \leq z$ a $y \leq z$.

Množina $A \subseteq X$ sa nazýva *počiatočný úsek* alebo *dolný rez* čiastočne usporiadanej množiny $(X, <)$, ak pre ľubovoľné $a \in A$, $x \in X$ platí $x \leq a \Rightarrow x \in A$. Pre každé $a \in X$ množina $X^{(a)} = \{x \in X;\, x < a\}$ je dolný rez v $(X, <)$. Zrejme v lineárne usporiadanej množine $(X, <)$ pre ľubovoľné počiatočné úseky A, $B \subseteq X$ platí $A \subseteq B$ alebo $B \subseteq A$.

Nech $(X, <)$, $(Y, <)$ sú čiastočne usporiadané množiny. Zobrazenie $f\colon X \to Y$ sa nazýva *izomorfizmom* $(X, <)$ na $(Y, <)$, ak f je bijekcia a pre všetky $x, y \in X$ platí $x < y \Leftrightarrow f(x) < f(y)$. Zápis $(X, <) \cong (Y, <)$ označuje, že $(X, <)$ a $(Y, <)$ sú izomorfné. t. j. existenciu nejakého izomorfizmu $(X, <)$ na $(Y, <)$. Zobrazenie f nazývame *počiatočným vnorením* z $(X, <)$ do $(Y, <)$, ak jeho definičný obor $\operatorname{dom} f$ je počiatočný úsek v $(X, <)$, jeho obor hodnôt $\operatorname{rng} f$ je počiatočný úsek v $(Y, <)$ a $f\colon \operatorname{dom} f \to \operatorname{rng} f$ je izomorfizmus čiastočne usporiadaných množín.

Pre každú čiastočnú uporiadanú množinu $(X, <)$ značíme $o(X, <)$ jej *ordinálny typ*. Nie je dôležité, čo sú ordinálne typy – pre nás je podstatná len ich nasledujúca vlastnosť: Pre ľubovoľné čiastočne usporiadané množiny $(X, <)$, $(Y, <)$ platí

$$o(X, <) = o(Y, <) \;\Leftrightarrow\; (X, <) \cong (Y, <).$$

Nech $(I, <)$ je čiastočne usporiadaná množina a pre každé $i \in I$ je $(X_i, <)$ čiastočne usporiadaná množina. *Lexikografickou sumou* systému $\big((X_i, <);\, i \in I\big)$ nazývame množinu

$$\sum_{i \in I} X_i = \bigcup_{i \in I} \{i\} \times X_i$$

spolu s *lexikografickým čiastočným usporiadaním* definovaným vzťahom

$$(i, x) <_{\text{lex}} (j, y) \;\Leftrightarrow\; i < j \;\vee\; (i = j \;\&\; x < y)$$

pre $i, j \in I$, $x \in X_i$, $y \in X_j$, a značíme ju $\sum_{i \in (I, <)} (X_i, <)$. Zrejme ak $(I, <)$ aj všetky $(X_i, <)$ sú lineárne usporiadané, tak aj ich lexikografická suma je lineárne usporiadaná.

Ak I aj všetky X_i sú konečné, tak Hasseovej diagram príslušnej lexikografickej sumy dostaneme tak, že namiesto každého vrcholu i Hasseovj diagramu čiastočne usporiadanej množiny $(I, <)$ dosadíme Hasseovej diagram čiastočne usporiadanej množiny $(X_i, <)$ a pre každú pokrývajúcu sa dvojicu $i \prec j$ v I spojíme stúpajúcou hranou každý maximálny prvok množiny X_i s každým minimálnym prvkom množiny X_j.

Ak $I = \{0, 1\}$ je dvojprvkový reťazec, tak príslušnú lexikografickú sumu značíme jednoducho $(X_0, <) + (X_1, <)$ a nazývame ju *lexikografickým súčtom* alebo len krátko *súčtom* čiastočne usporiadaných množín $(X_0, <)$, $(X_1, <)$.

Ak $(X_i, <) = (X, <)$ pre každé $i \in I$, tak príslušnú lexikografickú sumu značíme $(I, <) \cdot (X, <)$ a nazývame *lexikografickým súčinom* čiastočne usporiadaných množín $(I, <)$, $(X, <)$.

Zrejme konštrukcia lexikografickej sumy dáva pre izomorfné argumenty izomorfné výsledky. Pesnejšie, ak $q : (I, <) \to (J, <)$ a $f_i \colon (X_i, <) \to (Y_{q(i)}, <)$ pre každé $i \in I$ sú izomorfizmy čiastočne usporiadaných množín, tak aj priradenie $(i, x) \mapsto (q(i), f_i(x))$ definuje izomorfizmus

$$F \colon \sum_{i \in (I, <)} (X_i, <) \to \sum_{j \in (J, <)} (Y_j, <)$$

čiastočne usporiadaných množín.

To nám umožňuje zaviesť operáciu lexikografickej sumy, špeciálne lexikografického súčtu a súčinu pre ľubovoľné ordinálne typy. Napríklad, ak $\alpha = o(X, <)$, $\beta = o(Y, <)$, tak ordinálne typy

$$\alpha + \beta = o\big((X, <) + (Y, <)\big),$$
$$\alpha \cdot \beta = o\big((X, <) \cdot (Y, <)\big)$$

nazývame súčtom resp. súčinom ordinálnych typov α, β. Zrejme súčet i súčin ordinálnych typov nezávisia na výbere príslušných čiastočne usporiadaných množín daného typu.

Pre každé $n \in \mathbb{N}$ ordinálny typ lineárne usporiadanej n-prvkovej množiny označíme priamo číslom n; ω označuje ordinálny typ množiny $\mathbb{N}$ všetkých prirodzených čísel v obvyklom usporiadaní. Zrejme uvedené definície ordinálneho súčtu a súčinu splývajú pre prirodzené čísla s obyčajným súčtom resp. súčinom.

Overte si, že pre ľubovoľné ordinálne typy α, β, γ platí

$$\begin{aligned} \alpha + (\beta + \gamma) &= (\alpha + \beta) + \gamma, & 0 + \alpha &= \alpha = \alpha + 0, \\ \alpha \cdot (\beta \cdot \gamma) &= (\alpha \cdot \beta) \cdot \gamma, & 1 \cdot \alpha &= \alpha = \alpha \cdot 1, \\ (\alpha + \beta) \cdot \gamma &= (\alpha \cdot \gamma) + (\beta \cdot \gamma), & 0 \cdot \alpha &= 0 = \alpha \cdot 0. \end{aligned}$$

Na druhej strane však

$$\begin{gathered} 1 + \omega = \omega \neq \omega + 1, \\ \omega \cdot (1 + 1) = \omega \cdot 2 = \omega \neq 2 \cdot \omega = \omega + \omega = (\omega \cdot 1) + (\omega \cdot 1). \end{gathered}$$

To znamená, že sčítanie ani násobenie ordinálnych typov nie je komutatívne, rovnako ako násobenie nie je zľava distributívne vzhľadom na sčítanie.

Základné vlastnosti dobre usporiadaných množín

Hovoríme, že $(X, <)$ je *dobre usporiadaná množina*, ak X je lineárne usporiadaná reláciou $<$ a každá neprázdna množina $A \subseteq X$ má v tomto usporiadaní najmenší prvok. Zrejme každá podmnožina dobre usporiadanej množiny je v tomto usporiadaní sama dobre usporiadná.

Ako cvičenie si overte nasledujúci výsledok.

Veta. *Množina X je konečná práve vtedy, keď existuje relácia $<$ na X taká, že $(X, <)$ aj $(X, >)$ sú dobre usporiadané množiny.*

Veta. *Nech $(X, <)$, $(Y, <)$ sú dobre usporiadané množiny, $A \subseteq X$ je počiatočý úsek v X a $f\colon A \to Y$, $g\colon X \to Y$ sú počiatočné vnorenia. Potom $f \subseteq g$, t. j. pre všetky $a \in A$ platí $f(a) = g(a)$.*

Dôkaz.
Predpokladajme, že $f(a) \neq g(a)$ pre nejaké $a \in A$, teda $\{a \in A;\, f(a) \neq g(a)\} \neq \emptyset$; označme m najmenší prvok tejto množiny. Potom $f(x) = g(x)$ pre každé $x < m$. Platí $f(m) < g(m)$ alebo $g(m) < f(m)$. V prvom prípade existuje $b \in X$ také, že $g(b) = f(m) < g(m)$, teda $b < m$. Potom $f(b) = g(b) = f(m)$, čo je spor s injektívnosťou f. Podobne, v druhom prípade existuje $a \in A$ také, že $f(a) = g(m) < f(m)$. Preto $a < m$, v dôsledku čoho $g(m) = f(a) = g(a)$, a to je zas spor s injektívnosťou g.

Dôsledok. *Nech $(X, <)$ je dobre usporiadaná množina. Potom*

(a) identické zobrazenie $X \to X$ je jediným automorfizmom na $(X, <)$;
(b) ak A, B sú dva dolné rezy v $(X, <)$ tak $(A, <) \cong (B, <) \;\Leftrightarrow\; A = B$.

Veta. *Nech $(X, <)$, $(Y, <)$ sú dobre usporiadané množiny. Potom existuje práve jedno zobrazenie f, ktoré je izomorfizmom X na počiatočný úsek v Y alebo izomorfizmom počiatočného úseku v X na Y.*

Dôkaz.
Podľa predchádzajúcej vety také zobrazenie f existuje najviac jedno. Nech F je množina všetkých počiatočných vnorení X do Y. Na základe tej istej vety ľahko nahliadneme, že aj $f = \bigcup F$ je počiatočné vnorenie X do Y. Teda f je najväčší prvok množiny F vzhľadom na inklúziu. Položme $A = \operatorname{dom} f$, $B = \operatorname{rng} f$. Ukážeme, že platí $A = X$ alebo $B = Y$. Pripusťme, že obe mmnožiny $X \setminus \operatorname{dom} f$, $Y \setminus \operatorname{rng} f$ sú neprázdne a označme x resp. y ich najmenšie prvky. Ľahko sa overí, že $f \cup \{(x, y)\}$ je počiatočné vnorenie X do Y, ktoré je vlastnou nadmnožinou f, čo je spor.

Na dobre usporiadané množiny možno zovšeobecniť princíp indukcie, ako aj vetu o rekurzii platné v (dobre usporiadanej) množine prirodzených čísel $(\mathbb{N}, <)$. V takomto prípade hovoríme o tzv. *transfinitnej indukcii* resp. *transfinitnej rekurzii.*

Veta. *(O transfinitnej indukcii) Nech $(X, <)$ je dobre usporiadaná množina. Nech $A \subseteq X$ je množina taká, že*

$$\big(\forall\, a \in X\big)\big(X^{(a)} \subseteq A \;\Rightarrow\; a \in A\big).$$

Potom $A = X$.

Dôkaz.
Nech $A \neq X$ a m je najmenší prvok množiny $X \setminus A$. Potom $X^{(m)} \subseteq A$, teda $m \in A$, čo je spor.

Rovnako ľahko možno nahliadnuť, že ľubovoľná lineárne usporiadaná množina, ktorá spĺňa princíp indukcie v uvedenej podobe, je dobre usporiadaná.

Veta. *(O transfinitnej rekurzii) Nech $(X, <)$ je dobre usporiadaná množina, Z je ľubovoľná množina a g je funkcia taká, že*

$$\operatorname{dom} g = \bigcup_{a \in X} Z^{X^{(a)}}.$$

Potom existuje jediná funkcia $f\colon X \to Z$ taká, že pre každé $a \in X$ platí

$$f(a) = g\big(f \restriction X^{(a)}\big).$$

Dôkaz.
Najprv dokážeme jednoznačnosť. Nech f_1, f_2 sú dve také funkcie. Ukážeme, že $f_1 = f_2$. Označme $A = \{a \in X;\, f_1(a) = f_2(a)\}$. Stačí overiť, že platí $A = X$. Nech $a \in X$ je také, že $X^{(a)} \subseteq A$, t. j. $f_1 \restriction X^{(a)} = f_2 \restriction X^{(a)}$. Potom

$$f_1(a) = g\big(f_1 \restriction X^{(a)}\big) = g\big(f_2 \restriction X^{(a)}\big) = f_2(a),$$

teda $a \in A$. Podľa vety o indukcii $A = X$.

Ukážeme, že také f existuje. Označme H množinu všetkých zobrazení $h\colon X^{(a)} \to Z$ takých, že $a \in X$ a pre všetky $x < a$ platí $h(x) = g\big(h \restriction X^{(x)}\big)$. Z práve dokázanej jednoznačnosti vyplýva, že pre ľubovoľné $h_1, h_2 \in H$ platí $h_1 \subseteq h_2$ alebo $h_2 \subseteq h_1$. Z toho vyplýva, že $f = \bigcup H$ je zobrazenie nejakého počiatočného úseku množiny X do Z. Zrejme aj podmienka $f(a) = g\big(f \restriction X^{(a)}\big)$ platí pre každé $a \in \operatorname{dom} f$. Zostáva overiť rovnosť $\operatorname{dom} f = X$. Ak však $X^{(a)} \subseteq \operatorname{dom} f$, tak $f \restriction X^{(a)} \in H$. Potom tiež $f \restriction X^{(a)} \cup \big\{\big(a, g\big(f \restriction X^{(a)}\big)\big)\big\} \in H$, teda $a \in \operatorname{dom} f$. Podľa vety o indukcii $\operatorname{dom} f = X$.

Veta. *Nech $(I, <)$ je dobre usporiadaná množina a pre každé $i \in I$ je $(X_i, <)$ dobre usporiadaná množina. Potom aj lexikografická suma*

$$\sum_{i \in (I,<)} (X_i, <)$$

je dobre usporiadaná množina.

Dôkaz.
Nech $\emptyset \neq C \subseteq \sum_{i \in I} X_i$. Potom aj podmnožina $\{i \in I;\ (\{i\} \times X_i) \cap C \neq \emptyset\}$ dobre usporiadanej množiny $(I, <)$ je neprázdna. Ak m je jej najmenší prvok a z je najmenší prvok neprázdnej podmnožiny $\{x \in X^{(m)};\ (m, x) \in C\}$ dobre usporiadanej množiny $(X_i, <)$, tak (m, z) je zrejme najmenší prvok množiny C.

Teda špeciálne lexikografický súčet aj lexikografický súčin dvoch dobre usporiadaných množín sú opäť dobre usporiadané množiny.

Ordinálne čísla

Ordinálne typy dobre usporiadaných množín budeme nazývať *ordinálnymi číslami*. Na rozdiel od všeobecných ordinálnych typov však jestvuje kanonický spôsob ako každej dobre usporiadanej množine priradiť jednoznačne určenú s ňou izomorfnú množinu dobre usporiadanú reláciou náležania $\in$.

Hovoríme, že množina x je *tranzitívna*, ak $z \in y \ \& \ y \in x \Rightarrow z \in x$ pre všetky y, z. Hovoríme, že x je *ordinálne číslo* alebo len krátko *ordinál*, ak x je tranzitívna množina a relácia $\in_x = \{(z, y) \in x^2;\ z \in y\}$ je dobrým usporiadaním množiny x. Hovoríme, že x je *prirodzené číslo*, ak x je konečná množina a ordinálne číslo.

Ľahko nahliadneme, že množina $\mathbb{N}$ všetkých prirodzených čísel je ordinálne číslo. V tomto význame ju budeme značiť $\mathbb{N} = \omega$. Zrejme ω je najmenšie nekonečné ordinálne číslo.

Podobne ako pre množiny možno zaviesť tiež pojmy čiastočne usporiadanej triedy, dobre usporiadanej triedy, tranzitívnej triedy a pod., a dokázať pre ne podobné výsledky ako pre množny.

Triedu všetkých ordinálov budeme značiť $\mathbf{\Omega}$. Ľahko sa overí, že $\mathbf{\Omega}$ je tranzitívna trieda, dobre usporiadaná reláciou $\in$. Príslušné neostré usporiadanie je potom dané reláciou inklúzie $\alpha \subseteq \beta$. Ďalej pre každé $\alpha \in \mathbf{\Omega}$ platí

$$\mathbf{\Omega}^{(\alpha)} = \{\beta \in \mathbf{\Omega};\ \beta \in \alpha\} = \alpha.$$

Z toho okamžite vyplýva, že trieda $\mathbf{\Omega}$ nie je množinou. V opačnom prípade by totiž platilo $\mathbf{\Omega} \in \mathbf{\Omega}$. Ale pre žiadny ordinál nemôže platiť $\alpha \in \alpha$ – relácia náležania $\in$ je totiž ostré lineárne usporiadanie na $\mathbf{\Omega}$.

Veta. *Nech $\mathbf{X}$ je tranzitívna trieda dobre usporiadaná reláciou $\in_{\mathbf{X}}$. Potom $\mathbf{X}$ je vlastná trieda práve vtedy, keď $\mathbf{X} = \mathbf{\Omega}$.*

Dôkaz. Zostáva dokázať, že pre každé také $\mathbf{X}$ platí $\mathbf{X} = \mathbf{\Omega}$. Ak $\mathbf{X}$ je tranzitívna a $\in$ je dobré usporiadanie na X, tak každý prvok triedy $\mathbf{X}$ je zrejme ordinál. Nech $\mathbf{X} \neq \mathbf{\Omega}$ a α je najmenší ordinál taký, že $\alpha \notin \mathbf{X}$. Potom $\mathbf{X} \subseteq \alpha$, teda $\mathbf{X}$ je množina.

Ordinálne číslo $\alpha \cup \{\alpha\}$ nazývame *nasledovníkom* ordinálneho čísla α. Hovoríme, že α je *limitné* ordinálne číslo, ak α nie je nasledovníkom žiadneho ordinálu. Zrejme 0 a ω sú limitné ordinálne čisla a každé $0 \neq n \in \omega$ je nasledovníkom čísla $n-1$.

Aj pre triedu všetkých ordinálnych čísel možno vysloviť tvrdenia o transfinitnej indukcii a transfinitnej rekurzii, podobne ako pre dobre usporiadané množiny. Keďže toto je vlastne ten najčastejšie používaný prípad, osobitne sformulujeme i tieto tvrdenia, ich dôkazy však vynecháme. Vopred si ešte uvedomme, že každá tranzitívna trieda $\mathbf{X} \subseteq \mathbf{\Omega}$ je alebo množina, a potom $\mathbf{X} \in \mathbf{\Omega}$, alebo $\mathbf{X} = \mathbf{\Omega}$

Veta. *(O transfinitnej indukcii) Nech $\mathbf{X} \subseteq \mathbf{\Omega}$ je tranzitívna trieda. Nech $\mathbf{A} \subseteq \mathbf{X}$ je trieda taká, že*

$$(\forall\, \alpha \in \mathbf{X})(\alpha \subseteq \mathbf{A} \;\Rightarrow\; \alpha \in \mathbf{A}).$$

Potom $\mathbf{A} = \mathbf{X}$.

Veta. *(O transfinitnej rekurzii) Nech $\mathbf{X} \subseteq \mathbf{\Omega}$ je tranzitívna trieda, $\mathbf{Z}$ je ľubovoľná trieda a $\mathbf{G}$ je funkcia (možno triedová) taká, že*

$$\operatorname{dom} \mathbf{G} = \bigcup_{\alpha \in \mathbf{X}} \mathbf{Z}^{\alpha}.$$

Potom existuje jediná funkcia $\mathbf{F}\colon \mathbf{X} \to \mathbf{Z}$ (možno triedová) taká, že pre každé $\alpha \in \mathbf{X}$ platí

$$\mathbf{F}(\alpha) = \mathbf{G}(\mathbf{F} \restriction \alpha).$$

Veta o transfinitnej rekurzii má aj iné ekvivalentné podoby. Niekedy je výhodnejší tvar, v ktorom sa hodnota $\mathbf{F}(\alpha)$ zostrojí zvlášť pre nasledovník α a zvlášť pre limitné α.

Veta. *(O transfinitnej rekurzii) Nech $\mathbf{X} \subseteq \mathbf{\Omega}$ je tranzitívna trieda, $\mathbf{Z}$ je ľubovoľná trieda $z \in \mathbf{Z}$ a $\mathbf{G}_1$, $\mathbf{G}_2$ sú funkcie (možno triedové) také, že*

$$\operatorname{dom} \mathbf{G}_1 = \mathbf{Z}, \qquad \operatorname{dom} \mathbf{G}_2 = \bigcup_{0 \neq \alpha \in \mathbf{X}} \mathbf{Z}^{\alpha}.$$

Potom existuje jediná funkcia $\mathbf{F}\colon \mathbf{X} \to \mathbf{Z}$ (možno triedová) taká, že

$$\begin{aligned}
&\mathbf{F}(0) = z \\
&\mathbf{F}(\alpha) = \mathbf{G}_1(\mathbf{F}(\beta)), \qquad &&\text{ak } \alpha \in \mathbf{X} \text{ je nasledovníkom } \beta, \text{ a} \\
&\mathbf{F}(\alpha) = \mathbf{G}_2(\mathbf{F} \restriction \alpha) \qquad &&\text{pre limitné } 0 \neq \alpha \in \mathbf{X}.
\end{aligned}$$

Nasledujúcou vetou plníme sľub daný na začiatku tohto odstavca – reprezentovať každý ordinálny typ dobre usporiadanej množiny nejakým ordinálnym číslom z triedy $\mathbf{\Omega}$.

Veta. *Nech $(X, <)$ je dobre usporiadaná množina. Potom existuje práve jedno ordinálne číslo α také, že $(X, <) \cong (\alpha, \in)$.*

Dôkaz.
Zrejme taký ordinál existuje najviac jeden. Pre $\alpha \in \beta$ je totiž α počiatočným úsekom v $(\beta, \in)$, teda nemôže platiť $(\alpha, \in) \cong (\beta, \in)$.

Na základe výsledkov predošlého odstavca pre každé $\alpha \in \mathbf{\Omega}$ existuje (dokonca jediné) zobrazenie f_α, ktoré je izomorfizmom nejakého počiatočného úseku $A \subseteq \alpha$ na $(X, <)$ alebo izomorfizmom $(\alpha, <)$ na nejaký počiatočný úsek $B \subseteq X$. Keby pre všetky $\alpha \in \mathbf{\Omega}$ nastala druhá možnosť, tak $\mathbf{F} = \bigcup_{\alpha\in\mathbf{\Omega}} f_\alpha$ by bolo izomorfizmom $(\mathbf{\Omega}, \in)$ na nejaký počiatočný úsek v $(X, <)$, čo je nemožné, lebo X je množina a $\mathbf{\Omega}$ je vlastná trieda. Preto existuje ordinál α taký, že f_α je izomorfizmom nejakého počiatočného úseku v $(\alpha, \in)$ na $(X, <)$. Ak si vezmeme najmenšie také α, tak $\operatorname{dom} f_\alpha = \alpha$.

Teda pre dobre usporiadanú množinu $(X, <)$ definujeme jej ordinálne číslo $o(X, <)$ ako ten jednoznačne určený ordinál α, pre ktorý platí $(X, <) \cong (\alpha, \in)$. Základná vlastnosť ordinálnych typov $o(X, <) = o(Y, <) \;\Leftrightarrow\; (X, <) \cong (Y, <)$ zostáva zrejme zachovaná.

Na triede $\mathbf{\Omega}$ máme navyše definované asociatívne operácie súčtu a súčinu, ktoré rozširujú sčítanie a násobenie prirodzených čísel a prvky 0, 1 si v nich zachovávajú svoje výsadné postavenie. Taktiež pre každé $\alpha \in \mathbf{\Omega}$ platí $\alpha+1 = \alpha\cup\{\alpha\}$, rovnako ako pre prirodzené čísla. Na druhej strane, ako sme už videli, ani jedna z týchto operácií nie je komutatívna a násobenie je distributívne vzhľadom na sčítanie len zľava no nie sprava. Takisto pre ne neplatí zákon o krátení.

Transfinitnou rekurziou (v premennej β) možno tiež definovať operáciu umocňovania ordinálnych čísel α^β pre všetky $\alpha, \beta \in \mathbf{\Omega}$. Kladieme

$$\begin{aligned} \alpha^0 &= 1, \\ \alpha^\beta &= \alpha \cdot \alpha^\gamma, && \text{ak } \beta \text{ je nasledovníkom } \gamma, \text{ a} \\ \alpha^\beta &= \bigcup_{\gamma\in\beta} \alpha^\gamma && \text{pre limitné } \beta. \end{aligned}$$

Zrejme aj táto operácia splýva na množine prirodzených čísel s obyčajným umocňovaním. Podrobnejšie štúdium ordinálnej aritmetiky už nie je našim cieľom.

Kardinálne čísla

Pripomíname, že pre ľubovoľné množiny X, Y formuly $X \approx Y$, $X \precsim Y$ označujú existenciu bijektívneho resp. injektívneho zobrazenia $X \to Y$. Zápis $X \prec Y$ znamená $X \precsim Y \;\&\; X \not\approx Y$.

Mohutnosť alebo *kardinálne číslo* množiny X označujeme $|X|$. Podobne ako pri zavedení pojmu ordinálneho typu, ani teraz nie je dôležité, čo sú mohutnosti množín – podstatný je pre nás jedine nasledujúci vzťah

$$|X| = |Y| \;\Leftrightarrow\; X \approx Y,$$

platný pre všetky množiny X, Y. Ďalej potom kladieme

$$\begin{aligned} |X| \precsim |Y| &\;\Leftrightarrow\; X \precsim Y, \\ |X| \prec |Y| &\;\Leftrightarrow\; X \prec Y. \end{aligned}$$

Taktiež známym spôsobom zavádzame operácie súčtu, súčinu a mocniny kardinálnych čísel. Ak $\alpha = |X|$, $\beta = |Y|$, tak

$$\begin{aligned} \alpha + \beta &= |(\{0\} \times X) \cup (\{1\} \times Y)|, \\ \alpha \cdot \beta &= |X \times Y|, \\ \alpha^\beta &= \left|X^Y\right|. \end{aligned}$$

Zrejme uvedené definície usporiadania aj operácií na kardinálnych číslach sú korektné, t. j. nezávisia od jednotlivých množín, len od ich mohutností. Z radu známych vlastností kardinálnej aritmetiky tu pripomenieme len Cantorovu-Bernsteinovu vetu:

$$|X| \precsim |Y| \ \& \ |Y| \precsim |X| \ \Leftrightarrow \ |X| = |Y|.$$

Teraz priradíme každej množine, ktorú možno dobre usporiadať (a ak platí axióma výberu, tak vôbec každej), konkrétnu s ňou ekvivalentnú množinu, ktorú oprávnene možno stotožniť s jej mohutnosťou.

Každé ordinálne číslo je zároveň množina, teda prostredníctvom injektívnych resp. bijektívnych zobrazení môžeme porovnávať jeho mohutnosť s inými množinami, špeciálne s inými ordinálmi.

Ordinálne číslo α nazývame *kardinálnym číslom* alebo len krátko *kardinálom*, ak pre každé $\beta \in \alpha$ platí $\beta \prec \alpha$. Teda zo všetkých ordinálnych čísel danej mohutnosti je príslušné kardinálne číslo to najmenšie. Preto pre kardinálne čísla $\alpha, \beta \in \mathbf{\Omega}$ platí $\alpha \prec \beta \ \Leftrightarrow \ \alpha \in \beta$, t. j. kardinálne a ordinálne usporiadanie na triede $\mathbf{\Omega}$ splývajú.

Uvedená definícia vyznačuje *niektoré* spomedzi ordinálnych čísel ako kardinálne čísla. Bez dodatočných predpokladov však nemožno zaručiť, že takto dostaneme *všetky* kardinálne čísla.

Zrejme každé prirodzené číslo je kardinálne číslo. Taktiež $\mathbb{N} = \omega$ je kardinálne číslo – v tomto význame ho väčšinou značíme $\aleph_0$. Aj najmenší nespočítateľný ordinál je kardinálom – v prvom význame ho značíme ω_1, v druhom $\aleph_1$.

Zrejme pre prirodzené čísla kardinálne operácie súčtu, súčinu a mocniny splývajú s ordinálnymi. Je však dôležité si uvedomiť, že pre nekonečné kardinálne čísla tomu tak nie je. Kardinálny súčet a súčin sú totiž komutatívne, kým ich ordinálne verzie nie sú. Podobne, podľa známej Cantorovej vety pre ľubovoľné kardinálne číslo α platí $\alpha \prec 2^\alpha$. Na druhej strane pre ordinálnu mocninu platí $2^\omega = \omega$. Taktiež ω^ω, ω^{ω^ω}, atď. sú stále len spočítateľné ordinály, teda nie sú to kardinály.

Zo skôr dokázaných výsledkov okamžite vyplýva

Veta. *Množinu X možno dobre usporiadať práve vtedy, keď $|X| \in \mathbf{\Omega}$. V takom prípade $X \approx |X|$.*

Pre každé ordinálne číslo $\alpha \in \mathbf{\Omega}$ označme

$$\alpha^+ = \{\beta \in \mathbf{\Omega};\ \beta \precsim \alpha\}.$$

Ak α je kardinálne číslo, tak α^+ nazývame *nasledovníkom* kardinálneho čísla α.

Veta. *Pre každé ordinálne číslo $\alpha \in \mathbf{\Omega}$ je α^+ najmenšie kardinálne číslo $\beta \in \mathbf{\Omega}$ také, že $\alpha \in \beta$.*

Dôkaz.
Zrejme $\alpha \in \alpha^+$. Z Cantorovej-Bernsteinovej vety vyplýva, že α^+ je počiatočný úsek v $(\mathbf{\Omega}, \in)$. Dokážeme, že α^+ nie je vlastná trieda. Potom α^+ je najmenší ordinál β taký, že $\beta \notin \alpha^+$. Zrejme $\alpha^+ = \alpha \cup \{\gamma \in \mathbf{\Omega};\ \gamma \approx \alpha\}$. Keby α^+ bola vlastná trieda, bola by aj $\alpha^+ \setminus \alpha = \{\gamma \in \mathbf{\Omega};\ \gamma \approx \beta\}$ vlastná trieda. To by znamenalo, že na množine α existuje vlastná trieda navzájom neizomorfných dobrých usporiadaní. Ale každé dobré usporiadanie množiny α je prvok množiny $\mathcal{P}(\alpha \times \alpha)$. To je spor. Teda $\alpha^+ \in \mathbf{\Omega}$. Zrejme $\beta \prec \alpha^+$ pre každé $\beta \in \alpha^+$, teda α^+ je kardinálne číslo a pre každé kardinálne číslo $\beta \in \mathbf{\Omega}$ platí $\alpha \in \beta \ \Rightarrow \ \alpha^+ \subseteq \beta$.

Na jednom mieste tohto dôkazu sme si neoprávnene trochu zjednodušili život. Skúste nájsť to miesto a premyslite si, ako možno dať celú vec do poriadku.

Veta. $\{\alpha \in \mathbf{\Omega};\ \alpha$ *je kardinálne číslo*$\}$ *je vlastná trieda.*

Dôkaz. Označme $\mathbf{C}$ uvedenú triedu. Potom $\mathbf{C} \subseteq \bigcup \mathbf{C}$ a $\bigcup \mathbf{C}$ je tranzitívna podtrieda v $\mathbf{\Omega}$. Keby $\mathbf{C}$ bola množina, bola by aj $\bigcup \mathbf{C}$ množina, teda $\bigcup \mathbf{C} = \gamma$ pre najmenšie $\gamma \in \mathbf{\Omega} \setminus \bigcup \mathbf{C}$. Ukážeme, že γ je kardinálne číslo. Potom $\gamma \notin \mathbf{C}$ bude hľadaný spor. Nech $\alpha \in \gamma$. Potom $\alpha \in \beta$ pre nejaké $\beta \in \mathbf{C}$. Keďže β je kardinálne číslo, $\alpha \prec \beta$. Tým skôr $\alpha \prec \gamma$.

Z posledných dvoch viet a z vety o transfinitnej rekurzii vyplýva, že všetky nekonečné kardinálne čísla z triedy $\mathbf{\Omega}$ možno zoradiť do rastúcej transfinitnej postupnosti

$$\aleph_0, \aleph_1, \ldots, \aleph_\omega, \ldots, \aleph_{\omega_1}, \ldots.$$

Presnejšie, existuje jediná triedová funkcia $\aleph\colon \mathbf{\Omega} \to \mathbf{\Omega}$ taká, že

$$\begin{aligned} \aleph_0 &= \omega, \\ \aleph_{\alpha+1} &= \aleph_\alpha^+ \qquad \text{pre každé } \alpha \in \mathbf{\Omega} \text{ a} \\ \aleph_\lambda &= \bigcup_{\alpha \in \lambda} \aleph_\alpha \quad \text{pre limitné } \lambda \in \mathbf{\Omega}. \end{aligned}$$

Jednoducho sa možno presvedčiť, že členmi tejto postupnosti sú práve všetky nekonečné kardinálne čísla z triedy $\mathbf{\Omega}$. Označenie $\aleph_\alpha$ používame väčšinou len v kardinálnom význame; $\aleph_\alpha$ ako ordinálne číslo značíme ω_α. To je zrejme v zhode s doteraz zavedeným označením $\aleph_0 = \omega_0$, $\aleph_1 = \omega_1$.

Čitateľovi je asi dobre známa rovnosť $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$. Toto kardinálne číslo nazývame *mohutnosťou kontinua*. Vieme len, že $\aleph_0 \prec 2^{\aleph_0}$, bez axiómy výberu však nevieme ani zaručiť, že sa mohutnosť kontinua nachádza niekde v rade alefov, nieto ešte určiť, ktorému z nich sa rovná. Tvrdenie $2^{\aleph_0} = \aleph_1$ sa nazýva *hypotéza kontinua* (CH). Zovšeobecnená hypotéza kontinua (GCH) tvrdí, že $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ pre každé $\alpha \in \mathbf{\Omega}$. Ako ukázal K. Gödel v r. 1938, zovšeobecnená hypotéza kontinua neprotirečí axiómam Zermelovho-Frankelovho systému s axiómou výberu. Presnejšie, pokiaľ je systém ZFC bezosporný, tak pridaním (GCH) k jeho axiómam vznikne opäť bezosporný systém. V r. 1963 P. Cohen ukázal, že ani hypotéza kontinua nie je dokázateľná v systéme ZFC. Obe hypotézy sú teda na základných axiómach teórie množín *nezávislé*.

Axióma výberu, princíp dobrého usporiadania a princípy maximality

Cieľom tohto odstavca je sformulovať princípy vymenované v jeho názve a dokázať ich ekvivalenciu a niekoľko ich dôsledkov.

Axióma výberu (v jej pôvodnej podobe) je nasledujúce tvrdenie:

Axióma výberu (AC). *Nech $\mathcal{S}$ je množina, ktorej prvkami sú neprázdne, po dvoch disjunktné množiny. Potom existuje množina Z taká, že pre každé $X \in \mathcal{S}$ množina $X \cap Z$ obsahuje práve jeden prvok.*

Teda uvedená množina Z vyberá z každej množiny $X \in \mathcal{S}$ po jednom prvku.

Jestvuje a používa sa viacero očividne evivalentných formulácií axiómy výberu. Väčšinu z nich zhŕňa nasledujúca veta. Jej dôkaz prenechávame čitateľovi ako cvičenie.

Veta. *Axióma výberu je ekvivalentná s každým z nasledujúcich tvrdení:*

(a) *Nech E je ekvivalencia na množine X. Potom existuje množina $Y \subseteq X$ taká, že $(\forall\, x \in X)(\exists!\, y \in Y)(x\, E\, y)$.*
(b) *Na každej množine X (ktorej prvkami sú množiny) existuje selektor, t. j. zobrazenie $h\colon X \to \bigcup X$ také, že $(\forall\, x \in X)(x \neq \emptyset \;\Rightarrow\; h(x) \in x)$.*
(c) *Pre každú reláciu R existuje funkcia f taká, že $\operatorname{dom} f = \operatorname{dom} R$ a $f \subseteq R$.*
(d) *Ku každej surjekcii $f\colon X \to Y$ existuje pravé inverzné zobrazenie, t. j. zobrazenie $g\colon Y \to X$ také, že $f \circ g = \mathrm{Id}_Y$.*
(e) *Ak $(X_i;\, i \in I)$ je systém neprázdnych množín, tak jeho karteziánsky súčin $\prod_{i\in I} X_i$ je neprázdny.*

Príklad. Rozmyslite si, na ktorom mieste a ako sa používa axióma výberu v dôkaze nasledujúcich tvrdení:

(a) Zjednotenie spočítateľného systému spočítateľných množín je spočítateľná množina.
(b) Funkcia $f\colon \mathbb{R} \to \mathbb{R}$ je spojitá v bode $a \in \mathbb{R}$ práve vtedy, keď pre každú postupnosť $\{a_n\}_{n=0}^{\infty}$ platí $\lim\limits_{n\to\infty} a_n = a \;\Rightarrow\; \lim\limits_{n\to\infty} f(a_n) = f(a)$.

Uvedomte si, že v oboch prípadoch vystačíme už tzv. *slabou axiómou výberu*, postulujúcou existenciu selektora len pre spočítateľné systémy množín nanajvýš mohutnosti kontinua.

Iným vyjadrením axiómy výberu je *princíp dobrého usporiadania.*

Princíp dobrého usporiadania (WO). *Každú množinu možno dobre usporiadať.*

Aj princíp dobrého usporiadanie má niekoľko očividných ekvivalentov.

Veta. *Princíp dobrého usporiadania je ekvivalentný s každým z nasledujúcich tvrdení:*

(a) *Pre každú množinu X platí $|X| \in \boldsymbol{\Omega}$.*
(b) *Pre každú nekonečnú množinu X existuje $\alpha \in \boldsymbol{\Omega}$ také, že $|X| = \aleph_\alpha$.*
(c) *Pre ľubovoľné množiny X, Y platí $X \precsim Y$ alebo $Y \precsim X$.*
(d) *Pre ľubovoľné kardinálne čísla α, β platí $\alpha \precsim \beta$ alebo $\beta \precsim \alpha$.*

Dôkaz.
Ukážeme len, že z (c) vyplýva princíp dobrého usporiadania. Nech X je ľubovoľná množina. Potom pre každý ordinál α platí $X \precsim \alpha$ alebo $\alpha \precsim X$. Ak pre nejaké α nastane prvá možnosť, sme hotoví, lebo injekciou $X \to \alpha$ sa na X prenesie dobré usporiadanie z α. Predpokladajme teda, že pre každé $\alpha \in \boldsymbol{\Omega}$ platí $\alpha \prec X$. Označme

$$E = \big\{(A, B) \in \mathcal{P}(X)^2;\; A \approx B\big\}.$$

Zrejme E je ekvivalencia na $\mathcal{P}(X)$. Pre každé $\alpha \in \boldsymbol{\Omega}$ položme

$$\mathbf{F}(\alpha) = \{A \in \mathcal{P}(A);\; \alpha \approx A\}.$$

Potom $\mathbf{F}(\alpha) \neq \emptyset$ pre každé $\alpha \in \boldsymbol{\Omega}$, teda $\mathbf{F}\colon \boldsymbol{\Omega} \to \mathcal{P}(X)/E$ je (triedové) zobrazenie. Zúženie $\mathbf{F}$ na triedu $\mathbf{C}$ všetkých kardinálnych čísel z triedy $\boldsymbol{\Omega}$ je potom prosté zobrazenie z $\mathbf{C}$ do $\mathcal{P}(X)/E$. Ale to je spor, lebo $\mathcal{P}(X)/E$ je množina a $\mathbf{C}$ je vlastná trieda.

Z početných dôsledkov princípu dobrého usporiadania uvedieme len tri, týkajúce sa kardinálnej aritmetiky.

Veta. *Predpokladajme platnosť (WO).*

(a) *Množina X je nekonečná práve vtedy, keď $\mathbb{N} \precsim X$, t.j. $\aleph_0$ je najmenšie nekonečné kardinálne číslo.*

(b) *Ak α, β sú kardinálne čísla a aspoň jedno z nich je nekonečné, tak $\alpha + \beta = \max(\alpha, \beta)$.*

(c) *Ak α, β sú kardinálne čísla rôzne od 0 a aspoň jedno z nich je nekonečné, tak $\alpha \cdot \beta = \max(\alpha, \beta)$.*

Dôkaz.
(a) je zrejmým dôsledkom predchádzajúcej vety; (b) aj (c) dokážeme súčasne. Stačí dokázať, že pre ľubovoľné kardinálne čísla $\alpha, \beta \in \mathbf{\Omega}$ platí:

$$0 \prec \alpha \precsim \beta \;\Rightarrow\; \alpha + \beta = \alpha \cdot \beta = \beta.$$

Za uvedených podmienok

$$\beta \precsim \alpha + \beta \precsim \beta + \beta \precsim \beta \cdot \beta, \qquad \text{a taktiež} \qquad \beta \precsim \alpha \cdot \beta \precsim \beta \cdot \beta.$$

Vďaka Cantorovej-Bernsteinovej vete teda stačí overiť nerovnosť $\beta^2 \precsim \beta$ pre každý nekonečný kardinál β. Budeme postupovať transfinitnou indukciou cez dobre usporiadanú triedu všetkých nekonečných kardinálov z triedy $\mathbf{\Omega}$. Na základe (WO) táto trieda obsahuje všetky nekonečné kardinály. Pre $\beta = \aleph_0$ to možno jednoducho overiť priamo. Nech teda $\aleph_0 \prec \beta$ a predpokladajme, že pre každý nekonečný kardinál $\kappa \prec \beta$ platí $\kappa^2 \precsim \kappa$. Na množine $\beta \times \beta$ si zadefinujeme tzv. *maximo-lexikografické usporiadanie* vzťahom:

$$\begin{aligned}(\gamma, \delta) \sqsubset (\gamma', \delta') \;\Leftrightarrow\; & \max(\gamma, \delta) \in \max(\gamma', \delta') \vee \\ & \big(\max(\gamma, \delta) = \max(\gamma', \delta') \;\&\; (\gamma, \delta) <_{\text{lex}} (\gamma', \delta')\big),\end{aligned}$$

kde $<_{\text{lex}}$ označuje lexikografické usporiadanie na $(\beta, \in) \cdot (\beta, \in)$. Možno ukázať, že $\sqsubset$ je dobré usporiadanie na $\beta \times \beta$ (doplňte si sami). Označme $o(\beta \times \beta, \sqsubset) = \varrho \in \mathbf{\Omega}$. Stačí, keď dokážeme, že $\varrho = \beta$. Keďže β je kardinál a $\beta \precsim \beta \times \beta \approx \varrho$, určite neplatí $\varrho \in \beta$. Vylúčime aj možnosť $\beta \in \varrho$. V takom prípade by pre nejakú dvojicu $(\gamma, \delta) \in \beta \times \beta$ platilo

$$\{(\gamma', \delta') \in \beta \times \beta;\, (\gamma', \delta') \sqsubset (\gamma, \delta)\} \approx \beta.$$

Označme η ordinálny nasledovník ordinálu $\max(\gamma, \delta)$. Potom uvedená množina je podmnožinou množiny $\eta \times \eta$. Ale $\eta \in \beta$, teda $\aleph_0 \precsim |\eta| \prec \beta$. Podľa indukčného predpokladu $|\eta \times \eta| = |\eta|^2 \precsim |\eta| \prec \beta$, čo je hľadaný spor.

Čitateľa, ktorý pozná jednoduchý dôkaz rovnosti $\aleph_0^2 = \aleph_0$, možno prekvapil pomerne zložitý dôkaz zovšeobecnenia tohto vzťahu na ľubovoľné nekonečné kardinály β. Ešte raz podčiarknime, že bez dodatočných predpokladov typu (WO) však pre ne nemožno dokázať ani jednu z rovností $2 \cdot \beta = \beta = \beta^2$.

Konečne poslednú skupinu princípov, ktorými sa tu budeme zaaoberať a ktoré sú v matematickej praxi najčastejšie využívanými ekvivalentmi axiómy výberu, tvoria tzv. *princípy maximality.* Tieto princípy sú najčastejšie súhrnne označované názvom *Zornova lema,* no ešte pred M. Zornom (1935) boli (aspoň niektoré z nich) sformulované F. Hausdorffom (1914) a K. Kuratowskim (1922).

Princípy maximality (a s nimi ekvivalentné *princípy minimality*) sa líšia najmä rôznym stupňom všeobecnosti svojich predpokladov a tak trochu i formou svojich záverov. Rôznymi ich kombináciami možno vytvoriť najmenej tucet takýchto princípov. Aby sme čitateľa zbytočne neunavovali ich dlhým výčtom, obmedzíme sa len na dva krajné prípady: *Princíp maximality* (MP0), ktorý z najslabších predpokladov vyvodzuje najsilnejší záver, a *princíp maximality* (MP1), ktorý z najsilnejších predpokladov vyvodzuje najslabší záver. Zrejme za týchto podmienok je (MP0) najsilnejší a (MP1) najslabší z celej skupiny princípov.

Princíp maximality (MP0). *Nech $(X, <)$ je čiastočne usporiadaná množina, v ktorej je každý reťazec zhora ohraničený. Potom pre každé $x \in X$ existuje maximálny prvok $m \in X$ taký, že $x \leq m$.*

Princíp maximality (MP1). *Nech X je ľubovoľná množina a $\mathcal{S} \subseteq \mathcal{P}(X)$ je systém jej podmnožín taký, že pre každý usmernený podsystém $\mathcal{D}$ v $(\mathcal{S}, \subseteq)$ platí $\bigcup \mathcal{D} \in \mathcal{S}$. Potom S obsahuje maximálny prvok.*

Veta. *Princípy maximality (MP0) a (MP1) sú ekvivalentné.*

Dôkaz.
Keďže implikácia (MP0) $\Rightarrow$ (MP1) je triviálna (podrobne si rozmyslite prečo), budeme dokazovať len implikáciu (MP1) $\Rightarrow$ (MP0).

Nech $(X, <)$ je čiastočne usporiadaná množina, v ktorej je každý reťazec zhora ohraničený, a $x \in X$. Položme

$$\mathcal{S} = \{C \subseteq X;\ x \in C \ \&\ C \text{ je reťazec v } (X, <)\}.$$

Zrejme $\mathcal{S} \subseteq \mathcal{P}(X)$ a pre každý usmernený podsystém $\mathcal{D}$ v $(\mathcal{S}, \subseteq)$ platí $\bigcup \mathcal{D} \in \mathcal{S}$ (overte sami). Podľa (MP1) existuje maximálny prvok $M \in \mathcal{S}$. Potom $x \in M$ a M je maximálny reťazec v $(X, <)$ s touto vlastnosťou. Ako každý reťazec v $(X, <)$, aj M je zhora ohraničený nejakým prvkom $m \in X$. Zrejme $m \in M$. V opačnom prípade by totiž reťazec $M \cup \{m\} \in \mathcal{S}$ bol vlastnou nadmnožinou M, čo odporuje maximalite M. Potom $x \leq m$ a z maximality M opäť ľahko nahliadneme, že m je maximálny prvok v $(X, <)$.

Ďalej budeme pod *princípom maximality* (MP) rozumieť ktorýkoľvek z ekvivalentných princípov nachádzajúcich sa niekde medzi (MP0), (MP1). Uveďme ešte aspoň dva príklady.

Princíp maximality (MP0'). *Nech $(X, <)$ je čiastočne usporiadaná množina, v ktorej každá usmernená množina $D \subseteq X$ má supremum. Potom v $(X, <)$ existuje maximálny prvok.*

Princíp maximality (MP1'). *Nech X je ľubovoľná množina a $\mathcal{S} \subseteq \mathcal{P}(X)$ je systém jej podmnožín taký, že každý reťazec v $(\mathcal{S}, \subseteq)$ je zhora ohraničený. Potom pre každé $A \in \mathcal{S}$ existuje maximálna množina $M \in \mathcal{S}$ taká, že $A \subseteq M$.*

Premyslite si, prečo (triviálne) platia implikácie (MP0) $\Rightarrow$ (MP0') $\Rightarrow$ (MP1) a (MP0) $\Rightarrow$ (MP1') $\Rightarrow$ (MP1).

Ako príklad použitia princípu maximality naznačíme dôkaz existencie netriviálnych ultrafiltrov. Systém podmnožín $\mathcal{D}$ nejakej množiny X nazývame *ultrafiltrom* na X,

ak $\mathcal{D} \neq \emptyset$, $\emptyset \notin \mathcal{D}$ a pre ľubovoľné A, $B \subseteq X$ platí

$$A \in \mathcal{D} \;\&\; A \subseteq B \;\Rightarrow\; B \in \mathcal{D},$$
$$A,\, B \in \mathcal{D} \;\Rightarrow\; A \cap B \in \mathcal{D},$$
$$A \cup B \in \mathcal{D} \;\Rightarrow\; A \in \mathcal{D} \vee B \in \mathcal{D}.$$

Ultrafiler $\mathcal{D}$ nazývame *triviálnym* alebo tiež *hlavným*, ak čiastočne usporiadaná množina $(\mathcal{D}, \subseteq)$ má najemnší prvok; v opačnom prípade hovoríme, že $\mathcal{D}$ je *netriviálny ultrafilter*.

Hovoríme, že systém $\mathcal{C}$ podmnožín množiny X je *centrovaný*, ak pre každý konečný podsystém $\mathcal{C}_0 \subseteq \mathcal{C}$ platí $\bigcap \mathcal{C}_0 \neq \emptyset$.

Veta o ultrafiltroch. *Nech X je ľubovoľná množina a $\mathcal{C}$ je nejaký centrovaný systém jej podmnožín. Potom existuje ultrafilter $\mathcal{D}$ na X taký, že $\mathcal{C} \subseteq \mathcal{D}$.*

Dôkaz.
Označme $\mathcal{S}$ systém všetkých centrovaných systémov podmnožín množiny X. Potom $\mathcal{S} \subseteq \mathcal{P}(\mathcal{P}(X))$ a jednoducho možno overiť, že pre každý reťazec $\mathcal{R}$ v $(\mathcal{S}, \subseteq)$ platí $\bigcup \mathcal{R} \in \mathcal{S}$ (teda $\mathcal{R}$ je zhora ohraničený v $(\mathcal{S}, \subseteq)$). Podľa (MP1') existuje maximálny centrovaný systém $\mathcal{D} \in \mathcal{S}$ taký, že $\mathcal{C} \subseteq \mathcal{D}$. Prenechávame čitateľovi, aby si sám doplnil jednoduchý dôkaz, že $\mathcal{D}$ je ultrafilter na X.

Dôsledok. *Na každej nekonečnej množine existuje netriviálny ultrafilter.*

Dôkaz.
Nech X je nekonečná. Potom $\mathcal{C} = \{A \subseteq X;\, X \setminus A \text{ je konečná}\}$ je centrovaný sýstém podmnožín množiny X. Keďže $\bigcap \mathcal{C} = \emptyset$, ľubovoľný ultrafilter $\mathcal{D} \supseteq \mathcal{C}$ je netriviálny.

Hoci existencia netriviálnych ultrafiltrov je dôsledkom axiómy výberu, presnejšie jedným špeciálnym prípadom princípu maximality, stojí za zmienku, že len z tohto špeciálneho prípadu ešte nevyplýva princíp maximality v plnej všeobecnosti (teda ani axióma výberu). Jednako prijatie už len samotnej *vety o ultrafiltroch* (a odmietnutie axiómy výberu v plnom rozsahu) nám umožňuje dokázať napr. *Gödelovu vetu o úplnosti predikátového počtu* pre spočítateľné jazyky, ako aj *Hahnovu-Banachovu vetu*, ktorá je jedným zo základných kameňov funkcionálnej analýzy. Dôkaz týchto tvrdení však už výrazne presahuje rámec nášho textu.

Popri spomínaných „príjemných“ dôsledkoch však má axióma výberu aj rad dobre známych dôsledkov „menej príjemných“. K nim patrí napr. existencia *lebesguovsky nemerateľných* množín resp. množín, ktoré nemajú *Bairovu vlastnosť*, na reálnej osi. Keďže existencia takýchto množín sa vo väčšine učebníc zvykne dokazovať tzv. Vitaliho konštrukciou, ktorá využíva axiómu výberu v značne širšom rozsahu (presnejšie selektor na systéme mohutnosti kontinua podmnožín množiny $\mathbb{R}$, resp. dobré usporiadanie množiny reálnych čísel), natíska sa otázka, či by sme sa týmto „neželaným“ dôsledkom nemohli nejako vyhnúť tým, že by sme miesto axiómy výberu prijali za axiómy len niektoré jej „želané“ dôsledky. Ako kandidáti sa nám ponúkajú práve spomínaná veta o ultrafiltroch spolu so slabou axiómou výberu, nehyhnutnou na dôkaz nektorých základných výsledkov matematickej analýzy. Žiaľ, ide o planú nádej. Bude preto poučné aspoň stručne a bez dôkazu naznačiť, ako možno množiny podobných „patologických“ vlastností získať už z netriviálnych ultrafiltrov na množine $\mathbb{N}$.

Pre istotu pripomíname, že množina $X \subseteq \mathbb{R}$ je lebesguovsky merateľná práve vtedy, keď pre každé $\varepsilon > 0$ existujú uzavretá množina $U \subseteq \mathbb{R}$ a otvorená množina $V \subseteq \mathbb{R}$

také, že $U \subseteq X \subseteq V$ a vonkajšia miera množiny $V \setminus U$ je menšia než ε, t. j. existuje konečný počet intervalov $\langle a_1, b_1\rangle, \dots, \langle a_n, b_n\rangle$ takých, že

$$V \setminus U \subseteq \bigcup_{i=1}^{n} \langle a_i, b_i\rangle \qquad \text{a} \qquad \sum_{i=1}^{n} (b_i - a_i) < \varepsilon.$$

Podobne, $X \subseteq \mathbb{R}$ má Bairovu vlastnosť práve vtedy, keď existuje otvorená množina $V \subseteq \mathbb{R}$ taká, že obe množiny $X \setminus V$, $V \setminus X$ sú prvej kategórie, t. j. každá z nich je zjednotením spočítateľne mnohých riedkych množín. Pritom nmožina $Z \subseteq \mathbb{R}$ sa nazýva riedka, ak vnútro jej uzáveru je prázdna množina, t. j.

$$\big(\forall\, x \in \mathbb{R}\big)\big(\forall\, \varepsilon > 0\big)\big(\exists\, y \in (x-\varepsilon, x+\varepsilon)\big)\big(\exists\, \delta > 0\big)\big((y-\delta, y+\delta) \cap Z = \emptyset\big).$$

Pre ľubovoľnú množinu $A \subseteq \mathbb{N}$ označme

$$\varrho(A) = \sum_{n \in A} 2^{-n-1}.$$

Zrejme týmto predpisom je definované surjektívne zobrazenie $\varrho\colon \mathcal{P}(\mathbb{N}) \to \langle 0, 1\rangle$.

Veta. *Nech $\mathcal{D} \subseteq \mathcal{P}(\mathbb{N})$ je nejaký netriválny ultrafilter na $\mathbb{N}$. Potom*

$$\varrho[\mathcal{D}] = \{\varrho(A);\ A \in \mathcal{D}\}$$

je lebesguovsky nemerateľná podmnožina intervalu $\langle 0, 1\rangle$ reálnych čísel, ktorá nemá Bairovu vlastnosť.

Na záver nám ešte zostáva vyjasniť vzťah medzi axiómou výberu, princípom dobrého usporiadania a princípom maximality. Ako sme už viackrát spomínali, platí nasledujúca

Veta. *Axióma výberu (AC), princíp dobrého usporiadania (WO) a princíp maximality (MP) sú ekvivalentné.*

Dôkaz.
(AC) $\Rightarrow$ (WO): Nech X je ľubovoľná množina. Ukážeme, že existuje ordinál α a bijekcia $f\colon \alpha \to X$. Touto bijekciou sa dobré usporiadanie z $(\alpha, \in)$ prenesie na X.

Ak $X = \emptyset$, niet čo dokazovať; budeme teda predpokladať, že X je neprázdna. Nech h je selektor na množine $\mathcal{P}(X)$, t. j. zobrazenie $h\colon \mathcal{P}(X) \to X$ také, že $h(A) \in A$ pre každé $A \subseteq X$, $A \neq \emptyset$. Transfinitnou rekurziou cez triedu $\mathbf{\Omega}$ zostrojíme (triedovú) funkciu $\mathbf{F}\colon \mathbf{\Omega} \to X$ takú, že pre každý ordinál α platí

$$\mathbf{F}(\alpha) = h\big(X \setminus \mathbf{F}[\alpha]\big) = h\big(X \setminus \{\mathbf{F}(\beta);\ \beta \in \alpha\}\big).$$

Nech α je najmenší ordinál taký, že $X = \mathbf{F}[\alpha] = \{\mathbf{F}(\beta);\ \beta \in \alpha\}$. Také α existuje, lebo inak by $\mathbf{F}$ bolo prosté zobrazenie vlastnej triedy $\mathbf{\Omega}$ do množiny X, čo je nemožné. Potom $f = \mathbf{F} \restriction \alpha\colon \alpha \to X$ je hľadaná bijekcia.

(WO) $\Rightarrow$ (MP0): Nech $(X, <)$ je čiastočne usporiadaná množina, v ktorej každý reťazec je zhora ohraničený a $x \in X$. Pripusťme, že neexistuje maximálny prvok $m \in X$ taký, že $x \leq m$. To znamená, že pre každé $y \in X$, $y \geq x$, existuje $z \in X$, $y < z$. Zhrnutím týchto dvoch podmienok dostávame:

(∗) *Nech $C \subseteq X$ je ľubovoľný (konečný alebo nekonečný) reťazec v $(X, <)$ taký, že $x \in C$. Potom existuje $z \in X$ také, že $c < z$ pre každé $c \in C$.*

Nech $\lhd$ je nejaké dobré usporiadanie množiny X. Transfinitnou rekurziou cez triedu $\mathbf{\Omega}$ zostrojíme (triedovú) funkciu $\mathbf{F}\colon \mathbf{\Omega} \to X$ takú, že pre každé $\alpha \in \mathbf{\Omega}$ je $\mathbf{F}(\alpha)$ najmenší prvok množiny $\{y \in X;\, x \leq y \,\&\, (\forall\, \beta \in \alpha)(\mathbf{F}(\beta) < y)\}$ v usporiadaní $\lhd$. Transfinitnou indukciou možno ľahko dokázať, že pre každé $\alpha \in \mathbf{\Omega}$ je $\{x\} \cup \mathbf{F}[\alpha]$ reťazec v $(X, <)$. Preto podľa $(*)$ je takto korektne definované prosté zobrazenie vlastnej triedy $\mathbf{\Omega}$ do množiny X, čo je spor.

(MP1) $\Rightarrow$ (AC): Nech X je množina neprázdnych po dvoch disjunktných množín. Označme $\mathcal{S}$ systém všetkých množín $Z \subseteq \bigcup X$ takých, že pre každé $x \in X$ množina $x \cap Z$ je nanajvýš jednoprvková. Potom $\mathcal{S} \subseteq \mathcal{P}\big(\bigcup X\big)$. Ľahko nahliadneme, že pre každý usmernený systém $\mathcal{D} \subseteq \mathcal{S}$ platí $\bigcup \mathcal{D} \in \mathcal{S}$. Preto existuje nejaká maximálna množina $Z \in \mathcal{S}$. Predpoklad, že by pre niektoré $x \in X$ platilo $x \cap Z = \emptyset$, by nás rýchlo doviedol k sporu s maximalitou Z. Teda $x \cap Z$ je jednoprvková pre každé $x \in X$.

Ako cvičenie si skúste dokázať poslednú vetu podľa schémy (MP) $\Rightarrow$ (WO) $\Rightarrow$ (AC) $\Rightarrow$ (MP). Prvé dve implikácie sú jednoduché. Značne náročnejší je však dôkaz tretej implikácie, ktorý možno nájsť napríklad v [1]. Dôkaz podľa uvedenej schémy si navyše v žiadnej časti nevyžaduje transfinitnú rekurziu.

Literatúra

[1] B. Balcar, P. Štepánek, *Teorie množin*, Academia, Praha, 1986.

[2] L. Bukovský, *Štruktúra reálnej osi*, Veda, Bratislava, 1979.