1. Množiny

Pojem množiny je základním pojmem matematiky. Množina je určena svými prvky, t.j., množinou rozumíme souhrn prvků. Teorii množin vybudoval německý matematik G.Cantor v roce 1872. Výše uvedené vymezení pojmu množiny není přesnou definicí. Vede také k rozporům neboť jsou "souhrny", které za množiny považovat nemůžeme. Později uvidíme, že nemůžeme vytvořit "množinu" všech množin. Nejjednodušší příklad takové zakázané "množiny" nalezl B.Russel v roce 1900. Je to souhrn $M = \{x \setminus \notin x\}$ všech množin x, které neobsahují sebe jako prvek. Totiž, pokud by M byla množina, můžeme si položit otázku, zda $M \in M$. Pokud ano, pak, podle definice M platí $M \notin M$. Pokud ne, pak, opět podle definice M, platí $M \in M$. V obou případech dostáváme spor. Řešení problému definice pojmu množiny podává axiomatická teorie množin. My budeme pracovat v tzv. naivní teorii množin, t.j., na základě výše uvedené nepřesné "definice". Budeme však opatrní v jejím používání: ne všechny souhrny budeme považovat za množiny. Zároveň si naznačíme, jak vypadá axiomatická teorie množin.

Základní (a vlastně jedinou) vlastností množin je, že mají prvky. Píšeme $a \in A$, což znamená, že a je prvkem množiny A. Malá a velká písmena používáme pro názornost; ve skutečnosti v teorii množin není nic jiného než množiny, t.j., i a je množina. Fakt, že množina je určena svými prvky je vyjádřen následujícím axiomem (který je prvním axiomem axiomatické teorie množin):
Axiom extensionality: Dvě množiny jsou stejné, právě když mají stejné prvky.

Pomocí predikátové logiky (v jazyce s jediným binárním relačním symbolem $\in$, což je jazyk axiomatické teorie množin) se tento axiom zapíše následovně:

$$(\forall x, y)(x = y \leftrightarrow (\forall z)(z \in x \leftrightarrow z \in y)).$$

Máme-li množiny A, B, můžeme utvořit novou množinu $\{A, B\}$, která má za prvky právě A a B. Tento způsob tvorby množin se nazývá *axiom dvojice*. Pomocí formule predikátové logiky se zapíše následovně:

$$(\forall x, y)(\exists z)(\forall t)(t \in z \leftrightarrow t = x \vee t = y).$$

Pro libovolnou množinu A a libovolnou "množinovou vlastnost" $\varphi(x)$ můžeme utvořit novou množinu

$$\{a \in A \setminus \varphi(a) \text{ platí}\}.$$

Přesná definice množinové vlastnosti je, že se jedná o formuli predikátové logiky v jazyce s jediným binárním relačním symbolem $\in$. Tento způsob tvorby množin se nazývá *axiom vyčlenění*. Tímto způsobem vznikly množiny:

$$A \cap B = \{a \in A \setminus a \in B\}$$

$$A - B = \{a \in A \setminus a \notin B\}.$$

Pro libovolnou množinu $\mathcal{A}$ také můžeme utvořit množinu

$$\bigcap \mathcal{A} = \{a \setminus a \in A \text{ pro libovolné } A \in \mathcal{A}\}.$$

Psací písmo jsme opět použili pouze pro názornost. Obvyklé označení je pomocí indexů: máme množinu I a množiny A_i pro libovolné $i \in I$ a vytváříme množinu

$$\bigcap_{i \in I} A_i = \{a \setminus a \in A_i \text{ pro libovolné } i \in I\}.$$

Existuje množina, která se vyznačuje tím, že nemá žádné prvky. Nazývá se *prázdná*, označuje se $\emptyset$ a získáme ji vyčleněním

$$\emptyset = \{a \in A \backslash a \neq a\}.$$

Pomocí axiomu dvojice můžeme z prázdné množiny vytvořit nové množiny, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}\}$, atd. Tímto způsobem můžeme definovat nezáporná celá čísla: $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, atd. Vždy $n = \{0, 1, \cdots, n-1\}$.

Pro sjednocení množin potřebujeme nový způsob tvorby množin nazývaný *axiom sjednocení*. Říká, že pro libovolnou množinu $\mathcal{A}$ můžeme utvořit novou množinu

$$\bigcup \mathcal{A} = \{a \backslash \text{ existuje } A \in \mathcal{A} \text{ tak, že } a \in A\}.$$

V predikátové logice se zapíše

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (\exists t)(t \in x \wedge z \in t)).$$

Zejména

$$A \cup B = \bigcup \{A, B\}.$$

Obvyklé značení opět je

$$\bigcup_{i \in I} A_i = \{a \backslash a \in A_i \text{ pro nějaké } i \in I\}.$$

Je-li A množina, můžeme utvořit množinu

$$\mathcal{P}(A) = \{X \backslash X \subseteq A\}$$

všech podmnožin množiny A. Nazýváme to *axiom množiny podmnožin* a jeho formální zápis je

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow z \subseteq x).$$

Zde $z \subseteq x$ zkracuje $(\forall t)(t \in z \rightarrow t \in x)$.

Uspořádaná dvojice (a, b) se definuje jako množina

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

Tato definice je v duchu teorie množin: vše je množina, tedy i uspořádaná dvojice. Snadno se ověří, že platí

$$(a, b) = (c, d) \Leftrightarrow a = c \text{ a } b = d.$$

Kartézský součin množin A, B nyní definujeme jako

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

Za pomocí axiomů se zapíše následovně

$$A \times B = \{(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) \backslash a \in A \wedge b \in B\}.$$

Potřebujeme utvořit množinu všech nezáporných celých čísel

$$\omega = \{0, 1, 2, \cdots, n, \cdots\}.$$

To umožňuje *axiom nekonečna*. Jeho přesná formulace je následující

$$(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \to y \cup \{y\} \in x)).$$

Množiny x z axiomu nekonečna se nazývají *induktivní*. Pak

$$\omega = \bigcap \{x \backslash x \text{ induktivní}\}.$$

Tento průnik existuje neboť se můžeme omezit na podmnožiny dané induktivní množiny a těch je pouze množina.

Dosud jsme se seznámili s následujícími axiomy teorie množin: axiom extensionality, axiom dvojice, axiom vyčlenění, axiom sjednocení, axiom množiny podmnožin a axiom nekonečna. První udává, kdy jsou dvě množiny stejné, další popisují "povolené" způsoby tvorby množin. K úplné Zermelo-Fraenkelově teorii množin (což je standartní axiomatika teorie množin, označuje se ZF) nám chybí již jen dva dosti technické axiomy: axiom regularity a axiom nahrazení, kterým se budeme věnovat později.

Ideální teorie množin by kromě axiomu extensionality obsahovala pouze axiom říkající, že pro libovolnou množinovou vlastnost $\varphi(x)$ je

$$\{a \backslash \varphi(a) \text{ platí}\}$$

množina. Russelův paradox však ukazuje, že tato teorie je sporná. Axiomy Zermelo-Fraenkelovy teorie množin uvádějí povolené případy výše uvedeného "ideálního" axiomu.

2. Kardinální čísla

Každé množině A přiřadíme symbol $|A|$ takový, že $|A| = |B|$, právě když množiny A, B mají stejnou mohutnost. Symboly $|A|$ se nazývají *kardinální čísla*.

Kardinální číslo $|A|$ rovněž nazýváme *mohutnost* množiny A. Poněvadž "mít stejnou mohutnost" je relace ekvivalence, postup je korektní. Není však podán v termínech teorie množin neboť kardinální čísla nejsou definována jako množiny. Později naznačíme, jak lze kardinální čísla definovat v termínech teorie množin.

Příklady. (1) Nezáporná celá čísla považujeme za kardinální čísla a sice za mohutnosti konečných množin.

(2) Mohutnost spočetné množiny značíme $\aleph_0$.

(3) Mohutnost množiny reálných čísel nazýváme *mohutnost kontinua* a značíme ji c.

Položíme $|A| \leq |B|$, jestliže existuje prosté zobrazení $A \to B$. Relace $\leq$ mezi kardinálními čísly je zřejmě reflexivní a tranzitivní. Ukážeme, že je uspořádání.

Především si uvědomíme, že pokud $A \subseteq B$, pak $|A| \leq |B|$ (neboť zobrazení inkluze $A \to B$ je prosté).

2.1. Cantor-Bernsteinova věta. *Z* $|A| \leq |B|$ *a* $|B| \leq |A|$ *plyne* $|A| = |B|$.

Důkaz. Mějme prostá zobrazení $f : A \to B$ a $g : B \to A$. Musíme ukázat, že pak existuje bijekce $A \to B$.

Uvažujme zobrazení $h : \mathcal{P}(A) \to \mathcal{P}(A)$ definované vztahem

$$h(X) = A - g(B - f(X))$$

Nechť $X, Y \in \mathcal{P}(A)$, $X \subseteq Y$. Pak postupně platí $f(X) \subseteq f(Y)$, $B - f(Y) \subseteq B - f(X)$, $g(B - f(Y)) \subseteq g(B - f(X))$ a $h(X) \subseteq h(Y)$. Tedy $h : \mathcal{P}(A) \to \mathcal{P}(B)$ je isotonní zobrazení (obě množiny $\mathcal{P}(A), \mathcal{P}(B)$ jsou uspořádané množinovou inkluzí). Podle Věty 6.3., existuje $C \subseteq A$ tak, že

$$C = A - g(B - f(C)).$$

Definujme zobrazení $t : A \to B$ takové, že $t(x) = f(x)$ pro $x \in C$ a $t(x) = g^{-1}(x)$ pro $x \notin C$. Definice je korektní neboť pro $x \notin C$ platí $x \in g(B - f(C))$. Ukážeme, že $t : A \to B$ je bijekce.

Předpokládejme, že pro $x \in C$ a $y \notin C$ platí $t(x) = t(y)$. Pak $f(x) = g^{-1}(y)$, takže $g(f(x)) = y \notin C$. Zároveň $f(x) \notin B - f(C)$ (neboť $x \in C$), takže $g(f(x)) \notin g(B - f(C))$ a tedy $g(f(x)) \in C$; spor. Tedy t je prosté zobrazení neboť obě zúžení t na C a $A - C$ jsou prostá.

Nechť $y \in B$, $y \notin t(A)$. Pak $y \notin f(C)$, takže $y \in B - f(C)$ a tedy $g(y) \notin C$. To však znamená, že $y = t(g(y))$, spor. Tedy t je zobrazení na. □

Poznámka 2.2. (1) Poněvadž zobrazení $f : A \to \mathcal{P}(A)$, $f(a) = \{a\}$ je vždy prosté, pro libovolnou množinu A platí $|A| \leq |\mathcal{P}(A)|$. Z Cantorovy věty plyne, že vždy

$$|A| < |\mathcal{P}(A)|.$$

Odsud plyne, že *neexistuje největší kardinální číslo.*

Věta 2.3. *Kardinální čísla netvoří množinu.*

Důkaz. Předpokládejme, že existuje množina I a množiny A_i, $i \in I$ tak, že $|A_i|$, $i \in I$ vyčerpává všechna kardinální čísla. Poněvadž $A_i \subseteq \bigcup_{i \in I} A_i$, platí $|A_i| \leq |\bigcup_{i \in I} A_i|$. Tedy $|\bigcup_{i \in I} A_i|$ je největší kardinální číslo, což odporuje poznámce 2.2. □

Z Cantorovy a Cantor-Bernsteinovy věty rovněž plyne, že neexistuje množina všech množin. Pro takovou množinu M by totiž platilo, že $|\mathcal{P}(M)| \leq |M|$ neboť libovolná podmnožina M je prvkem M. Tedy $|\mathcal{P}(M)| = |M|$, spor.

Zatím nejsme schopni zjistit, zda uspořádání kardinálních čísel je lineární.

Dosud známá kardinální čísla jsou

$$0 < 1 < \cdots < \aleph_0 < c.$$

Z 4.4. plyne, že $\aleph_0$ je minimální nekonečné kardinální číslo. Otázka, zda c je nejmenší nespočetné kardinální číslo je nerozhodnutelná.

Věta 2.4. $c = |\mathcal{P}(\omega)|$.

Důkaz. Definujme zobrazení $f : 2^\omega \to \mathbb{R}$ desetinným rozvojem

$$f(h) = 0, h(0)h(1)h(2)\dots$$

kde $h : \omega \to 2$. Poněvadž f je prosté zobrazení, víme, že $c \geq |\mathcal{P}(\omega)|$. Z konstrukce reálných čísel jako řezů ve spočetné množině $\mathbb{Q}$ víme, že $c \leq |\mathcal{P}(\omega)|$. Tedy $c = |\mathcal{P}(\omega)|$. □

Operace s kardinálními čísly: Nechť $\alpha = |A|$ a $\beta = |B|$, přičemž množiny A, B jaou v (1) disjunktní. Položme

(1) $\alpha + \beta = |A \cup B|$
(2) $\alpha \cdot \beta = |A \times B|$
(3) $\alpha^\beta = |A^B|$

Buďte I, $A_i, i \in I$ množiny, přičemž A_i jsou navzájem disjunktní.

(4) $\sum_{i \in I} \alpha_i = |\bigcup_{i \in I} A_i|$

Definice je korektní neboť operace nezavisí na volbě množin A, B. Skutečně, jsou-li $f : A \to A'$ a $g : B \to B'$ bijekce, pak

$$f \cup g : A \cup B \to A' \cup B' \text{ pro } A, B \text{ a } A', B' \text{ disjunktní}$$

$$f \times g : A \times B \to A' \times B'$$

a

$$h : A^B \to (A')^{B'}, \quad h(u) = f \cdot u \cdot g^{-1}$$

jsou bijekce.

Operace $+, \cdot$ jsou asociativní, komutativní a distributivní, což plyne z vlastností množinových operací $\cup, \times$. Navíc, z Věty 4.1. plyne, že platí

$$(\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$$

$$(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$$

$$\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma.$$

Dále platí

$$\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$$

$$\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma.$$

Skutečně, je-li $f : A \to B$ prosté zobrazení, pak zobrazení $f \cup id_C : A \cup C \to B \cup C$ a $f \times id_C : A \times C \to B \times C$ jsou rovněž prostá.

Tvrzení věty 2.4 lze přepsat ve tvaru

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

Věta 2.5. $\aleph_0 \cdot \aleph_0 = \aleph_0$, $\aleph_0 + \aleph_0 = \aleph_0$.

Důkaz. Platí

$$\aleph_0 + \aleph_0 = |\mathbb{N}| + |\omega| = |\mathbb{Z}| = \aleph_0$$

Podobně $\aleph_0 \cdot \aleph_0 = \aleph_0$ plyne z toho, že $\mathbb{Q}$ je spočetná množina (viz 4.2. (4)). □

Věta 2.6. *Je-li S spočetná množina reálných čísel, pak $|\mathbb{R} - S| = c$.*

Důkaz. Máme $|\mathbb{R} \times \mathbb{R}| = 2^{\omega} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}$. Tedy místo $\mathbb{R}$ můžeme vzít množinu $\mathbb{R} \times \mathbb{R}$. Buď tedy $S \subseteq \mathbb{R} \times \mathbb{R}$ spočetná množina. Existuje $x \in \mathbb{R}$ tak, že $S \cap (\mathbb{R} \times \{x\}) = \emptyset$. Tedy $\{x\} \times \mathbb{R} \subseteq \mathbb{R} - S$, takže $|\mathbb{R} - S| = c$. □

Důsledek. *Mohutnost množiny iracionálních čísel je c.*

Věta 2.7. *Mohutnost množiny všech konečných posloupností přirozených čísel je $\aleph_0$.*

Důkaz. Buď P množin všech konečných posloupností přirozených čísel. Zřejmě $\aleph_0 \leq |P|$. Pro důkaz opačné nerovnosti zapišme libovolné přirozené číslo a v dvojkové soustavě. Posloupnost $a_1 \dots a_n$ pak určuje racionální číslo $0, a_1 2 a_2 2 \dots a_n$. Poněvadž různé posloupnosti zřejmě určují různá racionální čísla, platí $|P| \leq |\mathbb{Q}| = \aleph_0$. □

Důsledek. *Mohutnost množiny konečných podmnožin spočetné množiny je $\aleph_0$.*

Připomeňme, že reálné číslo se nazývá *algebraické*, pokud je kořenem polynomu s celými koeficienty. Libovolné racionální číslo je zřejmě algebraické. Reálná čísla, která nejsou algebraická se nazývají *transcendentní*. Transcendentní jsou například čísla π, e; důkaz je však obtížný. Ukážeme, že transcendentní čísla existují (a že jich je víc než algebraických).

Věta 2.8. *Množina $\mathbb{A}$ všech algebraických čísel je spočetná.*

Důkaz. Množina všech polynomů s celými koeficienty se označuje $\mathbb{Z}[x]$. Z věty 2.7. plyne, že to je spočetná množina, t.j., existuje bijekce $f : \omega \to \mathbb{Z}[x]$. Definujme zobrazení $g : \mathbb{A} \to \omega \times \omega$ vztahem $g(a) = (n, k)$, kde n je nejmenší číslo takové, že a je kořen polynomu $f(n)$ a a je přitom k-tý reálný kořen tohoto polynomu v uspořádání podle velikosti. Zobrazení g je zřejmě prosté, takže $|\mathbb{A}| \leq \aleph^0$. Poněvadž $\mathbb{Q} \subseteq \mathbb{A}$, $\mathbb{A}$ je spočetná množina. □

Důsledek. *Množina všech transcendentních čísel má mohutnost kontinua.*

Důkaz plyne z věty 2.6. a 2.8.

3. Dobře uspořádané množiny

Definice. Řekneme, že lineárně uspořádaná množina je *dobře uspořádaná*, jestliže libovolná její neprázdná podmnožina má nejmenší prvek.

Přídavné jméno lineárně jsme mohli v definici vynechat neboť to plyne z existence nejmenších prvků dvouprvkových podmnožin. Libovolná podmnožina dobře uspořádané množiny je zřejmě dobře uspořádaná.

Příklady. (1) Libovolná konečná lineárně uspořádaná množina je dobře uspořádaná. ω je dobře uspořádaná.

(2) $\omega^{op}, \mathbb{Z}, \mathbb{Q}$ a $\mathbb{R}$ nejsou dobře uspořádané.

Věta 3.1. *Buď A dobře uspořádaná množina a $f : A \to A$ prosté izotonní zobrazení. Pak pro všechna $a \in A$ platí $a \leq f(a)$.*

Důkaz. Buď $X = \{a \in A \backslash f(a) < a\}$. Pokud $X \neq \emptyset$, existuje nejmenší prvek $a_0 \in X$. Platí $f(a_0) < a_0$, takže $f(a_0) < a_0$. Tedy $f(a_0) \in X$, což je spor s $f(a_0) < a_0$. □

Předpoklad, že f je prosté je podstatný; pro konstantní zobrazení tvrzení neplatí.

Definice. Podmnožina Z uspořádané množiny A se nazývá *začátek*, pokud $x \in Z$, $y \leq x$ implikuje $y \in Z$. Začátek Z se nazývá *vlastní*, pokud $Z \neq A$.

Důsledek. *Dobře uspořádaná množina není isomorfní s žádným svým vlastním začátkem.*

Důkaz. Předpokládejme, že Z je vlastní začátek dobře uspořádané množiny A a $f : A \to Z$ isomorfismus. Existuje prvek $a \in A - Z$. Poněvadž $f(a) \in Z$ musí platit $f(a) < a$, což je spor s větou 3.1. □

Je-li A uspořádaná množina a $a \in A$, pak položíme

$$A(a) = \{x \in A \backslash x < a\}$$

Zřejmě $A(a)$ je vlastní začátek v A. V dobře uspořádané množině A je libovolný vlastní začátek Z tvaru $A(a)$ pro nějaké $a \in A$. Za a je třeba vzít nejmenší prvek množiny $A - Z$.

Věta 3.2. *Buďte A, B dobře uspořádané množiny. Pak existuje nejvýše jeden isomorfismus $A \to B$.*

Důkaz. Buďte $f, g : A \to B$ isomorfismy. Předpokládejme, že $f \neq g$. Pak existuje $a \in A$ takové, že $f(a) < g(a)$. Poněvadž $A(a) \cong B(f(a))$ a $A(a) \cong B(g(a))$ platí $B(f(a)) \cong B(g(a))$. Navíc $B(f(a))$ je začátek v $B(g(a))$. Totiž pro libovolné $c < f(a)$ existuje $d \in A$ tak, že $c = f(d)$. Zřejmě $d < a$, takže $c \in B(f(a))$. Dostáváme spor s důsledkem věty 3.1. □

Důsledek. *Buď A dobře uspořádaná množina a $f : A \to A$ isomorfismus. Pak $f = id_A$.*

Věta 3.3. *Buďte A, B dobře uspořádané množiny. Pak nastane právě jedna z následujících možností:*
(1) $A \cong B$
(2) A je isomorfní s vlastním začátkem B
(3) B je isomorfní s vlastním začátkem A.

Důkaz. Je-li jedna z množin A, B prázdná, tvrzení zřejmě platí. Předpokládejme, že obě množiny A, B jsou neprázdné. Položme

$$A_0 = \{a \in A \backslash \text{ existuje } b \in B \text{ s } A(a) \cong B(b)\}$$

$$B_0 = \{b \in B \backslash \text{ existuje } a \in A \text{ s } B(b) \cong A(a)\}.$$

Poněvadž A_0 obsahuje nejmenší prvek A a B_0 obsahuje nejmenší prvek v B, množiny A_0, B_0 jsou neprázdné. Navíc to zřejmě jsou začátky (A_0 v A a B_0 v B). Dokážeme, že $A_0 \cong B_0$.

Definujme zobrazení $f : A_0 \to B_0$ tak, že $A(a) \cong B(f(a))$. Z definice množin A_0, B_0 a důsledku věty 3.1. plyne, že takové zobrazení existuje právě jedno. Navíc to je zřejmě isomorfismus.

Ukážeme, že nemůže nastat situace, kdy $A_0 \neq A$ a současně $B_0 \neq B$. V tomto případě však existují $a \in A$ a $b \in B$ tak, že $A_0 = A(a)$ a $B_0 = B(b)$. Tedy $a \in A_0$ a $b \in B_0$, což není možné.

Ověřili jsme, že vždy nastane jedna z možností (1)-(3) a zbývá ověřit, že tyto možnosti se navzájem vylučují. Nastanou-li však dvě možnosti současně, vznikne dobře uspořádaná množina isomorfní se svým vlastním začátkem, což odporuje důsledku věty 3.1. □

Poznámka. Z věty 3.3. plyne, že pro dobře uspořádané množiny A, B nastane právě jedna z možností

$$|A| = |B|, \quad |A| < |B|, \quad |B| < |A|.$$

Tedy kardinální čísla dobře uspořádaných množin jsou lineárně uspořádaná. Pokud by libovolná množina šla dobře uspořádat, kardinální čísla by byla lineárně uspořádaná. Uvidíme, že tomu tak je i naopak: pokud kardinální čísla jsou lineárně uspořádaná, pak libovolnou množinu lze dobře uspořádat.

Zatím umíme dobře uspořádat každou konečnou i spočetnou množinu. Neumíme např. dobře uspořádat množinu $\mathbb{R}$. Uvidíme, že problém, zda libovolnou množinu lze dobře uspořádat, je na základě dosavadních axiomů ZF nerozhodnutelný.

Význam dobře uspořádaných množin spočívá mimo jiné v tom, že poskytují prostředí pro rozšíření pojmu indukce.

Věta 3.4. *(transfinitní indukce): Buď A dobře uspořádaná množina. Nechť pro libovolný prvek $a \in A$ je dán výrok $V(a)$. Předpokládejme, že pro libovolné $a \in A$ platí:*

($\star$) Je-li pravdivý výrok $V(x)$ pro libovolné $x < a$, je pravdivý výrok $V(a)$.
Pak výrok $V(a)$ je pravdivý pro všechna $a \in A$.

Důkaz. Nechť $B = \{a \in A \backslash V(a)$ je nepravdivý$\}$. Předpokládejme. že množina B je neprázdná. Buď a nejmenší prvek v B. Dostáváme spor s ($\star$). □

Obvyklá matematická indukce je transfinitní indukce pro ω. Z ($\star$) plyne, že výrok V je pravdivý pro nejmenší prvek v A.

V kapitole 8 jsme viděli, že součin lineárně uspořádaných množin již nemusí být lineárně uspořádaný. V teorii dobře uspořádaných množin proto pracujeme s tzv. lexikografickým součinem.

Definice. *Lexikografický součin $A \cdot B$* dobře uspořádaných množin A, B je kartézský součin $A \times B$ vybavený uspořádáním

$$(a, b) \leq (c, d) \Leftrightarrow a < c \text{ nebo } a = c, b \leq d.$$

Věta 3.5. *Buďte A, B dobře uspořádané množiny. Pak $A \cdot B$ je dobře uspořádaná množina.*

Důkaz. Nechť $X \subseteq A \times B$ je neprázdná podmnožina lexikografického součinu $A \cdot B$. Buď a_0 nejmenší prvek v $p_1(X)$ a b_0 nejmenší prvek v $p_2(p_1^{-1}(a_0) \cap X)$. Zřejmě (a_0, b_0) je nejmenší prvek v X. □

Lexikografický součin není obecně komutativní. Např., $2 \cdot \omega$ a $\omega \cdot 2$ nejsou isomorfní. Totiž $\omega \cdot 2 \cong \omega$, zatímco $2 \cdot \omega$ jsou dvě kopie ω nad sebou.

Věta 3.6. *Pro libovolné uspořádané množiny A, B, C platí*

$$(A \cdot B) \cdot C \cong A \cdot (B \cdot C).$$

Důkaz. V $(A \cdot B) \cdot C$ platí

$$(a,b,c) \leq (a',b',c') \Leftrightarrow (a,b) < (a'b') \text{ nebo } (a,b) = (a',b'), c \leq c'$$
$$\Leftrightarrow a < a' \text{ nebo } a = a', b < b' \text{ nebo } a = a', b = b', c < c'.$$

Podobně, v $A \cdot (B \cdot C))$ platí

$$(a,b,c) \leq (a',b',c') \Leftrightarrow a < a' \text{ nebo } a = a', (b,c) \leq (b',c')$$
$$\Leftrightarrow a < a' \text{ nebo } a = a', b < b' \text{ nebo } a = a', b = b', c < c'.$$

□

Součet (kardinální) disjunktních uspořádaných množin A, B můžeme definovat jako jejich sjednocení $A \cup B$ spolu s uspořádáním, které na A, resp. B splývá se zadaným uspořádáním a libovolné prvky $a \in A$, $b \in B$ jsou nesrovnatelné. Takový součet dvou lineárně uspořádaných množin není lineárně uspořádaný. V teorii dobře uspořádáných množin proto pracujeme s jiným (tzv. ordinálním) součtem.

Definice. *Součet* $A+B$ dvou disjunktních dobře uspořádaných množin definujeme jako jejich sjednocení $A \cup B$ vybavené uspořádáním

$$\begin{aligned} x \leq y \Leftrightarrow & x, y \in A, x \leq y \text{ nebo} \\ & x, y \in B, x \leq y \text{ nebo} \\ & x \in A, y \in B. \end{aligned}$$

Součet dobře uspořádaných množin není komutativní. Např., $\omega+1$ není isomorfní s $1+\omega$. Totiž, $1+\omega \cong \omega$, zatímco $\omega+1$ není isomorfní s ω.

Věta 3.7. *Pro libovolné navzájem disjunktní dobře uspořádané množiny* A, B, C *platí*

$$(A+B)+C = A+(B+C).$$

Důkaz. V obou případech platí

$$\begin{aligned} x \leq y \Leftrightarrow & x, y \in A, x \leq y \text{ nebo} \\ & x, y \in B, x \leq y \text{ nebo} \\ & x, y \in C, x \leq y \text{ nebo} \\ & x \in A, y \in B \text{ nebo} \\ & x \in A, y \in C \text{ nebo} \\ & x \in B, y \in C. \end{aligned}$$

□

Budeme potřebovat i nekonečné součty.

Definice. Buď $I \neq \emptyset$ uspořádaná množina a A_i, $i \in I$ po dvou disjunktní uspořádané množiny. *Součet* $\sum_{i \in I} A_i$ definujeme jako $\bigcup_{i \in I} A_i$ spolu s uspořádáním

$$\begin{aligned} x \leq y \Leftrightarrow & \text{ existuje } i \in I \text{ tak, že } x, y \in A_i, x \leq y \\ & \text{nebo } x \in A_i, y \in A_j, i < j. \end{aligned}$$

Věta 3.8. *Buďte $I \neq \emptyset$ a A_i, $i \in I$ po dvou disjunktní dobře uspořádané množiny. Pak $\sum_{i\in I} A_i$ je dobře uspořádaná.*

Důkaz. Mějme $\emptyset \neq X \subseteq \bigcup_{i\in I} A_i$. Nechť $I_0 = \{i \in I \backslash X \cap A_i \neq \emptyset\}$. Buď i_0 nejmenší prvek v I_0 a a_0 nejmenší prvek v $A_{i_0} \cap X$. Zřejmě a_0 je nejmenší prvek v X. □

Věta 3.9. *(obecný asociativní zákon) Buď $I \neq \emptyset$ uspořádaná množina, A_i, $i \in I$ uspořádané množiny a $I = \sum_{j\in J} I_j$. Pak platí*

$$\sum_{i\in I} A_i = \sum_{j\in J} \sum_{i\in I_j} A_i$$

Důkaz je zřejmý.

Věta 3.10. *(pravý distributivní zákon)*

$$(\sum_{i\in I} A_i) \cdot B = \sum_{i\in I} (A_i \cdot B).$$

Důkaz. Především platí $\bigcup_{i\in I}(A_i \times B) = (\bigcup_{i\in I} A_i) \times B$. Uspořádání v $(\sum_{i\in I} A_i) \cdot B$ je dáno následovně:

$$\begin{aligned}(a,b) \leq (c,d) \Leftrightarrow & a,c \in A_i, a < c \text{ nebo} \\ & a \in A_i, c \in A_j, i < j \text{ nebo} \\ & a = c, b \leq d.\end{aligned}$$

Uspořádání v $(\sum_{i\in I}(A_i \cdot B)$ je dáno následovně:

$$\begin{aligned}(a,b) \leq (c,d) \Leftrightarrow & (a,b),(c,d) \in A_i \cdot B, (a,b) \leq (c,d) \text{ nebo} \\ & (a,b) \in A_i \cdot B, (c,d) \in A_j \cdot B, i < j.\end{aligned}$$

To však nastane právě když

$$\begin{aligned}& a,c \in A_i, a < c \text{ nebo} \\ & a = c, b \leq d \text{ nebo} \\ & a \in A_i, b \in A_j, i < j.\end{aligned}$$

Tím je tvrzení dokázáno. □

Levý distributivní zákon neplatí:

$$\omega \cdot (1+1) = \omega \neq \omega + \omega = \omega \cdot 1 + \omega \cdot 1.$$

Věta 3.11. *Buď I uspořádaná množina a $A_i \cong A$ po dvou disjunktní uspořádané množiny. Pak platí*

$$\sum_{i\in I} A_i \cong I \cdot A.$$

Důkaz. Buďte $f_i : A_i \to A$, $i \in I$ isomorfismy. Pak zobrazení $f : \bigcup_{i\in I} A_i \to I \times A$ dané předpisem $f(a) = (i, f_i(a))$ pro $a \in A_i$ je bijekce. Pro $a, b \in \bigcup_{i\in I} A_i$ platí

$$a \le b \text{ v } \sum_{i\in I} A_i \Leftrightarrow a, b \in A_i, a \le b \text{ nebo}$$
$$a \in A_i, b \in A_j, i < j.$$

To však nastane právě když $(i, f_i(a)) \le (j, f_j(b))$ v $I \times A$. □

4. Ordinální čísla

Každé dobře uspořádané množině A přiřadíme symbol $\overline{A}$ tak, že $\overline{A} = \overline{B}$, právě když $A \cong B$. Symboly $\overline{A}$ se nazývají *ordinální čísla*.

Poněvadž relace "být isomorfní" je relací ekvivalence, postup je korektní. Není však veden v termínech teorie množin, což později opravíme.

Příklad. Ordinální číslo n-prvkové dobře uspořádané množiny označíme n. Ordinální číslo dobře uspořádané množiny ω značíme ω.

Položíme $\overline{A} \le \overline{B}$, pokud A je isomorfní se začátkem B. Relace $\le$ je zřejmě reflexivní a tranzitivní. Z věty 4.3. plyne, že se jedná o lineární uspořádání (na třídě všech ordinálních čísel). Právě uvedená formulace je korektní neboť $\le$ zřejmě nezávisí na volbě reprezentantů. Uspořádání ordinálních čísel uvedených v příkladu nahoře je

$$0 < 1 < \ldots n < \ldots \omega$$

Pro libovolné ordinální číslo α položíme

$$W(\alpha) = \{\beta \backslash \beta < \alpha \text{ je ordinální číslo}\}$$

Například, $W(0) = \emptyset$, $W(n) = \{0, \ldots, n-1\}$ a $W(\omega) = \{0, 1, \ldots, n, \ldots\}$.

Věta 4.1. *Množina $W(\alpha)$ je dobře uspořádaná pro libovolné ordinální číslo α a platí $\overline{W(\alpha)} = \alpha$.*

Důkaz. Nechť $\alpha = \overline{A}$. Položme $f(x) = \overline{A(x)}$ pro libovolné $x \in A$. Zřejmě $f : A \to W(\alpha)$ je prosté zobrazení. Mějme $\beta < \alpha$, $\beta = \overline{B}$. Pak existuje $x \in A$ tak, že $B \cong A(x)$. Tedy $\beta = f(x)$, takže f je isomorfismus. □

Věta 4.2. *Ordinální čísla jsou dobře uspořádaná relací $\le$.*

Důkaz. Buď $Z \neq \emptyset$ množina ordinálních čísel. Uvažujme $\alpha \in Z$. Pak buď α je nejmenší prvek v Z nebo množina $W(\alpha) \cap Z$ je neprázdná. Pak její nejmenší prvek (který existuje neboť α je ordinální číslo) je zřejmě nejmenší prvek v Z. □

Ordinální číslo α se nazývá *limitní*, pokud množina $W(\alpha)$ nemá největší prvek. V opačném případě se nazývá *izolované*. Tedy ordinální číslo 0 je limitní.

Operace s ordinálními čísly: Nechť $\alpha = \overline{A}$ a $\beta = \overline{B}$, přičemž dobře uspořádané množiny A, B jsou v (1) disjunktní. Položme

(1) $\alpha + \beta = \overline{A + B}$

(2) $\alpha \cdot \beta = \overline{B \cdot A}$

Definice je korektní neboť operace zřejmě nezavisí na volbě dobře uspořádaných množin A, B.

Operace $+, \cdot$ jsou asociativní, což plyne z vět 4.6. a 4.7. Z věty 3.10. plyne platnost levého distributivního zákona

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

Dále platí

$$\alpha + 0 = 0 + \alpha = \alpha$$

$$\alpha \cdot 0 = 0 \cdot \alpha = 0$$

$$\alpha \cdot 1 = 1 \cdot \alpha = \alpha$$

$$\alpha \cdot 2 = \alpha + \alpha$$

.

Operace $+, \cdot$ nejsou komutativní. Např. platí

$$1 + \omega = \omega \neq \omega + 1$$

$$2 \cdot \omega = \omega \neq \omega \cdot 2 = \omega + \omega$$

Všimněme si faktu, že izolovaná ordinální čísla jsou právě ordinální čísla tvaru $\alpha + 1$.

Buď I dobře uspořádaná množina, A_i, $i \in I$, dobře uspořádané množiny a $\alpha_i = \overline{A_i}$. Pak ordinální číslo $\sum_{i \in I} \alpha_i$ definujeme předpisem

$$\sum_{i \in I} \alpha_i = \overline{\sum_{i \in I} A_i}$$

Definice zřejmě opět nezávisí na volbě dobře uspořádaných množin A_i. Z vět 3.10. a 3.11. plyne

$$\alpha \cdot \sum_{i \in I} \beta_i = \sum_{i \in I} \alpha_i \cdot \beta$$

$$\sum_{i \in I} \alpha = \alpha \cdot \overline{I}$$

Třídu všech ordinálních čísel označíme W. Symbol $W(\alpha)$ je ve shodě s obecným označením $A(x)$ pro začátek. Ve W má nejen každá podmnožina, ale i každá podtřída $Z \subseteq W$ má nejmenší prvek (důkaz je stejný).

Věta 4.3. *Buď M množina ordinálních čísel. Pak existuje ordinální číslo α takové, že $\beta < \alpha$ pro libovolné $\beta \in M$.*

Důkaz. Pokud $M = \emptyset$, pak $\alpha = 0$. Má-li M největší prvek β, pak $\alpha = \beta + 1$. Pokud M nemá největší prvek, uvažujeme množinu

$$A = \bigcup_{\beta \in M} W(\beta)$$

Poněvadž A je dobře uspořádaná nmožina, pro $\alpha = \overline{A}$ platí $\beta < \alpha$ pro všechna $\beta \in M$. □

Poznámka 4.4. Z věty 4.3. plyne, že W není množina a neobsahuje největší prvek.

Důsledek 4.5. *Pro libovolnou množinu M ordinálních čísel existuje $\sup M$ ve W.*

Důkaz. Tvrzení je zřejmé, pokud M má největší prvek. Nechť M nemá největší prvek. Bez újmy na obecnosti můžeme předpokládat, že z $\beta_1 < \beta_2 \in M$ plyne $\beta_1 \in M$. Ordinální číslo α z 4.3. patří do třídy $W - M$, která je proto neprázdná, takže obsahuje nejmenší prvek. Ten je zřejmě $\sup M$. □

Konečně, pro libovolná ordinální čísla α, β definujeme mocninu α^β následovně:

$$\alpha^0 = 1$$
$$\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$$
$$\alpha^\beta = \sup\{\alpha^\gamma \backslash \gamma < \beta\}$$

pro $0 < \beta$ limitní. (Zde je použito 4.3.) Definice je založena na větě 3.4., t.j. na transfinitní indukci.

Později (Lemma 7.9) uvidíme, že mocnina ordinálních čísel má následující vlastnosti

$$\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$$
$$(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$$

Nyní si můžeme udělat představu o začátku třídy W ordinálních čísel (v jejím uspořádání):

$$0, 1, 2, \ldots, n, \ldots, \omega, \omega+1, \ldots, \omega+\omega = \omega\cdot 2, \ldots, \omega\cdot n, \ldots \omega\cdot\omega = \omega^2, \ldots, \omega^n, \ldots \omega^\omega,$$
$$\omega^{(\omega^\omega)}, \ldots, \omega^{(\overset{\omega)}{\overset{\iddots}{\omega}}\Big\}n}, \ldots \epsilon_0, \ldots$$

Přitom každé limitní ordinální číslo je vždy supremum všech menších ordinálních čísel. Totiž, vztahy

$$\omega = \bigvee_{n<\omega} n$$
$$\omega + \omega = \bigvee_{n<\omega} \omega + n$$

jsou zřejmé. Rovnost

$$\omega \cdot \omega = \bigvee_{n<\omega} \omega \cdot n$$

plyne z toho, že pro libovolné $\beta < \omega\cdot\omega$ existují $m, n < \omega$ tak, že $\beta \in W(m, n)$. Tedy $\beta < \omega \cdot n$.

Konečně rovnost

$$\omega^\omega = \bigvee_{n<\omega} \omega^n$$

plyne z definice mocniny ordinálních čísel. Číslo ϵ_0 je supremum všech předchozích ordinálních čísel. Je to nejmenší ordinální číslo s vlastností $\omega^{\epsilon_0} = \epsilon_0$.

Všechna výše uvedená ordinální čísla jsou spočetná (t.j., jsou to ordinální čísla spočetných dobře uspořádaných množin). Nespočetná ordinální čísla však musí existovat neboť spočetných ordinálních čísel není víc než všech možných uspořádání na množině ω, t.j., nejvýše $2^{\omega\cdot\omega} = 2^\omega$ (a W není množina). Nejmenší nespočetné ordinální číslo se označuje ω_1.

5. Axiom výběru

Axiom výběru: Buď I množina a A_i, $i \in I$ neprázdné množiny. Pak množina $\prod_{i\in I} A_i$ je rovněž neprázdná.

Axiom říká, že libovolná množina neprázdných množin $\{A_i \backslash i \in I\}$ má tzv. *výběrovou funkci*, t.j. zobrazení

$$f : I \to \bigcup_{i\in I} A_i$$

takové, že $f(i) \in A_i$ pro libovolné $i \in I$. Axiom výběru se označuje AC. Zermelo-Fraenkelova teorie množin s axiomem výběru se označuje ZFC a je to v současné době "standartní" teorie množin. Příčinou zvláštního postavení axiomu výběru je jeho "nekonstruktivní" charakter. Zatímco všechny ostatní axiomy ZF přesně popisují, jakou množinu vytváří, AC pouze tvrdí, že určitá množina (t.j., výběrová funkce) existuje, aniž by řekl, jak vypadá. Výběrová funkce vždy existuje (bez AC), pokud množina I je konečná, např. $I = \{1, \ldots, n\}$. Stačí zvolit prvky $a_i \in A_i$ pro $i = 1, \ldots, n$ a položit $f = \{(1, a_1), \ldots, (n, a_n)\}$. Tato výběrová funkce je vytvořena použitím axiomu dvojice. Takovou možnost již nemáme pro nekonečnou množinu I a to ani v případě, pokud množiny A_i jsou konečné nebo dokonce dvouprvkové.

Princip dobrého uspořádání: Libovolnou množinu lze dobře uspořádat.

Tento princip má rovněž "nekonstruktivní" charakter neboť neříká, jak příslušné dobré uspořádání vypadá. Nahlédneme to např. na existenci dobrého uspořádání množiny $\mathbb{R}$ reálných čísel. Ukážeme, že princip dobrého uspořádání je (v ZF) ekvivalentní s axiomem výběru.

Věta 5.1. *Princip dobrého uspořádání implikuje axiom výběru.*

Důkaz. Buď I množina a $\emptyset \neq A_i$, $i \in I$. Podle principu dobrého uspořádání lze množinu

$$\bigcup_{i\in I} A_i$$

dobře uspořádat. V tomto dobrém uspořádání, má libovolná množina A_i nejmenší prvek a_i. Pak $f(i) = a_i$ definuje výběrovou funkci

$$f : I \to \bigcup_{i\in I} A_i.$$

□

Je poučné si uvědomit, že důkaz nelze vést následovně: libovolná množina A_i lze dobře uspořádat, takže má nejmenší prvek a_i, atd. Totiž existuje celá množina D_i dobrých uspořádání množiny A_i a k výběru nějakého z nich pro všechna $i \in I$ používáme axiom výběru (pro množiny D_i, $i \in I$). Ukážeme si další "skrytá" použití axiomu výběru. Tato použití dokumentují, že AC běžně užíváme.

Příklad 5.2. Známé tvrzení matematické analýzy říká, že funkce $f : \mathbb{R} \to \mathbb{R}$ je spojitá v bodě a, právě, když $a_n \to a$ implikuje $f(a_n) \to f(a)$ pro libovolnou posloupnost (a_n). Nutnost podmínky je zřejmá. Dostatečnost se dokazuje následovně. Nechť f není spojitá v a. Pak existuje okolí V bodu $f(a)$ takové, že pro

libovolné $0 < n$ existuje a_n s vlastnostmi $|a_n - a| < \frac{1}{n}$, $f(a_n) \notin V$. Pak $a_n \to a$, ale neplatí $f(a_n) \to f(a)$. Použitá posloupnost a_n je však výběrová funkce

$$\mathbb{N} \to \bigcup_{n\in\mathbb{N}} \{x \backslash |x - a| < \frac{1}{n}, f(x) \notin V\}$$

Lze ukázat, že (bez určité formy) AC tvrzení neplatí, t.j., že "nemáme dost posloupností".

Příklad 5.3. Dokážeme, že sjednocení spočetné množiny spočetných množin je spočetná množina. Mějme spočetné množiny A_i, $i \in \omega$. Množiny A_i lze tedy zapsat posloupnostmi

$$A_i = \{a_{i0}, a_{i1}, \dots, a_{in}, \dots\}$$

Uspořádáme-li množinu $A = \bigcup_{i\in\omega} A_i$ po diagonálách $A = \{a_{00}, a_{01}, a_{10}, \dots\}$, vidíme, že množina A je spočetná. Použití AC spočívá ve výběru uspořádání množin A_i do posloupností. Takových posloupností je vždy množina D_i a na množiny D_i musíme opět uplatnit AC.

Princip maximality Buď A uspořádaná množina taková, že libovolný řetězec v A má horní závoru. Pak ke každému $a \in A$ existuje maximální prvek $b \in A$ tak, že $a \leq b$.

Věta 5.4. *Princip maximality implikuje princip dobrého uspořádání.*

Důkaz. Buď A množina. Uvažujme množinu

$$D = \{(B, R) \backslash R \subseteq A \times A, R \text{ je dobré uspořádání na } B \subseteq A\}$$

Poněvadž $(\emptyset, \emptyset) \in D$, platí máme $D \neq \emptyset$. Pro $(B_1, R_1), (B_2, R_2) \in D$ položíme $(B_1, R_1) \leq (B_2, R_2)$, pokud (B_1, R_1) je začátek (B_2, R_2). Zřejmě $\leq$ je uspořádání množiny D. Ověříme, že D splňuje předpoklad principu maximality.

Buď $C \subseteq D$ řetězec. Pak

$$Q = \bigcup_{(B,R)\in C} R$$

je lineární uspořádání množiny

$$Z = \bigcup_{(B,R)\in C} B$$

Uvažujme $\emptyset \neq X \subseteq Z$. Pro libovolné $x \in X$ existuje $(B, R) \in C$ tak, že $x \in B$. Zřejmě nejmenší prvek podmnožiny $X \cap B$ je nejmenším prvkem množiny X. Tedy Q je dobré uspořádání množiny Z, takže $(Z, Q) \in D$. Zřejmě (Z, Q) je hledanou horní závorou řetězce C v D.

Podle principu maximality existuje maximální prvek (B, R) v D. Ukážeme, že pak $B = A$. V opačném případě existuje prvek $a \in A - B$ a pro $B_0 = B \cup \{a\}$ a $R_0 = R \cup (B \times \{a\}) \cup \{(a, a)\}$ platí $(B_0, R_0) \in D$ a zároveň $(B, R) < (B_0, R_0)$, což není možné. □

Věta 5.5. *Axiom výběru implikuje princip maximality.*

Důkaz. Buď A uspořádaná množina taková, že libovolný řetězec v A má horní závoru a nechť $a \in A$. Buď f výběrová funkce na množině všech neprázdných podmnožin množiny A. To znamená, že $f(X) \in X$ pro libovolné $\emptyset \neq X \subseteq A$.

Existuje dobře uspořádaná množina B taková, že $|B| \leq |A|$ neplatí. V opačném případě by se W skládala z ordinálních čísel podmnožin množiny A, které lze dobře uspořádat. Poněvadž dobrých uspořádání podmnožin množiny A je pouze množina, dostali bychom spor s poznámkou 5.4.

Transfinitní indukcí definujme zobrazení $g : C \to A$ definované na podmnožině C množiny B tak, že a je obrazem nejmenšího prvku množiny B a

$$g(b) = f(\{x \in A \backslash g(y) < x \text{ pro všechna } y < b\})$$

Zobrazení g je zřejmě prosté. Poněvadž $|B| \leq |A|$ neplatí, existuje $b \in B$ tak že g není definováno pro b. Buď b nejmenší prvek v B s touto vlastností. Pak existuje $c \in C$ tak že $c < b$ a neexistuje $x \in B$, $c < x < b$. V opačném případě by obraz g byl řetězec v A bez horní závory. Zřejmě $g(c)$ je hledaný maximální prvek v A takový, že $a \leq g(c)$. □

6. Kardinální aritmetika

Věta 6.1. *(AC) Kardinální čísla jsou dobře uspořádaná relací $\leq$.*

Důkaz. Libovolnému kardinálnímu číslu α přiřadíme ordinální číslo α^* tak, že

$$\alpha \leq \beta \Leftrightarrow \alpha^* \leq \beta^*$$

Odsud již vyplyne tvrzení věty neboť ordinální čísla jsou dobře uspořádaná relací $\leq$ dle 6.2.

Nechť $\alpha = |A|$. Buď M_α množina všech ordinálních čísel β takových, že $\beta = \overline{(A, \preceq)}$ pro nějaké dobré uspořádání $\preceq$ množiny A. Z AC víme, že $M_\alpha \neq \emptyset$, takže M_α má nejmenší prvek, který označíme α^*. Definice zřejmě nezávisí na volbě množiny A.

Implikace

$$\alpha^* \leq \beta^* \Rightarrow \alpha \leq \beta$$

je zřejmá. Nechť $\alpha \leq \beta$. Pak $\alpha^* \leq \beta^*$ nebo $\beta^* \leq \alpha^*$. V druhém případě platí $\beta \leq \alpha$, takže $\alpha = \beta$, takže $\alpha^* = \beta^*$. □

Předchozí věta nám umožňuje indexovat nekonečná kardinální čísla pomocí ordinálních čísel. Třída kardinálních čísel pak (ve svém uspořádání $\leq$) vypadá následovně

$$0, 1, \ldots, n, \ldots \aleph_0, \aleph_1, \ldots, \aleph_n, \ldots \aleph_\omega, \ldots \aleph_\alpha, \ldots$$

Indexování provedeme následovně. Již dříve jsme nejmenší nekonečné kardinální číslo označili $\aleph_0$. Nyní $\aleph_1$ je nejmenší nespočetné kardinální číslo. Z 6.1. víme, že takové kardinální číslo existuje. Máme-li již sestrojena kardinální čísla $\aleph_\beta$ pro všechna ordinální čísla $\beta < \alpha$, pak $\aleph_\alpha$ je nejmenší kardinální číslo větší než všechna $\aleph_\beta$ pro $\beta < \alpha$. Z 9.3. plyne, že takové kardinální číslo existuje. Poněvadž pro libovolné kardinální číslo $\aleph$ existuje pouze množina kardinálních čísel menších než

$\aleph$, $\aleph = \aleph_\alpha$ pro nějaké ordinální číslo α. Tímto postupem jsme vlastně sestrojili bijekci mezi ordinálními čísly a nekonečnými kardinálními čísly.

V důkazu větu 6.1. jsme libovolnému kardinálnímu číslu α přiřadili ordinální číslo α^* a sice nejmenší ordinální číslo mohutnosti α. Budeme značit

$$\aleph_\alpha^* = \omega_\alpha$$

Třídu W ordinálních čísel si pak můžeme představit následovně

$$0, 1, \ldots, n, \ldots \omega_0, \ldots \epsilon_0, \ldots \omega_1, \ldots \omega_\alpha, \ldots$$

(srv. s kapitolou 5; $\omega = \omega_0$).

Věta 6.2. *Axiom výběru je ekvivalentní s tím, že kardinální čísla jsou lineárně uspořádaná relací $\leq$.*

Důkaz. Implikace $\Rightarrow$ plyne z 6.1. Předpokládejme, že kardinální čísla jsou lineárně uspořádaná relací $\leq$. Ukážeme, že pak libovolnou množinu lze dobře uspořádat, což implikuje AC.

Buď A množina. Z důkazu věty 6.5. víme, že existuje dobře uspořádaná množina B taková, že $|B| \leq |A|$ neplatí. Tedy $|A| < |B|$ neboť předpokládáme, že kardinální čísla jsou lineárně uspořádána relací $\leq$. Tedy existuje prosté zobrazení $f : A \to B$, které nám umožní definovat dobré uspořádání množiny A:

$$a \leq b \Leftrightarrow f(a) \leq f(b).$$

□

Poznámka 6.3. Byli jsme si vědomi toho, že ani kardinální, ani ordinální čísla jsme nezavedli v termínech teorie množin. Za AC lze kardinální čísla zavést pomocí ordinálních čísel. Tím myslíme definovat $\aleph_\alpha$ jako ω_α, t.j., za kardinální číslo přímo považovat nejmenší ordinální číslo dané mohutnosti. Nyní naznačíme, jak lze v termínech ZF definovat ordinální čísla. Idea spočívá v "kanonické volbě" dobře uspořádané množiny A takové, že $\overline{A} = \alpha$. Touto volbou bude $W(\alpha)$. Máme-li

$$\alpha = W(\alpha)$$

pak

$$\beta < \alpha \Leftrightarrow \beta \in \alpha$$

t.j., α je množina všech menších ordinálních čísel. Zejména to znamená, že α je dobře uspořádané relací $\in$. Definice ordinálního čísla jako množiny dobře uspořádané relací $\in$ by však ještě nebyla v pořádku. Takovou je i množina $\{\{\emptyset\}\}$, kterou za ordinální číslo nechceme neboť ordinálním číslem jednoprvkové množiny je $\{\emptyset\}$. Množina $\{\{\emptyset\}\}$ však není *tranzitivní* ve smyslu

$$x \in X \Rightarrow x \subseteq X$$

Ordinální čísla tranzitivní jsou. Definice ordinálního čísla v ZF tedy zní: *ordinální číslo je tranzitivní množina dobře uspořádaná relací $\in$.*

Věta 6.4. *(AC) Pro libovolné nekonečné kardinální číslo* $\aleph$ *platí*

$$\aleph \cdot \aleph = \aleph$$

Důkaz. Již víme, že za AC jsou kardinální čísla právě $\aleph_\alpha$, kde $\alpha \in W$. Transfinitní indukcí budeme tedy dokazovat, že

$$\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$$

Pro $\alpha = 0$ tvrzení platí (viz 6.5). Předpokládejme, že $0 < \alpha$ a že tvrzení platí pro všechna $\beta < \alpha$. Dokážeme, že tvrzení platí pro α. Tím bude důkaz ukončen.

Na množině $W(\omega_\alpha) \times W(\omega_\alpha)$ budeme uvažovat tzv. *maximo-lexikografické* uspořádání. Je definováno tak, že $(\beta, \gamma) < (\delta, \epsilon)$, právě když

$$\max\{\beta, \gamma\} < \max\{\delta, \epsilon\}$$

nebo

$$\max\{\beta, \gamma\} = \max\{\delta, \epsilon\} \text{ a } \beta < \delta$$

nebo

$$\max\{\beta, \gamma\} = \max\{\delta, \epsilon\}, \beta = \delta \text{ a } \gamma < \epsilon$$

Zřejmě se jedná o dobré uspořádání. Označme

$$\eta = \overline{W(\omega_\alpha) \times W(\omega_\alpha)}$$

takže

$$W(\omega_\alpha) \times W(\omega_\alpha) \cong W(\eta)$$

Stačí, když dokážeme, že platí $\eta = \omega_\alpha$. Pak totiž bude platit

$$\aleph_\alpha \cdot \aleph_\alpha = |W(\omega_\alpha) \times W(\omega_\alpha)| = |W(\omega_\alpha)| = \aleph_\alpha$$

Především platí $\omega_\alpha \leq \eta$ neboť

$$|W(\omega_\alpha)| \leq |W(\omega_\alpha) \times W(\omega_\alpha)| = |W(\eta)|$$

a ω_α je nejmenší ordinální číslo mohutnosti $\aleph_\alpha$. Předpokládejme, že $\omega_\alpha < \eta$. Pak existují ordinální čísla $\gamma, \delta < \omega_\alpha$ tak, že

$$W(\omega_\alpha) \cong W((\gamma, \delta))$$

(druhý výraz zde označuje začátek určený dvojicí (γ, δ) v $W(\omega_\alpha) \times W(\omega_\alpha)$). Položme

$$\xi = \max\{\gamma, \delta\} + 1$$

Zřejmě $\xi < \omega_\alpha$. Z definice maximo-lexikografického uspořádání plyne, že

$$W((\gamma, \delta)) \subseteq W(\xi) \times W(\xi)$$

tedy

$$|W(\omega_\alpha)| = |W((\gamma, \delta))| \leq |W(\xi) \times W(\xi)| = |W(\xi)|$$

(poslední rovnost plyne z indukčního předpokladu). Poněvadž $\xi < \omega_\alpha$, platí

$$|W(\omega_\alpha)| \leq |W(\xi)| < |W(\omega_\alpha)|$$

Dostáváme spor a důkaz je tím ukončen. □

Důsledek 6.5. *(AC) Pro libovolná ordinální čísla α, β platí*

$$\aleph_\alpha \cdot \aleph_\beta = \ max\{\aleph_\alpha, \aleph_\beta\}$$

Důkaz. Nechť například $\alpha \leq \beta$. Pak platí

$$\aleph_\beta = 1 \cdot \aleph_\beta \leq \aleph_\alpha \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta$$

takže $\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$. □

Důsledek 6.6. *(AC) Pro libovolná ordinální čísla α, β platí*

$$\aleph_\alpha + \aleph_\beta = \ max\{\aleph_\alpha, \aleph_\beta\}$$

Důkaz. Nechť například $\alpha \leq \beta$. Pak platí

$$\aleph_\beta \leq \aleph_\alpha + \aleph_\beta = 2 \cdot \aleph_\beta = \aleph_\beta$$

□

Důsledek 6.7. *(AC) Pro libovolná ordinální čísla $\alpha \leq \beta$ platí*

$$\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$$

Důkaz. Platí

$$2^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\beta} \leq (2^{\aleph_\alpha})^{\aleph_\beta} = 2^{\aleph_\alpha \cdot \aleph_\beta} = 2^{\aleph_\beta}$$

□

Zobecněná hypotéza kontinua říká, že

$$2^{\aleph_\alpha} = \aleph_{\alpha+1}.$$

Toto tvrzení je nezávislé na ZFC.

Důsledek 6.8. *(AC) Buďte I, A_i, $i \in I$ množiny takové, že $|I|, |A_i| \leq \aleph_\alpha$ pro všechna $i \in I$. Pak platí*

$$|\bigcup_{i \in I} A_i| \leq \aleph_\alpha$$

Důkaz. Platí

$$|\bigcup_{i \in I} A_i| \leq |\sum_{i \in I} W(\omega_\alpha)| = |I \times W(\omega_\alpha)| = |I| \cdot \aleph_\alpha \leq \aleph_\alpha$$

(zde jsme použili 6.11.) □

Poznámka 6.9.. Zejména, za AC platí, že sjednocení spočetně mnoha spočetných množin je spočetná množina.

Definice 6.10. Kardinální číslo $\aleph_\alpha$ se nazývá *regulární*, jestliže sjednocení $< \aleph_\alpha$ množin mohutnosti $< \aleph_\alpha$ má mohutnost $< \aleph_\alpha$. V opačném případě se $\aleph_\alpha$ nazývá *singulární*.

Příkladem regulárního kardinálního čísla je $\aleph_0$.

Důsledek 6.11. *(AC) Pro libovolné ordinální číslo α je kardinální číslo $\aleph_{\alpha+1}$ regulární.*

Důkaz. Plyne z 6.11. a z toho, že

$$|X| < \aleph_\alpha + 1 \Leftrightarrow |X| \leq \aleph_\alpha$$

□

Nespočetné kardinální číslo $\aleph_\alpha$ se nazývá *(slabě) nedosažitelné*, je-li regulární a zároveň α je limitní. Nazývá se *nedosažitelné*, je-li regulární a platí

$$\aleph_\beta < \aleph_\alpha \Rightarrow 2^{\aleph_\beta} < \aleph_\alpha$$

Libovolné nedosažitelné kardinální číslo je zřejmě slabě nedosažitelné. Za zobecněné hypotézy kontinua oba pojmy splynou.

Existenci nedosažitelného kardinálního čísla nelze dokázat z axiomů ZFC.

7. Ordinální aritmetika

Lemma 7.1. *Buď A dobře uspořádaná množina a $B \subseteq A$. Pak $\overline{B} \leq \overline{A}$.*

Důkaz. Předpokládejme, že $\overline{B} > \overline{A}$. Pak existuje prosté izotonní zobrazení $f : A \to B$ na vlastní začátek B. Složení $g : A \to A$ zobrazení f s inkluzí $B \to A$ je prosté izotonní zobrazení. Pro $a \in B - f(A)$ platí $g(a) < a$. Dostáváme spor s 3.1. □

Lemma 7.2. *Pro libovolná ordinální čísla α, β, γ platí*
(1) $\alpha < \beta \Rightarrow \gamma + \alpha < \gamma + \beta$
(2) $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$.

Důkaz. (1) je zřejmé, (2) plyne z 7.1. □

Lemma 7.3. *Pro libovolná ordinální čísla α, β a pro libovolné $0 < \gamma$ platí*
(1) $\alpha < \beta \Rightarrow \gamma \cdot \alpha < \gamma \cdot \beta$
(2) $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$.

Důkaz. (1) je zřejmé, (2) plyne z 7.1. □

Lemma 7.4. *Pro libovolná ordinální čísla $\alpha \leq \beta$ existuje právě jedno ordinální číslo γ tak, že $\alpha + \gamma = \beta$.*

Důkaz. Je zřejmý. □

Lemma 7.5. *Pro libovolná ordinální čísla α a $0 < \beta$ existují ordinální čísla $\delta \leq \alpha$ a $\rho < \beta$ tak, že $\alpha = \beta \cdot \delta + \rho$.*

Důkaz. Podle 7.3 (2) platí $\alpha = 1 \cdot \alpha \leq \beta \cdot \alpha$. Pokud nastane rovnost, zvolíme $\delta = \alpha$ a $\rho = 0$. Nechť $\alpha < \beta \cdot \alpha$ a $\alpha = \overline{A}$, $\beta = \overline{B}$. Pak A je izomorfní vlastnímu začátku Z v lexikografickém součinu $A \cdot B$. Tedy existují $a \in A$, $b \in B$ tak, že $Z = \{(x, y) \backslash (x, y) < (a, b)\}$. Buď $\delta = \overline{A(a)}$ a $\rho = \overline{B(b)}$. Pak $\alpha = \beta \cdot \delta + \rho$. □

Poznámka 7.6. Jedná se o větu o dělení se zbytkem pro ordinální čísla. Lze ukázat, že δ a ρ jsou určeny jednoznačně.

Lemma 7.7. *Buď I množina. Pro libovolná ordinální čísla α a β_i, $i \in I$ platí*
(1) $\alpha + sup\beta_i = sup(\alpha + \beta_i)$
(2) $\alpha \cdot sup\beta_i = sup(\alpha \cdot \beta_i)$.

Důkaz. (1) je zřejmá. (2) platí pro $\alpha = 0$. Buď $0 < \alpha$. Pak

$$\alpha \cdot \sup\beta_i \geq \sup(\alpha \cdot \beta_i)$$

neboť $\alpha \cdot \beta_i \leq \alpha \cdot \sup\beta_i$ pro všechna $i \in I$ (podle 7.3 (1)). Je-li $\gamma = \sup\beta_i$ izolované ordinální číslo, pak existuje $j \in I$ tak že $\sup\beta_i = \beta_j$ a tvrzení platí. Buď γ limitní. Pak $\beta_j < \sup\beta_i$ pro všechna $j \in I$ a tedy $\alpha \cdot \beta_j < \alpha \cdot \sup\beta_i$ pro pro všechna $j \in I$ (podle 7.3 (1)). Předpokládejme, že $\sigma = \sup(\alpha \cdot \beta_i) < \alpha \cdot \gamma$. Podle 7.5. existují ordinální čísla $\delta \leq \sigma$ a $\rho < \alpha$ tak, že $\sigma = \alpha \cdot \delta + \rho$. Tedy, podle 7.2 (1)

$$\sigma = \alpha \cdot \delta + \rho < \alpha \cdot \delta + \alpha = \alpha \cdot \delta + \alpha \cdot 1 = \alpha \cdot (\delta + 1).$$

Platí $\delta < \gamma$ neboť v opačném případě $\gamma \leq \delta$ a tedy $\alpha \cdot \gamma \leq \alpha \cdot \delta$ (podle 7.3), Odsud by plynulo

$$\alpha \cdot \delta \leq \alpha \cdot \delta + \rho = \sigma < \alpha \cdot \gamma,$$

což je spor.

Tedy $\delta < \beta_j$ pro nějaké $j \in I$, takže

$$\sigma < \alpha \cdot (\delta + 1) \leq \alpha \cdot \beta_j,$$

což je spor. □

Lemma 7.8. *Pro ordinální čísla platí*
(1) $\alpha \leq \beta \Rightarrow \alpha^\gamma \leq \beta^\gamma$
(2) $1 < \alpha, \beta < \gamma \Rightarrow \alpha^\beta < \alpha^\gamma$
(3) $1 < \alpha \Rightarrow \alpha^{\sup\beta_i} = sup\alpha^{\beta_i}$.

Důkaz. (1) Důkaz provedeme transfinitní indukcí podle γ. Tvrzení platí pro $\gamma = 0$. Předpokládejme, že platí pro všechna $\delta < \gamma$. Je-li $\gamma = \delta + 1$, pak podle indukčního předpokladu a 7.3 (1) platí

$$\alpha^\gamma = \alpha^\delta \cdot \alpha \leq \beta^\delta \cdot \alpha \leq \beta^\delta \cdot \beta = \beta^\gamma.$$

Je-li γ limitní, pak

$$\alpha^\gamma = \sup\{\alpha^\delta \backslash \delta < \gamma\} \leq \sup\{\beta^\delta \backslash \delta < \gamma\} = \beta^\gamma.$$

(2) Podle 7.4 existuje $0 < \delta$ tak, že $\gamma = \beta + \delta$. Podle 7.3 (1) platí

$$\alpha^\beta = \alpha^\beta \cdot 1 < \alpha^\beta \cdot \alpha = \alpha^{\beta+1} \leq \alpha^{\beta+\delta} = \alpha^\gamma.$$

Poslední nerovnost přitom plyne z definice ordinální mocniny a z 7.3 (1).

(3) plyne z definice ordinální mocniny. □

Lemma 7.9. *Pro ordinální čísla α, β, γ platí*
(1) $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$
(2) $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$.

Důkaz. (1) Pro $\alpha \leq 1$ je tvrzení zřejmé. Nechť $1 < \alpha$. Důkaz provedeme transfinitní indukcí podle γ. Tvrzení platí pro $\gamma = 0$. Předpokládejme, že platí pro všechna $\delta < \gamma$. Je-li $\gamma = \delta + 1$, pak podle indukčního předpokladu a 7.3 (1) platí

$$\alpha^{\beta+\gamma} = \alpha^{\beta+\delta+1} = \alpha^{\beta+\delta} \cdot \alpha = \alpha^\beta \cdot \alpha^\delta \cdot \alpha = \alpha^\beta \cdot \alpha^\gamma.$$

Je-li γ limitní, pak, použitím 7.7. (2),

$$\alpha^\beta \cdot \alpha^\gamma = \alpha^\beta \cdot \sup\{\alpha^\delta \backslash \delta < \gamma\} = \sup\{\alpha^\beta \cdot \alpha^\delta \backslash \delta < \gamma\} = \alpha^{\beta+\gamma}.$$

(2) Pro $\alpha \leq 1$ je tvrzení zřejmé, rovněž pokud některé z β, γ je 0. Nechť $1 < \alpha$, $0 < \beta, \gamma$. Důkaz provedeme transfinitní indukcí podle γ. Tvrzení platí pro $\gamma = 0$. Předpokládejme, že platí pro všechna $\delta < \gamma$. Je-li $\gamma = \delta + 1$, pak podle indukčního předpokladu a (1)

$$(\alpha^\beta)^\gamma = (\alpha^\beta)^{\delta+1} = (\alpha^\beta)^\delta \cdot \alpha^\beta = \alpha^{\beta\cdot\delta} \cdot \alpha^\beta = \alpha^{\beta\cdot\delta+\beta} = \alpha^{\beta\cdot(\delta+1)} = \alpha^{\beta\cdot\gamma}.$$

Je-li γ limitní, pak (s použitím 7.7. (2)),

$$(\alpha^\beta)^\gamma = \sup\{(\alpha^\beta)^\delta \backslash \delta < \gamma\} = \sup\{\alpha^{\beta\cdot\delta} \backslash \delta < \gamma\} = \alpha^{\sup\{\beta\cdot\delta \backslash \delta<\gamma\}} = \alpha^{\beta\cdot\sup\{\delta\backslash\delta<\gamma\}}.$$

Poslední výraz je však roven $\alpha^{\beta\cdot\gamma}$. □

Věta 7.10. *Buď $0 < \alpha$ ordinální číslo. Pak existují přirozená čísla $k, m_0, \ldots, m_k$ a ordinální čísla $\gamma_0 > \gamma_1 > \cdots > \gamma_k$ tak, že*

$$\alpha = \omega^{\gamma_0} \cdot m_0 + \cdots + \omega^{\gamma_k} \cdot m_k.$$

Důkaz. Budeme postupovat transfinitní indukcí podle α. Pro $\alpha = 1$ máme $\alpha = \omega^0$. Buď $1 < \alpha$ a předpokládejme, že věta platí pro všechna $\beta < \alpha$. Buď $X = \{\gamma \backslash \omega^\gamma \leq \alpha\}$. Z 7.8 (2) plyne, že X je množina. Podle 7.8. (3),

$$\omega^{\sup X} = \sup\{\omega^\gamma \backslash \gamma \in X\} \leq \alpha,$$

takže X má největší prvek γ_0. Buď $Y = \{\delta \backslash \omega^{\gamma_0} \cdot \delta \leq \alpha\}$. Z 7.2 (1) plyne, že Y je množina. Podle 7.7. (2) $\omega^{\gamma_0} \cdot \sup Y \leq \alpha$, takže Y má největší prvek m_0. Platí $m_0 < \omega$ neboť

$$\omega^{\gamma_0} \cdot \omega = \omega^{\gamma_0+1} > \alpha.$$

Pokud $\omega^{\gamma_0} \cdot m_0 = \alpha$, věta je dokázána. Nechť $\omega^{\gamma_0} \cdot m_0 < \alpha$. Pak

$$\alpha = \omega^{\gamma_0} \cdot m_0 + \beta$$

(podle 7.4). Platí $\beta < \omega^{\gamma_0}$ neboť $\omega^{\gamma_0} \leq \beta$ implikuje

$$\alpha = \omega^{\gamma_0} \cdot m_0 + \beta \geq \omega^{\gamma_0} \cdot m_0 + \omega^{\gamma_0} = \omega^{\gamma_0} \cdot (m_0 + 1),$$

což je spor s maximalitou m_0.

Podle indukčního předpokladu existují přirozená čísla $k, m_1, \ldots, m_k$ a ordinální čísla $\gamma_1 > \cdots > \gamma_k$ tak že

$$\beta = \omega^{\gamma_1} \cdot m_1 + \cdots + \omega^{\gamma_k} \cdot m_k.$$

Z maximality γ_0 plyne že $\gamma_0 > \gamma_1$. Tedy

$$\alpha = \omega^{\gamma_0} \cdot m_0 + \cdots + \omega^{\gamma_k} \cdot m_k.$$

a důkaz je ukončen. □

Poznámka 7.11. Jedná se o rozvoj ordinálního čísla $0 < \alpha$ v mocninách ω . Lze ukázat, že přirozená čísla $k, m_0, \ldots, m_k$ a ordinální čísla $\gamma_0 > \gamma_1 > \cdots > \gamma_k$ jsou určena jednoznačně.