Teorie množin

Zermelo–Fraenkelova teorie množin s axiomem výběru (ZFC)

Přednášky pro studenty matematiky

Katedra matematiky | Akademický rok 2025/2026

Obsah přednášek

1. Axiomy teorie množin
2. Relace a funkce
3. Přirozená čísla
4. Mohutnosti množin
5. Transfinitní rekurze
6. Axiom výběru
7. Ordinální čísla
8. Kardinální čísla

Obsah

1 Axiomy teorie množin **3**
- 1.1 Axiomy ZFC — přehled . . . 3
- 1.2 Axiom extenzionality . . . 3
- 1.3 Základní axiomy existence . . . 3
- 1.4 Axiom sjednocení a potenční množiny . . . 4
- 1.5 Množinové operace a třídy . . . 5
- 1.6 Axiom fundovanosti (regularity) . . . 5

2 Relace a funkce **5**
- 2.1 Uspořádané dvojice a kartézský součin . . . 5
- 2.2 Důkaz klíčové vlastnosti uspořádané dvojice . . . 6
- 2.3 Relace . . . 6
- 2.4 Funkce . . . 6
- 2.5 Operace s funkcemi . . . 7
- 2.6 Relace uspořádání . . . 7
- 2.7 Relace ekvivalence . . . 7

3 Přirozená čísla **8**
- 3.1 Konstrukce přirozených čísel . . . 8
- 3.2 Peanovy axiomy . . . 8
- 3.3 Princip rekurze . . . 9
- 3.4 Důkaz Principu rekurze — existence . . . 9
- 3.5 Důkaz Principu rekurze — jednoznačnost . . . 9
- 3.6 Aplikace: Korektnost aritmetiky na ω . . . 10
- 3.7 Korektnost definic sčítání, násobení a mocniny . . . 10
- 3.8 Algebraické zákony na ω . . . 10
- 3.9 Důkaz komutativity sčítání na ω (náčrt) . . . 10
- 3.10 Uspořádání na ω a princip indukce . . . 11
- 3.11 Princip silné indukce . . . 12
- 3.12 Důkaz Principu silné indukce . . . 12

4 Mohutnosti množin **12**
- 4.1 Konečné a nekonečné množiny . . . 13
- 4.2 Cantorova věta a diagonalizace . . . 16
- 4.3 Srovnávání mohutností . . . 17

5 Axiom výběru **17**
5.1 Axiom výběru (AC) . . . 18
5.2 Ekvivalence AC, Zornova lemmatu a WOP . . . 18
5.3 Důsledky axiomu výběru . . . 19

6 Ordinální čísla **20**
6.1 Definice a příklady ordinálních čísel . . . 20
6.2 Vlastnosti ordinálních čísel . . . 22
6.3 Existence nespočetného ordinálu . . . 23
6.4 Ordinální aritmetika . . . 23

7 Transfinitní rekurze **27**
7.1 Princip transfinitní rekurze . . . 27
7.2 Úvod k Von Neumannovu univerzu množin . . . 28
7.3 Von Neumannova kumulativní hierarchie . . . 29

8 Kardinální čísla **29**
8.1 Kardinální čísla . . . 29
8.2 Kardinální aritmetika . . . 30

9 Nezávislost hypotézy kontinua a limity ZFC **30**

1. Axiomy teorie množin

1.1 Axiomy ZFC — přehled

1. Axiom extenzionality
2. Existence prázdné množiny
3. Schéma axiomů vydělení
4. Axiom neuspořádané dvojice
5. Axiom sjednocení
6. Axiom potenční množiny
7. Axiom nekonečna
8. Schéma axiomů nahrazení
9. Axiom fundovanosti
10. Axiom výběru

Axiomy 1–9 tvoří systém ZF, přidáním axiomu 10 dostáváme ZFC

1.2 Axiom extenzionality

Axiom extenzionality

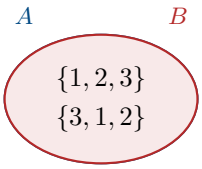
Dvě množiny jsou si rovny právě tehdy, když obsahují stejné prvky:

$$\forall A \forall B \left(A = B \iff \forall x \left(x \in A \iff x \in B\right)\right).$$

Důsledek pro důkaz rovnosti:

Chceme-li dokázat $A = B$, máme dvě strategie:

1. Dokázat $A \subseteq B$ a $B \subseteq A$.
2. Ukázat, že $\forall x$: $x \in A \iff x \in B$.



$A = B$ (stejné prvky)

Připomenutí:

$$A \subseteq B \iff \forall x \left(x \in A \Rightarrow x \in B\right).$$

1.3 Základní axiomy existence

Existence prázdné množiny

Existuje množina bez prvků:

$$\exists A \forall x \left(x \notin A\right).$$

Tato množina se značí $\emptyset$ a je jednoznačná dle axiomu extenzionality.

Schéma axiomů vydělení

Pro formuli $\varphi(x)$ a množinu A existuje

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

Axiom neuspořádané dvojice

Pro množiny u, v existuje $\{u, v\}$:

$$\forall u \forall v \exists A \forall x \left(x \in A \iff x = u \vee x = v\right).$$

Důsledky

- Průnik: $A \cap B = \{x \in A : x \in B\}$
- Rozdíl: $A \setminus B = \{x \in A : x \notin B\}$
- Jednoprvková: $\{u\} = \{u, u\}$

1.4 Axiom sjednocení a potenční množiny

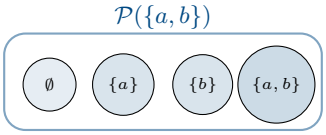
Axiom sjednocení

Pro každou množinu F existuje $\bigcup F$:

$$x \in \bigcup F \iff \exists C\,(x \in C \wedge C \in F).$$

Axiom potenční množiny

Pro množinu A existuje $\mathcal{P}(A) = \{u : u \subseteq A\}$.



1.5 Množinové operace a třídy

De Morganovy zákony

Je-li A množina a $F \neq \emptyset$:

$$A \setminus \bigcup F = \bigcap \{A \setminus C : C \in F\},$$
$$A \setminus \bigcap F = \bigcup \{A \setminus C : C \in F\}.$$

Distributivní zákony

$$A \cup (\bigcap F) = \bigcap \{A \cup C : C \in F\},$$
$$A \cap (\bigcup F) = \bigcup \{A \cap C : C \in F\}.$$

Třídy

Je-li $\varphi(x)$ logická formule, pak $\{x : \varphi(x)\}$ je **třída**.

Třída C je **množinou**, pokud $\exists M\, \forall x\, (x \in M \iff \varphi(x))$.

Jinak je C **vlastní třídou**.

Russellův paradox

Třída $\{x : x \notin x\}$ **není** množina!

Kdyby byla množinou R, pak $R \in R \iff R \notin R$ — spor. Proto potřebujeme schéma axiomů vydělení.

1.6 Axiom fundovanosti (regularity)

Axiom fundovanosti

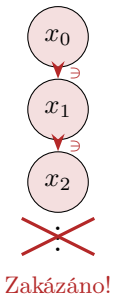
Každá neprázdná množina x obsahuje prvek y takový, že $y \cap x = \emptyset$:

$$\forall x \left(x \neq \emptyset \implies \exists y \in x\, (y \cap x = \emptyset)\right).$$

Důsledky:

- Žádná množina neobsahuje sama sebe: $\neg(x \in x)$.
- Neexistují cykly: $\neg(x \in y \in x)$.
- Neexistují nekonečné klesající $\in$-řetězce: $\neg(x_0 \ni x_1 \ni x_2 \ni \cdots)$.

Důkaz $A \notin A$: Uvažujme $\{A\}$. Jediný prvek A má s $\{A\}$ společný prvek A jen pokud $A \in A$. To je spor s axiomem.



Zakázáno!

2. Relace a funkce

2.1 Uspořádané dvojice a kartézský součin

Uspořádaná dvojice (Kuratowski, 1921)

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\}.$$

Klíčová vlastnost: $\langle x, y \rangle = \langle u, v \rangle \iff x = u \wedge y = v$.

Kartézský součin

$$A \times B = \{\langle x, y \rangle \in \mathcal{P}(\mathcal{P}(A \cup B)) : x \in A \wedge y \in B\}.$$

Příklad

Pro $A = \{2, 3\}$ a $B = \{a, b, c\}$:

$$A \times B = \{\langle 2, a\rangle, \langle 2, b\rangle, \langle 2, c\rangle, \langle 3, a\rangle, \langle 3, b\rangle, \langle 3, c\rangle\}.$$

2.2 Důkaz klíčové vlastnosti uspořádané dvojice

Věta (Kuratowski)

$\langle x, y\rangle = \langle u, v\rangle \iff x = u \wedge y = v.$

Důkaz ($\Leftarrow$): Zřejmé. ($\Rightarrow$): Nechť $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$.

Případ 1: $x = y$. Pak $\langle x, y\rangle = \{\{x\}\}$. Tedy $\{u\} = \{u, v\} = \{x\}$, odkud $u = v = x = y$. ✓

Případ 2: $x \neq y$. Pak $\{x, y\}$ je dvouprvková, takže $\{x\} \neq \{x, y\}$.

- Prvek $\{x\}$ musí být roven $\{u\}$ nebo $\{u, v\}$.
- Kdyby $\{x\} = \{u, v\}$, pak $u = v = x$, a potom $\{u\} = \{x\}$, tedy $\{x, y\} = \{u, v\} = \{x\}$, spor s $x \neq y$.
- Tedy $\{x\} = \{u\}$, odkud $x = u$.
- Dále $\{x, y\} = \{u, v\} = \{x, v\}$, a protože $y \neq x$, musí $y = v$. ✓

□

2.3 Relace

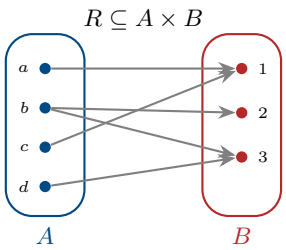
Binární relace

Relace R je množina uspořádaných dvojic. Relace mezi množinami A a B:

$$R \subseteq A \times B.$$

Definiční obor a obor hodnot

$$\begin{aligned} \mathrm{dom}(R) &= \{x : \exists y\, (\langle x, y\rangle \in R)\}, \\ \mathrm{ran}(R) &= \{y : \exists x\, (\langle x, y\rangle \in R)\}, \\ \mathrm{fld}(R) &= \mathrm{dom}(R) \cup \mathrm{ran}(R). \end{aligned}$$



2.4 Funkce

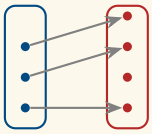
Funkce

Funkce F je jednoznačná binární relace: pro každé $x \in \mathrm{dom}(F)$ existuje právě jedno y t.ž. $\langle x, y\rangle \in F$.

$F\colon A \to B$, pokud $\mathrm{dom}(F) = A$, F je jednoznačná a $\mathrm{ran}(F) \subseteq B$.

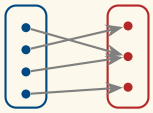
Injekce (prostá)

$F(x_1) = F(x_2)$
$\implies x_1 = x_2$



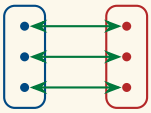
Surjekce („na")

$\text{ran}(F) = B$



Bijekce

Injekce + Surjekce



2.5 Operace s funkcemi

Inverze

$F^{-1} = \{\langle v, u\rangle : \langle u, v\rangle \in F\}$
Poznámka: F^{-1} nemusí být funkce!

Obraz a vzor

$F[A] = \{F(x) : x \in A\}$
$F^{-1}[B] = \{u \in \text{dom}(F) : F(u) \in B\}$

Restrikce

$F \restriction A = \{\langle u, v\rangle \in F : u \in A\}$
s $\text{dom}(F \restriction A) = \text{dom}(F) \cap A$.

Kompozice

$F \circ G = \{\langle u, v\rangle : \exists t\,(\langle u, t\rangle \in G \wedge \langle t, v\rangle \in F)\}$
$(F \circ G)(x) = F(G(x))$

Věta

Jsou-li $g\colon A \to B$ a $f\colon B \to C$ prosté, potom $f \circ g\colon A \to C$ je též prostá.

Důkaz. Nechť $(f \circ g)(x_1) = (f \circ g)(x_2)$, tj. $f(g(x_1)) = f(g(x_2))$. Protože f je prostá, plyne $g(x_1) = g(x_2)$. Protože g je prostá, plyne $x_1 = x_2$. □

2.6 Relace uspořádání

Částečné uspořádání

Relace $\preceq$ na A je **částečné uspořádání**, pokud $\forall x, y, z \in A$:

1. **Reflexivita:** $x \preceq x$
2. **Antisymetrie:** $x \preceq y \wedge y \preceq x \Rightarrow x = y$
3. **Tranzitivita:** $x \preceq y \wedge y \preceq z \Rightarrow x \preceq z$

Úplné (lineární) uspořádání

Částečné usp. + $\forall x, y \in A$: $x \preceq y \vee y \preceq x$.

Striktní částečné uspořádání

Relace $\prec$ na A:

1. **Ireflexivita:** $x \not\prec x$
2. **Tranzitivita:** $x \prec y \wedge y \prec z \Rightarrow x \prec z$

Příklad

$(\mathcal{P}(F), \subseteq)$ je částečně uspořádaná množina.
$(\mathbb{R}, \leq)$ je úplně uspořádaná.

2.7 Relace ekvivalence

Ekvivalence

Relace $\sim$ na A je **ekvivalence**, pokud $\forall x, y, z \in A$:

1. **Reflexivita:** $x \sim x$
2. **Symetrie:** $x \sim y \Rightarrow y \sim x$
3. **Tranzitivita:** $x \sim y \wedge y \sim z \Rightarrow x \sim z$

Třída ekvivalence

$[a]_\sim = \{x \in A : x \sim a\}$

Rozklad $A/\sim$ = množina všech tříd ekvivalence.

Příklad

Na $\mathbb{Z}$ definujme $a \sim b \iff 2 \mid (a-b)$.

Třídy: $[0] = \{\ldots, -2, 0, 2, 4, \ldots\}$, $[1] = \{\ldots, -1, 1, 3, 5, \ldots\}$.

Rozklad: $\mathbb{Z}/\sim = \{[0], [1]\}$.

Věta

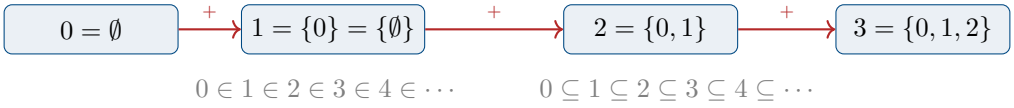
Třídy ekvivalence tvoří rozklad A (systém po dvou disjunktních neprázdných množin, jejichž sjednocení je A). Naopak, každý rozklad definuje ekvivalenci.

3. Přirozená čísla

3.1 Konstrukce přirozených čísel

Následovník

Pro množinu x definujeme **následovníka**: $x^+ = x \cup \{x\}$.



Induktivní množina

I je **induktivní**, pokud:

1. $\emptyset \in I$,
2. $\forall a \in I : a^+ \in I$.

Axiom nekonečna

Existuje alespoň jedna induktivní množina.

ω

ω = nejmenší induktivní množina
$= \{n : n$ patří do každé induktivní mn.$\}$

3.2 Peanovy axiomy

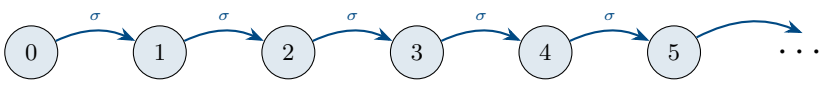
Peanův systém $\langle N, S, e\rangle$

Uspořádaná trojice, kde N je množina, $S : N \to N$ funkce, $e \in N$:

1. $e \notin \mathrm{ran}(S)$ (nula není následovníkem).
2. S je prostá funkce.
3. **Axiom indukce:** Pokud $e \in A \subseteq N$ a A je uzavřená vůči S, pak $A = N$.

Věta

Trojice $\langle \omega, \sigma, 0\rangle$, kde $\sigma(n) = n^+$ pro $n \in \omega$, tvoří Peanův systém.



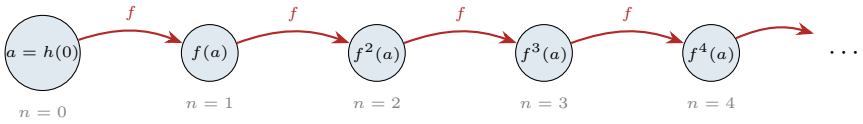
3.3 Princip rekurze

Věta (Princip rekurze)

Nechť A je množina, $a \in A$ a $f\colon A \to A$ funkce. Potom existuje **jediná** funkce $h\colon \omega \to A$ taková, že

1. $h(0) = a$,
2. $h(n^+) = f(h(n))$ pro všechna $n \in \omega$.

Říkáme, že funkce h je podmínkami 1 a 2 **definována rekurentně.**



3.4 Důkaz Principu rekurze — existence

Existence. Definujme relaci $R \subseteq \omega \times A$: $\langle n, b\rangle \in R$ právě tehdy, když existuje konečná posloupnost $b_0, b_1, \ldots, b_n \in A$ taková, že

$$b_0 = a, \qquad b_{i+1} = f(b_i) \text{ pro } i = 0, \ldots, n-1, \qquad b_n = b.$$

Indukcí dokážeme $(\forall n \in \omega)\,(\exists!\, b \in A)\,(\langle n, b\rangle \in R)$:

- **Základ** $(n = 0)$: Jediné $b = a$ splňuje $\langle 0, a\rangle \in R$. ✓
- **Krok** $(k \mapsto k^+)$: Dle IP existuje jediné b_k s $\langle k, b_k\rangle \in R$. Položíme $b_{k+1} = f(b_k)$; pak $\langle k^+, b_{k+1}\rangle \in R$ a b_{k+1} je určeno jednoznačně. ✓

Tedy R je funkce; položme $h = R$. Ověření:

1. $h(0) = a$, neboť $\langle 0, a\rangle \in R$.
2. Pro $n \in \omega$: Je-li $h(n) = b$, pak $\langle n^+, f(b)\rangle \in R$, tedy $h(n^+) = f(h(n))$. ✓

3.5 Důkaz Principu rekurze — jednoznačnost

Jednoznačnost. Nechť $h_1, h_2\colon \omega \to A$ obě splňují podmínky 1 a 2.

Dokážeme indukcí: $(\forall n \in \omega)\,(h_1(n) = h_2(n))$.

- **Základ** $(n = 0)$: $h_1(0) = a = h_2(0)$. ✓
- **Krok** $(k \mapsto k^+)$: Předpokládejme $h_1(k) = h_2(k)$. Potom

$$h_1(k^+) = f\big(h_1(k)\big) = f\big(h_2(k)\big) = h_2(k^+). \quad ✓$$

Tedy $h_1 = h_2$ a funkce h je určena jednoznačně. □

Příklad (Aritmetická posloupnost)

Pro $A = \mathbb{R}$, $a \in \mathbb{R}$, $f(x) = x + d$ (d je konstanta):
Princip rekurze dává jedinou $h\colon \omega \to \mathbb{R}$ s $h(0) = a$, $h(n^+) = h(n) + d$.
Tedy $h(n) = a + n \cdot d$ — aritmetická posloupnost!

3.6 Aplikace: Korektnost aritmetiky na ω

Věta

Nechť $g\colon \omega \to \omega$ a $f\colon \omega \times \omega \to \omega$ jsou dané funkce. Potom existuje jediná funkce $h\colon \omega \times \omega \to \omega$ taková, že pro každé $m \in \omega$:

1. $h(m, 0) = g(m)$,
2. $h(m, n^+) = f(h(m, n),\ m)$ pro všechna $n \in \omega$.

Důkaz. Pro pevné $m \in \omega$ definujme $A = \omega$, počáteční hodnotu $a = g(m)$ a funkci $\tilde{f}(x) = f(x, m)$.

Dle **Principu rekurze** existuje jediná $p_m\colon \omega \to \omega$ splňující:

$$p_m(0) = g(m), \qquad p_m(n^+) = f(p_m(n),\ m).$$

Definujme $h(m, n) = p_m(n)$. Funkce h splňuje podmínky 1 a 2 a je jednoznačná. □

3.7 Korektnost definic sčítání, násobení a mocniny

Předchozí věta zaručuje existenci a jednoznačnost:

Sčítání ($g(m) = m$, $f(x, m) = x^+$)

$$\begin{aligned} m + 0 &= m, \\ m + n^+ &= (m + n)^+. \end{aligned}$$

Mocnina ($g(m) = 1$, $f(x, m) = x \cdot m$)

$$\begin{aligned} m^0 &= 1, \\ m^{n^+} &= m^n \cdot m. \end{aligned}$$

Násobení ($g(m) = 0$, $f(x, m) = x + m$)

$$\begin{aligned} m \cdot 0 &= 0, \\ m \cdot n^+ &= m \cdot n + m. \end{aligned}$$

Příklad: $2 + 2 = 4$

$$\begin{aligned} 2 + 2 &= 2 + 1^+ \\ &= (2 + 1)^+ && \text{(A2)} \\ &= (2^+)^+ && \text{(A1)} \\ &= 3^+ = 4. \end{aligned}$$

3.8 Algebraické zákony na ω

Algebraické zákony

Pro $m, n, p \in \omega$:

- **Asociativita $+$:** $m + (n + p) = (m + n) + p$
- **Komutativita $+$:** $m + n = n + m$
- **Distributivita:** $m \cdot (n + p) = m \cdot n + m \cdot p$
- **Asociativita $\cdot$:** $m \cdot (n \cdot p) = (m \cdot n) \cdot p$
- **Komutativita $\cdot$:** $m \cdot n = n \cdot m$

Všechny důkazy pomocí matematické indukce!

3.9 Důkaz komutativity sčítání na ω (náčrt)

Cíl: $\forall m, n \in \omega\colon m + n = n + m$. Indukcí podle n (s m pevným).

Nejprve pomocné lemma: $m + 0 = 0 + m$ pro všechna m (indukcí dle m).

- Základ: $0 + 0 = 0 + 0$. ✓
- Krok: $0 + m^+ = (0 + m)^+ \overset{\text{IP}}{=} (m + 0)^+ = m^+ = m^+ + 0$. ✓

Hlavní důkaz (indukce dle n):

- Základ ($n = 0$): $m + 0 = m = 0 + m$ dle lemmatu. ✓
- Krok ($n \mapsto n^+$): Potřebujeme $m + n^+ = n^+ + m$.

$$\begin{aligned} m + n^+ &= (m + n)^+ \overset{\text{IP}}{=} (n + m)^+ \\ &= n + m^+ \overset{\text{lemma}}{=} n + m^+ \overset{?}{=} n^+ + m. \end{aligned}$$

K dokončení je potřeba ještě lemma $n + m^+ = (n + m)^+ = n^+ + m$, které se dokazuje analogickou indukcí.

3.10 Uspořádání na ω a princip indukce

Uspořádání

Pro $m, n \in \omega$: $\quad m < n \iff m \in n, \quad m \leq n \iff m \in n \vee m = n.$

Trichotomie

Pro každé $m, n \in \omega$ platí **právě jedna** z podmínek:

$$m \in n \quad \text{nebo} \quad m = n \quad \text{nebo} \quad n \in m.$$

Věta

$(\omega, \leq)$ je lineárně uspořádaná množina. Navíc $(\omega, \leq)$ je **dobře uspořádaná** — každá neprázdná podmnožina má nejmenší prvek.

Důkaz. Důkaz rozdělíme do několika logických kroků.

Krok 1: Částečné uspořádání (reflexivita, tranzitivita, antisymetrie).

- *Reflexivita:* Nechť $m \in \omega$. Podle definice $m \leq m \iff m \in m \vee m = m$. Druhá podmínka zjevně platí, takže $\leq$ je reflexivní.
- *Tranzitivita:* Nechť $k \leq m$ a $m \leq n$. Rozlišme případy. Pokud $k = m$ nebo $m = n$, je tvrzení $k \leq n$ zřejmé. Zbývá případ, kdy $k < m$ a $m < n$, tj. $k \in m$ a $m \in n$. Protože každý prvkem uspořádané struktury ω je tranzitivní množina (důsledek definice ω), tak $m \in n \implies m \subseteq n$. Z $k \in m$ a $m \subseteq n$ plyne $k \in n$, neboli $k < n$, a tedy $k \leq n$.
- *Antisymetrie:* Nechť $m \leq n$ a $n \leq m$. Obdobně jako výše, pokud by $m \neq n$, dostali bychom $m \in n$ a $n \in m$. Tranzitivitou by pak platilo $m \in m$, což je však spor s axiomem fundovanosti (žádná množina nemůže být prvkem sama sebe). Proto musí platit $m = n$.

Krok 2: Linearita (totálnost uspořádání). Máme ukázat, že pro libovolná $m, n \in \omega$ platí alespoň jedna z možností $m \leq n$ nebo $n \leq m$. To však přímo vyplývá ze dříve uvedené Věty o trichotomii — pro každé dvě přirozená čísla platí právě jedna relace z $\{m \in n, m = n, n \in m\}$. Relace $\leq$ je tedy lineární uspořádání.

Krok 3: Dobré uspořádání (existence nejmenšího prvku).

- Nechť $X \subseteq \omega$ je neprázdná množina. Podle axiomu fundovanosti (axiom regularity) existuje prvek $x \in X$ takový, že $x \cap X = \emptyset$.

- Chceme ukázat, že x je nejmenší prvek X vzhledem k relaci $\leq$. Vezměme libovolné $y \in X$. Pokud $y = x$, relace $x \leq y$ platí triviálně (z reflexivity). Předpokládejme tedy, že $y \neq x$. Z linearity uspořádání pak musí platit buď $y < x$ (tj. $y \in x$) nebo $x < y$.
- Pokud by ale platilo $y \in x$, znamenalo by to, že prvek y patří jak do X, tak do x, takže by platilo $y \in x \cap X$, což je spor s $x \cap X = \emptyset$. Musí tudíž nutně platit $x < y$, a tedy i $x \leq y$.
- Jelikož y bylo zvoleno libovolně, je x skutečně nejmenším prvkem množiny X.

Tím je věta dokázána. □

3.11 Princip silné indukce

Princip silné indukce

Nechť $\varphi(n)$ je vlastnost. Pokud pro každé $n \in \omega$ platí:

$$\big(\forall k < n\colon \varphi(k)\big) \implies \varphi(n),$$

pak $\varphi(n)$ platí pro všechna $n \in \omega$.

3.12 Důkaz Principu silné indukce

Důkaz. Sporem. Předpokládejme, že předpoklad platí, ale existuje $n_0 \in \omega$ takové, že $\neg\varphi(n_0)$.

Položme $S = \{n \in \omega : \neg\varphi(n)\}$. Pak $S \neq \emptyset$ (neboť $n_0 \in S$).

Jelikož $(\omega, \leq)$ je **dobře uspořádaná**, existuje **nejmenší prvek** $m \in S$.

Protože m je nejmenší prvek S, pro všechna $k < m$ platí $k \notin S$, tj.

$$\forall k < m\colon \varphi(k).$$

Z předpokladu věty pak vyplývá:

$$\big(\forall k < m\colon \varphi(k)\big) \implies \varphi(m),$$

a tedy $\varphi(m)$ platí. To znamená $m \notin S$ — **spor** s tím, že $m \in S$.

Množina S je tudíž prázdná a $\varphi(n)$ platí pro všechna $n \in \omega$. □

4. Mohutnosti množin

4.1 Konečné a nekonečné množiny

Konečná množina

X je **konečná**, pokud existuje $n \in \omega$ a bijekce $f\colon X \to n$.
Mohutnost $|X| = n$ je (jediné) takové n.

Dirichletův princip

Pokud $m < n$ a $f\colon n \to m$, pak f není prostá.

(„Do m zásuvek nelze rozdělit $n > m$ předmětů tak, aby v každé byla max. 1.")

Nekonečná / spočetná množina

X je **nekonečná**, pokud není konečná.
X je **spočetná**, pokud existuje prostá $f\colon X \to \omega$.
Pozn.: Spočetná = nejvýše spočetná (konečná nebo spočetně nekonečná).

Příklady spočetných množin

ω, $\mathbb{Z}$, $\mathbb{Q}$, $\omega \times \omega$
Věta: Jsou-li A, B spočetné, pak i $A \cup B$, $A \times B$ jsou spočetné.

Důkaz (Dirichletova principu). Důkaz provedeme silnou indukcí podle n. Nechť $\varphi(n)$ je tvrzení:

$$\forall m < n\ \forall f\colon n \to m\colon f \text{ není prostá.}$$

Základ indukce ($n = 0$): Tvrzení $\varphi(0)$ platí prázdně, neboť neexistuje žádné $m \in \omega$ takové, že $m < 0$.

Indukční krok: Předpokládejme, že $\varphi(k)$ platí pro všechna $k < n$ (indukční předpoklad). Dokážeme $\varphi(n)$. Nechť $n > 0$, tj. $n = p^+$ pro nějaké $p \in \omega$. Nechť dále $m < n$ a uvažme funkci $f\colon n \to m$. Sporem předpokládejme, že f je prostá.

Jelikož $m < p^+$, máme $m \leq p$. Pokud $m = 0$, neexistuje zobrazení z neprázdné množiny do prázdné, což je spor. Lze tedy psát $m = q^+$ pro nějaké $q \in \omega$. Z $m \leq p$ navíc plyne $q < m \leq p$, a tedy $q < p$.

Položme $a = f(p) \in m$. Restrikcí f na podmnožinu p získáme funkci $f \restriction p\colon p \to m \setminus \{a\}$. Protože je f prostá, žádný prvek z p nezíská stejný obraz a jako prvek p. Zavedeme přeznačkovací bijekci $\sigma\colon m \setminus \{a\} \to q$ předpisem:

$$\sigma(x) = \begin{cases} x & \text{pokud } x \neq q, \\ a & \text{pokud } x = q. \end{cases}$$

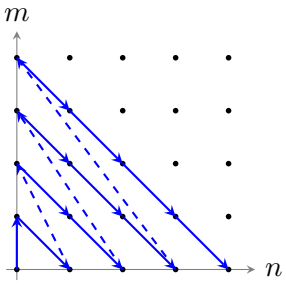
Složením $\sigma \circ (f \restriction p)$ dostaneme definované a prosté zobrazení z p do q. Toto je však v přímém rozporu s IP, neboť $p < n$ a $q < p$, a tudíž žádné prosté zobrazení na těchto množinách neexistuje. Kýžený spor potvrdil, že f není prostá. □

Důkaz spočetnosti uvedených množin.

1. **Spočetnost ω:** Zvolme identické zobrazení $f\colon \omega \to \omega$, $f(n) = n$. Je zjevně prosté, proto je ω spočetná (trivialita vyplývající z definice).

2. **Spočetnost $\mathbb{Z}$:** Definujme $f\colon \mathbb{Z} \to \omega$ předpisem $f(n) = 2n$ pro $n \geq 0$ a $f(n) = -2n - 1$ pro $n < 0$. Sudé hodnoty pokrývají nezáporná celá čísla, liché hodnoty záporná. Neexistuje překryv mezi sudými a lichými hodnotami a lineární funkce v sekcích jsou prosté, proto je f prosté.

3. **Spočetnost $\omega \times \omega$:** Množinu všech uspořádaných dvojic (n, m) si pro intuici můžeme představit jako nekonečnou tabulku. Dvojice můžeme počítat (číslovat) postupným procházením po „diagonálách": $(0,0) \mapsto 0$, $(0,1) \mapsto 1$, $(1,0) \mapsto 2$, $(0,2) \mapsto 3$, $(1,1) \mapsto 4$, $(2,0) \mapsto 5, \ldots$ Každé dvojici se tak dostane unikátní index (tzv. Cantorova párovací funkce).



Pro elegantní formální důkaz bez nutnosti konstruovat složitou bijekci (tzv. Cantorův polynom) využijeme vlastností prvočíselného rozkladu:

- **Definice zobrazení:** Uvažme funkci $f\colon \omega \times \omega \to \omega$ danou předpisem $f(n,m) = 2^n \cdot 3^m$.
- **Předpoklad rovnosti:** Jistě f nabývá hodnot v ω. Abychom ukázali, že je f prosté zobrazení, předpokládejme, že pro nějaké dvě uspořádané dvojice (n_1, m_1) a (n_2, m_2) platí $f(n_1, m_1) = f(n_2, m_2)$, tedy:

$$2^{n_1} \cdot 3^{m_1} = 2^{n_2} \cdot 3^{m_2}$$

- **Aplikace věty:** Základní věta aritmetiky říká, že každé přirozené číslo větší než 1 má jednoznačný rozklad na součin prvočísel (až na pořadí činitelů). Protože 2 a 3 jsou různá prvočísla, musí být jejich mocniny v obou rozkladech shodné.
- **Závěr:** Z toho bezprostředně plyne, že musí platit $n_1 = n_2$ a zároveň $m_1 = m_2$. Zobrazení f tedy stejnou hodnotu přiřazuje pouze zcela identickým dvojicím, a proto je f prosté. Existuje prosté zobrazení do ω, množina $\omega \times \omega$ je tedy spočetná.

4. **Spočetnost $A \cup B$ pro spočetné A, B:** Jelikož jsou A, B spočetné, existují prostá zobrazení $f_A\colon A \to \omega$ a $f_B\colon B \to \omega$. Definujme $h\colon A \cup B \to \omega$ tak, že $h(x) = 2f_A(x)$ pro $x \in A$ a $h(x) = 2f_B(x) + 1$ pro $x \in B \setminus A$.

   Ukážeme, že zobrazení h je prosté. Předpokládejme, že pro nějaké $x, y \in A \cup B$ platí $h(x) = h(y)$. Mohou nastat tyto situace v závislosti na paritě výsledné hodnoty:

   - **Hodnota je sudá:** Poté obě hodnoty z definice musely vzniknout z první větve předpisu, takže $x \in A$ i $y \in A$. Dostáváme rovnost $2f_A(x) = 2f_A(y)$, neboli po vykrácení dvojkou $f_A(x) = f_A(y)$. Z předpokladu, že f_A je prosté, bezprostředně plyne $x = y$.
   - **Hodnota je lichá:** Pak obě vznikly z druhé větve předpisu, takže $x \in B \setminus A$ i $y \in B \setminus A$. Odpovídající rovnice je $2f_B(x) + 1 = 2f_B(y) + 1$, odtud $2f_B(x) = 2f_B(y)$ a posléze $f_B(x) = f_B(y)$. Z prostoty zobrazení f_B opět vyplývá $x = y$.
   - Situace, kdy by pro $x \in A$ a $y \in B \setminus A$ platilo $h(x) = h(y)$, vůbec nemůže nastat, protože sudé číslo $(2f_A(x))$ se nemůže rovnat lichému $(2f_B(y) + 1)$.

   Zobrazení h tedy ve všech případech dává stejný obraz pouze pro identické vzory, z čehož vyplývá, že je prosté. $\implies$ $A \cup B$ je spočetná.

5. **Spočetnost $A \times B$ pro spočetné A, B:** Tento důkaz provedeme poskládáním dvou prostých zobrazení:

   - Nejdříve vytvoříme pomocné zobrazení $F\colon A \times B \to \omega \times \omega$ definované po složkách jako $F(a,b) = (f_A(a), f_B(b))$. Toto zobrazení je prosté, protože obě jeho složky pocházejí z prostých zobrazení v definici (pokud $F(a_1, b_1) = F(a_2, b_2)$, pak se rovnají obě souřadnice současně, z čehož díky prostotě f_A a f_B snadno plyne $a_1 = a_2$ i $b_1 = b_2$).

- Následně využijeme prosté zobrazení pro dvojice přirozených čísel $p\colon \omega \times \omega \to \omega$ (tzv. párovací funkci) dokázané výše v bodě 3.
- Zobrazení $g\colon A \times B \to \omega$ nakonec definujeme jako kompozici obou předešlých, tedy $g = p \circ F$, respektive $g(a,b) = p(f_A(a), f_B(b))$. Jelikož platí univerzální pravidlo, že složení jakýchkoli dvou prostých zobrazení (F a p) je vždy zobrazení prosté, je množina $A \times B$ prokazatelně spočetná.

6. **Spočetnost $\mathbb{Q}$:** Každé racionální číslo $q \in \mathbb{Q}$ lze jednoznačně zapsat v základním tvaru jako zlomek $q = \frac{z}{p}$, kde $z \in \mathbb{Z}$, $p \in \omega \setminus \{0\}$ a čísla z, p jsou nesoudělná. Tím je dáno prosté zobrazení z $\mathbb{Q}$ do $\mathbb{Z} \times \omega$, mapující $q \mapsto (z,p)$. Protože $\mathbb{Z}$ i ω jsou spočetné, je dle bodu 5 spočetný i jejich kartézský součin $\mathbb{Z} \times \omega \implies$ existuje prosté zobrazení z $\mathbb{Q}$ do ω.

□

Důkaz korektnosti definice mohutnosti konečné množiny. Nechť X je libovolná konečná množina. Chceme ukázat, že číslo $n \in \omega$, k němuž existuje bijekce od množiny X, je určeno zcela jednoznačně (tzn. neexistuje vícero takových čísel souběžně pro jedinou množinu). Důkaz provedeme sporem:

- **Předpoklad pro spor:** Předpokládejme, že definice jednoznačná není a existují dvě odlišná přirozená čísla $m, n \in \omega$ ($m \neq n$), přičemž obě splňují vlastnosti „mohutnosti konečné množiny“.
- **Existence bijekcí:** Z první podmínky definice musí tedy k oběma číslům existovat bijekce od naší množiny, a sice $f\colon X \to n$ a $g\colon X \to m$.
- **Uspořádání čísel:** Aniž bychom jakkoliv omezili platnost důkazu (tzv. *bez újmy na obecnosti*), můžeme rovnou o těchto dvou různých číslech nařídit, které z nich je menší. Nechť $m < n$.
- **Konstrukce inverzního zobrazení:** Z vlastností bijekcí víme, že ke zobrazení f je zaručena existence zobrazení inverzního, tj. $f^{-1}\colon n \to X$, které je navíc samo o sobě rovněž bijekcí.
- **Spojení dvou světů:** Z obou uvažovaných zobrazení si nyní „vyrobíme“ jediné složené zobrazení h ve formě $h = g \circ f^{-1}$. Zobrazení h tvoří nový most: nejprve přeloží množinu n do elementů X a ty posléze přemapuje do m. Celkově tedy tvoří zobrazení $h\colon n \to m$.
- **Propis vlastností:** Původní dvě využívaná zobrazení (tj. f^{-1} a g) jsou bijekce, platí pro ně tedy, že jsou obě současně prostá. Podle známé věty o kompozici prostých funkcí je pak i složené zobrazení h nutně prostým zobrazením.
- **Finální spor obou logik:** Postupnou strukturou důkazu se nám úspěšně podařilo prokázat existenci ryze prostého zobrazení $h\colon n \to m$. Číslo m je přitom menší nežli n. Avšak připomeňme si text prvního blokového rámečku této sekce (tzv. Dirichletův princip): ***do*** m ***zásuvek nelze prostým zobrazením rozdělit*** $n > m$ ***předmětů***. Nastává nevyhnutelný matematický spor!

Tato nesrovnalost ukazuje, že náš jediný dosazený nestandardní předpoklad na počátku důkazu („mohutnost není určena jednoznačně“) je naprosto mylný. Hodnota n je přiřazená pro každou konečnou množinu ojediněle a z pojmu se tedy definuje platná a korektní „mohutnost konečné množiny“. □

4.2 Cantorova věta a diagonalizace

Mohutnost $=_c$, $\leq_c$ a $<_c$

$$
\begin{aligned}
|A| =_c |B| &\iff \text{existuje bijekce } f\colon A \to B,\\
|A| \leq_c |B| &\iff \text{existuje prostá } f\colon A \to B,\\
|A| <_c |B| &\iff |A| \leq_c |B| \text{ a neexistuje bijekce } A \to B.
\end{aligned}
$$

Cantorova věta

Pro libovolnou množinu A platí $|A| <_c |\mathcal{P}(A)|$.

Důkaz (diagonální argument):

1. **Nerovnost:** Prosté zobrazení $f\colon A \to \mathcal{P}(A)$ zřejmě existuje (např. $f(a) = \{a\}$). Tedy $|A| \leq_c |\mathcal{P}(A)|$.
2. **Předpoklad pro spor:** Předpokládejme, že existuje surjekce $g\colon A \to \mathcal{P}(A)$.
3. **Diagonála D:** Definujme podmnožinu $D = \{a \in A \mid a \notin g(a)\}$. Jelikož $D \in \mathcal{P}(A)$ a g je na, musí existovat $d \in A$ takové, že $g(d) = D$.
4. **Spor:** Zeptejme se: Platí $d \in D$?
   - Pokud ano ($d \in D$), tak z definice množiny D musí platit $d \notin g(d) = D$. Spor.
   - Pokud ne ($d \notin D$), tak z definice D musí platit opak, tedy $d \in g(d) = D$. Opět spor.
5. **Závěr:** Surjekce g nemůže existovat. Platí proto ostrá nerovnost $|A| <_c |\mathcal{P}(A)|$. □

Aplikace diagonalizace: Nespočetnost intervalu $(0,1) \subset \mathbb{R}$

Podobný diagonální argument použil Georg Cantor k originálnímu historickému důkazu, že interval reálných čísel $(0,1)$ nelze seřadit do spočetné posloupnosti a má tedy ostře větší mohutnost než ω.

- **Předpoklad pro spor:** Předpokládejme, že množina reálných čísel $x \in (0,1)$ je spočetná a lze ji tedy uspořádat do kompletního očíslovaného seznamu (posloupnosti) $x_0, x_1, x_2, x_3, \ldots$
- **Desetinný rozvoj:** Každé takové číslo ze seznamu x_i si pro představu zapíšeme jeho desetinným rozvojem (k zamezení nejednoznačnosti nepoužijeme ty zápisy, které končí nekonečnou periodou devítek). Utvoří se nám nekonečná matice cifer:

$$
\begin{aligned}
x_0 &= 0, \mathbf{d_{00}} d_{01} d_{02} d_{03} \ldots\\
x_1 &= 0, d_{10} \mathbf{d_{11}} d_{12} d_{13} \ldots\\
x_2 &= 0, d_{20} d_{21} \mathbf{d_{22}} d_{23} \ldots\\
x_3 &= 0, d_{30} d_{31} d_{32} \mathbf{d_{33}} \ldots\\
&\vdots
\end{aligned}
$$

  kde $d_{ij} \in \{0, 1, \ldots, 9\}$ označuje j-tou cifru v i-tém čísle.
- **Konstrukce chybějícího čísla y:** Nyní schválně vyrobíme zbrusu nové reálné číslo $y \in (0,1)$ ve formátu $y = 0, y_0 y_1 y_2 y_3 \ldots$ Jeho cifry y_i vytvoříme záměrně tak, aby „nesouhlasilo“ zrovna s tou cifrou libovolného reálného čísla, která na našem výpisu leží

na diagonále (d_{ii}). Definujme např.:

$$y_i = \begin{cases} 4, & \text{pokud je na diagonále } d_{ii} \neq 4 \\ 5, & \text{pokud je na diagonále } d_{ii} = 4 \end{cases}$$

- **Důsledek a zpochybnění sporu:** Podle předpisu výše se zkonstruované číslo y liší od nultého čísla x_0 minimálně ve své nulté cifře. Od čísla x_1 se liší spolehlivě ve své první cifře a tak dále. Z definice nového čísla tedy nutně platí, že $y \neq x_i$ **pro libovolné** i.
- **Závěr:** Úspěšně jsme sestrojili reálné číslo intervalu $(0, 1)$, jež zřejmě chybí v našem původním seznamu, který měl pokrývat absolutně vše. To je **nepřekonatelný spor**. Nelze vypsat všechny hodnoty do jedné spočetné řady – interval reálných čísel je ryze **nespočetný**.

4.3 Srovnávání mohutností

Cantor–Bernstein–Schröderova věta

$$|A| \leq_c |B| \ \wedge \ |B| \leq_c |A| \implies |A| =_c |B|.$$

Idea důkazu: Jsou-li $f\colon A \to B$ a $g\colon B \to A$ prosté, rozdělíme A na části, které „patří f" a „patří g^{-1}", a z nich sestavíme bijekci. Důkaz nevyžaduje AC!

Důkaz (přesná konstrukce): Nechť $f\colon A \to B$ a $g\colon B \to A$ jsou prostá zobrazení. Sestrojíme bijekci $h\colon A \to B$. Induktivně definujeme posloupnost množin:

- $A_0 = A \setminus g[B]$ (prvky v ve výchozí množině A, které nemají vzor při zobrazení g),
- $A_{n+1} = g[f[A_n]]$ pro rovnice $n \in \mathbb{N}$ (zřetězené obrazy předchozích kroků).

Označme $A^* = \bigcup_{n=0}^{\infty} A_n$ (sjednocení všech těchto specifikovaných částí).

Definujme zobrazení $h\colon A \to B$ po částech takto:

$$h(x) = \begin{cases} f(x) & \text{pro } x \in A^*, \\ g^{-1}(x) & \text{pro } x \in A \setminus A^*. \end{cases}$$

Ověření korektnosti a vlastností zobrazení h:

1. **Definice a obor:** Pokud $x \notin A^*$, pak speciálně $x \notin A_0$, takže $x \in g[B]$. Protože g je prosté, existuje k němu právě jeden vzor $g^{-1}(x) \in B$.
2. **Injektivita (prostota):** Restrikce f na A^* a g^{-1} na $A \setminus A^*$ jsou prosté. Dále platí $f[A^*] \cap g^{-1}[A \setminus A^*] = \emptyset$, obraz z obou větví se nepřekrývá.
3. **Surjektivita (na):** Každý prvek $y \in B$ má svůj vzor v A. Buď $g(y) \in A^*$, pak z konstrukce existuje vzor přes definiční větev f, anebo $g(y) \notin A^*$, pak se vzorem stává samo $g(y)$ aplikací $g^{-1}(g(y)) = y$.

Zobrazení h je vzájemně jednoznačné (bijekce), existuje tedy relace $|A| =_c |B|$.

Cantorova věta o $|\mathbb{R}|$

$|\omega| <_c |\mathbb{R}|$
Množina $\mathbb{R}$ je **nespočetná**.

Hypotéza kontinua (CH)

Neexistuje $A \subset \mathbb{R}$ t.ž. $|\omega| <_c |A| <_c |\mathbb{R}|$.
Gödel (1940): CH je konzistentní s ZFC.
Cohen (1963): ¬CH je konzistentní s ZFC.
$\Rightarrow$ CH je **nezávislá** na ZFC!

5. Axiom výběru

5.1 Axiom výběru (AC)

Axiom výběru

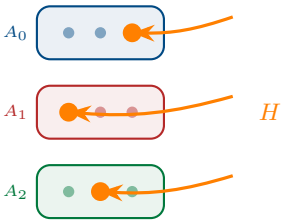
Pro každou kolekci $\mathcal{C}$ neprázdných množin existuje **výběrová funkce**

$$H : \mathcal{C} \to \bigcup \mathcal{C} \quad \text{taková, že} \quad \forall A \in \mathcal{C} : H(A) \in A.$$

Opakování: Sjednocení množiny a indexovaný systém množin

- **Sjednocení množiny (systému) $\mathcal{C}$:** Značíme $\bigcup \mathcal{C}$. Jedná se o množinu všech prvků x, pro které existuje alespoň jedna množina $A \in \mathcal{C}$ taková, že $x \in A$. Tedy se „slijí“ všechny prvky všech množin z kolekce do jednoho celku. Z této široké výsledné sbírky následně vybírá funkce H své hodnoty.
- **Indexovaný systém množin:** Místo libovolné „bezejmenné“ kolekce $\mathcal{C}$ můžeme mít sadu množin, kde každá dostala svůj „štítek“ z tzv. indexové množiny I. Matematicky se jedná o funkci F s definičním oborem $\mathrm{dom}(F) = I$, u níž funkční hodnotu $F(i)$ označíme jednoduše A_i. Celý systém se pak značí $\langle A_i : i \in I \rangle$ nebo $\{A_i\}_{i \in I}$.

Formulace pro indexované systémy:
Pro $\langle A_i : i \in I \rangle$ s $A_i \neq \emptyset$ existuje $\langle x_i : i \in I \rangle$ t.ž. $\forall i \in I : x_i \in A_i$.

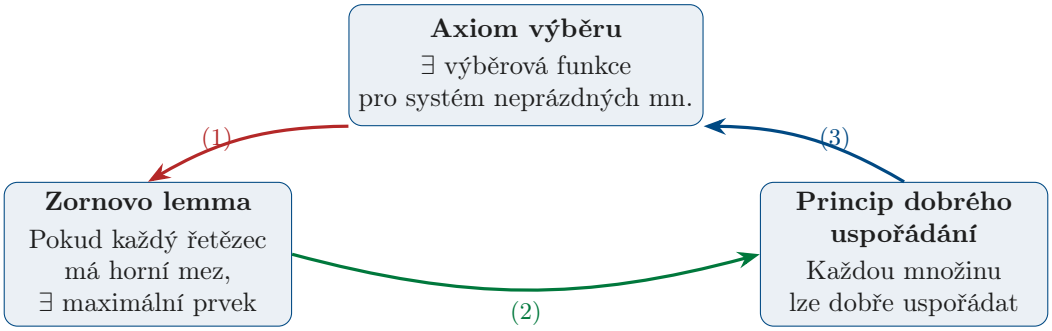


Historická poznámka:

- Formuloval Ernst Zermelo (1904).
- Gödel (1940): AC je konzistentní s ZF.
- Cohen (1963): ¬AC je konzistentní s ZF.

$\Rightarrow$ AC je **nezávislý** na ZF.

5.2 Ekvivalence AC, Zornova lemmatu a WOP



Tato tři tvrzení jsou v rámci ZF ekvivalentní.

5.3 Důsledky axiomu výběru

Zornovo lemma – definice

Řetězec: Podmnožina C částečně uspořádané množiny P, v níž jsou libovolné dva prvky navzájem porovnatelné. Tedy pro všechna $x, y \in C$ platí buď $x \leq y$, nebo $y \leq x$. Zatímco samotná částečně uspořádaná množina může obsahovat neporovnatelné položky, tak na vybraném řetězci tvoří relace $\leq$ vždy tzv. *totální (lineární)* uspořádání – prvky v něm lze seřadit jasně za sebe „do řetězce“.

Horní mez: u je horní mezí $S \subseteq P$, pokud $\forall s \in S\colon s \leq u$.

Maximální prvek: m t.j. $\neg\exists x\colon m < x$.

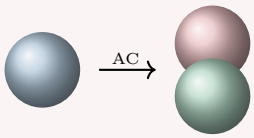
Aplikace: báze vekt. prostoru

Věta. Každý vektorový prostor má bázi.

Důkaz: Množina lineárně nezávislých podmnožin, uspořádaná inkluzí. Zornovo lemma $\Rightarrow \exists$ maximální lin. nezáv. množina = báze.

Banach–Tarského paradox

Kouli v $\mathbb{R}^3$ lze rozložit na konečně mnoho disjunktních částí, které lze rotacemi a translacemi složit ve **dvě** koule identické s původní!



Neměřitelné množiny — nelze fyzikálně realizovat.

Další důsledky AC

Tichonovova věta, existence ultrafiltrů, Hahn–Banachova věta.

6. Ordinální čísla

6.1 Definice a příklady ordinálních čísel

Ordinální číslo

α je **ordinální číslo** (ordinál), pokud:

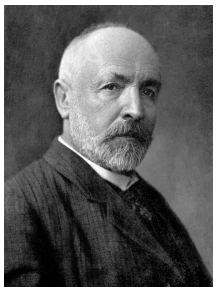
1. α je **tranzitivní množina** (pokud $x \in y \in \alpha$, pak $x \in \alpha$),
2. $(\alpha, \in)$ je **dobře uspořádaná** množina (kde $\in$ je relace $\in$ omezená na α).

Příklady netranzitivních množin (a tedy ne-ordinálů)

Aby byla množina ordinálním číslem, musí nutně splňovat vlastnost **tranzitivity**. Následující příklady ilustrují dobře uspořádané, leč netranzitivní množiny, které proto ordinálními čísly specifikovanými podle von Neumanna nejsou:

- **Konečná netranzitivní množina:** Mějme množinu $A = \{\{\emptyset\}\}$. Platí, že $\emptyset \in \{\emptyset\}$ a současně $\{\emptyset\} \in A$. Pokud by množina A byla tranzitivní, muselo by z definice vyplývat, že se každému prvku libovolného prvku z A dostane přímého členství v A, čili by platilo $\emptyset \in A$. Množina A ale obsahuje jako svůj naprosto jediný prvek množinu $\{\emptyset\}$, prázdná množina jako taková v ní prvkem není ($\emptyset \notin A$). Tranzitivita tak ihned selhává. Přestože je množina $(\{\{\emptyset\}\}, \in)$ triviálně dobře uspořádaná ve struktuře odpovídající ordinálu 1, přesně podle definice se o ordinální číslo nejedná.
- **Nekonečná netranzitivní množina:** Uvažujme množinu všech přirozených čísel bez nuly, $B = \omega \setminus \{0\} = \{1, 2, 3, \ldots\}$. Z předchozích definic víme, že číslo 1 ve své množinové reprezentaci odpovídá množině $\{0\}$. Kdykoliv nahlédneme na prvek $1 \in B$, zjevně zachytíme jeho prvek ve formě nuly, tedy $0 \in 1 \in B$. Kdyby B byla tranzitivní, musela by podle stejné logiky absorbovat samotnou nulu přímo jako svůj prvek ($0 \in B$). My jsme však číslo nula u množiny B úmyslně vyjmuli, $0 \notin B$. Obdobně tak i tato nekonečná a ostře dobře uspořádaná množina selhává na podmínce tranzitivity.

Historická poznámka: John von Neumann a pojem ordinálního čísla

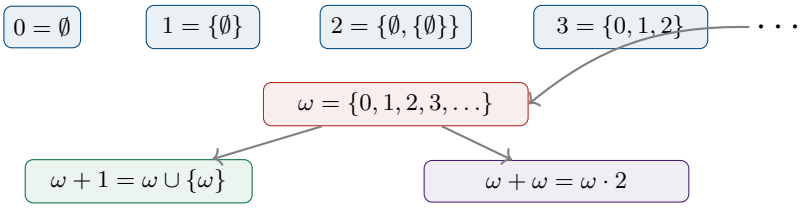


Georg Cantor
(1845–1918)

John von Neumann
(1903–1957)

Pojem ordinálního čísla pochází už od vzestupu teorie množin u Georga Cantora, který jej definoval a používal značně abstraktně – zprostředkovaně přes třídy izomorfních či strukturově plně korespondujících, dobře uspořádaných množin, které sdílely stejný „typ uspořádání“. Takto volný postup ovšem hrozil po vytvoření přísných rigidních axiomatických systémů jistým defektem. Obrovské „sbírky“ všech izomorfních množin totiž z definice nedokázaly složit relevantní platnou množinu (projevily se jako masivní vlastní třída tvořící paradox).
Klíčový koncepční zlom v nahlížení k exaktní a mnohem bezpečnější definici vykonal teprve roku 1923, zhruba ve svých dvaceti letech, proslulý maďarsko-americký matematický fenomén **John von Neumann**. Jeho revoluční řešení spočívalo ve fundamentální myšlence vymanit se z oné obrovské abstraktní „Cantorovy“ sbírky reprezentací spolehlivou volbou jednoho **kanonického zástupce**, jednoho striktně navrženého množinového modelu takového typu uspořádání, na který by se soustředil matematický aparát.

Jeho postup byl oslnivě úsporný: každý budoucí ordinál velmi účinně nadefinoval vyloženě *jako množinu všech ordinálů, které mu ostře předcházejí* ($\alpha = \{\beta : \beta < \alpha\}$). Z této nesmírně elegantní samonosné úvahy poté samočinně vyplynuly všechny požadované vlastnosti ordinálu. Především zaručovala, že všechny její obdržené prvky se vždy stávají zároveň automaticky i jejími podmnožinami (viz nutná vlastnost tranzitivity), a napříč všemi těmito posbíranými prvky dominuje zcela jednoznačné uspořádání čistou relací náležení ($\in$). Dnešní teorie množin a axiomatizovaná matematika od této úspěšné vize většinou neuhýbá a obvyklé moderní ordinály tudíž precizněji zveme **von Neumannovými ordinály**.
Odkaz von Neumanna tímto přínosem rozhodně nehasne. Následně o nedlouho později to byl s definitivní přesností opět on, kdo ve stejných sférách poprvé exaktně deklaroval jasný rozdíl mezi relativně malými ovladatelnými *množinami* (z nichž lze konstruovat další množiny) a příliš velikými **vlastními třídami** (gigantickými netestovatelnými komunitami stojícími mimo obavy z formálních paradoxů). Ten posléze podnítil odlišné vnímání matematické logiky, vybudování a formulaci plně striktní teorie nazývanou dnes jako **NBG** (Von Neumann–Bernays–Gödel axiomatický systém). Ta vyrostla v hrdou, plně konzervativní alternativu, mnohdy se obohacující a prostupující se se světovým standardem představovaným systémem ZFC.



Ověření: $3 = \{0, 1, 2\}$ je ordinál: (1) Tranzitivita: $0 \in 1 \in 3$, $0 \in 3$ ✓; $1 \in 2 \in 3$, $1 \in 3$ ✓. (2) Dobré uspořádání relací $\in$: ✓.

6.2 Vlastnosti ordinálních čísel

Klíčové vlastnosti

1. Každý prvek ordinálu je ordinál.
2. **Trichotomie:** Pro ordinály α, β:
$$\alpha \in \beta \ \vee \ \alpha = \beta \ \vee \ \beta \in \alpha.$$
3. Každá množina ordinálů je dobře uspořádaná relací $\in$.
4. $\alpha \notin \alpha$ pro každý ordinál.

Typologie ordinálů

Každý ordinál spadá právě do jedné z těchto

- **Nula:** $0 = \emptyset$. Odpovídá prázdné množině, nemá žádné prvky.
- **Následnický ordinál:** Existuje ordinál β takový, že $\alpha = \beta \cup \{\beta\}$ (značíme ho $\beta{+}1$ nebo $S(\beta)$). Ordinál α má tedy svého bezprostředního předchůdce β.
- **Limitní ordinál:** $\alpha \neq 0$ a α není následnický ordinál. Nemá bezprostředního předchůdce a platí pro něj $\alpha = \bigcup \alpha$ (je sjednocením všech svých prvků, tedy všech ostře menších ordinálů).

Příklady limitních ordinálů

- $\omega = \{0, 1, 2, \ldots\}$
- $\omega + \omega$
- $\omega \cdot \omega$
- ε_0 (nejmenší α t.ž. $\omega^\alpha = \alpha$)

Věta: Vlastnosti ordinálu ω

Množina ω je nejmenší nekonečné ordinální číslo a zároveň je to nejmenší limitní ordinál.

Důkaz:

- ω **je ordinál:** Prvky ω jsou přirozená čísla, množina ω je tranzitivní a dobře uspořádaná relací $\in$. Relace $\in$ na ω se shoduje s běžným uspořádáním $<$, takže ω je zjevně nekonečná.
- **Minimalita mezi nekonečnými:** Nechť α je nekonečný ordinál a předpokládejme pro spor $\alpha < \omega$ (tj. $\alpha \in \omega$). Všechny prvky ω jsou však konečná přirozená čísla, α by tedy muselo být konečné, což je spor s předpokladem.
- ω **je limitní ordinál:**
  - Jistě $\omega \neq 0$ (obsahuje 0).
  - Nechť pro spor ω je následnický ordinál, tj. $\omega = \beta + 1$. Pak ale $\beta \in \omega$, což znamená, že β je nějaké přirozené číslo n. Následník přirozeného čísla $(n + 1)$ je vždy přirozené (konečné) číslo, což je ve sporu s nekonečností ω.

6.3 Existence nespočetného ordinálu

Ačkoliv je ω nejmenší nekonečný ordinál, proces tvorby ordinálů jím zdaleka nekončí. Můžeme tvořit další spočetné ordinály, jako např. $\omega + 1$, $\omega + \omega$, ω^ω atd. Dokonce všechny ordinály, které můžeme z ω sestrojit běžnými aritmetickými operacemi, zůstávají vždy spočetnými množinami.

Je přirozenou otázkou, zda vůbec existuje i **nespočetný ordinál**. Podle **Hartogsovy věty** (a axiomu nahrazení) platí, že ke každé množině existuje ordinál, jenž se do ní nedá prostě zobrazit. Položíme-li jako základní množinu ω, dostáváme existenci ordinálu ω_1 (často značeného jako první nespočetný kardinál $\aleph_1$), který je již **nespočetný**.

Z konstrukce vyplývá, že ω_1 je množinou *všech spočetných ordinálů*. Nachází se "velmi daleko za ω"– nelze k němu nikdy dospět pouhým postupným přičítáním, násobením či umocňováním spočetných ordinálů (každé takové sjednocení spočetného množství spočetných ordinálů je totiž stále spočetné). Je z nich tedy "nedosažitelný".

6.4 Ordinální aritmetika

Věta (Princip transfinitní indukce)

Nechť $(W, \preceq)$ je dobře uspořádaná množina a P je nějaká vlastnost (formule). Pokud platí indukční krok:

$$\text{Pro každé } u \in W: \quad \big(\forall x \in W : x \prec u \implies P(x)\big) \implies P(u),$$

pak vlastnost $P(x)$ platí pro všechny prvky množiny W.

Strukturovaný důkaz věty: Důkaz provedeme sporem a zásadním způsobem využijeme jedinou klíčovou vlastnost dobrého uspořádání.

1. Konstrukce množiny protipříkladů: Definujme množinu S těch prvků v W, pro které vlastnost P **neplatí**. Formálně $S = \{u \in W \mid \neg P(u)\}$.

2. Předpoklad pro spor: Předpokládáme, že závěr věty neplatí, a tedy vlastnost P selhává alespoň pro jeden prvek tzn. množina chyb S je **neprázdná** ($S \neq \emptyset$).

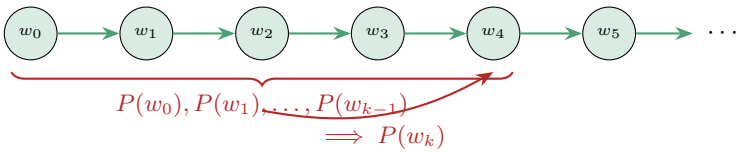
3. Definice dobrého uspořádání nám pro libovolnou neprázdnou podmnožinu $S \subseteq W$ garantuje existenci **nejmenšího prvku**. Nalezněme onen nejmenší prvek, označme jej $m \in S$ (platí, že $\neg P(m)$).

4. Jelikož je m absolutně nejmenší ve skupině S, pak všechny ostře menší prvky ($x \prec m$) do množiny selhání S zjevně patřit nemohou. Tedy pro všechna taková elementární $x \prec m$ tvrzení $P(x)$ zaručeně platí. To je přesně náš splněný předpoklad.

5. Jestliže mají podmínku P platnou všechny prvky ostře menší než m, z indukční premisy (která je daná) okamžitě usuzujeme a vynucujeme přímou platnost vlastnosti pro prvek samotný, tudíž $\implies P(m)$.

6. Tím však dospíváme ke sporu: víme ovšem (bod 3), že $m \in S$, neboli $\neg P(m)$, ale z indukčního kroku jsme vázáni nabýt zjištěním závěru $P(m)$. Protipříklady tudíž nemohou existovat, $S = \emptyset$. Důkaz je ukončen. □

Pozn.: Důkaz je analogický principu silné matematické indukce probíhající na ω, ale obejde se bez umělého budování základu indukce. Pro nejmenší absolutní prvek $w_0 \in W$, se předpoklad $\forall x \prec w_0 : P(x)$ pochopitelně splní vacuously (prázdně).



Věta (Princip transfinitní indukce pro ordinály – alternativní formulace)

Jelikož se třída všech ordinálů rozpadá na nulu, následníky a limitní ordinály, lze předchozí princip velmi často a prakticky přeformulovat to tří konkrétních kroků. Nechť $P(\alpha)$ je vlastnost formálně definovaná pro ordinální čísla. Pokud platí:

1. **Základní krok:** Platí $P(0)$.
2. **Následnický krok:** Pro každý ordinál α platí $P(\alpha) \implies P(\alpha + 1)$.
3. **Limitní krok:** Pro každý limitní ordinál λ platí $\big(\forall \alpha < \lambda \colon P(\alpha)\big) \implies P(\lambda)$.

Pak vlastnost $P(\alpha)$ platí pro všechna ordinální čísla α.

Důkaz věty (sporem přes existenci nejmenšího protipříkladu):

1. Předpokládejme, že závěr věty neplatí. Pak existují nějaké ordinály, pro které vlastnost P selhává. Množina všech takových selhání $S = \{\alpha \in \mathrm{On} \mid \neg P(\alpha)\}$ je tedy neprázdná.

2. Vzhledem k tomu, že ordinální čísla jsou dobře uspořádána relací $\in$, musí ve třídě S existovat její **nejmenší prvek**, označme jej μ.

3. Z absolutní minimality μ ihned vyplývá, že pro všechny ostře menší ordinály $\gamma < \mu$ sledovaná vlastnost P platit musí: $\forall \gamma < \mu \colon P(\gamma)$.

4. Nyní ukažme spor pro všechny tři možné typologické stavy, jakého druhu by ordinál μ mohl vůbec být:

- Je-li $\mu = 0$: Podle prvního předpokladu naší věty víme, že $P(0)$ platí. Avšak $\mu \in S$ říká, že pro μ daná vlastnost neplatí. Spor.
- Je-li μ **následnický ordinál**, tvaru $\mu = \beta+1$: Jelikož $\beta < \mu$, víme, že pro β už vlastnost pevně platí (tedy $P(\beta)$). Podle druhého předpokladu ale $\implies P(\beta+1)$. Tudíž by musela platit $P(\mu)$, což je opět spor s $\mu \in S$.
- Je-li μ **limitní ordinál**: Z bodu 3 bezpečně víme, že pro všechna $\gamma < \mu$ podmínka platí. Třetí předpoklad naší věty však říká, že v takovém případě už musí platnost přeskočit i na samotný limitní ordinál μ. Tudíž by mělo platit $P(\mu)$, třetí a konečný spor.

5. Jelikož μ musí bezesporu spadat do právě jedné z těchto tří kategorií a každá vede k jasnému sporu, ukazuje se, že neprázdnost skupiny omylů S byl chybný předpoklad. Tím je dokázáno, že platí $P(\alpha)$ pro všechna ordinální čísla. □

Sčítání ordinálů (transfinitní rekurze)

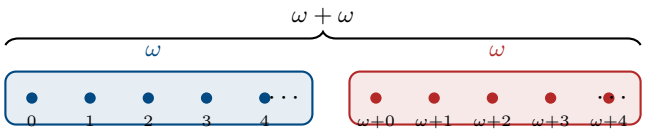
$$\begin{aligned} \alpha + 0 &= \alpha, \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1, \\ \alpha + \delta &= \sup\{\alpha + \gamma : \gamma < \delta\} \quad \text{pro limitní } \delta. \end{aligned}$$

Poznámka k existenci supréma ordinálů: V definici pro limitní ordinál δ se objevil operátor sup. V uspořádání ordinálních čísel tvoří každá množina ordinálů (zde konkrétně množina všech částečných součtů $X = \{\alpha + \gamma \mid \gamma < \delta\}$) množinu dobře uspořádanou relací $\in$. Každá taková *množina* ordinálů má nad sebou vždy nějakou horní závoru, a díky dobrému uspořádání i závoru *nejmenší* – své supremum. Formálně je toto suprémum jednoduše sjednocením množiny X, tedy $\sup X = \bigcup X$. Tím je zaručeno, že výraz $\sup\{\alpha + \gamma : \gamma < \delta\}$ dává vždy jednoznačný smysl, a tedy hodnota $\alpha + \delta$ pro limitní δ bezpečně a deterministicky existuje (a navíc je to opět ordinální číslo).

Zřetězení dobře uspořádaných množin (geometrická definice)

Nechť $(A, <_A)$ a $(B, <_B)$ jsou *disjunktní* dobře uspořádané množiny, přičemž typ množiny A je α a typ množiny B je β. Pak součet $\alpha + \beta$ je ordinální typ množiny $A \cup B$, na níž definujeme uspořádání $<_{A\cup B}$ tak, že **všechny prvky z A předcházejí všem prvkům z B**. Formálně:

$$x <_{A\cup B} y \iff (x, y \in A \wedge x <_A y) \vee (x, y \in B \wedge x <_B y) \vee (x \in A \wedge y \in B).$$



Pozor: Ordinální sčítání není komutativní!

Ukažme podrobný důkaz nerovnosti $1+\omega \neq \omega+1$ pomocí zřetězení dobře uspořádaných množin:

- **Výpočet $1 + \omega$:** Nechť $A = \{*\}$ je jednoprvková množina (typ 1) a $B = \{0, 1, 2, \dots\}$ (typ ω). Zřetězením, kde prvky A předcházejí prvkům z B, získáme uspořádání: $* <_{A\cup B} 0 <_{A\cup B} 1 <_{A\cup B} 2 \dots$ Výsledná množina je ostře rostoucí nekonečná posloupnost bez největšího prvku. Lze ji zjevně vzájemně jednoznačně a uspořádání zachovávajícím způsobem (izomorfně) zobrazit na ω (kde $*$ přejde na 0, 0 na 1, 1 na 2 atd.). Tedy $1 + \omega = \omega$.
- **Výpočet $\omega + 1$:** Nyní naopak prvky B (typ ω) předcházejí prvku z A (typ 1). Získáme uspořádání: $0 <_{B\cup A} 1 <_{B\cup A} 2 \cdots <_{B\cup A} *$ Tato uspořádaná množina má **největší prvek** $(*)$. Ordinál ω však žádný největší prvek nemá. Proto typ této množiny nemůže být ω. Je to ostře větší (následnický) ordinál.

Odtud je okamžitě vidět, že $1 + \omega = \omega \neq \omega + 1$.

Násobení ordinálů

Pomocí transfinitní rekurze definujeme $\alpha \cdot \beta$:

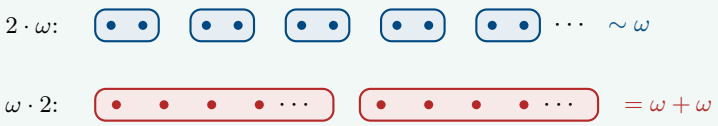
$$\begin{aligned} \alpha \cdot 0 &= 0, \\ \alpha \cdot (\beta + 1) &= (\alpha \cdot \beta) + \alpha, \\ \alpha \cdot \delta &= \sup\{\alpha \cdot \gamma : \gamma < \delta\} \quad \text{pro limitní } \delta. \end{aligned}$$

Geometrická interpretace násobení

Ordinální součin $\alpha \cdot \beta$ odpovídá **anti-lexikografickému uspořádání** na kartézském součinu množin typů α a β. Neformálně řečeno: vezmeme dobře uspořádanou množinu typu β a každý její prvek „nahradíme“ celou uspořádanou množinou typu α. Tedy druhá složka určuje pomyslný „makro-blok“ a první složka určuje izolovanou pozici uvnitř tohoto bloku.

Nekomutativita násobení: $2 \cdot \omega \neq \omega \cdot 2$

- $2 \cdot \omega$**:** Posloupnost délky ω, kde každý prvek je nahrazen dvěma prvky (blokem délky 2). Slitím konečných teček v nekonečné posloupnosti je výsledkem standardní ω.
- $\omega \cdot 2$**:** Posloupnost délky 2 (dva bloky), z nichž každý je vyplněn nekonečnou kapičkou prvků typu ω. Výsledkem je uspořádání ekvivalentní množině $\omega + \omega$.



Věta: Distributivní zákony pro ordinály

Pro libovolná ordinální čísla α, β, γ platí **levý distributivní zákon**:

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

Důkaz (transfinitní indukcí přes γ):

- **Pro** $\gamma = 0$**:** $\alpha \cdot (\beta + 0) = \alpha \cdot \beta = \alpha \cdot \beta + 0 = \alpha \cdot \beta + \alpha \cdot 0$.
- **Pro ne-limitní krok (následník)** $\gamma+1$**:** Nechť rovnost platí pro γ. Pak $\alpha \cdot (\beta + (\gamma + 1)) = \alpha \cdot ((\beta + \gamma) + 1)$. Dle definice násobení je to $\alpha \cdot (\beta + \gamma) + \alpha$. Z indukčního předpokladu nahradíme první člen a získáme $(\alpha \cdot \beta + \alpha \cdot \gamma) + \alpha$, což je díky asociativitě sčítání $\alpha \cdot \beta + (\alpha \cdot \gamma + \alpha) = \alpha \cdot \beta + \alpha \cdot (\gamma + 1)$.
- **Pro limitní** γ**:** Rovnost plyne z vlastností supréma při pevném $\alpha \cdot \beta$ a ze spojitosti operací sčítání a násobení ve druhé složce.

Oproti tomu **pravý distributivní zákon obecně NEPLATÍ**. Výše uvedený případ $2 \cdot \omega = (1 + 1) \cdot \omega = \omega$ se zjevně nerovná $1 \cdot \omega + 1 \cdot \omega = \omega + \omega$.

Důkaz identity $\omega \cdot 2 = \omega + \omega$

Toto tvrzení lze velmi přirozeně dokázat jak z definice, s využitím zavedeného distributivního zákona, tak geometricky:

- **Analyticky přes levou distributivitu:** Jistě platí $2 = 1 + 1$. Substitucí do zadání obdržíme $\omega \cdot (1 + 1)$. Protože násobení *je distributivní zleva k součtu* na množině ordinálů, můžeme závorku bez obav algoritmicky roznásobit: $\omega \cdot 1 + \omega \cdot 1$. Nakolik $\omega \cdot 1 = \omega$, dostáváme ihned $\omega \cdot 2 = \omega + \omega$. K stejnému závěru bychom došli i prostou aplikací pravidla pro následníka v definici rekurze sčítání/násobení.

▶ **Z geometrické interpretace:** Při součinu $\alpha \cdot \beta$ uvažujeme dobře uspořádanou množinu o délce (typu) β prvků a každý takový izolovaný prvek zevnitř „vyplníme“ či „nahradíme“ uspořádáním typu α. Uvažujeme-li náš problém $\omega \cdot 2$, potřebujeme dvouprvkovou množinu $\{0, 1\}$. Každý její prvek (nejprve index 0, poté za ním jdoucí index 1) vyměníme za celou kopii množiny prvků izomorfní množině ω. Získáme tím jasně první kopii ω a bezprostředně navazující i rovnocennou druhou kopii ω. Formálně toto přesně koresponduje se zřetězením typů, a typ je proto jednoznačně $\omega + \omega$.

Umocňování ordinálů

Pomocí transfinitní rekurze, pro pevné $\alpha > 0$, definujeme α^β:

$$\begin{aligned} \alpha^0 &= 1, \\ \alpha^{\beta+1} &= \alpha^\beta \cdot \alpha, \\ \alpha^\delta &= \sup\{\alpha^\gamma : \gamma < \delta\} \quad \text{pro limitní } \delta. \end{aligned}$$

7. Transfinitní rekurze

7.1 Princip transfinitní rekurze

Třídová funkce

Relaci (třídu) F nazveme **třídovou funkcí**, pokud splňuje podmínku jednoznačnosti: pro každé $x \in \mathrm{dom}(F)$ existuje právě jedno y takové, že $(x, y) \in F$. Tuto vlastnost často zapisujeme funkcionální formulí $\varphi(x, y)$, pro kterou platí $\forall x\, \exists!\, y\colon \varphi(x, y)$. Místo $\varphi(x, y)$ pak píšeme $F(x) = y$. Z definičního oboru i oboru hodnot takové „funkce“ mohou být vlastní třídy (např. třída On všech ordinálů).

Věta (Transfinitní rekurze)

Nechť $\varphi(x, y)$ je funkcionální formule (tj. $\forall g\, \exists!\, u\colon \varphi(g, u)$) a $(W, \preceq)$ je dobře uspořádaná množina. Pak existuje **jediná** funkce H s $\mathrm{dom}(H) = W$ taková, že pro každé $u \in W$:

$$\varphi(H \restriction_{s(u)},\ H(u)),$$

kde symbol $s(u) = \{x \in W \mid x \prec u\}$ označuje počáteční úsek množiny W určený prvkem u a $H \restriction_{s(u)}$ je zúžení (restrikce) funkce H na tento úsek.

Ekvivalentně: existuje jediné H takové, že $H(u) = F(H \restriction_{s(u)})$, kde F je třídová funkce definovaná formulí φ. To znamená, že hodnota funkce H v bodě u je jednoznačně určena pravidlem F aplikovaným na dosavadní průběh funkce H (na jejích hodnotách pro všechna $x \prec u$).

Poznámka k Větě o transfinitní rekurzi. Tato věta poskytuje korektní a formálně podložený způsob definice funkcí na dobře uspořádaných množinách, typicky na ordinálních číslech. Zatímco klasická rekurze zkoumá definici hodnoty $f(n + 1)$ ze známé hodnoty $f(n)$, transfinitní rekurze definuje $H(u)$ na základě *celé historie* (tj. všech prvků $x \prec u$) skryté ve funkci $H \restriction_{s(u)}$. Díky zúžení $H \restriction_{s(u)}$ má funkce F přístup ke všem dřívějším hodnotám a víme tak jednoznačně zkonstruovat další hodnotu $H(u)$.

Souvislost s Větou o rekurzi na přirozených číslech. Klasická věta o rekurzi (na množině přirozených čísel ω) je pouze velmi speciálním případem obecné věty o transfinitní rekurzi. Připomeňme si její znění: pro daný výchozí prvek $a \in A$ a generující funkci $g\colon A \to A$ existuje jediná posloupnost $f\colon \omega \to A$ splňující $f(0) = a$ a $f(n + 1) = g(f(n))$.

Aplikujeme-li Větu o transfinitní rekurzi na dobře uspořádanou množinu $(\omega, \in)$, potřebujeme de-

finovat vhodnou třídovou funkci F, pomocí níž bude rekurzivní sekvence generována. V případě relace náležení $\in$ na přirozených číslech určuje počáteční úsek $s(n)$ přesně množinu všech menších přirozených čísel, což je ve von Neumannově definici zjevně rovno samotnému číslu n. To znamená, že zúžení (restrikce) do tohoto počátečního úseku, funkce $f\restriction_{s(n)}$, je prostě zobrazení z s definičním oborem $\mathrm{dom}(z) = n$, zachycující hodnoty pro vstupy $0, 1, \ldots, n-1$.

Klíčovou příslušnou třídovou (zde pouze množinovou) funkci $F(z)$ pak stačí sestrojit jako předpis zpracovávající toto zúžení z:

- Pro „prázdnou historii“ (tj. pokud $z = \emptyset$) položíme $F(\emptyset) = a$. V praxi to znamená, že pro první prvek ω, kterým je 0 $(= \emptyset)$, platí $s(0) = \emptyset$. Dosazením do věty obdržíme $f(0) = F(f\restriction_{\emptyset}) = F(\emptyset) = a$.
- Pro „neprázdnou historii“ končící nějakým krokem, tedy pokud z má jako svůj definiční obor libovolné přirozené číslo obohacené o nulu (jakékoliv $n+1 = n \cup \{n\}$), tzn. největším prvkem definičního oboru v čase volání je číslo n: „podíváme se“ na naprosto poslední vygenerovanou hodnotu, tedy hodnotu argumentu modifikátoru v bodě n, zapsanou v $z(n)$, a tu s danou funkcí zprostředkujeme dál vložením předpisu $F(z) = g(z(n))$. Dosazením to pro transfinitní rekurzi znamená aplikaci pro bod $n+1$, kdy $s(n+1) = n+1$, a počítá se $f(n+1) = F(f\restriction_{n+1}) = g(f(n))$.
- Pro všechny formálně nevyčerpané případy argumentu $z \notin \omega$ definujeme $F(z) = \emptyset$. Kvůli specifikám ω, skládajícího se jedině ze zrodu na principu $n \cup \{n\}$ a elementu izolovaného počátku 0, však k tomuto vůbec nenastane uplatnění.

Díky tvrzení existence a jednoznačnosti f předpovídané Větou o transfinitní rekurzi s touto konkrétní funkcí F tak okamžitě dostáváme jednoznačnou existenci oné rekurzivně zadané posloupnosti na přirozených číslech. Zásadní rozdíl je tedy „jenom“ v tom, že pro klasickou rekurzi zkonstruované třídové funkci F postačuje odečítat a rekurzivně reagovat pouze na finální prvek prozatímního postupu ze sekvence $H(n)$, přičemž ale čistá transfinitní rekurze v plné obecnosti může aplikovat operace přes úhrnem všech doprovodných dosud definovaných prvků a zpracovat přirozeně jak izolované stavy tvořící následníky, tak i neizolované takzvané stavy spojené s limitními ordinály.

7.2 Úvod k Von Neumannovu univerzu množin

Než přistoupíme k formální definici univerza fundovaných množin (často nazývaného jako von Neumannovo univerzum), je namístě si ujasnit jeho hlubší smysl jak pro následující partie přednášky, tak pro celou teorii množin. Z historického pohledu bylo pro matematiky klíčové nalézt přirozený model, který by ztělesňoval všechny „rozumné“ množiny a přitom se vyhnul paradoxům (např. Russellovu paradoxu „množiny všech množin, které neobsahují samy sebe“).

Základní myšlenka von Neumannova univerza spočívá v **kumulativní hierarchii**. Namísto abychom uvažovali o množinách jako o entitách, které prostě odněkud „jsou“, představujeme si, že množiny „vznikají“ (jsou konstruovány) postupně v krocích. Nejedná se o proces v čase, ale v uspořádání, které reprezentují ordinální čísla:

- Na samém „počátku“ nemáme nic. První platnou strukturou ze „všeho ničeho“ je zjevně prázdná množina $\emptyset$. Ta tvoří počáteční "nulté"patro.
- Jak postoupit do dalšího patra? Pokud už máme k dispozici nějakou zásobu množin vytvořených v předchozích krocích, můžeme nové množiny vytvořit tak, že z dosud existujících prvků tvoříme libovolné podsoučiny. Za tento krok logicky odpovídá **operace potenční množiny** (tvorba všech podmnožin).
- Protože kroků je transfinitně mnoho (probíhají přes všechny ordinály), občas narazíme na „limitní“ krok (např. po nekonečně mnoha krocích tvaru $0, 1, 2, \ldots$ v kroku ω). V tomto patře

k žádné nové generaci skrze potenci nedochází, nýbrž zkrátka **sjednotíme** všechna dosavadní patra do jedné množiny.

Samotná formální definice této hierarchie pater (označovaných V_α pro libovolný ordinál α) je navíc učebnicovým využitím **Věty o transfinitní rekurzi** v praxi. Ordinály tvoří dobře uspořádanou třídu a my definujeme přiřazení $\alpha \mapsto V_\alpha$ přesně na základě předchozích hodnot.

Význam tohoto pojetí v teorii množin tkví v takzvaném **Axiomu fundovanosti** (či regularity). Ten exaktně postuluje, že *všechny* myslitelné (a v rámci teorie korektní) množiny lze vygenerovat tímto postupem. Jinými slovy, celá množinová matematika padne bezezbytku do tohoto kumulativního trychtýře. Tím axiomaticky zakazujeme jakékoliv neintuitivní patologické entity jako $x \in x$ (množina nesmí být prvkem sebe sama) a tvoříme tím standardní bezpečný západotvor pro Zermelo-Fraenkelovu teorii množin s axiomem výběru (ZFC). Cokoli z tohoto stromu vypadne či v něm nevznikne, z definice jednoduše systémem není chápáno za korektní množinu.

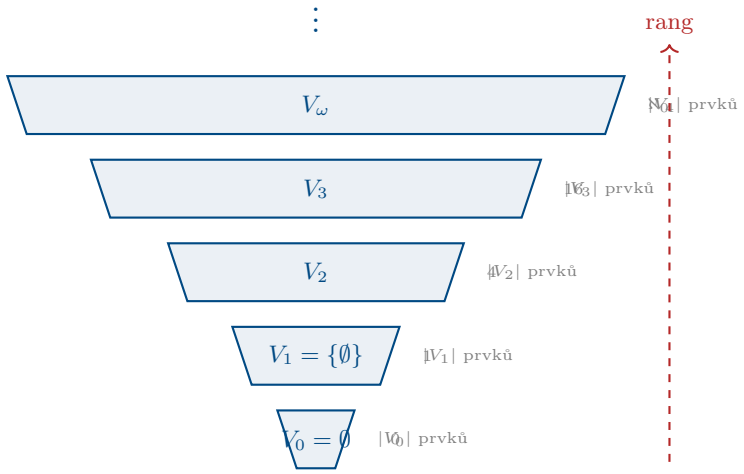
Univerzum fundovaných množin WF

Kumulativní hierarchie: $V_0 = \emptyset, \quad V_{\alpha+1} = \mathcal{P}(V_\alpha), \quad V_\lambda = \bigcup_{\beta<\lambda} V_\beta$ pro limitní λ.

$$\mathsf{WF} = V = \bigcup_{\alpha \in \mathrm{On}} V_\alpha.$$

Axiom fundovanosti $\iff$ každá množina patří do WF.
Rang: $\mathrm{rank}(x) = \bigcup\{\mathrm{rank}(y) + 1 : y \in x\}$.

7.3 Von Neumannova kumulativní hierarchie



8. Kardinální čísla

8.1 Kardinální čísla

Kardinální číslo (von Neumann)

Kardinál κ je ordinální číslo takové, že pro žádné $\beta \in \kappa$ neexistuje bijekce $f : \kappa \to \beta$. *Kardinalita je „nejmenší ordinál se stejnou mohutností".*

Kardinalita množiny

Pro množinu A: $|A|$ je nejmenší ordinál κ t.ž. existuje bijekce $f : A \to \kappa$. *(Existence takového κ vyžaduje axiom výběru.)*

Věta

1. Každé přirozené číslo $n \in \omega$ je kardinální číslo.
2. ω je kardinální číslo: $\aleph_0 = \omega$.
3. Každý nekonečný kardinál je **limitní ordinál**.

$\aleph_1$ a 2^κ

$\aleph_1$ je nejmenší nekonečný kardinál větší než $\aleph_0$.
$2^\kappa := |\mathcal{P}(\kappa)|$ (mohutnost potenční množiny).
Hypotéza kontinua: $2^{\aleph_0} = \aleph_1$.

8.2 Kardinální aritmetika

Operace s kardinály

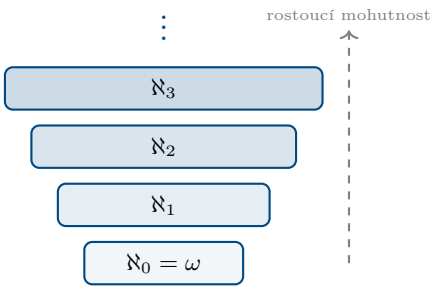
Pro kardinální čísla δ, κ:

$$\delta + \kappa := |(\{0\} \times \delta) \cup (\{1\} \times \kappa)|, \qquad \text{(disjunktní sjednocení)}$$
$$\delta \cdot \kappa := |\delta \times \kappa|.$$

Vlastnosti (pro nekonečné kardinály)

Pokud $\kappa \geq \aleph_0$:

- $\kappa + \kappa = \kappa$
- $\kappa \cdot \kappa = \kappa$
- $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$ pro nekonečné κ, λ.



9. Nezávislost hypotézy kontinua a limity ZFC

Hypotéza kontinua (CH)

Hypotéza kontinua, kterou v roce 1878 vyslovil Georg Cantor, tvrdí, že neexistuje žádná množina, jejíž mohutnost by ležela ostře mezi mohutností přirozených čísel ($\aleph_0$) a mohutností reálných čísel ($2^{\aleph_0}$). Matematicky: $2^{\aleph_0} = \aleph_1$. Byla prvním z 23 Hilbertových problémů (1900). Dlouhá desetiletí nikdo neuměl hypotézu dokázat ani vyvrátit. Dnes již víme, že CH je se standardními axiomy ZFC takzvaně **nezávislá** – nelze z nich analyticky odvodit její platnost ani její negaci.

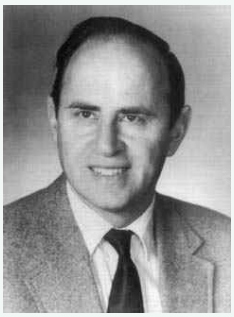
Klíčoví matematici a jejich role

Georg Cantor
(1845–1918)

Role: Zakladatel teorie množin. Vyslovil samotnou Hypotézu kontinua a zavedl značení systémem alefů pro nekonečné kardinály.
Zajímavost: Cantor po celou dobu obhajoval reálnou a absolutní povahu nekonečna dosti horlivým způsobem, dokonce věřil, že mu teorii množin sdělil přímo Bůh. Čelil drtivému odporu tehdejších matematiků v čele s Leopoldem Kroneckerem a na sklonku života trpěl opakovanými hlubokými depresemi.

Kurt Gödel
(1906–1978)

Role: V roce 1940 dokázal, že přidáním Hypotézy kontinua k axiomům ZFC nevznikne žádný spor. K tomu účelu vymyslel tzv. třídu konstruovatelných množin (označovanou L). Učinil první nutný úkon k nezávislosti – prokázal tzn. „částečnou bezespornost“ CH.
Zajímavost: Svými větami o neúplnosti navždy naboural vizi axiomatické matematiky. V osobním životě byl dobrým přítelem A. Einsteina. Později propadal extrémní paranoie, neustále se domníval, že je trávován. Jedl pouze jídlo, které mu osobně připravila a ochutnala jeho žena. Jakmile byla žena dočasně hospitalizována v nemocnici, Gödel skutečně úmyslně přes veškerou péči ošetřovatelů vyhladověl k smrti ze samotného strachu.



Paul Cohen
(1934–2007)

Role: V roce 1963 završil boj o CH tím, že sestrojil exaktní důkaz **nezávislosti CH**. K ZFC přidal platnou negaci CH pomocí zbrusu nové přelomové metody zvané **forcing**. Tím bylo završeno poznání, že CH není ani dokazatelná, ani vyvratitelná.
Zajímavost: Za zásadní a neuvěřitelnou metodu forcingu a vyřešení neřešitelného obdržel v roce 1966 Fieldsovu medaili (matematická obdoba Nobelovy ceny). Až dodnes tak navždy drží statut *historicky jediného* matematika, jenž toto ocenění kdy získal prvořadě za matematickou logiku.

Další velká nezdokazatelná tvrzení a limity ZFC

Díky Cohenovu vynálezu forcingu se ukázalo obrovské množství dalších známých a fundamentálních problémů jako naprosto nezávislých na ZFC. Objevilo se velké téma: čím nahradit či případně obohatit ZFC?

- **Martinův axiom (MA):** Výrok ležící svým duchem kdesi „v půli cesty“ ke zmítnutí CH. Týká se částečných uspořádání a spočetných antřetězců (často se zkoumá ve verzi MA + ¬CH). Zajišťuje, že se množiny s ostře menší mohutností než kontinuum chovají topologicky de facto jako množiny nanejvýš spočetné.
- **Diamantový princip ($\diamondsuit$):** Velmi silný kombinatorický předpoklad postihující celou strukturu tzv. stacionárních množin a tvoření lokálních protipříkladů (jistý modifikátor $\aleph_1$). Zavedl ho Ronald Jensen, prokazatelně platí v Gödelově univerzu L. Diamant mj. implikuje negaci klasické **Suslinovy hypotézy (SH)** a implikuje i CH.
- **Existence velkých kardinálů:** Tvrzení v ZFC nedokazatelná, např. slabě či silně nepřípustné kardinály, měřitelné či Woodinovy kardinály. Umožňují existenci rozměrově tak obrovských množinových entit, že je vůbec nelze rekurzním systémem podloženým ordinály ze ZFC shromáždit. Tyto nové axiomy mají zásadní dopad v analýze v rámci tzv. projektivních množin a deskriptivní teorie „pěkných“ podmnožin reálné osy.

Děkuji za pozornost

Teorie množin — ZFC