MODEL ARITMETIKY CELÝCH NEZÁPORNÝCH ČÍSEL V TEÓRII MNOŽÍN

JURAJ ČINČURA

1. Axiomatický prístup k teórii množín

Intuitívny prístup k teórii množín, kde množina bola definovaná ako súhrn určitých vecí uvažovaný ako celok (určený napríklad nejakou vlastnosťou) viedol k rôznym paradoxom.

Známe sú napríklad tieto paradoxy:

1. Nech M je množina všetkých množín X, pre ktoré platí $X \notin X$. Potom platí $M \in M$ vtedy a len vtedy, ak $M \notin M$, a to je spor.

2. Nech M je množina všetkých prirodzených čísel k s nasledujúcou vlastnosťou: k sa nedá opísať slovenskou vetou, ktorá má menej ako 100 písmen. Zrejme $M \neq \emptyset$ (lebo $\mathbb{N} \setminus M$ je konečná) a preto má najmenší prvok n. Veta "n je najmenšie prirodzené číslo, ktoré sa dá opísať slovenskou vetou, ktorá má menej ako 100 písmen" opisuje n a má menej ako 100 písmen, pričom $n \in M$. Dostali sme spor.

To si vyžiadalo spresnenie jazyka teórie množín a spôsobu vytvárania množín a malo za následok axiomatizáciu teórie množín. V tomto texte stručne popíšeme Zermelov - Fraenkelov axiomatický systém teórie množín.

Základným pojmom tejto teórie je pojem množina.

Do jazyka teórie množín patria:

1. Písmená označujúce množiny: $A, B, C, \ldots, X, Y, Z, a, b, c, \ldots, x, y, z, \ldots$ (množinové premenné), symboly $\in$, $=$, logické symboly $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$, $\neg$, pomocné symboly $(,), \ldots$ ďalšie symboly $1, 2, 3, \ldots \emptyset, \ldots, \subseteq, \ldots, \{, \}, \ldots$.

2. Formuly teórie množín (FTM) definované nasledovne:

(a) Ak x, y sú množinové premenné, tak $(x \in y)$ a $(x = y)$ sú (atomické) FTM.

(b) Ak φ, ψ sú FTM a x je množinová premenná, tak aj $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftrightarrow \psi)$, $\forall_x \varphi$, $\exists_x \varphi$ sú tiež formuly teórie množín.

Príklady 1. 1. $\forall_x((x = y) \vee (x \in y))$ je FTM (s voľnou premennou y, x je viazaná premenná)

2. $\forall_x((x \in A) \Rightarrow (x \in B))$ je FTM, ktorú skrátene zapíšeme $A \subseteq B$.

3. $\exists_x$, a tiež $(x \vee y)$ nie sú FTM.

2. Axiómy teórie množín a niektoré ich dôsledky

I. Axióma o rovnosti množín

$\forall_A \forall_B((\forall_x((x \in A) \Leftrightarrow (x \in B)) \Leftrightarrow (A = B))$

II. Axióma o zjednotení množín

$\forall_S \exists_M \forall_x((x \in M) \Leftrightarrow \exists_A((A \in S) \wedge (x \in A)))$

III. Axióma o existencii dvojprvkovej množiny

$\forall_a \forall_b \exists_A \forall_x((x \in A) \Leftrightarrow ((x = a) \vee (x = b)))$

IV. Axióma o existencii prázdnej množiny

$\exists_x \forall_y \neg(y \in x)$

V. Axióma o existencii potenčnej množiny

$\forall_A \exists_B \forall_x ((x \in B) \Leftrightarrow (x \subseteq A))$

VI$_\varphi$. Zermelova schéma axióm separácie

Nech $\varphi(x)$ je formula teórie množín s jednou voľnou premennou x. Potom

$\forall_A \exists_B \forall_x ((x \in B) \Leftrightarrow ((x \in A) \wedge \varphi(x)))$

VII$_\varphi$. Schéma axióm substitúcie

Nech $\varphi(x, y)$ je formula teórie množín s dvoma voľnými premennými x, y. Potom

$(\forall_x \forall_y \forall_z (((\varphi(x, y) \wedge \varphi(x, z)) \Rightarrow (y = z)) \Rightarrow (\forall_A \exists_B \forall_u ((u \in B) \Leftrightarrow (\exists_v ((v \in A) \wedge \varphi(x, y)))))$

VIII. Axióma o existencii nekonečnej množiny

$\exists_H ((\emptyset \in H) \wedge (\forall_x ((x \in H) \Rightarrow ((x \cup \{x\}) \in H)))$

IX. Axióma výberu

$\forall_S ((\forall_A ((A \in S) \Rightarrow (A \neq \emptyset)) \wedge (\forall_B \forall_C ((B \in S) \wedge (C \in S) \wedge (B \neq C)) \Rightarrow$
$\Rightarrow (B \cap C = \emptyset)))) \Rightarrow (\exists_V \forall D ((D \in S) \Rightarrow (\exists_x (V \cap D = \{x\})))))$

V axiómach V, VIII a IX sme použili skrátené zápisy FTM (napr. $x \subseteq A$ a pod.) aby boli zrozumiteľnejšie. Obvyklé skrátené zápisy FTM budeme používať aj v nasledujúcom texte.

Príklad 2.1. Na základe II. axiómy pre každú množinu množín S existuje taká množina M, že $\forall_x ((x \in M) \Leftrightarrow (\exists_A ((A \in S) \wedge (x \in A))))$ (M je zjednotenie systému S). Zo VI. axiómy vyplýva, že takáto množina je jediná. Skutočne, ak K je množina a $\forall_x ((x \in K) \Leftrightarrow (\exists_A ((A \in S) \wedge (x \in A)))$, tak platí $\forall_x ((x \in M) \Leftrightarrow (x \in K))$ a teda $M = K$. Podobne možno dokázať jednoznačnosť prázdnej množiny, potenčnej množiny a ďalších.

Príklad 2.2. Označme $\mathcal{P}(X)$ potenčnú množinu množiny X. Potom $y = \mathcal{P}(X)$ je FTM (skrátený zápis) s dvoma voľnými premennými spĺňajúca podmienky požadované v axióme substitúcie. Nech teraz A je množina. Potom podľa axiómy substitúcie existuje množina B, ktorá obsahuje práve potenčné množiny množín, ktoré sú prvkami množiny A (t.j. „$B = \{\mathcal{P}(a) : a \in A\}$“).

Príklad 2.3. Nech A, B sú množiny. Dokážte, že existuje práve jedna množina C, pre ktorú platí: $\forall_X ((x \in C) \Leftrightarrow ((x \in A) \vee (x \in B)))$, t. j. C je zjednotenie množín A, B.

Riešenie: Podľa III. axiómy existuje množina $S = \{A, B\}$. Podľa II. axiómy existuje C taká, že $\forall_x ((x \in C) \Leftrightarrow (\exists_D ((D \in S) \wedge (x \in D))))$. Teda
$\forall_x ((x \in C) \Leftrightarrow ((x \in A) \vee (x \in B)))$. Jednoznačnosť vyplýva z Príkladu 2.1.

Veta 2.4. *Ak $\mathcal{S}$ je neprázdna množina (=systém množín), tak existuje práve jedna množina C taká, že*

$$\forall_x (x \in C) \qquad \Leftrightarrow \qquad \forall_A ((A \in \mathcal{S}) \Rightarrow (x \in A)).$$

Označenie: $C = \bigcap_{A \in \mathcal{S}} A$.

Dôkaz. Podľa II. axiómy existuje $D = \bigcup_{A \in \mathcal{S}} A$. Potom

$$C = \{x \in D : \forall_A ((A \in \mathcal{S}) \Rightarrow (x \in A))\}.$$

□

Dôsledok 2.5. *Ak A, B sú množiny, tak existuje práve jedna množina C tak, že* $\forall_x ((x \in C) \Leftrightarrow (x \in A) \wedge (x \in B))$

Dôkaz. Podľa III. axiómy existuje $S = \{A, B\}$. Stačí použiť vetu 2.4. □

Príklad 2.6. Nech A, B sú množiny. Potom existuje práve jedna množina C taká, že $C = \{x \in A : x \notin B\}$. Potom C sa nazýva *rozdiel množín A, B* a označuje sa $A \setminus B$.

Veta 2.7. *Nech A, B, C, $S \neq \emptyset$ sú množiny. Potom platí*

(a) $A \cup B = B \cup A$, $A \cap B = B \cap A$
(b) $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$
(c) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
(d) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
(e) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
(f) $A \cap (\bigcup_{D \in S} D) = \bigcup_{D \in S} (A \cap D)$
(g) $A \cup (\bigcap_{D \in S} D) = \bigcap_{D \in S} (A \cup D)$
(h) $A \setminus (\bigcup_{D \in S} D) = \bigcap_{D \in S} (A \setminus D)$
(i) $A \setminus (\bigcap_{D \in S} D) = \bigcup_{D \in S} (A \setminus D)$

Definícia 2.8. Nech a, b sú množiny. Potom množina $\{\{a\}, \{a, b\}\}$ sa nazýva *usporiadaná dvojica* prvkov a, b. Označenie: (a, b).

Ľahko sa overí, že pre ľubovoľné množiny a, b, c, d platí:

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

Nech A, B sú množiny, $a \in A$, $b \in B$. Potom $a, b \in A \cup B$, $\{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$ a $(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. Množina

$$\{v \in \mathcal{P}(\mathcal{P}(A \cup B)) : \exists_a \exists_b ((a \in A) \wedge (b \in B) \wedge (v = (a, b)))\} (= \{(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) : a \in A \wedge b \in B\})$$

sa nazýva *karteziánsky súčin množín A, B* a označuje $A \times B$.

Pripomeňme, že každá podmnožina $S \subseteq A \times B$ sa nazýva *binárna relácia* medzi prvkami množiny A a prvkami množiny B.

Zobrazenie $f \colon A \to B$ je potom binárna relácia $f \subseteq A \times B$, ktorá má nasledujúce vlastnosti

(1) $\forall_{a \in A} \exists_{b \in B} ((a, b) \in f)$,
(2) $\forall_a \forall_b \forall_c (((a, b) \in f \wedge (a, c) \in f) \Rightarrow (b = c))$.

Potom množina $\{f \in \mathcal{P}(A \times B) : f \text{ je zobrazenie } A \text{ do } B\}$ je množina všetkých zobrazení A do B a označuje sa ${}^A B$.

3. Množina $\mathbb{N}$ celých nezáporných čísel

Definícia 3.1. Nech X je množina. Množina $X' = X \cup \{X\}$ sa nazýva *nasledovník* množiny X.

Je zrejmé, že množina X' existuje a je jednoznačne určená. (podľa III. axiómy existuje $\{X\}$ a podľa príkladu 2.3 existuje práve jedna množina $X' = X \cup \{X\}$.)

Veta 3.2. *Existuje práve jedna množina $\mathbb{N}$, ktorá má nasledujúce vlastnosti:*

(1) $\emptyset \in \mathbb{N}$
(2) *Ak $X \in \mathbb{N}$, tak aj $X' \in \mathbb{N}$.*
(3) *Ak K je množina, ktorá má vlastnosti* (1), (2), *tak $\mathbb{N} \subseteq K$.*

Dôkaz. Podľa VIII. axiómy existuje množina H, ktorá spĺňa (1) a (2). Podľa II. axiómy existuje množina $\mathcal{P}(H)$ všetkých podmnožín množiny H. Podľa VI. axiómy existuje množina

$$S = \{B \in \mathcal{P}(H) : (\emptyset \in B) \wedge \forall_x ((x \in B) \Rightarrow x' \in B)\}.$$

Platí $S \neq \emptyset$, lebo $H \in S$. Potom existuje $\mathbb{N} = \bigcap_{B \in S} B$.

Zrejme $\mathbb{N}$ spĺňa (1) a (2). Nech K je množina spĺňajúca (1) a (2). Potom aj $L = \mathbb{N} \cap K$ spĺňa (1) a (2), a pretože $L \subseteq \mathbb{N}$ a $\mathbb{N} \subseteq H$, platí $L \subseteq H$ a teda $L \in S$. Potom ale $\mathbb{N} \subseteq L$, a teda $\mathbb{N} = L = \mathbb{N} \cap K$. Odtiaľ dostávame, že $\mathbb{N} \subseteq K$.

Jednoznačnosť $\mathbb{N}$: Nech $\mathbb{N}'$ je množina spĺňajúca (1), (2), (3). Pretože $\mathbb{N}'$ spĺňa (1), (2), máme $\mathbb{N} \subseteq \mathbb{N}'$. Pretože $\mathbb{N}'$ spĺňa (3) a $\mathbb{N}$ spĺňa (1), (2), dostávame $\mathbb{N}' \subseteq \mathbb{N}$. Teda $\mathbb{N}' = \mathbb{N}$. □

Dôsledok 3.3. *Ak $U \subseteq \mathbb{N}$ a U spĺňa (1) a (2), tak $U = \mathbb{N}$.*

Množina $\mathbb{N}$ sa nazýva množina (všetkých) celých nezáporných čísel a jej prvky sa nazývajú *celé nezáporné čísla.* Budeme ich obyčajne označovať $m, n, k, p, q, \ldots$

Pretože $\emptyset \in \mathbb{N}$, $\emptyset$ je nezáporné celé číslo, ktoré sa nazýva *nula* a označuje sa 0 (teda 0 je v tomto modeli celých nezáporných čísel len iné označenie pre $\emptyset$).

$$0' = 0 \cup \{0\} = \{0\} = 1 \in \mathbb{N},$$
$$1' = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\} = 2 \in \mathbb{N},$$
$$2' = \{0, 1, 2\} = 3 \in \mathbb{N}', \ldots$$

V nasledujúcom budeme definovať usporiadanie a operácie $+$ a $\cdot$ na $\mathbb{N}$.

Veta 3.4. *Pre všetky $m, n \in \mathbb{N}$ platí:*

(1) *Ak $m \in n$, tak $m' \subseteq n$.*
(2) *$n \notin n$*
(3) *Ak $m' = n'$, tak $m = n$.*

Dôkaz. (1) Položme $U = \{n \in \mathbb{N} : \forall_{m \in \mathbb{N}}((m \in n) \Rightarrow (m' \subseteq n))\}$. Zrejme $U \subseteq \mathbb{N}$ a $0 \in U$. $((m \in 0) \Rightarrow (m' \subseteq 0)$ je pravdivý výrok, lebo $m \in 0$ je nepravdivý výrok.)

Nech $n \in U$. Nech $m \in \mathbb{N}$ a $m \in n' = n \cup \{n\}$. Potom $m \in n$ alebo $m = n$. Potom, pretože $n \in U$, máme $m' \subseteq n$ alebo $m' = n'$. Teda $m' \subseteq n \subseteq n'$ alebo $m' = n'$, a preto $m' \subseteq n'$. Dokázali sme, že ak $n \in U$, tak aj $n' \in U$, a teda $U = \mathbb{N}$.

(2) Položme $U = \{n \in \mathbb{N} : n \notin n\}$. Potom $U \subseteq \mathbb{N}$ a $0 \in U$. Nech $n \in U$, t.j. $n \notin n$. Ak $n' \in n' = n \cup \{n\}$, tak $n' \in n$ alebo $n' = n$. Potom $n \in n' \subseteq (n')' \subseteq n$ alebo $n \in n' = n$. Teda $n \in n$ a to je spor s tým, že $n \in U$. Preto platí $n' \in n'$, t.j. $n' \in U$ a $U = \mathbb{N}$.

(3) Nech $m' = n'$. Potom $m \in n'$ a teda $m \in n$ alebo $m = n$. Odtiaľ dostávame, že $m \subseteq m' \subseteq n$ alebo $m = n$. Teda $m \subseteq n$. Podobne z toho, že $n \in m'$ dostaneme $n \subseteq m$. □

Dôsledok 3.5. *Pre každé $n \in \mathbb{N}$ platí $n \subseteq n'$ a $n \neq n'$ (ak $n = n'$, tak $n \in n$).*

Cvičenie 3.6. Dokážte, že pre každé $n \in \mathbb{N}$ platí: $0 = n$ alebo $0 \in n$.

Veta 3.7 (Peanove axiómy)**.** *Množina $\mathbb{N}$ má nasledujúce vlastnosti:*

(P1) $0 \in \mathbb{N}$
(P2) *Ak $n \in \mathbb{N}$, tak aj $n' \in \mathbb{N}$.*
(P3) *Ak $n \in \mathbb{N}$, tak $n' \neq 0$.*
(P4) *Ak $m, n \in \mathbb{N}$ a $m' = n'$, tak $m = n$.*
(P5) *Ak $U \subseteq \mathbb{N}$, $0 \in U$ a platí: ak $n \in U$, tak aj $n' \in U$, potom $U = \mathbb{N}$.*

Dôkaz. (P3) $n \in n' \Rightarrow n' \neq 0$ □

Definícia 3.8. Nech $n, k \in \mathbb{N}$. Hovoríme, že n je menšie ako k, ak $n \in k$. Označenie $n < k$.

Veta 3.9. *Pre ľubovoľné $m, n, k \in \mathbb{N}$ platí:*

(1) *$n \not< n$*
(2) *Ak $m < n$ a $n < k$, tak $m < k$.*
(3) *Nastáva práve jedna z možností: $m < n$, $m = n$, $n < m$.*

Dôkaz. (1) $n \not< n \Leftrightarrow n \notin n$ – platí

(2) Nech $m < n$ a $n < k$. Potom $m \in n$ a $n \in k$. Potom $m \in n \subseteq n'$ a $n' \subseteq k$. Teda $m \in k$ a to znamená, že $m < k$.

(3) Najprv dokážeme, že nastáva najviac jedna z uvedených možností. Ak $m < n$ a súčasne $m = n$, tak $m \in n$ a $m = n$, a teda $m \in m$, čo je spor. Podobne $m = n$ a $n < m$ vedie k tomu,

že $m \in m$ a teda k sporu. Nech $m \in n$ a súčasne $n \in m$. Potom $m \in n \subseteq n'$ a $n' \subseteq m$. Z toho dostávame, že $m \in m$, a to je spor.

Teraz dokážeme, že pre ľubovoľné $m, n \in \mathbb{N}$ platí $m < n$ alebo $m = n$ alebo $n < m$, t.j. platí

$$(m \in n) \vee (m = n) \vee (n \in m).$$

Nech $n \in \mathbb{N}$. Položme $U(n) = \{m \in \mathbb{N}; (m \in n) \vee (m = n) \vee (n \in m)\}$. Ukážeme, že pre každé $n \in \mathbb{N}$ platí $U(n) = \mathbb{N}$.

Nech teda $V = \{n \in \mathbb{N}; U(n) = \mathbb{N}\}$.

$$U(0) = \{m \in \mathbb{N} : (m \in 0) \vee (m = 0) \vee (0 \in m)\}.$$

Pretože pre každé $m \in \mathbb{N}$ platí $(m = 0) \vee (0 \in m)$, tak $U(0) = \mathbb{N}$. Teda $0 \in V$.

Nech $n \in V$, t.j. $U(n) = \mathbb{N}$. Ukážeme, že $U(n') = \mathbb{N}$. Platí $0 \in U(n')$, lebo $0 \in n'$, a preto platí $(0 \in n') \vee (0 = n') \vee (n' \in 0)$.

Nech $m \in U(n')$, t.j. platí $(m \in n') \vee (m = n') \vee (n' \in m)$.

Ak $m = n'$, tak $n' \in m \cup \{m\} = m'$, t.j. $n' \in m'$.

Ak $n' \in m$, tak $n' \in m \subseteq m'$ a teda $n' \in m'$.

Nech $n' \notin m$ a súčasne $m \neq n'$. Potom platí $m \in n'$ a preto $m' \subseteq n'$. Sú dve možnosti: $m' = n'$ alebo $m' \subsetneqq n'$.

Nech $m' \neq n'$. Potom $m' \subsetneqq n'$. Pretože $m' \in \mathbb{N} = U(n)$, pre čísla m, n nastáva práve jedna z možností: $m' \in n$, $m' = n$, $n \in m'$. Ak $n \in m'$, tak $n' \subseteq m'$ a to spolu s $m' \subseteq n'$ dáva $m' = n'$, pričom predpokladáme, že $m' \neq n'$. Preto táto možnosť nemôže nastať a teda nastane jedna z možností $m' \in n$ alebo $m' = n$. Z obidvoch týchto možností vyplýva, že $m' \in n'$. [1]

Ukázali sme, že platí $(n' \in m') \vee (n' = m') \vee (m' \in n')$, a teda $m' \in U(n')$. Preto $U(n') = \mathbb{N}$ a $n' \in V$. Teda $V = \mathbb{N}$. □

Dôsledok 3.10. $(\mathbb{N}, <)$ *je usporiadaná množina.*

Dôsledok 3.11. *Ak* $m, n, k \in \mathbb{N}$, $m \in n$ *a* $n \in k$, *tak* $m \in k$.

Označenie: $(n \leq k) \Leftrightarrow ((n < l) \vee (n = k))$. Je zrejmé, že $(n \not\leq k) \Leftrightarrow (k < n)$.

Cvičenie 3.12. Dokážte, že pre každé $p, n \in \mathbb{N}$ platí: Ak $p < n$, tak $p' \leq n$.

Riešenie: Nech $p' \not\leq n$. Potom $n < p'$, a teda $n \in p' = p \cup \{p\}$. Potom $n \in p$ alebo $n = p$, a pretože podľa predpokladu $p \in n$, dostávame $(p \in p) \vee (p \in p)$, a teda $p \in p$, čo je spor. Teda $p' \leq n$.

Cvičenie 3.13. Dokážte, že pre ľubovoľné $n, k \in \mathbb{N}$ platí $n \leq k \Leftrightarrow n \subseteq k$.

Riešenie: $\boxed{\Rightarrow}$ $n \leq k \Rightarrow n < k \vee n = k \Rightarrow n \in k \vee n = k \Rightarrow n' \subseteq k \vee n = k \Rightarrow n \subseteq k \vee n = k \Rightarrow n \subseteq k$

$\boxed{\Leftarrow}$ Nech $n > k$. Potom $k \in n$ a teda $k \subseteq n$. Podľa predpokladu platí $n \subseteq k$ a teda dostávame $n = k$, čo je v spore s tým, že $n > k$. Teda $n \leq k$.

Veta 3.14. *Usporiadaná množina* $(\mathbb{N}, <)$ *je dobre usporiadaná, t.j. každá neprázdna podmnožina* K *množiny* $\mathbb{N}$ *má najmenší prvok.*

Dôkaz. Nech $K \subseteq \mathbb{N}$, $K \neq \emptyset$. Utvorme množinu $V = \{n \in \mathbb{N}; \forall_{k \in K} n \leq k\}$. Zrejme $0 \in V$.

Nech $k_0 \in K$. Potom zrejme $k_0' \not\leq k_0$, a teda $k_0' \notin V$. Teda $V \neq \mathbb{N}$ a teda existuje $p \in \mathbb{N}$ tak, že $p \in V$ a $p' \notin V$. Teda $\forall_{k \in K} p \leq k$.

Ak $p \notin K$, tak pre každé $k \in K$ platí $p < k$, a teda $p' \leq k$. Potom $p' \in V$; čo je spor.

Teda $p \in K$ a p je najmenší prvok množiny K. □

[1] $m' \in n \subseteq n' \Rightarrow (m' \in n')$; $(m' = n \in n') \Rightarrow (m' \in n')$

4. Dôkaz matematickou indukciou

Lema 4.1. $\mathbb{N} = \{0\} \cup \{n' : n \in \mathbb{N}\}$.

Dôkaz. Nech $U = \{n \in \mathbb{N} : n = 0$ alebo existuje $k \in \mathbb{N}$ tak, že $k' = n\}$. Zrejme $0 \in U$.
Nech $n \in U$. Potom n' je nasledovník n, a preto $n' \in U$.
Teda $U = \mathbb{N}$. □

Dôsledok 4.2. *Pre každé $n \in \mathbb{N}$, $n \neq 0$. existuje $k \in \mathbb{N}$ tak, že $n = k'$.*

Nech $m \in \mathbb{N}$. Položme

$$\mathbb{N}_m = \{n \in \mathbb{N} : m \leq n\}$$

Veta 4.3 (Prvý typ dôkazu matematickou indukciou)**.** *Nech $m \in \mathbb{N}$, pre každé $n \in \mathbb{N}_m$ je $P(n)$ výrok a platí:*

(1) *$P(m)$ je pravdivý výrok.*
(2) *Ak $n \in \mathbb{N}_m$ a $P(n)$ je pravdivý výrok, tak aj $P(n')$ je pravdivý výrok.*

Potom pre každé $n \in \mathbb{N}_m$ je $P(n)$ pravdivý výrok.

Dôkaz. Nech $V = \{k \in \mathbb{N}_m : P(k)$ je nepravdivý$\} \neq \emptyset$.
Pretože $V \subseteq \mathbb{N}$, existuje najmenší prvok $q \in V$. Z (1) vyplýva, že $q > m$. Zrejme $q \neq 0$, a preto existuje $k \in \mathbb{N}$ tak, že $q = k'$. Ak $k < m$, tak $k' = q \leq m$, čo je spor. Teda $m \leq k$, t.j. $k \in \mathbb{N}_m$ a pretože $k < k' = q$, $k \notin V$. Teda $P(k)$ je pravdivý a podľa (2) aj $P(k') = P(q)$ je pravdivý, čo je spor. Teda $V = \emptyset$. □

Veta 4.4 (Druhý typ dôkazu matematickou indukciou)**.** *Nech $m \in \mathbb{N}$, pre každé $n \in \mathbb{N}_m$ je $P(n)$ výrok a platí:*

(1) *$P(m)$ je pravdivý výrok.*
(2) *Ak $n > m$ a pre všetky $k \in \mathbb{N}_m$, $k < n$, je $P(k)$ pravdivý výrok, tak aj $P(n)$ je pravdivý.*

Potom pre každé $n \in \mathbb{N}_m$ je $P(n)$ pravdivý výrok.

Dôkaz. Nech $V = \{k \in \mathbb{N}_m : P(k)$ je nepravdivý$\} \neq \emptyset$. Potom V má najmenší prvok q. Zrejme $m < q$ (podľa (1)) a pre všetky $k \in \mathbb{N}_m$, $k < q$, je $P(k)$ pravdivý. Potom podľa (2) je aj $P(q)$ pravdivý, t.j. $q \notin V$ a to je spor. Teda $V = \emptyset$. □

Cvičenie 4.5. Dokážte, že pre každé $n \in \mathbb{N}$, $n \geq 2$, existuje prvočíslo p tak, že $p \mid n$.

5. Definícia súčtu a súčinu celých nezáporných čísel

Nech $k \in \mathbb{N}$. Definujeme $k + n$ nasledovne:

(1) $k + 0 = k$
(2) $k + n' = (k + n)'$

Týmto je pre každé $n \in \mathbb{N}$ jednoznačne definované celé nezáporné číslo $k + n$. Skutočne, položme $U_k = \{n \in \mathbb{N} : k + n$ je jednoznačne definované$\}$. Potom $0 \in U_k$ a ak $n \in U_k$, t.j. $k + n$ je jednoznačne definované, tak aj číslo $(k+n)' = k+n'$ je jednoznačne definované. Teda $n' \in U_k$ a $U_k = \mathbb{N}$.

Teda pre ľubovoľné $k \in \mathbb{N}$ platí $U_k = \mathbb{N}$, t.j. pre každé $k, n \in \mathbb{N}$ je $k+n$ jednoznačne definované celé číslo.

Teraz budeme definovať súčin analogickým spôsobom:

Nech $k \in \mathbb{N}$. Definujme $k.n$ nasledovne:

(1) $k.0 = 0$
(2) $k.n' = k.n + k$

Podobne ako pre súčet je týmto pre každú dvojicu $k, n \in \mathbb{N}$ jednoznačne určené celé nezáporné číslo $k.n$.

Z definície súčtu dostávame, že pre každé $k \in \mathbb{N}$

$$k' = (k + 0)' = k + 0' = k + 1.$$

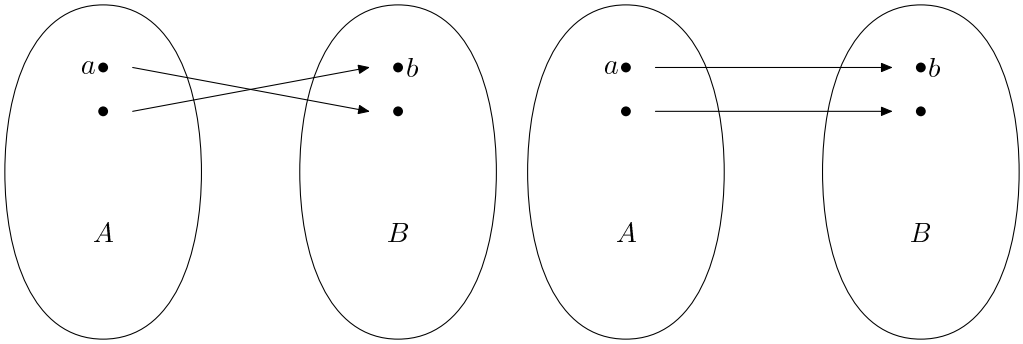
6. Konečné a nekonečné množiny

Definícia 6.1. Hovoríme, že množina A je *ekvivalentná* s množinou B, ak existuje bijektívne zobrazenie $f\colon A \to B$. Označenie: $A \sim B$.

Pre ľubovoľné množiny A, B, C platí:

(1) $A \sim A$ (identické zobrazenie $id\colon A \to A$, $id(x) = x$, je bijektívne)
(2) Ak $A \sim B$, tak $B \sim A$. (Ak $f\colon A \to B$ je bijektívne, tak $f^{-1}\colon B \to A$ je bijektívne.)
(3) Ak $A \sim B$ a $B \sim C$, tak $A \sim C$. (Ak $f\colon A \to B$, $g\colon B \to C$ sú bijektívne zobrazenia, tak $g \circ f\colon A \to C$ je bijektívne zobrazenie.)

Lema 6.2. *Nech $C = A \cup \{a\}$, $D = B \cup \{b\}$, $a \notin A$, $b \notin B$ (A, B, C, D, a, b sú množiny). Potom $C \sim D \Leftrightarrow A \sim B$.*



Obr. 1. Ilustrácia k dôkazu lemy 6.2

Dôkaz. $\boxed{\Rightarrow}$ Nech $C \sim D$. Potom existuje bijektívne zobrazenie $f\colon C \to D$. Ak $f(a) = b$, tak zobrazenie $g\colon A \to B$, dané predpisom $g(x) = f(x)$ pre všetky $x \in A$ je bijektívne.

Nech $f(a) = d \neq b$. Potom existuje práve jedno $c \in C$ tak, že $f(c) = b$. Zrejme $c \in A$. Zobrazenie $h\colon A \to B$ dané predpisom $h(x) = f(x)$ pre $x \neq c$ a $h(c) = d$ je bijektívne. Teda $A \sim B$.

$\boxed{\Leftarrow}$ Nech $A \sim B$. Potom existuje bijektívne zobrazenie $f\colon A \to B$. Zobrazenie $g\colon C \to D$, $g(x) = f(x)$ pre každé $x \in A$ a $g(a) = b$, je bijektívne. Teda $C \sim D$. □

Veta 6.3. *Pre každé $k, n \in \mathbb{N}$ platí: Ak $k \sim n$, tak $k = n$.*

Dôkaz. Nech $U = \{k \in \mathbb{N} : \forall_{n \in \mathbb{N}}((k \sim n) \Rightarrow (k = n))\}$.

Potom $0 \in U$, pretože ak $0 = \emptyset \sim n$, tak $n = 0$. (Prázdna množina je ekvivalentná len s prázdnou množinou.)

Nech $k \in U$. Ukážeme, že potom $k' \in U$. Nech $n \in \mathbb{N}$ a $k' \sim n$. Pretože $k' \neq 0$, platí $n \neq 0$. Potom existuje $m \in \mathbb{N}$ tak, že $n = m'$. Teda máme $k' = k \cup \{k\} \sim m \cup \{m\} = m'$. Pretože $k \notin k$ a $m \notin m$, podľa lemy 6.2 dostávame, že $k \sim m$. Pretože $k \in U$, platí $k = m$. Potom ale $k' = m' = n$. Teda $k' \in U$ a $U = \mathbb{N}$. □

Definícia 6.4. Množina A sa nazýva *konečná,* ak existuje $n \in \mathbb{N}$ tak, že $A \sim n$. Ak $A \sim n$, hovoríme, že A má n prvkov. Označenie: $|A| = n$. Množina A sa nazýva nekonečná, ak nie je konečná.

Príklad 6.5. Množina $\emptyset$ je konečná a $|\emptyset| = 0$.

Pre každé $n \in \mathbb{N}$ je množina n konečná a $|n| = n$ (lebo $n \sim n$).

Príklad 6.6. Nech $m \in \mathbb{N}$. Potom $\mathbb{N} \setminus \{m\} \sim \mathbb{N}$. Špeciálne $\mathbb{N}_1 = \mathbb{N} \setminus \{0\} \sim \mathbb{N}$. Ľahko sa overí, že zobrazenie $f\colon \mathbb{N} \to \mathbb{N} \setminus \{m\}$

$$f(k) = \begin{cases} k & \text{pre } k < m, \\ k' & \text{pre } k \geq m. \end{cases}$$

je bijektívne.

Príklad 6.7. Množina $\mathbb{N}$ je nekonečná.

Nech $\mathbb{N}$ je konečná. Potom existuje $k \in \mathbb{N}$ tak, že $\mathbb{N} \sim k$. Pretože $\mathbb{N} \neq \emptyset$, $k \neq 0$ a existuje $m \in \mathbb{N}$ tak, že $k = m'$. Potom $\mathbb{N} = \{0\} \cup \mathbb{N}_1 \sim m \cup \{m\} = k$, pričom $0 \notin \mathbb{N}_1$, $m \notin m$. Podľa lemy 6.2 potom $\mathbb{N}_1 \sim m$. Pretože $m' \sim \mathbb{N}$, $\mathbb{N} \sim \mathbb{N}_1$ a $\mathbb{N}_1 \sim m$, dostávame, že $m' \sim m$ a podľa vety 6.3 potom $m' = m$ a to je spor. Teda $\mathbb{N}$ je nekonečná.

Veta 6.8. *Nech A, B sú konečné množiny, $|A| = n$, $|B| = k$. Potom $A \sim B \Leftrightarrow n = k$.*

Dôkaz. $\boxed{\Rightarrow}$ Pretože $n \sim A$, $A \sim B$ a $B \sim k$, platí $n \sim k$, a teda $n = k$.

$\boxed{\Leftarrow}$ Ak $A \sim n$, $n = k$, $k \sim B$, tak $A \sim B$. □

Veta 6.9. *Nech $n \in \mathbb{N}$ a $A \subseteq n$. Potom A je konečná a $|A| = k \leq n$. Ak $A \neq n$, tak $|A| < n$.*

Dôkaz. Matematickou indukciou. Nech $n = 0$. Ak $A \subseteq 0 = \emptyset$, tak $A = \emptyset$, a teda A je konečná a $|A| = 0 \leq 0$.

Nech tvrdenie platí pre n a $A \subseteq n' = n \cup \{n\}$. Potom $A \subseteq n$ alebo $n \in A$.

Ak $A \subseteq n$, tak podľa indukčného predpokladu A je konečná a $|A| = k \leq n < m'$.

Nech $n \in A$. Potom $B = A \setminus \{n\} \subseteq n$ a $A = B \cup \{n\}$, $n \notin B$. Ak $B \sim l$, tak $B \cup \{n\} \sim l \cup \{l\} = l'$ (keďže $l \notin l$) a teda $A = B \cup \{n\}$ je konečná a $|A| = l'$. Pretože $l \leq n < n'$ platí $l < n'$ a potom $l' \leq n'$ (cvičenie 3.12). Teda tvrdenie platí aj pre n'.

Nech $A \subseteq n$, $A \neq n$. Podľa prvej časti dôkazu $|A| = k \leq n$. Nech $p \in n \setminus A$. Potom $|A \cup \{p\}| = k'$, a pretože $A \cup \{p\} \subseteq n$, platí $k' \leq n$. Potom $k < k' \leq n$ a teda $k < n$. □

Dôsledok 6.10. *Ak B je konečná množina, $|B| = n$ a $A \subseteq B$, tak aj A je konečná a $|A| \leq n$*

Dôkaz. Ak $|B| = n$, tak existuje bijektívne zobrazenie $f\colon B \to n$. Označme $f[A] = A'$. Potom $A \sim A'$, $A' \subseteq n$. Podľa vety 6.9 A' je konečná a $|A'| = k \leq n$. Pretože $A \sim A'$ a $A' \sim k$, platí $A \sim k$, a teda A je konečná a $|A| = k$. □

Dôsledok 6.11. *Ak A je nekonečná množina a $A \subseteq B$, tak aj B je nekonečná.*

Dôsledok 6.12. *Ak B je konečná množina a $A \subsetneq B$, tak $A \not\sim B$.*

Veta 6.13. *Nech A, B sú konečné množiny, $|A| = n$, $|B| = k$ a $A \cap B = \emptyset$. Potom $A \cup B$ je konečná množina a $|A \cup B| = n + k$.*

Dôkaz. Indukciou vzhľadom na počet prvkov B.

Nech $|B| = k = 0$. Potom $B = \emptyset$ a $A \cup \emptyset = A$ je konečná. Platí tiež $|A \cup \emptyset| = |A| = n = n + 0$.

Predpokladajme, že tvrdenie platí pre $k \in \mathbb{N}$. Nech $|B| = k'$. Pretože $k' \neq 0$, $B \neq \emptyset$ a existuje $b \in B$. Nech $C = B \setminus \{b\}$. Potom $B = C \cup \{b\}$, $b \notin C$, $A \cap C = \emptyset$. Platí $C \cup \{b\} \sim k' = k \cup \{k\}$, a teda $C \sim k$, t.j. $|C| = k$. Podľa indukčného predpokladu $A \cup C$ je konečná a $|A \cup C| = n + k$. Súčasne $b \in B$, $B \cap A = \emptyset$, a teda $b \notin A$. Potom $b \notin A \cup C$ a $A \cup B = (A \cup C) \cup \{b\}$. Pretože $A \cup C \sim n + k$, platí $(A \cup C) \cup \{b\} \sim (n + k)'$, a teda $A \cup B$ je konečná a $|A \cup B| = (n + k)' = n + k'$. Teda výrok platí aj pre k' a veta je dokázaná. □

Dôsledok 6.14. *Ak A, B sú konečné množiny, tak aj $A \cup B$ je konečná množina.*

Dôkaz. Nech $C = B \setminus A$. Potom $A \cap C = \emptyset$ a $A \cup B = A \cup C$. Podľa vety 6.13 je $A \cup C$ konečná množina. □

Cvičenie 6.15. Dokážte, že ak A je konečná a $f\colon A \to B$ je surjektívne, tak aj B je konečná.

Dôsledok 6.16. *Pre ľubovoľné $m, n, k \in \mathbb{N}$ platí:*

(1) $m+n=n+m$
(2) $(m+n)+k=m+(n+k)$
(3) $m<n \Leftrightarrow m+k<n+k$
(4) *Ak* $m+k=n+k$, *tak* $m=n$.

Dôkaz. (1) Nech A, B sú množiny, $|A|=m$, $|B|=n$ a $A\cap B=\emptyset$. Také množiny existujú, napríklad $A=m\times\{0\}$, $B=n\times\{1\}$. Platí $A\cup B=B\cup A$. Potom

$$m+n=|A\cup B|=|B\cup A|=n+m.$$

(2) Nech A, B, C sú množiny, pre ktoré $|A|=m$, $|B|=n$, $|C|=k$, $A\cap B=\emptyset$, $A\cap C=\emptyset$, $B\cap C=\emptyset$ (napríklad $A=m\times\{0\}$, $B=n\times\{1\}$, $C=k\times\{2\}$). Potom aj $(A\cup B)\cap C=\emptyset$, $A\cap(B\cup C)=\emptyset$, $|A\cup B|=m+n$, $|B\cup C|=n+k$. Platí $(A\cup B)\cup C=A\cup(B\cup C)$. Potom

$$(m+n)+k=|(A\cup B)\cup C|=|A\cup(B\cup C)|=m+(n+k).$$

(3) $\boxed{\Rightarrow}$ Indukciou vzhľadom na k. Nech $k=0$. Ak $m<n$, tak $m+0<n+0$. Predpokladajme, že výrok platí pre $k\in\mathbb{N}$. Nech $m<n$. Potom $m+k<n+k$ a teda (cvičenie 3.12) $(m+k)'\leq n+k$. Potom $(m+k)'<(n+k)'$, a teda $m+k'<n+k'$.

$\boxed{\Leftarrow}$ Nepriamo: Ak $m\geq n$, tak $m>n$ alebo $m=n$, a preto $m+k>n+k$ alebo $m+k=n+k$. Teda $m+k\geq n+k$.

(4) Nepriamo: Ak $m\neq n$, tak $m<n$ alebo $n<m$. Potom $m+k<n+k$ alebo $n+k<m+k$, a teda $m+k\neq n+k$. □

Veta 6.17. *Nech A, B sú konečné množiny, $|A|=n$, $|B|=k$. Potom aj $A\times B$ je konečná množina a $|A\times B|=n.k$.*

Dôkaz. Indukciou vzhľadom na počet prvkov B.

Nech $|B|=k=0$. Potom $B=\emptyset$ a $A\times\emptyset=\emptyset$ je konečná množina a $|A\times\emptyset|=|\emptyset|=0=n.0$.

Nech výrok platí pre $k\in\mathbb{N}$ a $|B|=k'$. Pretože $k'\neq 0$, $B\neq\emptyset$ a existuje $b\in B$. Nech $C=B\setminus\{b\}$. Potom $b\notin C$, $B=C\cup\{b\}\sim k\cup\{k\}$, a teda $C\sim k$, t.j. $|C|=k$. Platí

$$A\times B=A\times(C\cup\{b\})=(A\times C)\cup(A\times\{b\}),\qquad (A\times C)\cap(A\times\{b\})=\emptyset$$

a $A\times\{b\}\sim A$, t.j. $|A\times\{b\}|=n$. Podľa indukčného predpokladu je $A\times C$ konečná, a preto aj $(A\times C)\cup(A\times\{b\})=A\times B$ je konečná a platí $|A\times B|=|(A\times C)\cup(A\times\{b\})|=n.k+n=n.k'$. Teda výrok platí aj pre k'. □

Dôsledok 6.18. *Pre ľubovoľné $m,n,k\in\mathbb{N}$ platí:*

(1) $m.n=n.m$
(2) $m.(n.k)=m.(n.k)$
(3) $m.1=1.m=m$
(4) $m.(n+k)=m.n+m.k$
(5) *Ak* $k>0$, *tak* $m<n \Leftrightarrow m.k<n.k$.
(6) *Ak* $k>0$ *a* $m.k=n.k$, *tak* $m=n$.

Dôkaz. Nech A, B, C sú množiny, $|A|=m$, $|B|=n$, $|C|=k$.

(1) Platí $A\times B\sim B\times A$. (Zobrazenie $f\colon A\times B\to B\times A$; $f(x,y)=(y,x)$; je bijektívne.) Potom

$$m.n=|A\times B|=|B\times A|=n.m.$$

(2) Platí $(A\times B)\times C\sim A\times(B\times C)$. (Zobrazenie $g\colon(A\times B)\times C\to A\times(B\times C)$; $((x,y),z)\mapsto(x,(y,z))$ je bijektívne.) Potom

$$(m.n).k=|(A\times B)\times C|=|A\times(B\times C)|=m.(n.k).$$

(3)

$$m.1=m.0'=m.0+m=0+m=m$$
$$1.m=m.1=m$$

(4) Nech teraz $B \cap C = \emptyset$. Potom $A \times B \cap A \times C = \emptyset$. Platí tiež $A \times (B \cup C) = (A \times B) \cup (A \times C)$. Potom

$$m(n+k) = |A \times (B \cup C)| = |(A \times B) \cup (A \times C)| = m.n + m.k$$
$$(m+n).k = k.(m+n) = k.m + k.n = m.k + n.k$$

(5) $\boxed{\Rightarrow}$ Indukciou vzhľadom na k, $k \in \mathbb{N}_1$.

Nech $k = 1$. Ak $m < n$, tak $m.1 < n.1$.

Nech výrok platí pre $k \in \mathbb{N}_1$. Nech $m < n$. Potom podľa indukčného predpokladu $m.k < n.k$. Potom

$$m.k + m < n.k + m < n.k + n.$$

Teda

$$m.k' = m.k + m < n.k + n = n.k',$$

t.j. výrok platí aj pre k'.

$\boxed{\Leftarrow}$ Nepriamo: Ak $m \geq n$, tak $m > n$ alebo $m = n$, a preto $m.k > n.k$ alebo $m.k = n.k$. Potom $m.k \geq n.k$.

(6) Nepriamo: Nech $m \neq n$. Potom $m < n$ alebo $n < m$. Podľa (5) potom $m.k < n.k$ alebo $n.k < m.k$. Potom $m.k \neq n.k$. □

Odteraz budeme namiesto n' používať označenie $n + 1$ (je to to isté číslo).

Cvičenie 6.19. Nech $m \in \mathbb{N}$. Definujme m^k nasledovne:

(1) $m^0 = 1$,
(2) $m^{k+1} = m^k.m$.

Tým je pre každé $k \in \mathbb{N}$ jednoznačne definované číslo $m^k \in \mathbb{N}$.

Dokážte, že pre ľubovoľné čísla $m, k, l \in \mathbb{N}$ platí:

(1) $(m.k)^l = m^l.k^l$,
(2) $m^{k+l} = m^k.m^l$,
(3) $(m^k)^l = m^{k.l}$.

Veta 6.20. *Ak $A \subseteq \mathbb{N}$, tak A je konečná alebo $A \sim \mathbb{N}$.*

Dôkaz. Nech existuje $k \in \mathbb{N}$ také, že pre všetky $l \in A$ platí $l \leq k$. Potom pre všetky $l \in A$ platí $l < k + 1$, a preto $A \subseteq k + 1$. Podľa vety 6.9 A je konečná množina.

Nech teraz pre každú $k \in \mathbb{N}$ existuje $l \in A$, $l > k$ (t.j. A je neohraničená v $\mathbb{N}$). Pretože existuje $l \in A$, $l > 0$, $A \neq \emptyset$. Definujme zobrazenie $f\colon \mathbb{N} \to A$ nasledovne: $f(0) = l_0$ je najmenší prvok množiny A. Nech $f(n) = l_n \in A$ je definované. Položme

$$A_n = \{l \in A : l_n < l\}.$$

Pretože $l_n \in \mathbb{N}$, $A_n \neq \emptyset$. Položme $f(n+1) = l_{n+1}$ =najmenší prvok A_n. Týmto je pre každé $n \in \mathbb{N}$ jednoznačne definovaný prvok $f(n) = l_n \in A$, a teda je definované zobrazenie $f\colon \mathbb{N} \to A$. (Nech $U = \{n \in \mathbb{N}; f(n)$ je jednoznačne definovaný prvok v $A\}$. Potom $0 \in U$ a ak $n \in U$, tak aj $n + 1 \in U$. Teda $U = \mathbb{N}$.) Z definície f je zrejmé, že pre každé $n \in \mathbb{N}$ platí $f(n) < f(n+1)$ a z toho vyplýva, že f je prosté.

Ukážeme, že f je surjektívne.

Nech $a \in A$. Množina $K = \{k \in \mathbb{N}; f(k) \geq a\} \neq \emptyset$. Ak $K = \emptyset$, tak pre všetky $n \in \mathbb{N}$ platí $f(n) < a$, a teda $f[\mathbb{N}] \subseteq a \in \mathbb{N}$. Potom $f[\mathbb{N}]$ je konečná a súčasne $f[N] \sim \mathbb{N}$, a teda aj $\mathbb{N}$ je konečná – spor.

Teda $K \neq \emptyset$ a má najmenší prvok m. Ak $m = 0$, tak $f(0) = l_0 \leq a$ a súčasne $a \leq f(0)$. Teda $f(0) = a = l_0$. Nech $m > 0$. Potom existuje $p \in \mathbb{N}$ tak, že $m = p + 1$, $p < m$ a preto $p \notin K$. Teda $f(p) < a$. Potom $a \in A_p = \{l \in A : f(p) < l\}$ a $f(p+1) = l_{p+1}$ je najmenší prvok A_p. Teda $f(m) = f(p+1) = l_{p+1} \leq a$ a súčasne $a \leq f(m)$. Teda $a = f(m)$.

Každý prvok $a \in A$ je obrazom nejakého $m \in \mathbb{N}$, t.j. f je surjektívne. Existuje teda bijektívne zobrazenie $f\colon \mathbb{N} \to A$, t.j. $\mathbb{N} \sim A$. □

Definícia 6.21. (1) Množina A sa nazýva *nekonečná spočítateľná,* ak $A \sim \mathbb{N}$.
(2) Množina A sa nazýva *spočítateľná,* ak A je konečná alebo nekonečná spočítateľná.

Je zrejmé, že ak A je spočítateľná a $B \sim A$, tak B je spočítateľná.
Z vety 6.20 vyplýva, že každá podmnožina množiny $\mathbb{N}$ je spočítateľná.

Príklad 6.22. Množina $\mathbb{Z}$ všetkých celých čísel je spočítateľná, lebo zobrazenia $f\colon \mathbb{Z} \to \mathbb{N}$,

$$f(z) = \begin{cases} 2z & \text{pre } z \geq 0, \\ 2(-z) - 1 & \text{pre } z < 0, \end{cases}$$

je bijektívne, a teda $\mathbb{Z} \sim \mathbb{N}$.

Veta 6.23. *Nech $A \neq \emptyset$. Potom nasledujúce výroky sú ekvivalentné:*
(1) *A je spočítateľná.*
(2) *Existuje surjektívne zobrazenie $f\colon \mathbb{N} \to A$.*
(3) *Existuje injektívne zobrazenie $g\colon A \to \mathbb{N}$.*

Dôkaz. (1)⇒ (2) Ak A je konečná, tak existuje $n \in \mathbb{N}$ tak, že $n \sim A$. Nech $h\colon n \to A$ je bijektívne zobrazenie a $c \in A$. Definujme $f\colon \mathbb{N} \to A$ tak, že $f(k) = h(k)$ pre $k \in \mathbb{N}$ a $f(k) = c$ pre $k \in \mathbb{N} \setminus n$ ($n \subseteq \mathbb{N}$). Zrejme f je surjektívne (lebo h je surjektívne). Ak $A \sim \mathbb{N}$, tak existuje bijektívne zobrazenie $f\colon \mathbb{N} \to A$ a toto je aj surjektívne.
(2)⇒ (3) Nech $f\colon \mathbb{N} \to A$ je surjektívne. Pre každé $c \in A$ je

$$f_{-1}(c) = \{k \in \mathbb{N}; f(k) = c\} \neq \emptyset$$

a $f_{-1}(c) \subseteq \mathbb{N}$. Teda $f_{-1}(c)$ má najmenší prvok k_c.
Definujme $g\colon A \to \mathbb{N}$; $g(c) = k_c$. Ak $c, d \in A$, $c \neq d$, tak $f_{-1}(c) \cap f_{-1}(d) = \emptyset$, a preto $k_c \neq k_d$. Teda g je injektívne zobrazenie.
(3)⇒ (1) Nech $g\colon A \to \mathbb{N}$ je injektívne zobrazenie. Potom $A' = g[A]$ je podmnožina $\mathbb{N}$ a $A \sim A'$. Množina A' je podľa vety 6.20 konečná alebo $A' \sim \mathbb{N}$. Teda aj A je konečná alebo $A \sim \mathbb{N}$, a preto A je spočítateľná. □

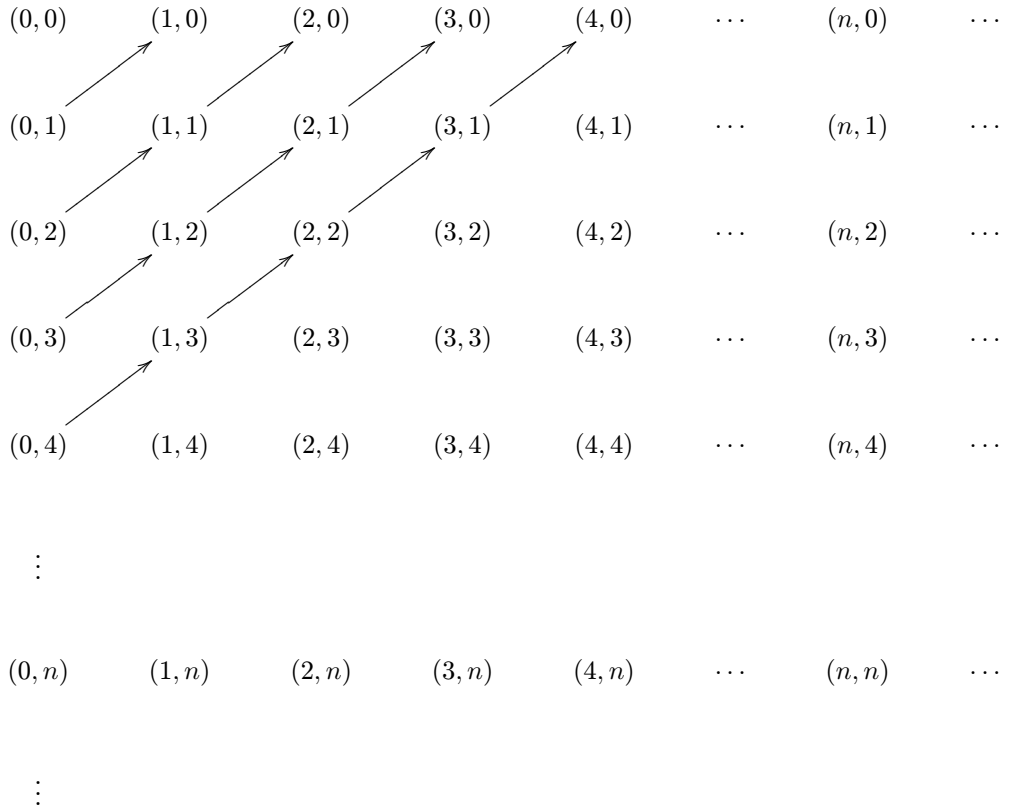
Príklad 6.24 (Príklad nespočítateľnej množiny)**.** Označme $P = {}^{\mathbb{N}}\{0, 1\}$ množinu všetkých zobrazení $\mathbb{N} \to \{0, 1\}$, t.j. množinu všetkých nekonečných postupností s hodnotami 0, 1.
Ukážeme, že P je nespočítateľná. Sporom.
Nech P je spočítateľná. Pretože $P \neq \emptyset$, existuje surjektívne zobrazenie $f\colon \mathbb{N} \to P$, $n \mapsto f_n$. Pre každé $n \in \mathbb{N}$, f_n je zobrazenie $\mathbb{N} \to \{0, 1\}$ a postupnosť $\{f_n\}_{n=0}^{\infty}$ obsahuje všetky prvky množiny P. Definujme $g\colon \mathbb{N} \to \{0, 1\}$; $g(n) = 1 - f_n(n)$. Potom pre každé $n \in \mathbb{N}$ platí $g(n) \neq f_n(n)$ a preto $g \neq f_n$. Teda existuje $g \in P$ tak, že $f_n \neq g$ pre ľubovoľné $n \in \mathbb{N}$ a to je spor.

Veta 6.25.
a) *Ak $f\colon A \to B$ je injektívne zobrazenie a B je spočítateľná množina, tak aj A je spočítateľná množina.*
b) *Každá podmnožina spočítateľnej množiny je spočítateľná.*
c) *Ak $f\colon A \to B$ je surjektívne zobrazenie a A je spočítateľná, tak aj B je spočítateľná.*

Dôkaz. a) B je spočítateľná, a preto existuje injektívne zobrazenie $g\colon B \to \mathbb{N}$ (aj v prípade, že $B = \emptyset$). Zobrazenie $g \circ f\colon A \to \mathbb{N}$ je injektívne a podľa vety 6.23 A je spočítateľná.
b) Ak $A \subseteq B$, tak zobrazenie $f\colon A \to B$; $f(x) = x$ je injektívne a tvrdenie vyplýva z a).
c) Ak $A = \emptyset$, tak aj $B = \emptyset$ a teda je konečná.
Ak $A \neq \emptyset$ (tak aj $B \neq \emptyset$), podľa vety 6.23 existuje surjektívne zobrazenie $g\colon \mathbb{N} \to A$. Potom $f \circ g\colon \mathbb{N} \to B$ je surjektívne a preto B je spočítateľná □

Veta 6.26. $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, *t.j.* $\mathbb{N} \times \mathbb{N}$ *je nekonečná spočítateľná množina.*

Dôkaz.



Zobrazenie $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ je dané tak, že postupujeme po uhlopriečkach a usporiadaným dvojiciam postupne priraďujeme celé nezáporné čísla.

$(0,0) \mapsto 0$, $(0,1) \mapsto 1$, $(1,0) \mapsto 2$, $(0,2) \mapsto 3$, $(1,1) \mapsto 4$, $(2,0) \mapsto 5$, $(0,3) \mapsto 6$, $(1,2) \mapsto 7$, $(2,1) \mapsto 8$, $(3,0) \mapsto 9, \dots$

Takto dostaneme bijektívne zobrazenie $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Ak chceme vyjadriť toto zobrazenie predpisom, všimnime si, že usporiadané dvojice na jednej uhlopriečke majú rovnaký súčet zložiek. Pričom počet usporiadaných dvojíc na uhlopriečke, ktorá obsahuje usporiadanú dvojicu (k,l) je $k+l+1$. Teda počet usporiadaných dvojíc na všetkých uhlopriečkach, ktoré predchádzajú uhlopriečku, v ktorej sa nachádza dvojica (k,l) je $1+2+\cdots+(k+l)$. Ďalej, dvojica (k,l) je v uhlopriečke, v ktorej sa nachádza, na $(k+1)$-vom mieste. (Poradie je: $(0,k+1),(1,k+l-1),(2,k+l-2),\dots$) Teda

$$f(k,l) = 1+2+\cdots+(k+l)+k+1 = \frac{(k+l)(k+l+1)}{2} + k + 1.$$

O tomto zobrazení sa ľahko aj formálne overí, že je to bijektívne zobrazenie $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. □

Veta 6.27. *Zjednotenie spočítateľného systému spočítateľných množín je spočítateľná množina.*

Dôkaz. Nech $\mathcal{S}$ je spočítateľný systém spočítateľných množín. Ak $\mathcal{S} = \emptyset$ alebo $\mathcal{S} = \{\emptyset\}$, tak $\bigcup_{A\in\mathcal{S}} A = \emptyset$ a toto je spočítateľná množina.

Nech $\mathcal{S} \neq \emptyset$ a pre každé $A \in \mathcal{S}$ nech $A \neq \emptyset$. Pretože $\mathcal{S}$ je spočítateľná množina, $\mathcal{S} \neq \emptyset$, existuje zobrazenie $f\colon \mathbb{N} \to \mathcal{S}$; $f(n) = A_n$, ktoré je surjektívne (t.j. pre každé $A \in \mathcal{S}$ existuje $n \in \mathbb{N}$ tak, že $A = A_n$). Pre každé $n \in \mathbb{N}$ existuje surjektívne zobrazenie $g_n\colon \mathbb{N} \to A_n$. (Množina A_n je spočítateľná, $A_n \neq \emptyset$.) Zrejme $\bigcup_{A\in\mathcal{S}} A = \bigcup_{n\in\mathbb{N}} A_n$.

Definujme teraz zobrazenie $h\colon \mathbb{N}\times\mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n$; $h(k,n) = g_n(k)$. Ukážeme, že h je surjektívne.

Nech $a \in \bigcup_{n\in\mathbb{N}} A_n$. Potom existuje $n \in \mathbb{N}$ tak, že $a \in A_n$. Pretože $g_n\colon \mathbb{N} \to A_n$ je surjektívne, existuje $k \in \mathbb{N}$ tak, že $g_n(k) = a$. Potom $h(n,k) = g_n(k) = a$, t.j. existuje $(n,k) \in \mathbb{N}\times\mathbb{N}$ tak, že $h(n,k) = a$. Pretože $\mathbb{N}\times\mathbb{N}$ je spočítateľná a h je surjektívne, je aj množina $\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{A\in\mathcal{S}} A$ spočítateľná. □

Veta 6.28. *Ak A, B sú spočítateľné množiny, tak aj $A \times B$ je spočítateľná množina.*

Dôkaz. Ak $A = \emptyset$ alebo $B = \emptyset$, tak $A \times B = \emptyset$, a teda je spočítateľná.

Nech $A \neq \emptyset$ aj $B \neq \emptyset$. Potom existujú surjektívne zobrazenia $f\colon \mathbb{N} \to A$, $g\colon \mathbb{N} \to B$. Definujme zobrazenie $h\colon \mathbb{N}\times\mathbb{N} \to A \times B$; $h(n,k) = (f(n), g(k))$. Zrejme h je surjektívne, lebo ak $(a,b) \in A \times B$, tak $a \in A$ a existuje $n \in \mathbb{N}$ tak, že $f(n) = a$, $b \in B$ a existuje $k \in \mathbb{N}$ tak, že $g(k) = b$. Potom

$$h(n,k) = (f(n), g(k)) = (a,b).$$

Pretože $\mathbb{N}\times\mathbb{N}$ je spočítateľná, je aj $A \times B$ spočítateľná. □

Dôsledok 6.29. *Ak $A_1, \ldots, A_k$ sú spočítateľné množiny a $k \in \mathbb{N}_1$, tak $A_1 \times \cdots \times A_k$ je spočítateľná množina.*

Príklad 6.30. Ukážte, že množina $\mathbb{Q}$ všetkých racionálnych čísel je spočítateľná.

Riešenie: Vieme, že množina $\mathbb{Z}$ všetkých celých čísel aj množina $\mathbb{N}_1$ všetkých prirodzených čísel je spočítateľná. Potom aj $\mathbb{Z}\times\mathbb{N}_1$ je spočítateľná množina.

Zobrazenie $f\colon \mathbb{Z}\times\mathbb{N}_1 \to Q$; $h(z,k) = \frac{z}{k}$, je zrejme surjektívne, a preto $\mathbb{Q}$ je spočítateľná.

Príklad 6.31. Ukážte, že množina $\mathbb{R}$ všetkých reálnych čísel je nespočítateľná.

Riešenie: Najprv ukážeme, že množina $\langle 0,1\rangle = \{r \in \mathbb{R} : 0 \leq r \leq 1\}$ je nespočítateľná.

Sporom. Predpokladajme, že $\langle 0,1\rangle$ je spočítateľná. Potom existuje surjektívne zobrazenie $f\colon \mathbb{N} \to \langle 0,1\rangle$, $f(k) = r_k$. Teda $\langle 0,1\rangle = \{r_k; k \in \mathbb{N}\}$.

Teraz budeme definovať indukciou dve postupnosti, $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ tak, že pre každé $n \in \mathbb{N}$

$$0 \leq a_n < b_n \leq 1,$$
$$b_n - a_n = \frac{1}{3^n},$$
$$r_n \notin \langle a_n, b_n\rangle.$$

Rozdeľme interval $\langle 0,1\rangle$ na tri intervaly rovnakej dĺžky: $\langle 0, \frac{1}{3}\rangle$, $\langle \frac{1}{3}, \frac{2}{3}\rangle$, $\langle \frac{2}{3}, 1\rangle$. Vyberme ten z nich, ktorý neobsahuje r_0 a označme ho $\langle a_0, b_0\rangle$. Zrejme $0 \leq a_0 < b_0 \leq 1$, $b_0 - a_0 = \frac{1}{3}$, $r_0 \notin \langle a_0, b_0\rangle$.

Predpokladajme, že už máme definovaný interval $\langle a_n, b_n\rangle$ tak, že $0 \leq a_n < b_n \leq 1$, $b_n - a_n = \frac{1}{3^n}$, $r_n \notin \langle a_n, b_n\rangle$. Rozdelíme tento interval na tri intervaly rovnakej dĺžky: $\langle a_n, a_n + \frac{1}{3^{n+1}}\rangle$, $\langle a_n + \frac{1}{3^{n+1}}, a_n + \frac{2}{3^{n+1}}\rangle$, $\langle a_n + \frac{2}{3^{n+1}}, b_n\rangle$. Vyberme ten z nich, ktorý neobsahuje r_{n+1} a označme ho $\langle a_{n+1}, b_{n+1}\rangle$. Potom platí

$$0 \leq a_n \leq a_{n+1} < b_{n+1} \leq b_n \leq 1,$$
$$b_{n+1} - a_{n+1} = \frac{1}{3^{n+1}},$$
$$r_{n+1} \notin \langle a_{n+1}, b_{n+1}\rangle.$$

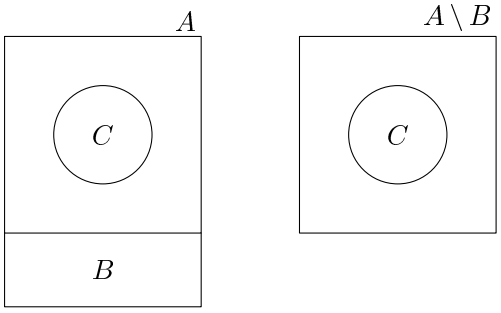
Tým sú postupnosti $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ definované.

Pretože pre každé $n \in \mathbb{N}$ platí $a_n \leq a_{n+1} \leq 1$, postupnosť $\{a_n\}_{n=1}^{\infty}$ je neklesajúca zhora ohraničená postupnosť, a teda existuje limita $\lim_{n\to\infty} a_n = c$. Pre každé $n \in \mathbb{N}$ platí $a_n \leq c$.

Pretože $\lim_{n\to\infty}(b_n - a_n) = \lim_{n\to\infty} \frac{1}{3^n} = 0$,

$$\lim_{n\to\infty} b_n = \lim_{n\to\infty}(a_n + (b_n - a_n)) = c + 0 = c,$$

a pretože pre každé $n \in \mathbb{N}$ platí $b_{n+1} \leq b_n$, dostávame, že $c \leq b_n$ pre všetky $n \in \mathbb{N}$.



Obr. 2. Ilustrácia k dôkazu lemy 6.34

Teda pre každé $n \in \mathbb{N}$

$$a_n \leq c \leq b_n.$$

Pretože $c \in \langle 0,1\rangle$ ($\langle a_n, b_n\rangle \subseteq \langle 0,1\rangle$ pre každé $n \in \mathbb{N}$), existuje $k \in \mathbb{N}$ tak, že $c = r_k$. Potom ale $r_k = c \in \langle a_k, b_k\rangle$ a súčasne, z definície postupností $\{a_n\}_{n=1}^{\infty}$ a $\{b_n\}_{n=1}^{\infty}$ vyplýva, že $r_k \notin \langle a_k, b_k\rangle$, čo je spor.

Teda $\langle 0,1\rangle$ je nespočítateľná množina, a pretože $\langle 0,1\rangle \subseteq \mathbb{R}$, dostávame, že $\mathbb{R}$ je nespočítateľná množina. (Ak by $\mathbb{R}$ bola spočítateľná, tak podľa vety 6.25b) aj množina $\langle 0,1\rangle$ by bola spočítateľná.)

Veta 6.32. *Každá nekonečná množina A obsahuje nekonečnú spočítateľnú podmnožinu.*

Dôkaz. Definujme $f\colon \mathbb{N} \to A$ nasledovne: Pretože A je nekonečná, $A \neq \emptyset$ a môžeme vybrať $a_0 \in A$. Položme $f(0) = a_0$.

Nech $n > 0$ a pre všetky $k \in \mathbb{N}$, $k < n$ je $f(k) \in A$ (jednoznačne) definované. Potom množina $B = \{f(k); k < n\}$ je konečná podmnožina množiny A (zobrazenie $g\colon n \to B$; $g(k) = f(k)$, je surjektívne a n je konečná množina). Preto $B \neq A$ a môžeme vybrať prvok $a_n \in A \setminus B$. Položme $f(n) = a_n$. Týmto je zobrazenie f (jednoznačne) definované. (Nech $D = \{n \in \mathbb{N} : f(n)$ nie je definované$\} \neq \emptyset$. Potom D má najmenší prvok p a $p > 0$. Pre všetky $k \in \mathbb{N}$, $k < p$ je $f(k)$ definované, a teda je definované aj $f(p)$. Potom $p \notin D$ a to je spor.)

Z definície zobrazenia f je zrejmé, že f je prosté zobrazenie $\mathbb{N} \to A$. Potom zrejme $\mathbb{N} \sim f[\mathbb{N}] = \{f(k); k \in \mathbb{N}\} \subseteq A$ a podmnožina $f[\mathbb{N}]$ množiny A je nekonečná spočítateľná. □

Cvičenie 6.33. Nech A je nekonečná množina a $B \subseteq A$ je konečná množina. Dokážte, že $A \setminus B \sim A$.

Riešenie: Množina $A \setminus B$ je nekonečná. (Ak by $A \setminus B$ bola konečná, tak $A = (A \setminus B) \cup B$ by bola konečná.) Preto existuje nekonečná spočítateľná množina $C \subseteq A \setminus B$. Množina $C \cup B$ je nekonečná spočítateľná podmnožina množiny A. Pretože C aj $C \cup B$ sú nekonečné spočítateľné, existuje bijektívne zobrazenie $g\colon C \to C \cup B$ ($C \cap B = \emptyset$). Zrejme

$$(A \setminus B) \setminus C = A \setminus (C \cup B) = D.$$

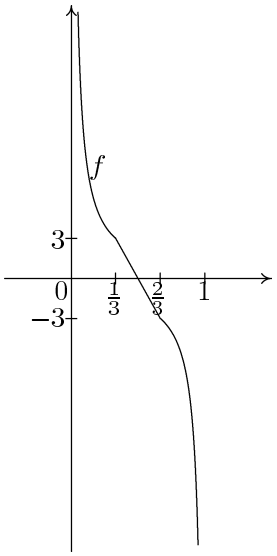
Teda $A \setminus B = C \cup D$, $C \cap D = \emptyset$ a $A = (C \cup B) \cup D$, $(C \cup B) \cap D = \emptyset$. Potom zobrazenie $f\colon A \setminus B \to A$

$$f(x) = \begin{cases} g(x) & \text{pre všetky } x \in C, \\ x & \text{pre všetky } x \in D. \end{cases}$$

je bijektívne, a teda $A \setminus B \sim A$

Podobne sa dokáže:

Lema 6.34. *Ak A je nespočítateľná množina a $B \subseteq A$ je spočítateľná, tak $A \sim A \setminus B$.*



Obr. 3. Príklad bijekcie medzi $(0,1)$ a $\mathbb{R}$

Dôkaz. Množina $A \setminus B$ je nespočítateľná (v opačnom prípade by A bola spočítateľná). Potom existuje nekonečná spočítateľná podmnožina $C \subseteq A \setminus B$. Množina $B \cup C$ je nekonečná spočítateľná, a preto $B \cup C \sim C$, a teda existuje bijektívne zobrazenie $g\colon B \cup C \to C$. Platí

$$A \setminus (B \cup C) = (A \setminus B) \setminus C = D.$$

Potom $A = B \cup C \cup D$, $D \cap (B \cup C) = \emptyset$, $A \setminus B = C \cup D$, $C \cap D = \emptyset$. Zobrazenie $f\colon A \to A \setminus B$; $f(x) = g(x)$ pre $x \in B \cup C$ a $f(x) = x$ pre $x \in D$ je bijektívne a $A \sim A \setminus B$. □

Dôsledok 6.35. $\mathbb{R} \sim \mathbb{R} \setminus \mathbb{Q}$, *t.j. množina všetkých iracionálnych čísel je nespočítateľná a ekvivalentná s* $\mathbb{R}$.

Príklad 6.36. Dokážte, že $\langle 0,1) \sim \mathbb{R}$.

Riešenie: Pretože $\{0\}$ je konečná podmnožina množiny $\langle 0,1)$, ktorá je nekonečná, $\langle 0,1\rangle \sim \langle 0,1) \setminus \{0\} = (0,1)$. Ukážeme, že $(0,1) \sim \mathbb{R}$. Zobrazenie $f\colon (0,1) \to \mathbb{R}$

$$f(x) = \begin{cases} \frac{1}{x} & \text{pre } 0 < x \leq \frac{1}{3}, \\ -18x + 9 & \text{pre } \frac{1}{3} < x < \frac{2}{3}, \\ \frac{1}{x-1} & \text{pre } \frac{2}{3} \leq x < 1, \end{cases}$$

je bijektívne, a teda $(0,1) \sim \mathbb{R}$. Pretože $\langle 0,1) \sim (0,1)$, máme $\langle 0,1) \sim \mathbb{R}$.

Príklad 6.37. a) Dokážte, že pre každé $n \in \mathbb{N}$ je množina $\mathcal{P}_n(\mathbb{N})$ všetkých n-prvkových podmnožín množiny $\mathbb{N}$ spočítateľná.

b) Dokážte, že množina $\mathcal{P}_{kon}(\mathbb{N})$ všetkých konečných podmnožín množiny $\mathbb{N}$ je spočítateľná.

c) Dokážte, že množina všetkých nekonečných podmnožín množiny $\mathbb{N}$ je ekvivalentná s $\mathcal{P}(\mathbb{N})$.

Literatúra

[B1] Lev Bukovský. *Teória množín (skriptum).* UPJŠ, Košice, 1980.
[B2] Lev Bukovský. *Množiny a všeličo okolo nich.* Alfa, Bratislava, 1985.
[BŠ] Bohuslav Balcar and Petr Štěpánek. *Teorie množin.* Academia, Praha, 2001.
[KM] K. Kuratowski and A. Mostowski. *Set theory, with an introduction to descriptive set theory.* North-Holland, Amsterdam, 1976. Studies in Logic and The Foundations of Mathematics.
[ŠS] Tibor Šalát and Jaroslav Smítal. *Teória množín.* UK, Bratislava, 1995.