

Přirozená čísla

Úvod

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

Definice.

- $0 = \emptyset$.
- $1 = 0^+ = 0 \cup \{0\} = \{0\}$.
- $2 = 1^+ = 1 \cup \{1\} = \{0, 1\}$.
- $3 = 2^+ = 2 \cup \{2\} = \{0, 1, 2\}$.
- $4 = 3^+ = 3 \cup \{3\} = \{0, 1, 2, 3\}$.

Důsledkem uvedených definic dostáváme:

- $0 \in 1 \in 2 \in 3 \in 4 \in 5 \in \dots$
- $0 \subseteq 1 \subseteq 2 \subseteq 3 \subseteq 4 \subseteq 5 \subseteq \dots$

Induktivní množiny

Připomeňme si

Axiom nekonečna. Existuje množina A taková, že jejím elementem je prázdná množina (tj. $\emptyset \in A$) a pro každé $x \in A$ platí $x^+ \in A$.

Definice. Množina I se nazývá **induktivní**, jestliže jsou splněny podmínky:

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

Definice. Množina n se nazývá **přirozeným číslem**, jestliže pro každou induktivní množinu I je $n \in I$.

Poznámky.

1. Množina $\emptyset$ je přirozeným číslem jak plyne z definice induktivní množiny.
2. Axiom nekonečna tvrdí, že existuje aspoň jedna induktivní množina.
3. Třída $\{x : x \text{ náleží do každé induktivní množiny}\}$ je množina v důsledku axiomu nekonečna.

Definice. Množina všech přirozených čísel se bude značit symbolem ω .

Poznámka. Platí tedy $n \in \omega \Leftrightarrow \forall I (I \text{ je induktivní} \Rightarrow n \in I)$.

Věta. Množina ω je induktivní množinou a je podmnožina každé induktivní množiny. Tudíž lze říci, že množina ω je nejmenší induktivní množinou.

Důkaz. (a) Ukažme, že množina ω je induktivní. Tedy ukažme, že

1. $\emptyset \in \omega$,
2. $(\forall a \in \omega)(a^+ \in \omega)$.

Protože pro každou induktivní množinu I je $\emptyset \in I$, plyne odsud, že $\emptyset \in \omega$. Dále předpokládejme, že $a \in \omega$. Potom z definice ω plyne, že pro každou induktivní množinu I je $a \in I$. Odtud pro každou induktivní množinu I platí, že $a^+ \in I$. Tedy $a^+ \in \omega$. Ukázali jsme, že ω je induktivní množinou. Nakonec zvolme libovolnou induktivní množinu I a ukažme, že $\omega \subseteq I$. Je-li $x \in \omega$, potom nutně $x \in I$. Tedy skutečně platí $\omega \subseteq I$. $\square$

Důsledek. Je-li $I \subseteq \omega$ induktivní množina, potom platí $I = \omega$.

Princip matematické indukce. Předpokládejme, že $P(n)$ je logická formule, kde n je tzv. volná (nekvantifikovaná) proměnná. Abychom nyní dokázali tvrzení

$$(\forall n \in \omega)P(n), \tag{1}$$

postupujeme podle následujícího schématu. Položíme $I = \{n \in \omega : P(n)\}$. Potom je zřejmě $I \subseteq \omega$. Pokud nyní dokážeme:

1. $0 \in I$,
2. $(\forall n \in \omega)(n \in I \Rightarrow n^+ \in I)$,

potom je množina I induktivní a tudíž $I = \omega$. To znamená, že platí tvrzení (1).

Jako ukázkou si dokažme následující tvrzení:

Věta. Pro každé $n \in \omega$ platí buď $n = 0$ nebo pro jisté $k \in \omega$ platí $n = k^+$.

Důkaz. Položme $I = \{n \in \omega : n = 0 \vee (\exists k \in \omega)(n = k^+)\}$. Potom zřejmě $0 \in I$. Necht' nyní $n \in I$. Z definice množiny plyne, že pak $n = 0$ nebo pro jisté $k \in \omega$ je $n = k^+$. Potom je buď $n^+ = 0^+$ nebo $n^+ = (k^+)^+$. V prvním případě protože $0 \in \omega$, je tudíž $n^+ = 0^+ \in I$. Ve druhém případě jelikož $k \in \omega$, je i $k^+ \in \omega$. Tudíž pak $n^+ = (k^+)^+ \in I$. Takto jsme dokázali, že je-li $n \in I$, potom je $n^+ \in I$, tj. dokázali jsme induktivnost množiny I . Z principu matematické indukce pak vyplývá dokazované tvrzení. $\square$

Definice. Množina A se nazývá **tranzitivní**, jestliže

$$(\forall a \in A)(a \subseteq A),$$

nebo

$$\forall a(a \in A \Rightarrow a \subseteq A).$$

tj. každý element množiny A je též její podmnožinou.

Tranzitivnost množiny A je vlastnost, kterou lze formulovat také takto:

$$(\forall x)(\forall y) (x \in y \in A \Rightarrow x \in A).$$

Příklad. (a) Množina $A = \emptyset$ je tranzitivní množinou.

(b) Množina $A = 1 = \{0\}$ je tranzitivní množinou.

(c) Množina $A = \{1\}$ není tranzitivní množinou!

Poznámka. Lze se snadno přesvědčit, že tranzitivnost množiny A je ekvivalentní vlastnosti

$$\bigcup A \subseteq A.$$

Věta. Jsou-li A, B množiny, potom platí

$$\bigcup(A \cup B) = (\bigcup A) \cup (\bigcup B).$$

Důkaz. Dokažte sami! $\square$

Řešení.

Abychom dokázali, že $\bigcup(A \cup B) = (\bigcup A) \cup (\bigcup B)$, musíme ukázat oboustrannou inkluzi.

1) Nejprve dokážeme, že $\bigcup(A \cup B) \subseteq (\bigcup A) \cup (\bigcup B)$:

Nechť $x \in \bigcup(A \cup B)$. To znamená, že existuje množina $C \in (A \cup B)$ taková, že $x \in C$.

Protože $C \in (A \cup B)$, platí buď $C \in A$ nebo $C \in B$.

- Pokud $C \in A$, pak $x \in C$ a $C \in A$, což znamená $x \in \bigcup A$. Proto $x \in (\bigcup A) \cup (\bigcup B)$.
- Pokud $C \in B$, pak $x \in C$ a $C \in B$, což znamená $x \in \bigcup B$. Proto $x \in (\bigcup A) \cup (\bigcup B)$.

V obou případech je $x \in (\bigcup A) \cup (\bigcup B)$, tedy $\bigcup(A \cup B) \subseteq (\bigcup A) \cup (\bigcup B)$.

2) Nyní dokážeme, že $(\bigcup A) \cup (\bigcup B) \subseteq \bigcup(A \cup B)$:

Nechť $x \in (\bigcup A) \cup (\bigcup B)$. To znamená, že buď $x \in \bigcup A$ nebo $x \in \bigcup B$.

- Pokud $x \in \bigcup A$, pak existuje množina $C \in A$ taková, že $x \in C$. Protože $C \in A$, platí také $C \in (A \cup B)$. Proto $x \in C$ a $C \in (A \cup B)$, což znamená $x \in \bigcup(A \cup B)$.
- Pokud $x \in \bigcup B$, pak existuje množina $D \in B$ taková, že $x \in D$. Protože $D \in B$, platí také $D \in (A \cup B)$. Proto $x \in D$ a $D \in (A \cup B)$, což znamená $x \in \bigcup(A \cup B)$.

V obou případech je $x \in \bigcup(A \cup B)$, tedy $(\bigcup A) \cup (\bigcup B) \subseteq \bigcup(A \cup B)$.

Protože jsme dokázali obě inkluze, $\bigcup(A \cup B) \subseteq (\bigcup A) \cup (\bigcup B)$ a $(\bigcup A) \cup (\bigcup B) \subseteq \bigcup(A \cup B)$, platí rovnost $\bigcup(A \cup B) = (\bigcup A) \cup (\bigcup B)$. $\square$

Věta. Je-li a tranzitivní množinou, potom $\bigcup(a^+) = a$.

Důkaz. Předpokládejme, že a je tranzitivní množinou. Potom

$$\begin{aligned}
\bigcup (a^+) &= \bigcup (a \cup \{a\}) \\
&= \bigcup a \cup \bigcup \{a\} \quad \text{podle předchozí věty} \\
&= (\bigcup a) \cup a \quad \text{protože } \bigcup \{a\} = a \\
&= a \quad \text{protože je } \bigcup a \subseteq a.
\end{aligned}$$

Tudíž platí $\bigcup (a^+) = a$. $\square$

Věta. Každé přirozené číslo je tranzitivní množinou.

Důkaz. Důkaz provedeme podle principu matematické indukce. Nejdříve položíme

$$I = \{n \in \omega : n \text{ je tranzitivní množinou}\}.$$

Je zřejmé, že pak je $0 \in I$ protože je $0 = \emptyset$. Necht' dále je $n \in I$. Potom je n tranzitivní množinou. Ukažme, že i následovník $n^+ = n \cup \{n\}$ je tranzitivní množinou. Nyní v důsledku předchozí věty máme $\bigcup n^+ = n$. Dále zřejmě $n \subseteq n^+$. Odtud tedy plyne, že $\bigcup n^+ \subseteq n^+$. To dokazuje tranzitivnost množiny n^+ (viz předchozí poznámka!) Potom tudíž je $n^+ \in I$. To dokazuje tranzitivnost množiny I a tvrzení věty pak plyne z principu matematické indukce. $\square$

Samostatné cvičení. Dokažte následující tvrzení. Zobrazení $\sigma : \omega \rightarrow \omega$ definované pro každé $n \in \omega$ předpisem $\sigma(n) = n^+$ je prostým zobrazením.

Věta. Množina všech přirozených čísel ω je tranzitivní množinou.

Důkaz. Provádět podrobně nebudeme. V podstatě stačí dokázat toto:

$$(\forall n \in \omega)(n \subseteq \omega).$$

Položíme $I = \{n \in \omega : n \subseteq \omega\}$ a dále postupujeme podle schématu uvedeném v principu matematické indukce. $\square$

Samostatné cvičení. Dokažte si, že platí následující tvrzení:

$$(\forall n \in \omega)(n \neq n^+).$$

Princip rekurze

Věta. Necht' A je množina a necht' $a \in A$. Dále necht' $f : A \rightarrow A$ je funkce. Potom existuje jediná funkce $h : \omega \rightarrow A$ taková, že

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

říkáme, že funkce h podmínkami 1. a 2. definována rekurentně.

Důkaz. Máme tedy dokázat, že existuje jediná funkce $h : \omega \rightarrow A$ splňující podmínky 1. a 2.

Důkaz si rozdělíme do dvou částí: důkaz existence a důkaz jednoznačnosti.

Existence.

Defujme binární relaci $R \subseteq \omega \times A$ následovně:

$\langle n, b \rangle \in R$ právě tehdy, když existuje konečná posloupnost $b_0, b_1, \dots, b_n$ prvků z A taková, že

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

Nyní dokažme matematickou indukci podle n následující tvrzení:

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

Základní krok indukce. Pro $n = 0$ chceme dokázat, že existuje právě jedna $b \in A$ taková, že $\langle 0, b \rangle \in R$. To plyne z toho, že pro $b = a$ máme $b_0 = a$. Jednoznačnost je zřejmá.

Hlavní krok indukce. Předpokládejme, že pro nějaké $k \in \omega$ existuje právě jedno $b_k \in A$ takové, že $\langle k, b_k \rangle \in R$. Ukažme, že pak existuje právě jedno $b_{k+1} \in A$ takové, že $\langle k+1, b_{k+1} \rangle \in R$.

Potřebujeme tedy dokázat existenci konečné posloupnosti $b_0, b_1, \dots, b_{k+1}$ prvků z A takové, že $b_0 = a$, $b_{i+1} = f(b_i)$ pro všechna $i = 0, 1, \dots, k$ a $b_{k+1} = b$. Podle indukčního předpokladu existuje $k+1$ členná posloupnost $b_0, b_1, \dots, b_k$ taková, že $b_0 = a$, $b_{i+1} = f(b_i)$ pro všechna $i = 0, 1, \dots, k-1$ a $b_k = b$. A b_k je určeno jednoznačně. Pokud nyní položíme $b = b_{k+1} = f(b_k)$, pak $\langle k+1, b_{k+1} \rangle \in R$ a element b je jediný element, pro který platí $\langle k+1, b_{k+1} \rangle \in R$.

Podle principu matematické indukce tedy pro každé $n \in \omega$ existuje právě jeden prvek $b \in A$ takový, že $\langle n, b \rangle \in R$. Tedy relace R je funkce na ω a $R \subseteq \omega \times A$. Označme $h = R$.

Overme, že h splňuje podmínky 1. a 2.:

1. $h(0) = a$ protože $\langle 0, a \rangle \in R$.
2. Pro každé $n \in \omega$ máme $h(n^+) = f(h(n))$ protože z konstrukce R vyplývá, že pokud $\langle n, b \rangle \in R$, pak $\langle n^+, f(b) \rangle \in R$. Jelikož $h(n) = b$ a $h(n^+) = f(b)$, máme $h(n^+) = f(h(n))$.

Existuje tedy funkce $h : \omega \rightarrow A$ splňující podmínky 1. a 2.

Jednoznačnost

Předpokládejme, že existují dvě funkce $h_1, h_2 : \omega \rightarrow A$ splňující:

1. $h_1(0) = h_2(0) = a$,
2. $h_1(n^+) = f(h_1(n))$ a $h_2(n^+) = f(h_2(n))$ pro všechna $n \in \omega$.

Dokažme matematickou indukci podle n následující tvrzení:

$$(\forall n \in \omega)(h_1(n) = h_2(n)).$$

- **Základní krok indukce.** Pro $n = 0$ máme $h_1(0) = h_2(0) = a$. Tedy $h_1(0) = h_2(0)$.
- **Hlavní krok indukce.** Předpokládejme, že pro nějaké $k \in \omega$ platí $h_1(k) = h_2(k)$.

Příklad. Uvažujme funkci $f : \mathbb{R} \rightarrow \mathbb{R}$ danou předpisem $f(x) = x + d$, kde $d \in \mathbb{R}$ je daná konstanta. Dále necht' je dáno $a \in \mathbb{R}$. Nyní podle principu rekurze existuje jediná funkce $h : \omega \rightarrow \mathbb{R}$ taková, že $h(0) = a$ a pro každé $n \in \omega$ je $h(n+1) = h(n^+) = f(h(n)) = h(n) + d$. Funkce je jak je vidět reálnou posloupností, která se nazývá **aritmetickou posloupností s diferencí d** .

Samostatné cvičení. Aplikujte větu o rekurzi podobným způsobem a dokažte existenci tzv. geometrické posloupnosti s kvocientem q .

Peanovy axiomy

Italský matematik [Giuseppe Peano](#) ve své knize z roku 1889 publikoval systém axiomů definující množinu přirozených čísel na jejichž základě je možné rozvinout teorii přirozených čísel a následně zavést další číselné množiny jako je množina celých, racionálních a reálných čísel.

Nejdříve přešleme následující definici:

Definice. Necht' N je množina, $S : N \rightarrow N$ a necht' $A \subseteq N$. Řekneme, že množina A je **uzavřená vzhledem k funkci S** , jestliže pro všechna $x \in A$ platí $S(x) \in A$.

Definice uspořádané trojice. Mějme dány tři množiny x, y, z . Potom definujeme:

$$\langle x, y, z \rangle := \langle \langle x, y \rangle, z \rangle.$$

Definice. Uspořádanou trojici $\langle N, S, e \rangle$, kde N je množina, $S : N \rightarrow N$ je funkce a $e \in N$ nazveme **Peanovým systémem**, jsou-li splněny následující podmínky:

1. $e \notin \text{ran}(S)$.
2. S je prostá funkce.
3. Pro všechna $A \subseteq N$ jestliže $e \in A$ a množina A je uzavřená vůči funkci S , pak platí $A = N$.

Třetí axiom se nazývá **axiom matematické indukce**.

Pokud budeme uvažovat funkci $\sigma : \omega \rightarrow \omega$ definovanou předpisem: $\sigma(n) = n^+$ pro všechna $n \in \omega$, pak platí následující

Věta. Uspořádaná trojice $\langle \omega, \sigma, 0 \rangle$ tvoří Peanův systém.

Důkaz. Proved'te jako samostatné cvičení. $\square$

Aritmetika na množině ω

Věta. Necht' $g : \omega \rightarrow \omega$ a $f : \omega \times \omega \rightarrow \omega$ jsou dané funkce. Potom existuje jediná funkce $h : \omega \times \omega \rightarrow \omega$ taková, že pro každé $m \in \omega$ platí:

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

Důkaz. Z předpokladů plyne s ohledem na princip rekurze, že pro každé $m \in \omega$ existuje jediná funkce $p_m : \omega \rightarrow \omega$ taková, že

$$(a) \ p_m(0) = g(m),$$

$$(b) \ p_m(n^+) = f(p_m(n), m), \text{ pro všechna } n \in \omega.$$

Takto je definována funkce q jejíž definičním oborem je množina ω a pro nichž platí pro každé $m \in \omega$, $q(m) = p_m$. Konečně lze definovat funkci $h : \omega \times \omega \rightarrow \omega$ předpisem: $h(m, n) = q(m)(n) = p_m(n)$ pro každé $n, m \in \omega$. Funkce h nyní splňuje podmínky 1. a 2. a je určena jednoznačně. $\square$

Definice. Necht' $A : \omega \times \omega \rightarrow \omega$ je jednoznačně definovaná funkce splňující podmínky:

1. $A(m, 0) = m$,
2. $A(m, n^+) = A(m, n)^+$

pro všechna $m, n \in \omega$. Funkci A pak nazveme **součtem**. Následně budeme definovat binární operaci "+" na množině ω vztahem

$$m + n = A(m, n)$$

pro všechna $m, n \in \omega$.

Okamžitým důsledkem definice součtu přirozených čísel je následující tvrzení:

Věta. Pro všechna přirozená čísla m, n platí:

$$(A1) \ m + 0 = m,$$

$$(A2) \ m + n^+ = (m + n)^+.$$

Důsledek. Pro všechna $m \in \omega$ platí $m + 1 = m^+$.

Důkaz. Necht' $m \in \omega$. Protože $1 = 0^+$, dostaneme:

$$m + 1 = m + 0^+ \tag{1}$$

$$= (m + 0)^+ \text{ díky vlastnosti (A2)} \tag{2}$$

$$= m^+ \text{ díky vlastnosti (A1)} \tag{3}$$

a tudíž máme: $m + 1 = m^+$. $\square$

Příklad. Ukažme, že $2 + 2 = 4$.

Řešení.

$$2 + 2 = 2 + 1^+ \text{ protože platí: } 2 = 1^+ \quad (4)$$

$$= (2 + 1)^+ \text{ díky vlastnosti (A2)} \quad (5)$$

$$= (2^+)^+ \quad (6)$$

$$= (3)^+ \text{ protože } 2^+ = 3 \quad (7)$$

$$= 4. \quad (8)$$

□

Definice. Necht' $M : \omega \times \omega \rightarrow \omega$ je jednoznačně definovaná funkce splňující vlastnosti:

$$1. M(m, 0) = 0,$$

$$2. M(m, n^+) = M(m, n) + m$$

pro všechna $m, n \in \omega$. Funkci M pak nazveme **součinem**. Následně budeme definovat binární operaci na množině ω vztahem

$$m \cdot n = M(m, n)$$

pro všechna $m, n \in \omega$.

Věta. Pro všechna přirozená čísla m, n platí:

$$(M1) m \cdot 0 = 0,$$

$$(M2) m \cdot n^+ = m \cdot n + m.$$

Důkaz. Je zřejmým důsledkem definice součinu. □

Věta (Asociativní zákon pro sčítání). Pro všechna přirozená čísla m, n a p platí:

$$m + (n + p) = (m + n) + p.$$

Důkaz. Důkaz provedme matematickou indukci podle p . Nejdříve zvolme libovolně přirozená čísla m, n a položme

$$I = \{p \in \omega : m + (n + p) = (m + n) + p\}.$$

(i) Ukažme, že $0 \in I$.

$$m + (n + 0) = m + n \text{ plyne z (A1)} \quad (9)$$

$$= (m + n) + 0 \text{ plyne opět z (A1)}. \quad (10)$$

Tedy $0 \in I$.

(ii) Předpokládejme, že $p \in I$ a ukažme, že pak $p^+ \in I$.

$$m + (n + p^+) = m + (n + p)^+ \text{ v důsledku vlastnosti (A2)} \quad (11)$$

$$= [m + (n + p)]^+ \text{ v důsledku vlastnosti (A2)} \quad (12)$$

$$= [(m + n) + p]^+ \text{ neboť } p \in I \quad (13)$$

$$= (m + n) + p^+ \text{ v důsledku vlastnosti (A2)}. \quad (14)$$

Ukázali jsme tedy, že $m + (n + p^+) = (m + n) + p^+$ a tudíž $p^+ \in I$. Dokázali jsme, že I je induktivní podmnožinou množiny ω a tedy $I = \omega$. □

Věta (Komutativní zákon pro sčítání). Pro každé $m, n \in \omega$ platí

$$m + n = n + m.$$

Důkaz. Přecháme jako problém pro samostatnou přípravu. $\square$

Věta (Distributivní zákon). Pro každé $m, n, p \in \omega$ platí

$$m \cdot (n + p) = m \cdot n + m \cdot p.$$

Důkaz (náznak). Zvolme libovolně přirozená čísla m a n . Dále položme

$$I = \{p \in \omega : m \cdot (n + p) = m \cdot n + m \cdot p\}.$$

Nyní se dokáže, že množina I je induktivní množinou odkud plyne $I = \omega$. $\square$

Věta (Asociativní zákon pro násobení). Pro každé $m, n, p \in \omega$ platí

$$m \cdot (n \cdot p) = (m \cdot n) \cdot p.$$

Důkaz. Důkaz provedme matematickou indukcí podle p . Nejdříve zvolme libovolně přirozená čísla m, n a položme

$$I = \{p \in \omega : m \cdot (n \cdot p) = (m \cdot n) \cdot p\}.$$

Ukažme, že množina I je induktivní množinou. (i) Ukažme, že $0 \in I$.

$$m \cdot (n \cdot 0) = m \cdot 0 \quad \text{plyne z (M1)} \quad (15)$$

$$= 0 \quad \text{plyne z (M1)} \quad (16)$$

$$= (m \cdot n) \cdot 0 \quad \text{plyne z (M1)}. \quad (17)$$

Tedy $0 \in I$. (ii) Předpokládejme, že $p \in I$ a ukažme, že pak $p^+ \in I$.

$$m \cdot (n \cdot p^+) = m \cdot (n \cdot p + n) \quad \text{v důsledku vlastnosti (M2)} \quad (18)$$

$$= m \cdot (n \cdot p) + m \cdot n \quad (19)$$

$$= (m \cdot n) \cdot p + m \cdot n \quad \text{neboť } p \in I \quad (20)$$

$$= (m \cdot n) \cdot p^+ \quad \text{v důsledku vlastnosti (M2)}. \quad (21)$$

Tudíž platí: $m \cdot (n \cdot p^+) = (m \cdot n) \cdot p^+$ a tedy $p^+ \in I$. Dokázali jsme, že I je induktivní podmnožinou množiny ω a tedy $I = \omega$. $\square$

Věta (Komutativní zákon pro násobení). Pro každé $m, n \in \omega$ platí $m \cdot n = n \cdot m$.

Důkaz. Přecháme jako problém pro samostatnou přípravu. $\square$

Definice mocniny. Necht' $E : \omega \times \omega \rightarrow \omega$ je je jednoznačně definovaná funkce, která pro každé $m, n \in \omega$ přiřazuje číslo $E(m, n) \in \omega$ takové, že

$$1. E(m, 0) = 1 \text{ a}$$

$$2. E(m, n^+) = E(m, n) \cdot m.$$

Funkci E nazýváme **mocninovou funkcí** a číslo $E(m, n)$ se nazývá **mocnina čísla m s exponentem n** . Zavedme označení: $m^n = E(m, n)$ pro každé $m, n \in \omega$.

Je možné dokázat následující větu.

Věta (Mocnina čísla m s exponentem n). Pro každé $m, n \in \omega$ platí:

$$(E1) m^0 = 1,$$

$$(E2) m^{n^+} = m^n \cdot m.$$

Uspořádání množiny ω

Definice. Řekneme, že přirozené číslo m je **menší než** přirozené číslo n , právě tehdy, když $m \in n$.

Tvrzení. Necht' n je přirozené číslo. Pak

1. jestliže $k \in n$, pak $k \subseteq n$,
2. jestliže $a \in k$ a $k \in n$, pak $a \in n$.
3. jestliže $k \in \omega$, pak $k \subseteq \omega$.
4. jestliže $a \in k$ a $k \in \omega$, pak $a \in \omega$.

Důkaz. Uvedené vlastnosti plynou z toho, že každé přirozené číslo n je tranzitivní množinou a množina ω je též tranzitivní množina. $\square$

Cvičení. Bez použití axiomu regularity dokažte, že pro každé $n \in \omega$ platí $n \notin n$.

(**Návod.** Důkaz proveďte pomocí principu matematické indukce.

1. Definujte množinu $I = \{n \in \omega : n \notin n\}$. Cílem je ukázat, že $I = \omega$.
2. Ukažte, že $0 \in I$. (Využijte toho, že $0 = \emptyset$.)
3. Předpokládejte, že pro nějaké $k \in \omega$ platí $k \in I$ (tj. $k \notin k$). Dokažte, že pak také $k^+ \in I$ (tj. $k^+ \notin k^+$).
4. Pro důkaz kroku 3 postupujte sporem. Předpokládejte, že $k^+ \in k^+$. Protože $k^+ = k \cup \{k\}$, musí platit buď $k^+ \in k$ nebo $k^+ = k$.
5. Ukažte, že oba případy vedou ke sporu s indukčním předpokladem $k \notin k$. Využijte faktu, že přirozená čísla jsou tranzitivní množiny (tj. pokud $x \in k$, pak $x \subseteq k$).

)

Definice. Pro každé $m, n \in \omega$ píšeme $m \subseteq n$ právě tehdy, když $m \in n$ nebo $m = n$.

Věta (Trichotomie). Pro každé $m, n \in \omega$ platí právě jedna z následujících podmínek:

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

Důkaz. Provádět jej nebudeme. $\square$

Cvičení. Dokažte, že pro každé $m, n \in \omega$ platí:

$$m \in n \iff m \subset n.$$

Cvičení. Předpokládejme, že $n, a \in \omega$. Ukažte, že jestliže $n \in a$, potom $n^+ \subseteq a$.

Věta. Uspořádaná dvojice $(\omega, \subseteq)$ je lineárně uspořádaná množina.

Náznak důkazu. Je třeba ověřit, že relace $\subseteq$ na množině ω je reflexivní, antisymetrická, tranzitivní a že platí trichotomie.

1. **Reflexivita:** Pro každé $n \in \omega$ platí $n = n$, tedy $n \subseteq n$.

2. **Antisymetrie:** Necht' $m \subseteq n$ a $n \subseteq m$. Pokud $m \neq n$, pak musí platit $m \in n$ a $n \in m$. To by ale znamenalo $m \in n$ a $n \in m$. Protože ω je tranzitivní a $n \in \omega$, platí $n \subseteq \omega$. Protože $m \in n$, je i $m \in \omega$. Protože m je tranzitivní, z $n \in m$ plyne $n \subseteq m$. Podobně z $m \in n$ plyne $m \subseteq n$. Pokud $m \in n$ a $n \in m$, pak $m \subseteq n$ a $n \subseteq m$, což implikuje $m = n$. To je spor s předpokladem $m \neq n$. Tedy musí platit $m = n$. (Alternativně lze využít $n \notin n$ a tranzitivitu $\in$).

3. **Tranzitivita:** Necht' $k \subseteq m$ a $m \subseteq n$.

- Pokud $k = m$ a $m = n$, pak $k = n$, tedy $k \subseteq n$.
- Pokud $k = m$ a $m \in n$, pak $k \in n$, tedy $k \subseteq n$.
- Pokud $k \in m$ a $m = n$, pak $k \in n$, tedy $k \subseteq n$.
- Pokud $k \in m$ a $m \in n$. Protože n je přirozené číslo, je tranzitivní. Tedy z $k \in m \in n$ plyne $k \in n$. Tedy $k \subseteq n$.

4. **Linearita (Trichotomie):** Pro libovolné $m, n \in \omega$ podle Věty o trichotomii platí právě jedna z možností: $m \in n$ (tj. $m < n$), $m = n$, nebo $n \in m$ (tj. $n < m$). To znamená, že platí buď $m \subseteq n$ nebo $n \subseteq m$.

□

Věta (Princip dobrého uspořádání). Necht' A je neprázdna podmnožina množiny ω . Pak v množině A existuje nejmenší prvek. To znamená, že existuje element $a \in A$ takový, že pro každé $b \in A$ platí $a \subseteq b$.

Důkaz. Necht' A je neprázdna podmnožina množiny ω . Sporem předpokládejme, že množina A nemá nejmenší prvek. Nyní položme

$$I = \{n \in \omega : n \subseteq a \text{ pro každé } a \in A\}.$$

Protože podle předpokladu v množině A neexistuje nejmenší prvek, je

$$I \cap A = \emptyset. \quad (*)$$

Ukažme, že I je induktivní množinou.

(i) Ukažme, že $0 \in I$. Za tím účelem dokažme:

$$0 \subseteq m \text{ pro každé } m \in \omega. \quad (**)$$

Položme $J = \{m \in \omega : 0 \subseteq m\}$. Dokažme nyní, že J je induktivní množinou. Je zřejmé, že $0 \in J$. Dále předpokládejme, že $m \in J$, tj. $0 \subseteq m$. Pak je buď $m = 0$ nebo $0 \in m$. V prvním případě neboť z definice následovníka plyne $m \in m^+$. A tedy $0 \in m^+$. V druhém případě je současně $0 \in m$ a $m \in m^+$. Tedy $0 \in m^+$. Tudíž v obou případech

platí $0 \in m^+$. To znamená, že $m^+ \in J$. Tedy J je induktivní množinou a tedy $J = \omega$.
Dokázali jsme tedy platnost tvrzení (**).

Z tvrzení (**) plyne, že pro každé $a \in A$ platí $0 \in a$. To znamená, že $0 \in I$.

(ii) Nyní předpokládejme, že pro nějaké $n \in \omega$ platí $n \in I$ a ukažme, že pak $n^+ \in I$.
Podle předpokladu tedy platí $n \in a$ pro každé $a \in A$. Podle výše uvedeného cvičení pak pro každé $a \in A$ platí $n^+ \in a$. Tedy $n^+ \in I$. Dokázali jsme tedy, že I je induktivní množinou. Tedy $I = \omega$.

Tedy existuje $n \in \omega$ takové, že $n \in A$. To je v rozporu s tvrzením (*). Tedy předpoklad, že množina A nemá nejmenší prvek, je nepravdivý. $\square$

Označení. Necht' $m, n \in \omega$. Potom pokud je m menší než n , píšeme $m < n$. Pokud je m menší nebo rovno n , píšeme $m \leq n$. Tj. pro $m, n \in \omega$ platí:

$$m < n \iff m \in n,$$

a

$$m \leq n \iff m \subseteq n.$$