Přirozená čísla pěkně přirozeně

Lenka Macálková

Hutník 2011

28.8.-3.9.2011

Začínáme

Definice

Množinu $\mathcal{N}$ nazveme množinou přirozených čísel a každý její prvek přirozeným číslem, jestliže ke každému prvku $x \in \mathcal{N}$ je přiřazen prvek $\overline{x} \in \mathcal{N}$ (který nazýváme následník prvku x) tak, že platí:

1. Existuje jeden prvek množiny $\mathcal{N}$, který není následníkem žádného prvku z $\mathcal{N}$ (budeme jej značit $1_{\mathbb{N}} = 1$)
2. Pro $\forall\, x, y \in \mathcal{N} : \overline{x} = \overline{y} \Longrightarrow x = y$
3. Nechť $\mathcal{M} \subseteq \mathcal{N}$ má následující vlastnosti:
   1. $1 \in \mathcal{M}$,
   2. $x \in \mathcal{M} \Longrightarrow \overline{x} \in \mathcal{M}$.

   Pak $\mathcal{M} = \mathcal{N}$.

- v teorii množin se ukazuje, že tato množina opravdu existuje. Je to množina kardinálních čísel konečných neprázdných množin.
- ukážeme (důkaz časem), že tato množina je určena jednoznačně

Věta

Nechť $x, y \in \mathcal{N}$. Pak platí:

1. $x \neq y \Longrightarrow \overline{x} \neq \overline{y}$
2. $x \neq \overline{x}$
3. $x \neq 1 \Longrightarrow \exists u \in \mathcal{N} : x = \overline{u}$

Důkaz

1. Z 2. části definice
2. Indukcí. $\mathcal{M} = \{z \in \mathcal{N} | z \neq \overline{z}\}$. Podle 1. z definice $1 \in \mathcal{M}$. Buď $x \in \mathcal{M}$, $\overline{x} \notin \mathcal{M}$. Pak $\overline{x} = \overline{\overline{x}}$, dle definice je pak $x = \overline{x}$, spor.
3. Indukcí. Stačí položit $\mathcal{M} = \{z \in \mathcal{N} | \exists v \in \mathcal{N}, \overline{v} = z\} \cup \{1\}$.

Věta

Na množině $\mathcal{N}$ existuje právě jedna operace $+$ taková, že pro každé $x, y \in \mathcal{N}$ platí:

1. $x + 1 = \overline{x}$,
2. $x + \overline{y} = \overline{x + y}$

   Dále pro tuto operaci a každé $x, y \in \mathcal{N}$ platí:
3. $1 + x = \overline{x}$,
4. $\overline{x} + y = \overline{x + y}$

Idea důkazu

Indukcí. $\mathcal{M}$ je množina $x \in \mathcal{N}$, pro které existuje zobrazení $f_x : \mathcal{N} \to \mathcal{N}$ tak, že

$$f_x(1) = \overline{x}, f_x(\overline{y}) = \overline{f_x(y)}$$

Věta

$(\mathcal{N}, +)$ je komutativní pologrupa, ve které platí zákony o odečítání, tj.
$\forall x, y, z \in \mathcal{N} : x + y = y + z \Longrightarrow x = z$

Idea důkazu

Indukce.
Asociativita: $\mathcal{M} = \{z \in \mathcal{N} | (x + y) + z = x + (y + z)\}$.
Komutativita: $\mathcal{M} = \{y \in \mathcal{N} | x + y = y + x\}$
Zákony o odečítání: Zvolíme pevně $y \neq z$ a položíme
$\mathcal{M} = \{x \in \mathcal{N} | x + y \neq x + z\}$

Věta

Pro $\forall x, y \in \mathcal{N}$ platí, že $x \neq x + y$

Důkaz

Plyne ze zákona odečítání.

Věta

Nechť $x, y \in \mathcal{N}$. Pak nastane právě jedna z následujících možností:

1. $x = y$,
2. $\exists u \in \mathcal{N} : x = y + u$
3. $\exists u \in \mathcal{N} : y = x + u$

Idea důkazu

Nechť $\mathcal{M}_x = \{y \in \mathcal{N} | \text{pro } x, y \text{ nastává jedna z možností 1,2,3}\}$. Je třeba dokázat, že pro každé $x \in \mathcal{N}$ je $\mathcal{M}_x = \mathcal{N}$.

Díky tomuto jsme schopni na množině $\mathcal{N}$ zavést uspořádání. Toto uspořádání je lineární s nejmenším prvkem 1. Reflexivita a tranzitivita je zřejmá. Antisymetrie a úplnost plyne z předchozí věty.

Propojení uspořádání s operací plus

Věta

1. $x < y \iff x + z < y + z$
2. $x \leq y \iff x + z \leq y + z$
3. pokud $x < y, r < s$ nebo $x \leq y, r < s$ nebo $x < y, r \leq s$, pak $x + r < y + s$
4. $x \leq y, r \leq s \implies x + r \leq y + s$
5. $x < y \implies \overline{x} \leq y$

Věta

$\mathcal{N}$ je dobře uspořádáná, tj. každá podmnožina má nejmenší prvek

Věta

Nechť $\emptyset \neq \mathcal{M} \subseteq \mathcal{N}$ je shora ohraničená množina. Pak má $\mathcal{M}$ největší prvek.

Příklad

Ukážeme si, že na $\mathcal{N}$ existuje injekce, která není surjekce. Buď $b \in \mathcal{N}$ libovolné. Hledaným zobrazením může být f_b definované následovně:

$$f_b(x) = \begin{cases} x, & \text{pro } x < b \\ \overline{x}, & \text{pro } x \geq b. \end{cases}$$

Je injektivní, neboť $x < y \Longrightarrow f_b(x) < f_b(y)$. Surjektivní není, neboť neexistuje x tak, že $f_b(x) = b$.

Věta

Nechť $m \in \mathcal{N}$. Označme $A(m) = \{s \in \mathcal{N} | s \leq m\}$. Pak neexistuje injekce $f : \mathcal{N} \longrightarrow A(m)$

Z předchozí věty dostáváme, že shora ohraničené podmnožiny množiny $\mathcal{N}$ jsou konečné.

Jak poznám nekonečnou množinu M?

- existuje vlastní podmnožina $S \subset M$ a bijekce $f : M \to S$
- existuje injekce $f : M \to M$, která není surjekcí
- existuje injekce $f : \mathcal{N} \to M$.

Násobení

Věta

Na množině $\mathcal{N}$ existuje právě jedna operace $\cdot$ taková, že pro každé $x, y \in \mathcal{N}$ platí:

1. $x \cdot 1 = x$,
2. $x \cdot \overline{y} = x \cdot y + x$.

   Pro tuto operaci a pro každé $x, y \in \mathcal{N}$ pak platí:
3. $1 \cdot x = x$
4. $\overline{x} \cdot y = x \cdot y + y$

Definice

Operaci $\cdot$ z předchozí věty nazýváme násobení.

Věta

Operace $\cdot$ na množině $\mathcal{N}$ je komutativní a asociativní. S operací $+$ je svázána tzv. distributivním zákonem:

$$\forall x, y, z \in \mathcal{N} \Longrightarrow x \cdot (y + z) = x \cdot y + x \cdot z$$

Důsledek

Pro $x, y, z, v \in \mathcal{N}$ platí:

$$(x + y) \cdot (u + v) = x \cdot u + x \cdot v + y \cdot u + y \cdot v$$

Věta

Nechť $x, y, z, r, s \in \mathcal{N}$. Pak platí:

1. $x < y \Longleftrightarrow x \cdot z < y \cdot z$
2. $x \cdot z = y \cdot z \Longrightarrow x = y$
3. $x \leq y \Longleftrightarrow x \cdot y \leq y \cdot z$
4. jestliže $x < y, r < s$ nebo $x \leq y, r < s$ nebo $x < y, r \leq s$, pak $x \cdot r < y \cdot s$
5. $x \leq y, r \leq s \Longrightarrow x \cdot z < y \cdot z$

Věta

Nechť M je libovolná neprázdná množina, $\varphi : \mathcal{N} \times M \to M$ a $m \in M$ libovolné. Pak existuje právě jedno zobrazeení $P : \mathcal{N} \to M$ takové, že:

1. $P(1) = m$,
2. pro $x \in \mathcal{N}$ platí $\varphi(x, P(x)) = P(\overline{x})$.

Definice

Jestliže jsou splněny předpoklady předchozí věty, řekneme, že jsme dvojicí (φ, m) rekurentně definovali zobrazení P.

Tato definice se nazývá rekurentní definice. Lze ji interpretovat i následujícím způsobem:

Pro každé $x \in \mathcal{N}$ chceme definovat pojem pojem $P(x)$. Označíme M množinu pojmů, které přicházejí v úvahu. Pojem $P(x) \in M$ je pak definován pro každé $x \in \mathcal{N}$, jestliže

- *he definován pojem $P(1)$,*
- *pokud je definován pojem $P(x)$ pro $s \in \mathcal{N}$, definujeme pak pojem $P(\overline{s})$*

Tímto způsobem je pak podle předchozí věty jednoznačně určen pojem $P(x)$ pro každé $x \in \mathcal{N}$

Lemma

Nechť $\mathcal{N}, \mathcal{N}^*$ jsou množiny přirozených čísel, $\mu \in \mathcal{N}^*$. Pak existuje právě jedno zobrazení $f : \mathcal{N} \to \mathcal{N}^*$ takové, že

1. $f(1) = \mu$,
2. pro $x \in \mathcal{N}$ je $\overline{f(x)} = f(\overline{x})$.

Toto zobrazení je navíc injekce a $f(\mathcal{N}) = \{\nu \in \mathcal{N}^* | \mu \leq \nu\}$.

Věta

Nechť $\mathcal{N}, \mathcal{N}^*$ jsou množiny přirozených čísel. Pak existuje právě jedna bijekce $f : \mathcal{N} \to \mathcal{N}^*$ taková, že pro každé $x \in \mathcal{N}$ platí, že $f(\overline{x}) = \overline{f(x)}$.