Obory přirozených, celých a racionálních čísel

V této kapitole ukážeme, jak lze vybudovat teorii přirozených čísel, celých čísel a racionálních čísel. Budeme předpokládat, že známe jen intuitivní teorii množin, s kterou byl čtenář seznámen v dřívějších učebních textech. Na základě této teorie zavedeme pojem „přirozené číslo" jako pojem, který vyhovuje speciálnímu axiomatickému systému. Tento axiomatický systém byl zaveden na konci 19. století italským matematikem G. Peanem, který jím úspěšně charakterizoval přirozená čísla. Z těchto axiomů odvodíme některé základní vlastnosti přirozených čísel, které jsou čtenáři dobře známy ze střední školy. Celá čísla pak dostaneme jako „rozdílovou grupu" aditivní pologrupy přirozených čísel a čísla racionální definujeme pomocí „podílového tělesa" okruhu celých čísel.

Pojem přirozeného čísla patří k nejzákladnějším pojmům v matematice, který člověk používal od pradávných dob a který je jedním z prvních matematických pojmů, s kterými se seznamuje dítě. V těchto dobách však jsou znalosti o přirozených číslech získávány jen intuitivní cestou. Podobně je tomu s pojmem celého čísla, k jehož poznání dochází velmi brzo po přirozeném čísle, a s pojmem racionálního čísla.

Náš způsob výkladu je proveden abstraktní cestou, uvedené pojmy jsou definovány jako abstraktní objekty splňující jisté vlastnosti.

4. Polookruh přirozených čísel

4.1. Definice. Libovolnou množinu $\mathcal{N}$ budeme nazývat *množinou přirozených čísel* a každý prvek z $\mathcal{N}$ *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:

i) Existuje alespoň jeden prvek množiny $\mathcal{N}$, který není následníkem žádného prvku z $\mathcal{N}$. (Jeden z těchto prvků označme symbolem $1 = 1_{\mathcal{N}}$.)

ii) Pro libovolné $x, y \in \mathcal{N}$, z $\overline{x} = \overline{y}$ plyne $x = y$.

iii) Nechť $\mathcal{M} \subseteq \mathcal{N}$ má následující vlastnosti

a) $1 \in \mathcal{M}$,

b) $x \in \mathcal{M} \Longrightarrow \overline{x} \in \mathcal{M}$.

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

Vlastnost iii) se nazývá *axiom úplné indukce*. Vlastnosti i)–iii) jsou ekvivalentní s tzv. *Peanovými axiomy*.

4.2. Poznámky.

a) Přiřazení následníků v množině $\mathcal{N}$ je vlastně zobrazení $^- : \mathcal{N} \to \mathcal{N}$. Přesnější než o množině přirozených číslech by bylo hovořit o algebraické struktuře

přirozených čísel, čímž bychom měli na mysli uspořádanou dvojici $(\mathcal{N}, ^-)$. Z důvodů stručnosti a větší přehlednosti textu to však nebudeme dělat a budeme psát o množině $\mathcal{N}$, majíce na mysli, že přiřazení následníků v množině $\mathcal{N}$ je pevně zvoleno.

b) V teorii množin se ukazuje, že taková množina $\mathcal{N}$ existuje. Je to množina kardinálních čísel konečných neprázdných množin. Závěrem tohoto odstavce (věta 4.30) ukážeme jednoznačnost množiny $\mathcal{N}$.

c) Z tvrzení 4.3 (c) plyne, že prvek množiny $\mathcal{N}$ s vlastností i) je určen jednoznačně.

V dalším textu budeme předpokládat, že $\mathcal{N}$ je množina přirozených čísel, tj. má vlastnosti i)–iii) z definice 4.1.

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

(a) $x \neq y \Longrightarrow \overline{x} \neq \overline{y}$,

(b) $x \neq \overline{x}$,

(c) $x \neq 1 \Longrightarrow \exists\, u \in \mathcal{N} : x = \overline{u}$.

Důkaz. Část (a) plyne ihned z vlastnosti ii) definice 4.1.

Položme $\mathcal{M} = \{z \in \mathcal{N} \mid z \neq \overline{z}\}$. Výrok (b) je ekvivalentní s $\mathcal{M} = \mathcal{N}$. Podle i) v definici 4.1 platí $1 \in \mathcal{M}$. Buď nyní $x \in \mathcal{M}$ takové, že $\overline{x} \notin \mathcal{M}$. Tedy $\overline{x} = \overline{\overline{x}}$ a podle ii) v definici 4.1 platí $x = \overline{x}$, což je spor s $x \in \mathcal{M}$. Proto $x \in \mathcal{M} \Longrightarrow \overline{x} \in \mathcal{M}$ a z axiomu úplné indukce plyne $\mathcal{M} = \mathcal{N}$.

Položme $\mathcal{M} = \{z \in \mathcal{N} \mid \exists\, v \in \mathcal{N}, \overline{v} = z\} \cup \{1\}$. Je-li $x \in \mathcal{M}$, pak zřejmě $\overline{x} \in \mathcal{M}$ a z axiomu úplné indukce tedy plyne $\mathcal{M} = \mathcal{N}$, tudíž (c).

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

(a) $x + 1 = \overline{x}$,

(b) $x + \overline{y} = \overline{x + y}$.

Pro tuto operaci $+$ a pro každé $x, y \in \mathcal{N}$ pak platí:

(c) $1 + x = \overline{x}$,

(d) $\overline{x} + y = \overline{x + y}$.

Důkaz. Nejdříve ukažme existenci takové operace $+$. Nechť $\mathcal{M}$ je množina všech $x \in \mathcal{N}$, ke kterým existuje zobrazení f_x množiny $\mathcal{N}$ do sebe takové, že platí:

$$f_x(1) = \overline{x}, \quad f_x(\overline{y}) = \overline{f_x(y)} \text{ pro každé } y \in \mathcal{N}. \quad (*)$$

Poznamenejme, že f_x bude vlastně přičtení x zleva.

Položíme-li $f_1(y) = \overline{y}$ pro $y \in \mathcal{N}$, pak f_1 je takové zobrazení pro $x = 1$. Tudíž $1 \in \mathcal{M}$.

Buď $x \in \mathcal{M}$ a f_x nechť je zobrazení splňující $(*)$ pro toto x. Zkonstruujeme nyní $f_{\overline{x}}$. Pro $y \in \mathcal{N}$ položíme $f_{\overline{x}}(y) = \overline{f_x(y)}$. Pak $f_{\overline{x}}(1) = \overline{f_x(1)} = \overline{\overline{x}}$ a pro $y \in \mathcal{N}$ máme

$$f_{\overline{x}}(\overline{y}) = \overline{f_{\overline{x}}(y)} = \overline{\overline{f_x(y)}} = \overline{f_{\overline{x}}(y)}.$$

Tudíž $f_{\overline{x}}$ splňuje $(*)$, a proto $\overline{x} \in \mathcal{M}$. Z axiomu úplné indukce plyne $\mathcal{M} = \mathcal{N}$.

Předpokládejme, že pro některé $x \in \mathcal{N}$ existují dvě zobrazení vlastností $(*)$. Označme je f_x, g_x a položme $\mathcal{M} = \{y \in \mathcal{N} \mid f_x(y) = g_x(y)\}$. Zřejmě $1 \in \mathcal{M}$. Pokud $z \in \mathcal{M}$, pak

$$f_x(\overline{z}) = \overline{f_x(z)} = \overline{g_x(z)} = g_x(\overline{z}),$$

tudíž $\overline{z} \in \mathcal{M}$ a z axiomu úplné indukce dostáváme $\mathcal{M} = \mathcal{N}$. Tedy $f_x = g_x$ a pro každé x existuje právě jedno zobrazení vlastností $(*)$.

Nyní můžeme operaci $+$ pro $x, y \in \mathcal{N}$ definovat vztahem $x + y = f_x(y)$. Tato operace, vzhledem k $(*)$, splňuje podmínky (a) a (b).

Z uvedeného vztahu $x + y = f_x(y)$ dostáváme $1 + x = f_1(x) = \overline{x}$ a $\overline{x} + y = f_{\overline{x}}(y) = \overline{f_x(y)} = \overline{x + y}$. Platí tudíž i (c) a (d).

Jednoznačnost uvedené operace $+$ plyne z přechozího, neboť každá operace $+$ splňující (a), (b) indukuje pro libovolné $x \in \mathcal{N}$ zobrazení f_x, definované vztahem $f_x(y) = x + y$, které splňuje vlastnosti $(*)$. Pokud by existovaly dvě různé operace splňující (a), (b), pak by pro nějaké x musela existovat dvě různá zobrazení vlastností $(*)$, což dle předchozího není možné.

Věta je tím dokázána.

4.5. Definice. V dalším pro operaci na množině $\mathcal{N}$ uvažovanou ve větě 4.4 vyhradíme symbol $+$ a budeme ji nazývat *sčítání*. Dvojice $(\mathcal{N}, +)$ je pak grupoid.

Odvodíme si nyní některá tvrzení o této operaci $+$.

4.6. Věta. *Operace $+$ na množině přirozených čísel $\mathcal{N}$ je asociativní a komutativní.*

Důkaz. Nechť $x, y \in \mathcal{N}$. Položme $\mathcal{M} = \{z \in \mathcal{N} \mid (x + y) + z = x + (y + z)\}$. Jelikož

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

je $1 \in \mathcal{M}$. Je-li $z \in \mathcal{M}$, pak

$$(x + y) + \overline{z} = \overline{(x + y) + z} = \overline{x + (y + z)},$$

$$x + (y + \overline{z}) = x + \overline{y + z} = \overline{x + (y + z)}.$$

Tudíž $\overline{z} \in \mathcal{M}$ a z axiomu úplné indukce plyne $\mathcal{M} = \mathcal{N}$. Operace $+$ je tedy asociativní.

Nechť $x \in \mathcal{N}$ a nechť $\mathcal{M} = \{y \in \mathcal{N} \mid x + y = y + x\}$. Podle 4.4 (a), (c) je $1 \in \mathcal{M}$. Pokud $z \in \mathcal{M}$, pak

$$x + \overline{z} = \overline{x + z} = \overline{z + x} = \overline{z} + x$$

podle 4.4 (b), (d), tudíž $\overline{z} \in \mathcal{M}$. Odtud plyne $\mathcal{M} = \mathcal{N}$ a operace $+$ je komutativní.

4.7. Věta. *V grupoidu $(\mathcal{N}, +)$ platí zákon o odečítání, tj. platí:*

$$x, y, z \in \mathcal{N}, \quad x + y = x + z \Longrightarrow y = z.$$

Důkaz. Tvrzení dokážeme nepřímo. Nechť $y, z \in \mathcal{N}$, $y \neq z$ jsou pevně zvoleny. Položme $\mathcal{M} = \{x \in \mathcal{N} \mid x + y \neq x + z\}$. Jelikož $1 + y = \overline{y} \neq \overline{z} = 1 + z$, platí $1 \in \mathcal{M}$. Jestliže $u \in \mathcal{M}$, pak $u + y \neq u + z$, odkud plyne $\overline{u} + y = \overline{u + y} \neq \overline{u + z} = \overline{u} + z$, tudíž $\overline{u} \in \mathcal{M}$. Z axiomu úplné indukce dostáváme $\mathcal{M} = \mathcal{N}$.

4.8. Tvrzení. *Pro $x, y \in \mathcal{N}$ platí $x \neq x + y$.*

Důkaz. Jestliže $x = x + y$, pak $x + 1 = x + y + 1$ a ze zákona o odečítání plyne $1 = y + 1 = \overline{y}$, což je spor s i) v definici 4.1.

4.9. Tvrzení. *Nechť $x, y \in \mathcal{N}$. Pak nastane právě jeden z následujících tří případů:*

(a) $x = y$,

(b) *existuje $u \in \mathcal{N}$ tak, že $x = y + u$,*

(c) *existuje $v \in \mathcal{N}$ tak, že $y = x + v$.*

Důkaz. Podle 4.8 nemohou nastat současně případy (a), (b) a (a), (c). Kdyby nastaly současně případy (b), (c), pak $x = y + u = x + (v + u)$, což není možné podle 4.8.

Buď $x \in \mathcal{N}$ a nechť $\mathcal{M}_x$ je množina všech $y \in \mathcal{N}$ takových, že pro x, y nastane některý z případů (a), (b), (c). Tvrzení bude dokázáno, pokud pro každé $x \in \mathcal{N}$ ukážeme, že $\mathcal{M}_x = \mathcal{N}$.

Jestliže $x = 1$, pak pro každé $y \in \mathcal{N}, y \neq 1$ existuje $v \in \mathcal{N}$ tak, že $y = \overline{v} = 1 + v$, tudíž $\mathcal{M}_1 = \mathcal{N}$.

Jestliže $x \neq 1$, pak existuje $u \in \mathcal{N}$ tak, že $x = \overline{u} = 1 + u$, tudíž $1 \in \mathcal{M}_x$.

Nechť $z \in \mathcal{M}_x$. Rozlišme nyní, který z případů (a), (b), (c) nastal pro dvojici x, z. Jestliže nastal první případ, tj. $z = x$, potom $\overline{z} = x + 1$, tudíž pro dvojici $x, \overline{z}$ nastane případ (c). Jestliže nastal druhý případ, tj. existuje $u \in \mathcal{N}$ tak, že $x = z + u$, pak pro $u = 1$ máme $x = z + 1 = \overline{z}$, a tudíž pro prvky $x, \overline{z}$ nastane případ (a). Je-li $u \neq 1$, pak existuje $v \in \mathcal{N}$ tak, že $u = \overline{v}$, a pak $x = z + u = z + \overline{v} = \overline{z + v} = \overline{z} + v$. Pro prvky $x, \overline{z}$ pak nastane případ (b). Zbývá nám třetí případ, kdy existuje $v \in \mathcal{N}$, $z = x + v$. Pak $\overline{z} = \overline{x + v} = x + \overline{v}$, tudíž pro prvky $x, \overline{z}$ nastane případ (c). Odtud plyne $\overline{z} \in \mathcal{M}_x$. Z axiomu úplné indukce dostáváme $\mathcal{M}_x = \mathcal{N}$.

Důkaz je dokončen.

4.10. Definice. Pro $x, y \in \mathcal{N}$ položme $x \leq y$, jestliže $x = y$, nebo existuje $u \in \mathcal{N}$ tak, že $y = x + u$. Jestliže $x \leq y$ a $x \neq y$, klademe $x < y$. Neboli $x < y$ právě tehdy, když existuje $u \in \mathcal{N}$ tak, že $y = x + u$.

4.11. Věta. *Relace $\leq$ na množině $\mathcal{N}$ je lineární uspořádání s nejmenším prvkem 1.*

Důkaz. Reflexivita a tranzitivita relace $\leq$ je zřejmá. Antisymetrie a úplnost plyne z 4.9.

Nechť $x \in \mathcal{N}$. Je-li $x = 1$, pak $1 \leq x$. Jestliže $x \neq 1$, pak existuje $u \in \mathcal{N}$ tak, že $\overline{u} = x$, tudíž $x = u + 1$, odkud plyne $1 < x$. Tím jsme ukázali, že 1 je nejmenší prvek uspořádané množiny $(\mathcal{N}, \leq)$.

Lineární uspořádání $\leq$ na množině $\mathcal{N}$ je spojeno s operací $+$ následujícími vztahy.

4.12. Věta. *Nechť $x, y, z, r, s \in \mathcal{N}$. Pak platí:*
(a) $x < y \iff x + z < y + z$,
(b) $x \leq y \iff x + z \leq y + z$,
(c) *pokud* $x < y, r < s$ *nebo* $x \leq y, r < s$ *nebo* $x < y, r \leq s$, *pak* $x + r < y + s$,
(d) $x \leq y, r \leq s \implies x + r \leq y + s$,
(e) $x < y \implies \overline{x} \leq y$.

Důkaz. Jestliže $x < y$, pak existuje $u \in \mathcal{N}$ tak, že $x + u = y$, odkud $y + z = (x + z) + u$, z čehož dostáváme $x + z < y + z$.

Jestliže $x + z < y + z$, pak existuje $u \in \mathcal{N}$ tak, že $x + z + u = y + z$. Ze zákona o odečítání pak plyne $x + u = y$, tedy $x < y$. Platí (a), odkud se snadno odvodí platnost výroku (b).

Nechť $x < y, r < s$. Pak podle (a) $x + r < y + r$, $r + y < s + y$ a z tranzitivity plyne $x + r < y + s$. Podobně se ukáží ostatní části výroku (c). Výrok (d) pak snadno plyne z (c).

Nechť $x < y$, pak existuje $u \in \mathcal{N}$ tak, že $x + u = y$. Jestliže $u = 1$, pak $\overline{x} = y$. Jestliže $u \neq 1$, pak existuje $v \in \mathcal{N}$ tak, že $u = \overline{v}$, tudíž $y = x + \overline{v} = \overline{x + v} = \overline{x} + v$, odkud plyne $\overline{x} < y$. Platí tedy $\overline{x} = y$ nebo $\overline{x} < y$, což je tvrzení (e).

Věta je dokázána.

4.13. Poznámka. Výrok (e) můžeme interpretovat tak, že mezi prvky $x, \overline{x}$ neexistuje žádný jiný prvek. Poznamenejme ještě, že vždy platí $x < \overline{x}$.

4.14. Definice. Nechť P je neprázdná množina a $\preceq$ lineární uspořádání na P. Relace $\preceq$ se nazývá *dobré uspořádání*, jestliže každá neprázdná podmnožina množiny P má nejmenší prvek. Říkáme též, že $(P, \preceq)$ je *dobře uspořádaná množina*.

4.15. Věta. *Množina $(\mathcal{N}, \leq)$ je dobře uspořádaná množina.*

Důkaz. Nechť $\mathcal{M}$ je libovolná neprázdná podmnožina $\mathcal{N}$. Ukážeme, že má nejmenší prvek. Položme $\mathcal{M}^* = \{x \in \mathcal{N} \mid \forall\, m \in \mathcal{M} : x \leq m\}$. Protože je množina $\mathcal{M}$ neprázdná, můžeme zvolit prvek $r \in \mathcal{M}$. Protože $\overline{r} = r + 1 > r$, nepatří $\overline{r}$ do množiny $\mathcal{M}^*$. Jelikož $1 \in \mathcal{M}^*$, plyne z axiomu úplné indukce existence prvku $s \in \mathcal{M}^*$ takového, že $\overline{s} \notin \mathcal{M}^*$. Ukážeme, že s je nejmenší prvek množiny $\mathcal{M}$.

Poněvadž $s \in \mathcal{M}^*$ platí $s \leq m$ pro každý prvek $\mathcal{M}$. Jestliže $s \notin \mathcal{M}$, pak $s < m$ pro každý prvek $m \in \mathcal{M}$ a podle 4.12 (e) je $\overline{s} \leq m$ pro každý prvek $m \in \mathcal{M}$, což je spor s předpokladem $\overline{s} \notin \mathcal{M}^*$. Tudíž $s \in \mathcal{M}$ a věta je dokázána.

4.16. Tvrzení. *Nechť $\emptyset \neq \mathcal{M} \subseteq \mathcal{N}$ je shora ohraničená množina, tj. existuje $z \in \mathcal{N}$ tak, že pro každý prvek $m \in \mathcal{M}$ platí $m \leq z$. Pak $\mathcal{M}$ má největší prvek.*

Důkaz. Položme $\mathcal{M}^* = \{x \in \mathcal{N} \mid \forall\, m \in \mathcal{M} : x \geq m\}$. Jelikož $\mathcal{M}^* \neq \emptyset$, existuje nejmenší prvek s množiny $\mathcal{M}^*$. Ukážeme-li, že $s \in \mathcal{M}$, pak s bude největší prvek množiny $\mathcal{M}$.

Je-li $s = 1$, pak nutně $\mathcal{M} = \{1\}$. Nechť $s \neq 1$. Pak existuje $v \in \mathcal{N}$ tak, že $\overline{v} = s$.

Protože s je nejmenší prvek $\mathcal{M}^*$, platí $v \notin \mathcal{M}^*$, a tedy existuje $m \in \mathcal{M}$ takové, že $v < m$. Zároveň však $m \leq s = \overline{v}$, a tedy podle 4.12 (e) je $s = m \in \mathcal{M}$.

4.17. Příklad. Ukážeme si, že existuje injekce $\mathcal{N} \to \mathcal{N}$, která není surjekce. Buď $b \in \mathcal{N}$ libovolné a definujme $f_b : \mathcal{N} \to \mathcal{N}$ takto

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

Ověřte sami rozepsáním, že pro libovolné $x, y \in \mathcal{N}$ z $x < y$ plyne $f_b(x) < f_b(y)$, a tedy f_b je injektivní. Na druhou stranu pro žádné $x \in \mathcal{N}$ neplatí $f_b(x) = b$, a proto f_b není surjekce.

4.18. Věta. *Nechť $m \in \mathcal{N}$. Označme $A(m) = \{s \in \mathcal{N} \mid s \leq m\}$. Pak neexistuje injekce $f : \mathcal{N} \to A(m)$.*

Důkaz. Označme $\mathcal{M} = \{m \in \mathcal{N} \mid$ neexistuje injekce $f : \mathcal{N} \to A(m)\}$. Snadno se vidí, že $f : \mathcal{N} \to \{1\}$ není injekce, a tedy $1 \in \mathcal{M}$.

Buď $m \in \mathcal{M}$ a předpokládejme, že $\overline{m} \notin \mathcal{M}$, tj. existuje injekce $f : \mathcal{N} \to A(\overline{m})$. Připomeňme, že z 4.12 (e) plyne $A(\overline{m}) = A(m) \cup \{\overline{m}\}$. Rozlišme dva případy podle toho, zda existuje $b \in \mathcal{N}$ s vlastností $f(b) = \overline{m}$. Pokud neexistuje, můžeme uvážit injektivní zobrazení $g : \mathcal{N} \to A(m)$ určené předpisem $g(x) = f(x)$, což je však spor s $m \in \mathcal{M}$. Pokud takové b existuje, pak je jediné, neboť f je injekce. Položme $g = f \circ f_b$, kde f_b je definováno v předchozím příkladu. Pak $g : \mathcal{N} \to A(\overline{m})$ je injekce a neexistuje $x \in \mathcal{N}$ s vlastností $g(x) = \overline{m}$, což je opět podle předchozího spor.

Pro $\mathcal{M}$ jsme tedy ukázali $m \in \mathcal{M} \implies \overline{m} \in \mathcal{M}$. Proto $\mathcal{M} = \mathcal{N}$ a věta je dokázána.

4.19. Poznámka. V teorii množin lze definovat *nekonečnou množinu* jako takovou množinu M, která splňuje některou z následujících navzájem ekvivalentních podmínek:
- existuje vlastní podmnožina $S \subsetneq M$ a bijekce $f : M \to S$;
- existuje injekce $f : M \to M$, která není surjekcí;
- existuje injekce $f : \mathcal{N} \to M$.

Z věty 4.18 plyne, že shora ohraničené podmnožiny množiny $\mathcal{N}$ jsou konečné.

Zavedeme nyní další operaci na $\mathcal{N}$.

4.20. Věta. *Na množině $\mathcal{N}$ existuje právě jedna operace $\cdot$ taková, že pro každé $x, y \in \mathcal{N}$ platí:*
(a) $x \cdot 1 = x$,
(b) $x \cdot \overline{y} = x \cdot y + x$.
Pro tuto operaci a pro každé $x, y \in \mathcal{N}$ pak platí:
(c) $1 \cdot x = x$,
(d) $\overline{x} \cdot y = x \cdot y + y$.

Důkaz. Provádí se analogicky jako důkaz věty 4.4.

Ukážeme nejdříve existenci takové operace. Nechť $\mathcal{M}$ je množina všech $x \in \mathcal{N}$, ke kterým existuje zobrazení f_x množiny $\mathcal{N}$ do sebe s vlastnostmi:

$$f_x(1) = x, \quad f_x(\overline{y}) = f_x(y) + x \text{ pro každé } y \in \mathcal{N}. \quad (*)$$

Položíme-li $f_1(y) = y$ pro každé $y \in \mathcal{N}$, pak f_1 je takové zobrazení pro $x = 1$. Tudíž $1 \in \mathcal{M}$. Buď f_x uvedené zobrazení pro $x \in \mathcal{M}$. Pro $y \in \mathcal{N}$ položíme $f_{\overline{x}}(y) = f_x(y) + y$. Pak $f_{\overline{x}}(1) = f_x(1) + 1 = x + 1 = \overline{x}$ a $f_{\overline{x}}(\overline{y}) = f_x(\overline{y}) + \overline{y} = f_x(y) + x + y + 1 = f_{\overline{x}}(y) + \overline{x}$ pro $y \in \mathcal{N}$. Tudíž $\overline{x} \in \mathcal{M}$ a $\mathcal{M} = \mathcal{N}$.

Předpokládejme, že pro některé $x \in \mathcal{N}$ existují dvě zobrazení vlastností $(*)$. Označme je f_x, g_x a položme $\mathcal{M} = \{y \in \mathcal{N} \mid f_x(y) = g_x(y)\}$. Zřejmě $1 \in \mathcal{M}$. Pokud $z \in \mathcal{M}$, pak $f_x(\overline{z}) = f_x(z) + x = g_x(z) + x = g_x(\overline{z})$, tudíž $\overline{z} \in \mathcal{M}$ a $\mathcal{M} = \mathcal{N}$. Tedy $f_x = g_x$ a pro každé x existuje právě jedno zobrazení vlastností $(*)$.

Nyní můžeme operaci $\cdot$ definovat vztahem $x \cdot y = f_x(y)$. Tato operace, vzhledem k $(*)$, splňuje podmínky (a) a (b).

Ze vztahu $x \cdot y = f_x(y)$ pak dostáváme $1 \cdot x = f_1(x) = x$ a $\overline{x} \cdot y = f_{\overline{x}}(y) = f_x(y) + y = x \cdot y + y$. Platí tudíž (c) i (d).

Jednoznačnost uvedené operace plyne z přechozího. Stačí si uvědomit, že každá operace $\cdot$ splňující (a) a (b) indukuje zobrazení splňující $(*)$ (předpisem $f_x(y) = x \cdot y$).

Věta je tím dokázána.

4.21. Definice. Operaci uvedenou ve větě 4.20 nazýváme *násobení* a vyhradíme pro ni symbol $\cdot$. Máme tudíž na množině $\mathcal{N}$ dvě operace $+$ a $\cdot$ a uspořádání $\leq$. Často budeme množinu $\mathcal{N}$ uvažovat jako čtveřici $(\mathcal{N}, +, \cdot, \leq)$. Jestliže v zápisu nepoužijeme závorky, dáváme přednost jako v okruhu operaci $\cdot$ před operací $+$. Tedy $a \cdot b + c$ značí $(a \cdot b) + c$ a nikoliv $a \cdot (b + c)$. Při zápisu operace násobení často vynecháváme označení operace $\cdot$, tudíž místo $a \cdot b$ píšeme ab.

Odvodíme nyní některé vlastnosti operace násobení.

4.22. Věta. *Operace násobení $\cdot$ na množině přirozených čísel $\mathcal{N}$ je komutativní a asociativní a s operací $+$ je svázána tzv. distributivním zákonem:*

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

Důkaz. Nechť $x \in \mathcal{N}$. Položme $\mathcal{M} = \{y \in \mathcal{N} \mid x \cdot y = y \cdot x\}$. Z 4.20 (a), (c) plyne $1 \in \mathcal{M}$. Pro $y \in \mathcal{M}$ podle 4.20 (b), (d) dostáváme $\overline{y} \cdot x = y \cdot x + x = x \cdot y + x = x \cdot \overline{y}$, tudíž $\overline{y} \in \mathcal{M}$. Tedy $\mathcal{M} = \mathcal{N}$, což dokazuje komutativitu násobení.

Buď $x, y \in \mathcal{N}$. Položme $\mathcal{M} = \{z \in \mathcal{N} \mid x \cdot (y + z) = x \cdot y + x \cdot z\}$. Platí $x \cdot (y + 1) = x \cdot \overline{y} = x \cdot y + x = x \cdot y + x \cdot 1$, tudíž $1 \in \mathcal{M}$. Nechť $z \in \mathcal{M}$, pak

$$x \cdot (y + \overline{z}) = x \cdot \overline{(y + z)} = x \cdot (y + z) + x = x \cdot y + x \cdot z + x = x \cdot y + x \cdot \overline{z},$$

tedy $\overline{z} \in \mathcal{M}$. Opět z axiomu úplné indukce dostáváme $\mathcal{M} = \mathcal{N}$. Odtud plyne distributivní zákon.

Nechť $x, y \in \mathcal{N}$. Položme $\mathcal{M} = \{z \in \mathcal{N} \mid (x \cdot y) \cdot z = x \cdot (y \cdot z)\}$. Zřejmě $1 \in \mathcal{M}$. Je-li $z \in \mathcal{M}$, pak $(x \cdot y) \cdot \overline{z} = (x \cdot y) \cdot z + x \cdot y = x \cdot (y \cdot z) + x \cdot y = x \cdot (y \cdot z + y) = x \cdot (y \cdot \overline{z})$, tedy $\overline{z} \in \mathcal{M}$. Tedy $\mathcal{M} = \mathcal{N}$, což dokazuje asociativitu násobení.

Z distributivního zákona ihned obdržíme:

4.23. Tvrzení. *Pro $x, y, u, v \in \mathcal{N}$ platí:*

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

Z 4.20 (a), (c) plyne:

4.24. Tvrzení. *V grupoidu $(\mathcal{N}, \cdot)$ je 1 jednotkový prvek.*

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

(a) $x < y \iff x \cdot z < y \cdot z$,
(b) $x \cdot z = y \cdot z \Longrightarrow x = y$,
(c) $x \leq y \iff x \cdot z \leq y \cdot z$,
(d) *jestliže* $x < y, r < s$ *nebo* $x \leq y, r < s$ *nebo* $x < y, r \leq s$, *pak* $x \cdot r < y \cdot s$,
(e) $x \leq y, r \leq s \Longrightarrow x \cdot r \leq y \cdot s$.

Důkaz. Nechť $x < y$. Pak existuje $u \in \mathcal{N}$ tak, že $y = x + u$. Odtud plyne $y \cdot z = x \cdot z + u \cdot z$, tudíž $x \cdot z < y \cdot z$.

Je-li $x \cdot z < y \cdot z$ a $y \leq x$, pak podle předešlého $y \cdot z \leq x \cdot z$, což je spor. Platí tudíž část (a).

Nechť $x \cdot z = y \cdot z$. Jestliže $x \neq y$, pak můžeme předpokládat $x < y$ a z (a) dostaneme spor. Platí tedy (b).

Výrok (c) je obměnou (a).

Nechť $x < y, r < s$. Pak podle (a) $x \cdot r < y \cdot r$, $y \cdot r < y \cdot s$, tudíž $x \cdot r < y \cdot s$. Podobně se dokáží ostatní části výroku (d) a výrok (e).

4.26. Poznámka. Jestliže v nějakém grupoidu $(G, \cdot)$ pro libovolné $x, y, z \in G$ platí obě implikace

$$x \cdot y = x \cdot z \Longrightarrow y = z,$$

$$y \cdot x = z \cdot x \Longrightarrow y = z,$$

říkáme, že v $(G, \cdot)$ platí *zákon o krácení*. Věta 4.25 (b) tedy tvrdí, že v grupoidu $(\mathcal{N}, \cdot)$ platí zákon o krácení. V případě, kdy užíváme aditivní terminologie, zákonu o krácení se říká zákon o odečítání (srovnej s větou 4.7).

Závěrem tohoto odstavce si uvedeme metodu rekurentní definice.

4.27. Věta. *Nechť M je libovolná neprázdná množina, $\varphi : \mathcal{N} \times M \to M$ a m je libovolný prvek z M.*

Pak existuje právě jedno zobrazení $P : \mathcal{N} \to M$ takové, že platí:

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

Důkaz. Pro $x \in \mathcal{N}$ položme $A(x) = \{t \in \mathcal{N} \mid t \leq x\}$. Zřejmě $1 \in A(x)$. Množinu $A(x)$ nazveme *úsekem určeným prvkem* x. Zobrazení $p : A(x) \to M$ nazveme *přípustné*, jestliže platí

(a) $p(1) = m$,

(b) $s \in A(x), \overline{s} \in A(x) \Longrightarrow \varphi(s, p(s)) = p(\overline{s})$.

Ukážeme, že každý úsek má nejvýše jedno přípustné zobrazení. Nechť p, q jsou různá přípustná zobrazení úseku $A(x)$ a nechť $u \in A(x)$ je nejmenší přirozené číslo z úseku $A(x)$ takové, že platí $p(u) \neq q(u)$; existenci takového u zaručuje 4.15. Protože $p(1) = m = q(1)$, je $u \neq 1$, a existuje tedy $t \in A(x)$ tak, že $\overline{t} = u$. Podle (b) je $p(u) = \varphi(t, p(t)) = \varphi(t, q(t)) = q(u)$, což je spor.

Označme nyní $\mathcal{M}$ množinu všech $x \in \mathcal{N}$ takových, že úsek $A(x)$ má přípustné zobrazení. Zřejmě $1 \in \mathcal{M}$. Pro $x \in \mathcal{M}$ platí též $\overline{x} \in \mathcal{M}$, protože $A(\overline{x}) = A(x) \cup \{\overline{x}\}$; je-li totiž p přípustné zobrazení úseku $A(x)$, pak zobrazení $q : A(\overline{x}) \to M$, které je určené předpisem $q(t) = p(t)$ pro $t \in A(x)$ a $q(\overline{x}) = \varphi(x, p(x))$, je přípustné zobrazení úseku $A(\overline{x})$. Tudíž $\mathcal{M} = \mathcal{N}$.

Snadno se vidí, že zúžení přípustného zobrazení úseku $A(x)$ na úsek $A(y)$ pro $x, y \in \mathcal{N}, y < x$, je opět přípustné zobrazení.

Pro $x \in \mathcal{N}$ položme $P(x) = p(x)$, kde p je přípustné zobrazení úseku $A(x)$. Pak $P(1) = m$. Nechť $x \in \mathcal{N}$ a nechť p je přípustné zobrazení úseku $A(x)$ a q přípustné zobrazení úseku $A(\overline{x})$. Potom

$$P(\overline{x}) = q(\overline{x}) = \varphi(x, q(x)) = \varphi(x, p(x)) = \varphi(x, P(x)).$$

Jednoznačnost zobrazení P plyne z jednoznačnosti přípustného zobrazení, neboť libovolné P splňující vlastnosti i), ii) indukuje přípustná zobrazení pro všechna $A(x)$.

4.28. Definice. Jestliže jsou splněny předpoklady věty 4.27, řekneme, že jsme *dvojicí* (φ, m) *rekurentně definovali zobrazení* P.

Uvedený druh definice se nazývá *rekurentní definice*. Rekurentní definici můžeme také interpretovat následujícím způsobem: Pro každé přirozené číslo $x \in \mathcal{N}$ máme definovat nějaký pojem $P(x)$. Označíme M množinu pojmů, které přicházejí v úvahu. Pojem $P(x) \in M$ je definován pro každé $x \in \mathcal{N}$, jestliže

i) je definován pojem $P(1)$,

ii) pokud je definován pojem $P(s)$ pro $s \in \mathcal{N}$, definujeme pak pojem $P(\overline{s})$.

Tímto způsobem je podle 4.27 jednoznačně určen pojem $P(x)$ pro každé $x \in \mathcal{N}$.

Na základě rekurentní definice si odvodíme následující *větu o jednoznačnosti množiny přirozených čísel* (4.30). Nejdříve uvedeme pomocné tvrzení.

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

i) $f(1) = \mu$,

ii) *pro $x \in \mathcal{N}$ je $\overline{f(x)} = f(\overline{x})$.*

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

Důkaz. Použijeme větu 4.27, ve které položíme $M = \mathcal{N}^*$, $m = \mu$ a pro $x \in \mathcal{N}$ položíme $\varphi(x, t) = \overline{t}$ pro každé $t \in \mathcal{N}^*$. Podle 4.27 existuje právě jedno zobrazení $f : \mathcal{N} \to \mathcal{N}^*$ tak, že $f(1) = \mu$ a pro $x \in \mathcal{N}$ je $\overline{f(x)} = f(\overline{x})$.

Ukážeme, že pro libovolná $x, y \in \mathcal{N}$, $x < y$ platí $f(x) < f(y)$. Označme za tím účelem $\mathcal{M} = \{x \in \mathcal{N} \mid \exists\, y \in \mathcal{N}, x < y, f(y) \leq f(x)\}$. Předpokládejme, že existuje $u \in \mathcal{M}$. Pro toto u uvažme množinu $\mathcal{O}_u = \{y \in \mathcal{N} \mid u < y, f(y) \leq f(u)\}$. Množina $\mathcal{O}_u$ je dle předpokladu $u \in \mathcal{M}$ neprázdná, tudíž existuje její nejmenší prvek; označme jej v. Protože $v \neq 1$, existuje $w \in \mathcal{N}$ tak, že $\overline{w} = v$. Z 4.12 (e) plyne $u \leq w$. Protože v je nejmenší prvek $\mathcal{O}_u$, musí platit $w \notin \mathcal{O}_u$, tzn. buď $u = w$ nebo $f(u) < f(w)$. V obou případech tedy

$$f(u) \leq f(w) < \overline{f(w)} = f(\overline{w}) = f(v),$$

což je spor s $v \in \mathcal{O}_u$. Tzn. $\mathcal{M} = \emptyset$, a tedy pro každé $x, y \in \mathcal{N}, x < y$ platí $f(x) < f(y)$. Odtud plyne, že f je injekce a $f(\mathcal{N}) \subseteq \{\nu \in \mathcal{N}^* \mid \mu \leq \nu\}$.

Nechť λ je nejmenší prvek množiny všech prvků z $\mathcal{N}^*$, které nemají vzor při zobrazení f a jsou větší než μ. Zřejmě $\lambda \neq 1_{\mathcal{N}^*}$, a proto musí existovat $\kappa \in \mathcal{N}^*$ takové, že $\overline{\kappa} = \lambda$. Prvek κ má vzor při zobrazení f, který označme m. Potom $f(\overline{m}) = \overline{f(m)} = \overline{\kappa} = \lambda$, což je spor. Tudíž $f(\mathcal{N}) = \{\nu \in \mathcal{N}^* \mid \mu \leq \nu\}$ a lemma je dokázáno.

Z lemmatu ihned dostáváme:

4.30. Věta (o jednoznačnosti přirozených čísel). *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: $f(\overline{x}) = \overline{f(x)}$.*

4.31. Poznámky.

a) Cílem předchozí věty je ukázat, že ačkoliv je různých množin přirozených čísel nepřeberné množství, všechny jsou v jistém smyslu stejné. Tyto množiny mohou mít samozřejmě zcela libovolné prvky, věta 4.30 však zaručuje, že prvky libovolných dvou takových množin lze ztotožnit (pomocí bijekce f) tak, že v obou množinách je pak přiřazení následníků stejné. A protože operace $+$, $\cdot$ i uspořádání $\leq$ byly definovány pouze pomocí následníků, všechny množiny přirozených čísel mají stejné algebraické vlastnosti. Jednu z těchto množin nyní pevně zvolíme a v dalším textu ji budeme značit $\mathbb{N}$. Budeme-li tedy v budoucích kapitolách hovořit o přirozených číslech, budeme mít na mysli prvky této množiny $\mathbb{N}$. Číslem 1 budeme značit nejmenší prvek množiny $\mathbb{N}$, tj. ten, který není následovníkem žádného přirozeného čísla. Číslo $\overline{1}$ (následovník 1) budeme značit symbolem 2, následovník 2 symbolem 3, atd..

b) Jelikož např. $1 < 1 + x$ pro každé $x \in \mathbb{N}$, neexistuje přirozené číslo x tak, aby platilo $1 = 1 + x$, tudíž trojice $(\mathbb{N}, +, \cdot)$ není okruh. Nicméně z dokázaných vlastností plyne, že $(\mathbb{N}, +, \cdot)$ je polookruh, přičemž polookruh je definován následujícím způsobem.