4.2 Zavedení přirozených čísel

Thurston dále popisuje, jak vznikla přirozená čísla:

1. Uvažujme posloupnost [*], [**], [***], [****], ... Pokud je možné množinu toho, co sčítáme, přiřadit k množině hvězdiček v [*], řekneme, že počet prvků množiny je jedna. Je-li obdobně možné ji přiřadit k množině [**], řekneme, že počet prvků je dva... Obdobně pro další čísla.

   Pozn. 4. Tento přístup zavedení čísla je blízký definici čísla ze sedmé knihy Eukleidových Základů (300 př. n. l.):

   i) „Jednotka jest, dle níž každé věci říká se jedna."

   ii) „Číslo pak je množství složené z jednotek."

   (Servít, 1907, s. 103).

2. Pro konstrukci čísel, jak je známe, nyní již stačí nahradit nešikovné symboly * obvyklými symboly. Tedy: [1], [1,2], [1,2,3], [1,2,3,4], ...

   Každá ze závorek obsahuje n-tici, jejíž pořadí musí být neměnné. Tyto množiny nazveme standardními.

3. Po přiřazení množiny k některé ze standardních množin stačí znát poslední číslo v závorce, abychom znali počet sčítaného. (Taková čísla čeština označuje pojmem ordinální.) Zavedeme následující označení, kdy každé uspořádané n-tici přiřadíme její poslední prvek. Symbol $\leftrightarrow$ značí přiřazení n-tice k číslu:

$$\begin{aligned}
[1] &\leftrightarrow 1,\\
[1,2] &\leftrightarrow 2,\\
[1,2,3] &\leftrightarrow 3,\\
&\dots\\
[1,2,3,\dots,n] &\leftrightarrow n.
\end{aligned}$$

Z této konstrukce čísel pro počítání množství Thurston (1956) dedukuje závěr, a sice že vše, co je potřeba k počítání, je uspořádaná sada různých symbolů, která pokračuje do nekonečna.

Takto definovaná čísla už nesou jisté vlastnosti, které mají přirozená čísla definovaná pomocí Peanových axiomů, například, že každé číslo má svého následníka (viz definice 3), nebo vlastnost, že různá čísla mají různé následníky (viz definice 3).

4.2.1 Peanovy axiomy

Definice 3. Peanovy axiomy

1) $0 \in \mathbb{N}$,

2) $\forall a \in \mathbb{N} \quad \exists! \sigma(a)$, kde $\sigma(a)$ nazýváme následníkem čísla a,

3) $\sigma(a) = \sigma(b) \implies a = b$,

4) $\nexists a, \sigma(a) = 0$,

5) Nechť V je vlastnost přirozených čísel a nechť:

   I. Pro nulu vlastnost V platí.

   II. Jestliže vlastnost V platí pro a, platí vlasnost V i pro $\sigma(a)$.

   Pak platí vlastnost V pro všechna přirozená čísla.

(Kubínová, Novotná, 1997)

Jak je popsáno ve skriptech *Posloupnosti a řady* (Kubínová, Novotná, 1997), lze pro tento systém vytvořit také množinový model následujícím způsobem:
Na množině $\mathbb{N}$ je definována nula a zobrazení σ: $\mathbb{N} \longrightarrow \mathbb{N}$ a platí:

(i) σ je injektivní,

(ii) $0 \notin \sigma(\mathbb{N})$,

(iii) Nechť $U \subset \mathbb{N}$ má tyto vlastnosti:

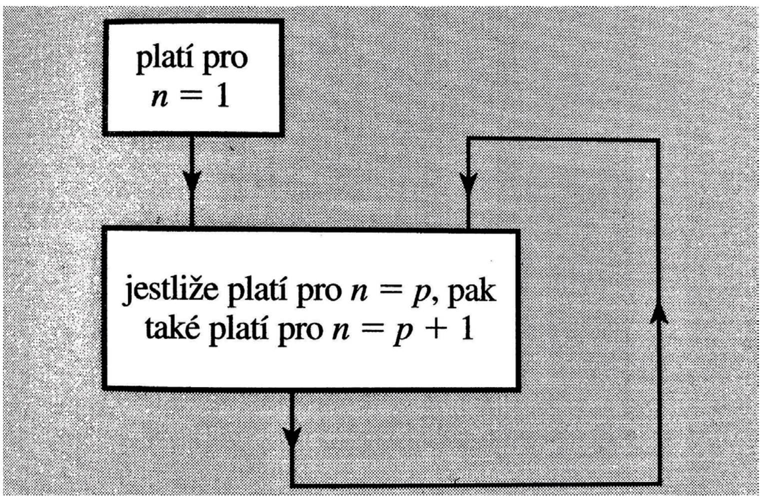
a) $0 \in U$,

b) $n \in U \implies \sigma(n) \in U$.

Pak $U = \mathbb{N}$.

- Třetí Peanův axiom říká, že zobrazení σ je prosté zobrazení množiny přirozených čísel do množiny přirozených čísel.

- Pátý Peanův axiom nazýváme axiomem indukce. Je na něm založena známá metoda důkazu vlastností přirozených čísel. Následující schéma 3 ze strany 87 knihy *1089 a další parádní čísla* od Davida Achesona princip ilustrativně znázorňuje.



Obrázek 3: Myšlenka principu matematické indukce (Acheson, 2006, s. 87)

Tento bod je někdy zaměňován za následující axiom:

5*) Nejsou jiná přirozená čísla než ta, která vzniknou z axiomů 1) a 2).

Následující věta ukazuje, že jsou oba axiomatické systémy ekvivalentní:

Věta 2. *Systém Peanových axiomů* $1) - 5)$ *je ekvivalentní se systémem* $1) - 4), 5^{\star})$.

Ekvivalence dvou systémů z věty 2 je zřejmá.

Pozn. 5. Nulu v definici 3 chápeme jako první prvek množiny přirozených čísel. Pokud z nějakého důvodu nulu jako takovou nepovažujeme za přirozené číslo, chápeme nulu v definici 2 jako jedničku.

Pozn. 6. Abychom předcházeli nedorozuměním, která by mohla být vyvolána zahrnutím či nezahrnutím nuly do množiny přirozených čísel, budeme v dalším textu, kde to bude mít význam, rozlišovat následující značení:

- $\mathbb{N}$ značí množinu přirozených čísel bez nuly,
- $\mathbb{N}_0$ značí množinu přirozených čísel včetně nuly.

Pozn. 7. Také je důležité zde zmínit, že v anglické literatuře (např. *The Number-System* [Thurston, 1956]) se nesetkáváme pouze s pojmem **natural numbers**, ale také **whole numbers**. **Whole numbers** ovšem nejsou chápána jako naše celá čísla, nýbrž právě jako čísla přirozená zahrnující nulu (tedy nezáporná). Pro celá čísla angličtina používá termín **integers**. Často je také v literatuře (např. *Number-System of Algebra* [Fine, 1907]) používán pouze výraz **Positive integers**, tedy kladná celá čísla.

4.3 Operace na množině přirozených čísel

Definice 4. Sčítání přirozených čísel je zobrazení $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, definované předpisem:

$$\forall a, b \in \mathbb{N} : a + b = \sigma^b(a).$$

Definice 5. Sčítání přirozených čísel definujeme za pomoci axiomu 5) z definice 3 takto:

(i) $\forall a \in \mathbb{N} : a + 0 = a$,

(ii) $\forall a, b \in \mathbb{N} : a + \sigma(b) = \sigma(a + b)$.

Věta 3. $\forall a, b \in \mathbb{N} : \sigma(a) + b = \sigma(a + b)$.

Důkaz. K důkazu použijeme matematickou indukci. Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že tvrzení platí pro $b = 0$:

$$\sigma(a) + 0 = \sigma(a + 0).$$

Podle definice 5 se levá strana rovná $\sigma(a)$ a pravá také $\sigma(a)$. Pro $b = 0$ a libovolné přirozené a tvrzení platí.

II. Předpokládejme, že pro $b \in \mathbb{N}$ platí $\sigma(a)+b = \sigma(a+b)$. Ověříme, že pak platí také $\sigma(a) + \sigma(b) = \sigma(a + \sigma(b))$:

$$\sigma(a) + \sigma(b) \overset{def.\,5}{=} \sigma(\sigma(a) + b) \overset{ind.předpoklad}{=} \sigma(\sigma(a + b)) \overset{def.\,5}{=} \sigma(a + \sigma(b)).$$

Tvrzení je pravdivé pro všechna $a, b \in \mathbb{N}$. □

Věta 4. *Definice sčítání na množině přirozených čísel 4 a 5 definují totožnou operaci.*

Důkaz. Sčítání z definice 4 budeme pro důkaz značit $+_1$. Obdobně sčítání z definice 5 označíme $+_2$.

K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b \in \mathbb{N}$ platí:

$$\forall a, b \in \mathbb{N} : a +_1 b = a +_2 b.$$

Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že rovnost platí pro $b = 0$. Chceme dokázat, že $a +_1 0 = = a +_2 0$. Levá strana se podle definice 5 rovná a. Pravá se také podle definice 5 rovná a. Tedy tvrzení platí pro $b = 0$ a libovolné přirozené a.

II. Nyní předpokládáme, že pro nějaké b přirozené platí $a +_1 b = a +_2 b$. Ověříme, že pak platí $a +_1 \sigma(b) = a +_2 \sigma(b)$:

$$a +_1 \sigma(b) \overset{def.\,4}{=} \sigma^{\sigma(b)}(a) = (\sigma \circ \sigma^b)(a) = \sigma(\sigma^b(a)) = \sigma(a +_1 b) =$$
$$\overset{ind.předpoklad}{=} \sigma(a +_2 b) \overset{def.\,5}{=} a +_2 \sigma(b).$$

Definice 4 a 5 definují stejnou operaci.

□

Věta 5. $\forall a, b, c \in \mathbb{N}$:

1) $a + b = b + a$, *(sčítání je komutativní)*

2) $(a + b) + c = a + (b + c)$, *(sčítání je asociativní)*

3) $0 + a = a + 0 = a$, *(nula je neutrální prvek vzhledem ke sčítání)*

4) $a + c = b + c \implies a = b$,
$a + b = 0 \implies (a = 0 \wedge b = 0)$. *(pravidla pro krácení)*

Důkaz. K většině důkazů použijeme matematickou indukci z definice 3. Také budeme používat definici 5.

1) Nejprve dokážeme komutativitu sčítání. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b \in \mathbb{N}$ platí:

$$a + b = b + a.$$

Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že rovnost platí pro $b = 0$. Chceme dokázat, že $a + 0 = 0 + a$. Levá strana se podle definice 5 rovná a. Pravá je podle definice 4 rovna $\sigma^a(0)$, což je také rovno a. Tedy komutativita platí pro libovolné a přirozené a $b = 0$.

II. Nyní předpokládáme, že pro $b \in \mathbb{N}$ platí $a + b = b + a$. Ověříme, že pak platí také $a + \sigma(b) = \sigma(b) + a$:

$$a + \sigma(b) \overset{def.\,5}{=} \sigma(a + b) \overset{ind.p\check{r}edpoklad}{=} \sigma(b + a) \overset{def.\,3}{=} \sigma(b) + a.$$

Sčítání je tedy komutativní pro všechna $a, b \in \mathbb{N}$.

2) Dokážeme asociativitu sčítání. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

$$(a + b) + c = a + (b + c).$$

Zvolme $a, b \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že rovnost platí pro $c = 0$. Chceme dokázat, že $(a+ +b) + 0 = a + (b + 0)$:

$$\left.\begin{aligned} L &: (a + b) + 0 \overset{def.5}{=} a + b \\ P &: a + (b + 0) \overset{def.5}{=} a + b \end{aligned}\right\} L = P.$$

Tedy asociativita sčítání platí pro libovolná přirozená a, b a $c = 0$.

II. Nyní předpokládejme, že pro nějaké c přirozené platí $(a+b)+c = a+(b+c)$. Ověříme, že pak platí také $(a + b) + \sigma(c) = a + (b + \sigma(c))$:

Nejprve upravíme levou stranu rovnosti:

$$L = (a+b)+\sigma(c) \overset{def.5}{=} \sigma((a+b)+c) \overset{ind.p\check{r}edpoklad}{=} \sigma(a+(b+c)) \overset{def.5}{=} a+\sigma(b+c).$$

Nyní upravíme stranu pravou:

$$P = a + (b + \sigma(c)) \overset{def.5}{=} a + \sigma(b + c).$$

Levá strana se rovná pravé.

Sčítání je tedy asociativní pro všechna $a, b, c \in \mathbb{N}$.

3) Platí, že $0+a = a+0 = a$? Víme již, že sčítání přirozených čísel je komutativní, platí tedy, že $a + 0 = 0 + a$. Z definice 5 také víme, že $a + 0 = a$. 0 je tedy neutrálním prvkem pro sčítání přirozených čísel.

4) Dokážeme první pravidlo pro krácení. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

$$a + c = b + c \Rightarrow a = b.$$

Zvolme $a, b \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že tvrzení platí pro $c = 0$. Chceme dokázat, že $a + 0 = = b + 0 \Rightarrow a = b$:

$$\left.\begin{aligned} L &: a + 0 \overset{def.5}{=} a \\ P &: b + 0 \overset{def.5}{=} b \end{aligned}\right\} \text{Tedy } a = b.$$

První pravidlo pro krácení tedy platí pro libovolná přirozená a, b a $c = 0$.

II. Nyní předpokládejme, že platí $(a+c = b+c) \Rightarrow a = b$ pro nějaké přirozené c. Ověříme, že pak platí také: $(a + \sigma(c) = b + \sigma(c)) \Rightarrow a = b$. Upravíme levou a pravou stranu předpokladu implikace:

$$\left.\begin{aligned} L &: a + \sigma(c) \overset{def.5}{=} \sigma(a + c) \\ P &: b + \sigma(c) \overset{def.5}{=} \sigma(b + c) \end{aligned}\right\} \text{Tedy } \sigma(a + c) = \sigma(b + c).$$

Peanův axiom 3) (viz definice 3) říká, že pokud se následníci dvou čísel rovnají, rovnají se čísla samotná. Tedy:

$$\sigma(a + c) = \sigma(b + c) \Rightarrow a + c = b + c.$$

Z indukčního předpokladu víme, že jestiže $a + c = b + c$, pak $a = b$.

$(a + c = b + c) \Rightarrow a = b$ tedy platí pro všechna $a, b, c \in \mathbb{N}$.

5) Platí $\forall a, b \in \mathbb{N} : a + b = 0 \Rightarrow (a = 0 \wedge b = 0)$?

   Důkaz povedeme sporem. Předpokládejme, že $\exists a, b \in \mathbb{N} : (a \neq 0 \vee b \neq 0) \wedge$ $\wedge (a + b = 0)$. Podle definice sčítání 4 přepíšeme $a + b$ jako $\sigma^b(a)$. Pro a, b mohou nastat následující situace:

   (a) $a \neq 0 \Rightarrow \sigma^b(a)$ je b-tým následníkem nenulového čísla a. Je-li $b = 0$, dostáváme $\sigma^0(a) = a$. Je-li $b \neq 0$, pak nenulový následník nenulového čísla rozhodně není nula (viz definice 3, axiom 4). To je spor s předpokladem, že $a + b = \sigma^b(a) = 0$.

   (b) $b \neq 0 \Rightarrow \sigma^b(a)$ je b-tým následníkem čísla a. Pokud je a nenulové, dostáváme případ, kdy jsou obě čísla nenulová, popsaný ve druhé části (a). Pokud je $a = 0$ nula, je b-tý následník nuly roven nenulovému číslu b. A to je spor s předokladem, že $a + b = \sigma^b(a) = 0$.

   Platí i druhé pravidlo pro krácení.

$\square$

Definice 6. Násobení přirozených čísel je zobrazení $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, definované předpisem:

$$\forall a, b \in \mathbb{N} : a \cdot b = (\sigma^a)^b(0).$$

Násobení přirozených čísel lze definovat také následujícím způsobem:

Definice 7. Násobení je operace splňující tyto podmínky:

(i) $\forall a \in \mathbb{N} : a \cdot 0 = 0$,

(ii) $\forall a, b \in \mathbb{N} : a \cdot \sigma(b) = a \cdot b + a$.

Věta 6. *Definice násobení 6 a 7 definují totožnou operaci.*

Důkaz. Násobení z definice 6 budeme v důkazu značit jako $\cdot_1$. Obdobně násobení z definice 7 označíme jako $\cdot_2$.

K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b \in \mathbb{N}$ platí:

$$\forall a, b \in \mathbb{N} : a \cdot_1 b = a \cdot_2 b.$$

Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že rovnost platí pro $b = 0$. Chceme dokázat, že $a \cdot_1 0 = a \cdot_2 0$. Levou a pravou stranu rovnosti přepíšeme podle příslušných definic násobení:

$$\left.\begin{aligned} L &: a \cdot_1 0 \overset{def.6}{=} (\sigma^a)^0(0) = 0 \\ P &: a \cdot_2 0 \overset{def.7}{=} 0 \end{aligned}\right\} L = P.$$

Definice 6 a 7 definují stejnou operaci pro a libovolné přirozené a $b = 0$.

II. Nyní předpokládáme, že pro nějaké b přirozené platí $a \cdot_1 b = a \cdot_2 b$. Ověříme, že pak platí také $a \cdot_1 \sigma(b) = a \cdot_2 \sigma(b)$:

$$\begin{aligned} & a \cdot_1 \sigma(b) = (\sigma^a)^{\sigma(b)}(0) = (\sigma^a \circ (\sigma^a)^b)(0) = \sigma^a((\sigma^a)^b(0)) = \sigma^a(a \cdot_1 b) = \\ & = a \cdot_1 b + a \overset{ind.předpoklad}{=} a \cdot_2 b + a = a \cdot_2 \sigma(b). \end{aligned}$$

Definice násobení přirozených čísel 6 a 7 tedy definují totožnou operaci.

□

Pozn. 8. Kde nebude hrozit nedorozumění, můžeme místo $a \cdot b$ psát pouze ab.

Definice 8. Prvek $\sigma(0)$ budeme značit 1 a nazývat jedničkou.

Věta 7. *Pro relaci $>$ na množině přirozených čísel definovanou takto:*

$$m > n \Leftrightarrow \exists r \in \mathbb{N} - \{0\} : m = n + r,$$

platí následující vlastnosti:

a) je tranzitivní,

b) je trichotomická.

Důkaz. a) Máme dokázat tranzitivitu relace $>$, tedy ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

$$(a > b) \wedge (b > c) \Rightarrow a > c.$$

Přepíšeme levou stranu implikace podle definice:

$$\exists r_1, r_2 \in \mathbb{N} - \{0\} : (a = b + r_1) \wedge (b = c + r_2).$$

Dosadíme do první rovnosti za b:

$$a = c + r_2 + r_1 = c + r_3, \text{ kde } r_3 = r_2 + r_1.$$

Protože r_3 je součet dvou nenulových přirozených čísel r_1, r_2, tedy také přirozené nenulové číslo, platí podle definice relace $>$, že $a > c$. Relace je tedy tranzitivní.

b) Dále máme dokázat, že relace je trichotomická. To znamená, že se ptáme, zda platí:

$$\forall a, b \in \mathbb{N} : (a > b) \oplus (b > a) \oplus (a = b),$$

kde symbol $\oplus$ značí logickou spojku XOR.
Z definice $+$ plyne, že nemůže nastat, že $(a = b) \wedge (a > b)$ nebo $(a = b) \wedge (b > a)$. Zbývá tedy ukázat, že nemůže nastat případ, kdy $(a > b) \wedge (b > a)$. Tvrzení dokážeme sporem. Předpokládejme, že:

$$\exists r_1, r_2 \in \mathbb{N} - \{0\} : a = b + r_1, b = a + r_2.$$

Dosadíme za b do první rovnosti:

$$a = a + r_2 + r_1 = a + (r_1 + r_2),$$

aby však tato rovnost platila, musela by obě čísla r_1, r_2 být rovna nule. To je však ve sporu s předpokladem, že $r_1, r_2 \neq 0$. Relace $>$ je tedy trichotomická.

$\square$

Pozn. 9. Relace $>$ je tranzitivní i trichotomická (viz věta 7). Je tedy uspořádáním na množině $\mathbb{N}$.

Věta 8. $\forall a, b \in \mathbb{N} : \sigma(b) \cdot a = b \cdot a + a.$

Důkaz. K důkazu použijeme matematickou indukci. Zvolme $b \in \mathbb{N}$ libovolné.

I. Ukážeme, že pro $a = 0$ tvrzení platí:

$$\sigma(b) \cdot 0 = b \cdot 0 + 0,$$

levá strana je podle definice 7 rovna nule. Pravá strana za využití věty 5 a definice 7 je také rovna nule. Tedy tvrzení pro libovolné přirozené b a $a = 0$ platí.

II. Předpokládejme, že pro nějaké a přirozené platí $\sigma(b) \cdot a = b \cdot a + a$. Ukážeme, že potom platí i pro $\sigma(a)$. Tedy, že platí:

$$\sigma(b) \cdot \sigma(a) = b \cdot \sigma(a) + \sigma(a).$$

Začneme upravovat levou stranu rovnosti:

$$\sigma(b) \cdot \sigma(a) \overset{def.\,7}{=} \sigma(b) \cdot a + \sigma(b) \overset{ind.\,předpoklad}{=} b \cdot a + a + \sigma(b) =$$
$$\overset{věta\,5}{=} a + \sigma(b) + b \cdot a \overset{věta\,3}{=} \sigma(a) + b + b \cdot a \overset{věta\,5}{=} \sigma(a) + b \cdot a + b =$$
$$\overset{def.\,7}{=} \sigma(a) + b \cdot \sigma(a) \overset{věta\,5}{=} b \cdot \sigma(a) + \sigma(a).$$

Tvrzení je tedy pravdivé pro všechna $a, b \in \mathbb{N}$. $\square$

Věta 9. $\forall a, b, c \in \mathbb{N}:$

1) $a \cdot b = b \cdot a$, *(násobení je komutativní)*

2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, *(násobení je asociativní)*

3) $0 \cdot a = a \cdot 0 = 0$, *(nula je tzv. agresivní prvek vzhledem k násobení)*

4) $1 \cdot a = a \cdot 1 = a$, *(jednička je neutrální prvek vzhledem k násobení)*

5) $(a + b) \cdot c = a \cdot c + b \cdot c$, *(násobení je distributivní vzhledem ke sčítání)*

6) $(c \neq 0 \wedge a \cdot c = b \cdot c) \implies a = b$,
$a \cdot b = 0 \implies (a = 0 \vee b = 0)$. *(pravidla pro krácení)*

Důkaz. 1) Nejprve ukážeme, že násobení je komutativní. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b \in \mathbb{N}$ platí:

$$a \cdot b = b \cdot a.$$

Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že tvrzení platí $b = 0$. Chceme tedy ukázat, že $a \cdot 0 = = 0 \cdot a$:

$$\left.\begin{array}{l} L : a \cdot 0 \overset{def.7}{=} 0 \\ P : 0 \cdot a \overset{def.6}{=} (\sigma^0)^a(0) = 0 \end{array}\right\} L = P.$$

Komutativita násobení tedy platí pro libovolné a a $b = 0$.

II. Nyní předpokládejme, že platí $a \cdot b = b \cdot a$ pro $b \in \mathbb{N}$. Ověříme, že pak platí také $a \cdot \sigma(b) = \sigma(b) \cdot a$.:

$$a \cdot \sigma(b) \overset{def.7}{=} a \cdot b + a \overset{\text{věta}\,5}{=} a + a \cdot b \overset{ind.předpoklad}{=} a + b \cdot a \overset{\text{věta}\,8}{=} \sigma(b) \cdot a.$$

Násobení je tedy komutativní pro všechna $a, b \in \mathbb{N}$.

5) Nyní dokážeme distributivitu násobení vzhledem ke sčítání, kterou později využijeme k důkazu asociativity násobení. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Zvolme $a, b \in \mathbb{N}$ libovolně.

I. Ukážeme, že tvrzení platí pro $c = 0$. Chceme dokázat, že $(a + b) \cdot 0 = = a \cdot 0 + b \cdot 0$. Z definice násobení 7 platí, že levá i pravá strana jsou rovny nule, a tedy se rovnají. Pro a, b libovolné přirozené a $c = 0$ distributivita násobení vzhledem ke sčítání platí.

II. Předpokládejme nyní, že platí $(a+b) \cdot c = a \cdot c+b \cdot c$ pro $c \in \mathbb{N}$. Dokážeme, že pak platí $(a + b) \cdot \sigma(c) = a \cdot \sigma(c) + b \cdot \sigma(c)$:

$$\left.\begin{aligned} L &: (a + b) \cdot \sigma(c) \overset{def.7}{=} (a + b) \cdot c + (a + b) \\ P &: a \cdot \sigma(c) + b \cdot \sigma(c) \overset{def.7}{=} a \cdot c + a + b \cdot c + b \overset{\star}{=} (a + b) \cdot c + (a + b) \end{aligned}\right\} L = P.$$

$\star$: Využili jsme komutativitu sčítání z věty 5 a indukční předpoklad.

Násobení je tedy distributivní vzhledem ke sčítání pro všechna $a, b, c \in \mathbb{N}$.

2) Nyní už můžeme ukázat, že násobení je asociativní. I zde k důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Zvolme $a, b \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že asociativita násobení platí pro $c = 0$. Chceme dokázat, že $(a \cdot b) \cdot 0 = a \cdot (b \cdot 0)$:

$$\left.\begin{aligned} L &: (a \cdot b) \cdot 0 \overset{def.7}{=} 0 \\ P &: a \cdot (b \cdot 0) \overset{def.7}{=} a \cdot 0 \overset{def.7}{=} 0 \end{aligned}\right\} L = P.$$

Asociativita násobení tedy platí pro libovolná přirozená čísla a, b a $c = 0$.

II. Nyní předpokládáme, že platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pro nějaké c přirozené. Ukážeme, že pak platí $(a \cdot b) \cdot \sigma(c) = a \cdot (b \cdot \sigma(c))$:

$$\left.\begin{aligned} L &: (a \cdot b) \cdot \sigma(c) \overset{def.7}{=} (a \cdot b) \cdot c + a \cdot b \overset{ind.předpoklad}{=} a \cdot (b \cdot c) + a \cdot b \\ P &: a \cdot (b \cdot \sigma(c)) \overset{def.7}{=} a \cdot (b \cdot c + b) \overset{distrib.nás.}{=} a \cdot (b \cdot c) + a \cdot b \end{aligned}\right\} L = P$$

Násobení je tedy asociativní pro všechna $a, b, c \in \mathbb{N}$.

3) Agresivita nuly vyplývá z definice 7 a již dokázané komutativity násobení.

4) Je 1 neutrální prvek vzhledem k násobení? Z již dokázané komutativity víme, že $1 \cdot a = a \cdot 1$. Také víme, že jednička je $\sigma(0)$. Za využití definice 7 dostáváme:

$$a \cdot \sigma(0) = a \cdot 0 + a = 0 + a.$$

Nula je neutrální prvek ke sčítání. Tedy $0 + a = a$.

1 je proto neutrálním prvkem vzhledem k násobení.

6) Nejprve dokážeme sporem druhé pravidlo pro krácení:

$$a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0).$$

Předpokládejme, že $\exists a, b \in \mathbb{N} : a \neq 0 \wedge b \neq 0 \wedge (a \cdot b = 0)$. Přepíšeme $a \cdot b$ podle definice 6:

$$a \cdot b = (\sigma^a)^b(0).$$

Pokud jsou však čísla a, b nenulová, pak $(\sigma^a)^b(0)$ nemůže být rovno nule, jelikož nula není následníkem žádného přirozeného čísla (viz definice 3, axiom 4). To je spor s předpokladem, že $(a \cdot b = 0)$ a původní věta o krácení platí.

Nyní dokážeme první z pravidel pro krácení. Ptáme se, zda pro všechna $a, b, c \in$ $\in \mathbb{N}$ platí:

$$(c \neq 0 \wedge a \cdot c = b \cdot c) \Rightarrow a = b.$$

Použijeme opět důkaz sporem. Předpokládejme, že $\exists a, b, c \in \mathbb{N} : a \neq b \wedge a \cdot c =$ $= b \cdot c \wedge c \neq 0$. Protože $a \neq b$, víme z věty 7, že nastává buď případ $a > b$, nebo $b > a$. Bez újmy na obecnosti můžeme předpokládat, že $a > b$. Platí potom, že $\exists d \in \mathbb{N} - \{0\} : a = b + d$. Potom $(b + d) \cdot c = b \cdot c$. Využijeme distributivitu násobení vzhledem ke sčítání a dostaneme $b \cdot c + d \cdot c = b \cdot c$. Podle věty 5 zkrátíme $b \cdot c$. Potom $d \cdot c = 0$. Z druhého pravidla o krácení víme, že $d = 0 \vee c = 0$. Protože podle předpokladu je $d \neq 0$, je 0 rovno c. To je ale spor s předpokladem, že $c \neq 0$. Původní věta o krácení je pravdivá.

$\square$

Pozn. 10. Definice a věty v kapitole 4.3 vycházejí ze skript *Posloupnosti a řady* (Kubínová, Novotná, 1997). Důkazy také vycházejí ze stejných skript, případně byly rozšířeny. Věty 3 a 8 jsou vlastní. Důkazy vět 3, 5, 8 a 9 jsou také vlastní.

4.4 Spočetnost

Pomocí přirozených čísel definujeme spočetnost, kterou se budeme zabývat i u nadoborů.

Definice 9. Množinu M nazveme spočetnou, jestliže existuje bijektivní zobrazení množiny M na množinu $\mathbb{N}$.

Pozn. 11. Je-li množina spočetná, lze ji chápat jako posloupnost.

Věta 10. *Množina přirozených čísel je spočetná množina.*

Důkaz. Plyne přímo z definice. Hledáme zobrazení $f\colon \mathbb{N} \to \mathbb{N}$, které je bijektivní. To splňuje například $f(x) = x$. □

Věta 11. *Množina přirozených čísel je nekonečná množina.*

Důkaz. Tvrzení dokážeme sporem. Předpokládejme, že existuje největší prvek množiny přirozených čísel m:

$$\exists m \in \mathbb{N} \quad \forall n \in \mathbb{N} : m \geqq n.$$

Z definice 3 však víme, že pro každý prvek $\mathbb{N}$ existuje jeho následník, který je také prvkem $\mathbb{N}$. Tedy i pro m existuje $\sigma(m)$. Pro takové číslo platí:

$$\sigma(m) > m.$$

To je ovšem ve sporu s předpokladem, že m je největším prvkem množiny $\mathbb{N}$. Množina přirozených čísel je tedy nekonečnou množinou. □

Pozn. 12. Indický matematik Ramanujan ukázal, že součet všech přirozených čísel je roven číslu $\frac{-1}{12}$. Způsob jeho argumentace a metodu sumace divergentní řady popisuje například článek *Divergent Series: why 1+2+3+. . . =-1/12* (Cais, 2010) dostupný online z http://math.arizona.edu/~cais/Papers/Expos/div.pdf.

4.5 Přirozená čísla jako algebraická struktura

Na množině přirozených číslech jsme definovali operace sčítání a násobení. Množina s nimi tvoří hned několik významných algebraických struktur.

Definice 10. Monoid je algebraická struktura s jednou vnitřní operací. Pro operaci platí, že je asociativní a má neutrální prvek.

(Bečvář, 2005)

Věta 12. *Množina* $\mathbb{N}_0$ *spolu s operací* $+$ *tvoří komutativní monoid.*

Důkaz.

1. $\forall a, b \in \mathbb{N}_0 : (a + b) \in \mathbb{N}_0$,
2. $\exists n \in \mathbb{N}_0 \quad \forall a \in \mathbb{N}_0 : n + a = a + n = a$,
3. $\forall a, b \in \mathbb{N}_0 : a + b = b + a$.

Uzavřenost operace $+$ na množině $\mathbb{N}$ platí podle definice 4. Bod druhý, tedy existence neutrálního prvku, platí podle věty 5. Komutativita sčítání je zaručena také z věty 5. □

Věta 13. *Množina* $\mathbb{N}_0$ *spolu s operací* $\cdot$ *tvoří komutativní monoid.*

Důkaz.

1. $\forall a, b \in \mathbb{N}_0 : (a \cdot b) \in \mathbb{N}_0$,
2. $\exists n \in \mathbb{N}_0 \quad \forall a \in \mathbb{N}_0 : n \cdot a = a \cdot n = a$,
3. $\forall a, b \in \mathbb{N}_0 : a \cdot b = b \cdot a$.

Uzavřenost operace násobení na množině přirozených čísel zaručuje definice 6. Existence neutrálního prvku stejně tak jako komutativita vyplývá z věty 9. □

Definice 11. Polookruh je algebraická struktura se dvěma vnitřními operacemi $+$ a $\cdot$. Vzhledem ke sčítání tvoří komutativní monoid a vzhledem k násobení monoid. Operace násobení je vzhledem ke sčítání distributivní.

(Hruša, 1970)

Věta 14. *Množina* $\mathbb{N}_0$ *tvoří spolu s operacemi* $+$ *a* $\cdot$ *polookruh.*

Důkaz. Podle vět 12 a 13 platí, že struktura $(\mathbb{N}, +)$ i struktura $(\mathbb{N}, \cdot)$ tvoří komutativní monoid.

Distributivita pak plyne z věty 9. $\square$

Pozn. 13. Přestože by se množina přirozených čísel mohla zdát jako probádaná, stále ji matematici se zájmem studují. V roce 2013 například český matematik Vopěnka v knize *Nová infinitní matematika* přišel se závěrem, že množina všech přirozených čísel neexistuje.