1 Teoria de conjuntos

2 Conjuntos Finitos e Infinitos

2.1 Números naturais

Temos como conceitos primitivos o conjunto dos naturais, denotado por $\mathbb{N}$, cujos elementos são os números naturais, e uma função $s : \mathbb{N} \to \mathbb{N}$. Para cada $n \in \mathbb{N}$, o número $s(n)$ é o sucessor de n. Temos os axiomas:

Axioma 1. *$s : \mathbb{N} \to \mathbb{N}$ é injetiva.*

Axioma 2. $\mathbb{N} - s(n) = \{1\}$. *Ou seja, só existe um número natural que não é sucessor de nenhum outro, e ele é denotado por* 1.

Proposição 1. *Todo natural diferente de* 1 *possui um antecessor.*

Proof. Seja $n \neq 1$ um número natural. Suponha que não exista n_0 natural com $s(n_0) = n$. Logo $n \notin s(\mathbb{N})$. Logo $n \in \mathbb{N} - s(n)$. Mas $\mathbb{N} - s(n) = \{1\}$. Logo $n = 1$. Contradição. Logo existe $n_0 \in \mathbb{N}$ tal que $s(n_0) = n$. □

Observação 2.1. Observe que a função $s : \mathbb{N} \to \mathbb{N} \setminus \{1\}$ é injetiva por definição e sobrejetiva pela proposicao 2.1, logo é uma bijeção entre um subconjunto dos naturais com os naturais.

Axioma 3 (Princípio de indução)**.** *Se $X \subset \mathbb{N}$ é um subconjunto tal que:*

$$\begin{cases} 1 \in X \\ \\ n \in X \implies s(n) \in X \end{cases}$$

Então $\mathbb{N} = X$.

Definição 2.1 (Soma)**.** Dados $m, n \in \mathbb{N}$, sua soma $m + n$ é definida como:

$$m + n := s^n(m).$$

A soma deve obedecer

$$m + 1 = s(m) \tag{1}$$

$$m + s(n) = s(m + n) \tag{2}$$

para todos os m, n naturais.

Observação 2.2. Dedekind prova o "Teorema da Definição por Indução" para garantir que a notação $s^n(m)$ faça sentido.

Proposição 2 (Associatividade da Soma)**.** *Para todos $p, m, n \in \mathbb{N}$, temos $m + (n + p) = (m + n) + p$.*

Proof. Seja $X = \{p \in \mathbb{N} \,|\forall m, n \in \mathbb{N} \,:\, m + (n + p) = (m + n) + p\}$. Da definição de adição, temos pra qualquer m, n que $n + 1 = s(n)$, logo $m + (n + 1) = m + s(n) = s(m + n) = (m + n) + 1 \implies m + (n + 1) = (m + n) + 1$. Logo $1 \in X$. Se $p \in X$, temos $m + (n + p) = (m + n) + p$. Logo

$$
\begin{aligned}
m + (n + s(p)) &= m + s(n + p) \\
&= s\,(m + (n + p)) \\
&= s\,((m + n) + p) \\
&= (m + n) + s(p).
\end{aligned}
$$

Logo $p \in X \implies s(p) \in X$. Temos que $X = \mathbb{N}$ pelo princípio de indução. Logo a soma é associativa nos naturais. ☐

Lema 1 (Comutatividade da soma com o 1)**.** *Para todo* $m \in \mathbb{N}$*, temos* $m + 1 = 1 + m$*.*

Proof. Seja $X = \{m \in \mathbb{N} \,|m + 1 = 1 + m\}$. Temos $1 \in X$, pois $1 + 1 = 1 + 1$. Supondo $m \in X$, logo $m + 1 = 1 + m$. Temos

$$
\begin{aligned}
1 + s(m) &= s(1 + m) \\
&= s(m + 1) \\
&= (m + 1) + 1 \\
&= s(m) + 1
\end{aligned}
$$

Como $m \in X \implies s(m) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. ☐

Proposição 3 (Comutatividade da soma)**.** *Para todos* $m, n \in \mathbb{N}$*, temos* $m + n = n + m$*.*

Proof. Seja $X = \{m \in \mathbb{N} \,|\forall n \in \mathbb{N} \,:\, m + n = n + m\}$. Temos $1 \in X$ pelo Lema

1. Supondo $m \in X$, logo $m + n = n + m$ para todo $n \in \mathbb{N}$. Temos

$$
\begin{aligned}
n + s(m) &= s(n + m) \\
&= s(m + n) \\
&= (m + n) + 1 \\
&= 1 + (m + n) \\
&= (1 + m) + n \\
&= (m + 1) + n \\
&= s(m) + n
\end{aligned}
$$

Como $1 \in X$ e $m \in X \implies s(m) \in X$, temos $X = \mathbb{N}$ pelo princípio de indução. $\square$

Proposição 4 (Lei do corte)**.** *Para todos $m, n, p \in \mathbb{N}$, temos $m+n = m+p \implies n = p$.*

Proof. Seja $X = \{m \in \mathbb{N} \,|\, \forall n \in \mathbb{N}\, \forall p \in \mathbb{N} \,:\, m + n = m + p \implies n = p\}$. Temos $1 \in X$ pois $1 + n = 1 + p \implies n + 1 = p + 1 \implies s(n) = s(p) \implies n = p$ pela injetividade de s. Supondo $m \in X$, temos $m + n = m + p \implies n = p$ para todos n, p naturais. Temos

$$
\begin{aligned}
s(m) + n = s(m) + p &\implies \\
n + s(m) = p + s(m) &\implies \\
s(n + m) = s(p + m) &\implies \\
n + m = p + m &\implies \\
m + n = m + p &\implies \\
n = p.&
\end{aligned}
$$

Logo $s(m) + n = s(m) + p \implies n = p$. Como $1 \in X$ e $m \in X \implies s(m) \in X$, temos $X = \mathbb{N}$ pelo princípio de indução. $\square$

Lema 2 (Não existem ciclos nos naturais)**.** *Para todos $m, p \in \mathbb{N}$, temos $m \neq m + p$.*

Proof. Suponha que $m = m + p$ com $m, p \in \mathbb{N}$. Logo $s(m) = s(m + p) \implies m+1 = (m+p)+1 \implies m+1 = m+(p+1) \implies 1 = p+1 \implies s(p) = 1$. Como 1 não é sucessor de nenhum natural, temos uma contradição. Logo $m \neq m + p$ para todos naturais m, p. □

Lema 3 (Unicidade da Tricotomia)**.** *Dados dois naturais m e n, apenas uma das 3 possibilidades ocorre:*

$$\begin{cases} m = n \\ \\ \exists p \in \mathbb{N} \,:\, m = n + p \\ \\ \exists q \in \mathbb{N} \,:\, n = m + q \end{cases}$$

Proof. Pelo lema 2, se $m = n$, não podemos ter $m = n + p = m + p$ ou $n = m + q = n + q$ para algum $p, q \in \mathbb{N}$. Se $\exists p \in \mathbb{N} \,:\, m = n + p$, não podemos ter $m = n$ pelo lema 2 e não podemos ter $\exists q \in \mathbb{N} \,:\, n = m + q$, pois teríamos $m = n + p = (m + q) + p = m + (q + p) \implies m = m + (q + p)$, que contradiz o lema 2. □

Proposição 5 (Tricotomia)**.** *Dados dois naturais m e n, exatamente uma das 3 possibilidades ocorre:*

$$\begin{cases} m = n \\ \\ \exists p \in \mathbb{N} \,:\, m = n + p \\ \\ \exists q \in \mathbb{N} \,:\, n = m + q \end{cases}$$

Proof. Seja $X = \{m \in \mathbb{N} | \forall n \in \mathbb{N} \,:\, (m = n) \vee (\exists p \in \mathbb{N} \,:\, m = n + p) \vee (\exists q \in \mathbb{N} \,:\, n = m + q)\}$, ou seja: o conjunto dos números naturais que satisfazem pelo menos uma das condições da tricotomia para todo n.

$1 \in X$, pois dado $n \in \mathbb{N}$, temos $n = 1$ ou $n \neq 1$. Se $n = 1$, temos $m = 1 = n$. Se $n \neq 1$, como $\mathbb{N} - s(\mathbb{N}) = \{1\}$, temos que existe um $n_0 \in \mathbb{N}$ tal que $s(n_0) = n$. Logo $n = n_0 + 1 \implies \exists q \,:\, n = q + 1 = q + m$.

Supondo $m \in X$. Dado $n \in \mathbb{N}$, se $m = n$, temos $s(m) = s(n) = n + 1$, logo $\exists p \in \mathbb{N} \,:\, s(n) = n + p$. Se $\exists p \in \mathbb{N} \,:\, m = n + p$, temos $s(m) = s(n + p) = (n + p + 1) = n + s(p)$, logo $\exists p' \in \mathbb{N} \,:\, s(n) = n + p'$. Se $\exists q \in \mathbb{N} \,:\, n = m + q$ com $q = 1$, temos $n = m + 1 = s(m)$. Se $\exists q \in \mathbb{N} \,:\, n = m + q$ com $q \neq 1$, existe $q_0 \in \mathbb{N}$ tal que $s(q_0) = q$, logo temos $n = m + q = m + s(q_0) = m + (q_0 + 1) = m + 1 + q_0 = s(m) + q_0 \implies \exists q' \in \mathbb{N} \,:\, n = s(m) + q'$.

Como $1 \in X$ e $m \in X \implies s(m) \in X$, temos $X = \mathbb{N}$. Logo para todo par $m, n \in \mathbb{N}$, pelo menos uma das condições da tricotomia ocorre. Pelo lema 3, apenas uma das possbilidades ocorre. □

Definição 2.2 ($<$)**.**

$$m < n \iff \exists p \in \mathbb{N} : n = m + p$$

Dados m, n naturais, dizemos que m é menor que n ($m < n$) quando existe $p \in \mathbb{N}$ tal que $n = m + p$.

Proposição 6. *Temos* $1 < n$ *para todo* $1 \neq n \in \mathbb{N}$ *.*

Proof. Como $n \neq 1$, temos pela proposição que n possui um antecessor. Logo existe n_0 tal que $s(n_0) = n \implies n = 1 + n_0$. Logo $1 < n$. □

Definição 2.3 ($\leq$)**.**

$$m \leq n \iff (m = n) \vee (m < n)$$

Proposição 7 (Transitividade da relação $<$)**.** $m < n \wedge n < p \implies m < p$

Proof. Se $m < n$ e $n < p$, temos $n = m + q$ e $p = n + r$ para algum par $q, r \in \mathbb{N}$. Logo $p = n + r = (m + q) + r = m + (q + r)$. Logo $m < p$. □

Proposição 8 (Tricotomia da relação $<$)**.** *Dados* $m, n \in \mathbb{N}$*, exatamente uma das afirmações ocorre:* $m = n$*, ou* $m < n$*, ou* $n < m$*.*

Proof. Segue diretamente da proposição 5. □

Proposição 9. *Dados* m, n, p *naturais, temos*

$$m + p < n + p \implies m < n.$$

Proof. Temos $m + p < n + p \implies \exists q \in \mathbb{N} : n + p = (m + p) + q \implies \exists q \in \mathbb{N} : n = m + q \implies m < n$. □

Definição 2.4 (Multiplicação)**.** Para todo $m \in \mathbb{N}$, seja $f_m : \mathbb{N} \to \mathbb{N}$ que associa cada $p \in \mathbb{N}$ a $f_m(p) = m + p$. Dados $m, n \in \mathbb{N}$, o produto entre naturais satisfaz $m \cdot 1 = m$ e $m \cdot (n + 1) = (f_m)^n(m)$.

Lema 4 (Distributiva do sucessor)**.**

$$m \cdot (n + 1) = mn + m$$

Proof. Se $n = 1$, temos $m \cdot (1 + 1) = (f_m)^1(m) = f_m(m) = m + m = m \cdot 1 + m$. Se $n \neq 1$, existe $n_0 \in \mathbb{N}$ tal que $s(n_0) = n$. Logo temos $m \cdot (n+1) = (f_m)^n(m) = (f_m)^{s(n_0)}(m) = f_m((f_m)^{n_0}(m)) = f_m(m(n_0 + 1)) = f_m(m \cdot n) = mn + m$. □

Proposição 10 (Distributiva à esquerda)**.**

$$m \cdot (n + p) = mn + mp$$

Proof. Seja $X = \{p \in \mathbb{N} | \forall m, n \in \mathbb{N} : n \cdot (m + p) = nm + np\}$. Temos $1 \in X$ pelo lema 2.1. Supondo $p \in X$. Temos

$$
\begin{aligned}
n \cdot (m + s(p)) &= n \cdot ((m + p) + 1) \\
&= n \cdot (m + p) + n \\
&= nm + np + n \\
&= nm + n(p + 1) \\
&= nm + n \cdot s(p)
\end{aligned}
$$

Como $p \in X \implies s(p) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. □

Proposição 11 (Distributiva à direita)**.**

$$(m + n) \cdot p = mp + np$$

Proof. Seja $X = \{p \in \mathbb{N} | \forall m, n \in \mathbb{N} : (m + n) \cdot p = mp + np\}$. Temos $1 \in X$, pos $(m + n) \cdot 1 = m + n = m \cdot 1 + n \cdot 1$. Supondo $p \in X$. Temos

$$
\begin{aligned}
(m + n) \cdot s(p) &= (m + n) \cdot (p + 1) \\
&= (m + n) \cdot p + (m + n) \\
&= mp + np + m + n \\
&= mp + m + np + n \\
&= m(p + 1) + n(p + 1) \\
&= m \cdot s(p) + n \cdot s(p)
\end{aligned}
$$

Como $p \in X \implies s(p) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. □

Proposição 12 (Associatividade)**.**

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

Proof. Seja $X = \{p \in \mathbb{N} | \forall m, n \in \mathbb{N} : m \cdot (n \cdot p) = (m \cdot n) \cdot p\}$. Temos $m \cdot (n \cdot 1) = m \cdot n = (m \cdot n) \cdot 1$, logo $1 \in X$.

Supondo $p \in X$. Temos

$$\begin{aligned} m \cdot (n \cdot s(p)) &= m \cdot (n \cdot (p+1)) \\ &= m \cdot (n \cdot p + n) \\ &= m \cdot (n \cdot p) + m \cdot n \\ &= (m \cdot n) \cdot p + (m \cdot n) \\ &= (m \cdot n) \cdot (p+1) \\ &= (m \cdot n) \cdot s(p) \end{aligned}$$

Como $p \in X \implies s(p) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. $\square$

Lema 5 (Comutatividade com 1)**.**

$$m \cdot 1 = 1 \cdot m$$

Proof. Seja $X = \{m \in \mathbb{N} | m \cdot 1 = 1 \cdot m\}$. Temos $1 \cdot 1 = 1 \cdot 1$, logo $1 \in X$. Supondo $m \in X$. Temos

$$\begin{aligned} s(m) \cdot 1 &= (m+1) \cdot 1 \\ &= m + 1 \\ &= m \cdot 1 + 1 \cdot 1 \\ &= 1 \cdot m + 1 \cdot 1 \\ &= 1 \cdot (m+1) \\ &= 1 \cdot s(m) \end{aligned}$$

Como $m \in X \implies s(m) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. $\square$

Proposição 13 (Comutatividade)**.**

$$m \cdot n = n \cdot m$$

Proof. Seja $X = \{n \in \mathbb{N} | \forall m \in \mathbb{N} : m \cdot n = n \cdot m\}$. Temos $1 \in X$ pelo lema 5. Supondo $n \in X$. Temos

$$\begin{aligned} m \cdot s(n) &= m \cdot (n+1) \\ &= mn + m \cdot 1 \\ &= nm + 1 \cdot m \\ &= (n+1) \cdot m \\ &= s(n) \cdot m \end{aligned}$$

Como $p \in X \implies s(p) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. □