

# 1 Teoria de conjuntos

**Proposição 1.1.**

$$(A - B) \cup B = A \cup B$$

*Proof.*

$$x \in (A - B) \cup B \iff$$

$$(x \in A \wedge x \notin B) \vee x \in B \iff$$

$$(x \in A \vee x \in B) \wedge (x \notin B \vee x \in B) \iff$$

$$(x \in A \vee x \in B) \wedge t \iff$$

$$x \in A \vee x \in B \iff$$

$$x \in A \cup B \iff$$

□

*Observação 1.1.* Acima,  $t$  representa tautologia. Algo que sempre tem valor lógico verdadeiro.

**Proposição 1.2.**

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

*Proof.*

$$(x, y) \in A \times (B \cup C) \iff x \in A \wedge (y \in B \cup C)$$

$$\iff x \in A \wedge (y \in B \vee y \in C)$$

$$\iff (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C)$$

$$\iff ((x, y) \in A \times B) \vee ((x, y) \in A \times C)$$

$$\iff (x, y) \in (A \times B) \cup (A \times C)$$

□

**Proposição 1.3.** Se  $A \subset B$  e  $B - A = \emptyset$ , então  $A = B$ .

*Proof.* O caso  $A = B = \emptyset$  é trivial. Supondo  $B \neq \emptyset$ . Supondo  $A \subset B$  e  $B - A = \emptyset$ . Como já temos  $A \subset B$ , basta provar  $B \subset A$ .

Supondo  $x \in B$  e  $x \notin A$ . Como  $B - A = \emptyset$ , temos  $x \in \emptyset$  (contradição). Logo se  $x \in B$ , devemos ter  $x \in A$ . Logo  $B \subset A$ . Logo  $A = B$ .  $\square$

**Lema 1.** *Existe uma bijeção entre  $X$  e  $X \times \{a\}$ .*

*Proof.* Seja a função  $g : X \rightarrow X \times \{a\}$ , dada por  $g(x) = (x, a)$ . Temos  $g(p) = g(q) \iff (p, a) = (q, a) \iff p = q$ , logo  $g$  é injetiva. Dado  $(x, a) \in X \times \{a\}$ , temos  $x \in X$  e  $a \in \{a\}$ . Logo existe  $x \in X$  tal que  $g(x) = (x, a)$ . Portanto  $g$  é sobrejetiva. Como  $g$  é injetiva e sobrejetiva, temos  $g$  bijetiva.  $\square$

**Lema 2.** *Existe uma bijeção entre  $X$  e  $\mathcal{F}(\{a\}, X)$ .*

*Proof.* Seja a função  $g : X \rightarrow \mathcal{F}(\{a\}, X)$ , dada por  $g(x) = f_x$ , onde  $f_x : \{a\} \rightarrow X$ ,  $f_x(a) = x$ . Temos  $g(p) = g(q) \iff f_p(a) = f_q(a) \iff p = q$ , logo  $g$  é injetiva. Dado  $f \in \mathcal{F}(\{a\}, X)$ , seja  $p = f(a)$ . Temos  $g(p) = f_p = f$ . Logo existe  $p \in X$  tal que  $g(p) = f$ . Portanto  $g$  é sobrejetiva. Como  $g$  é injetiva e sobrejetiva, temos  $g$  bijetiva.  $\square$

**Lema 3.** *Existe uma bijeção entre  $\mathcal{F}(X, Y) \times \mathcal{F}(\{a\}, Y)$  e  $\mathcal{F}(X \cup \{a\}, Y)$ , com  $a \notin X$ .*

*Proof.* Seja  $\phi : \mathcal{F}(X \cup \{a\}, Y) \rightarrow \mathcal{F}(X, Y) \times \mathcal{F}(\{a\}, Y)$ . Que associa  $f : X \cup \{a\} \rightarrow Y$  a  $(g, h)$ , onde  $g : X \rightarrow Y$ ,  $g(x) = f(x)$  e  $h : \{a\} \rightarrow Y$ ,  $h(a) = f(a)$ . Se  $\phi(f_1) = \phi(f_2)$ , temos  $(g_1, h_1) = (g_2, h_2)$ , que implica  $g_1 = g_2$  e  $h_1 = h_2$ . Logo  $f_1 = f_2$ . Logo  $\phi$  é injetiva.

Seja  $(g_0, h_0) \in \mathcal{F}(X, Y) \times \mathcal{F}(\{a\}, Y)$ . Seja  $f : X \cup \{a\} \rightarrow Y$ ,  $f(x) = \begin{cases} g_0(x), & x \in X \\ h_0(a), & x = a \end{cases}$ .

Temos  $\phi(f) = (g_0, h_0)$ , logo  $\phi$  é sobrejetiva.

Como  $\phi$  é injetiva e sobrejetiva, temos  $\phi$  bijetiva.  $\square$

**Proposição 1.4.** *Se  $f : X \rightarrow Y$  e  $g : Y \rightarrow Z$  são bijeções, então  $(g \circ f) : X \rightarrow Z$  é uma bijeção.*

*Proof.* Temos  $g(f(a)) = g(f(b)) \implies f(a) = f(b) \implies a = b$ . Logo  $g \circ f$  é injetiva.

Tomando  $z \in Z$ . Como  $g$  é sobrejetiva, existe  $y \in Y$  tal que  $g(y) = z$ . Como  $f$  é sobrejetiva, existe  $x \in X$  tal que  $f(x) = y$ . Logo existe  $x \in X$  tal que  $g(f(x)) = g(y) = z$ . Logo  $g \circ f$  é sobrejetiva.  $\square$

**Proposição 1.5.** *Seja  $f : X \rightarrow Y$  uma função sobrejetiva.  $f$  admite inversa à direita.*

*Proof.* Para todo  $y \in Y$ , temos  $f^{-1}(y) \neq \emptyset$ , logo existe  $x_y \in f^{-1}(y)$  tal que  $f(x_y) = y$ . Defina  $g : Y \rightarrow X$ , que associa  $y \rightarrow x_y$  (axioma da escolha). Logo temos  $f(g(y)) = f(x_y) = y$ .  $\square$

**Proposição 1.6.** *Se  $f : X \rightarrow Y$  é uma injeção então  $f' : X \rightarrow f(X)$ , definida como  $f'(x) = f(x)$ , é uma bijeção.*

*Proof.* Seja  $y \in f(X)$ . Por definição de  $f(X)$ , existe  $x \in X$  tal que  $f(x) = y$ . Logo  $f'$  é sobrejetiva. Dados  $a, b \in X$  com  $f'(a) = f(a) = f(b) = f'(b)$ . Como  $f$  é injetiva, temos  $a = b$ , logo  $f'$  é injetiva.  $\square$

**Proposição 1.7.** *Se  $f : A \cup B \rightarrow C$  é uma bijeção, então  $f' : A \rightarrow C - f(B)$ ,  $a \mapsto f(a)$  é uma bijeção.*

*Proof.* Se  $a, b \in A \subset A \cup B$ , temos  $f'(a) = f'(b) \iff f(a) = f(b) \implies a = b$  ( $f$  é injetiva). Logo  $f'$  é injetiva.

Tomando  $y \in C - f(B)$ . Como  $f$  é sobrejetiva, existe  $x \in A \cup B$  tal que  $f(x) = y$ . Se  $x \in B$ , teríamos  $f(x) \in f(B)$ , logo  $f(x) \notin C - f(B)$  (contradição). Logo devemos ter  $x \in A$ . Logo existe  $x \in A$  tal que  $f'(x) = f(x) = y$ . Logo  $f'$  é sobrejetiva.  $\square$

**Proposição 1.8.** *Se  $f : A \rightarrow B$  é uma bijeção e  $C \subset B$ , então  $f' : f^{-1}(C) \rightarrow C$ ,  $x \mapsto f(x)$  é uma bijeção.*

*Proof.* Se  $a, b \in f^{-1}(C) \subset A$ , temos  $f'(a) = f'(b) \iff f(a) = f(b) \implies a = b$  ( $f$  é injetiva). Logo  $f'$  é injetiva.

Tomando  $y \in C$ . Como  $f$  é sobrejetiva, existe  $x \in A$  tal que  $f(x) = y \in C$ . Como  $f(x) \in C$ , temos  $x \in f^{-1}(C)$ . Logo existe  $x \in f^{-1}(X)$  tal que  $f(x) = f'(x) = y$ . Logo  $f'$  é sobrejetiva.  $\square$

**Proposição 1.9.** *Seja  $f : A \rightarrow B$  uma função e  $X \subset Y \subset B$ . Temos  $f^{-1}(X) \subset f^{-1}(Y)$ .*

*Proof.* Se  $x \in f^{-1}(X)$ , temos  $f(x) \in X$ . Como  $X \subset Y$ , temos  $f(x) \in Y$ . Portanto  $x \in f^{-1}(Y)$ . Como  $x \in f^{-1}(X) \implies x \in f^{-1}(Y)$ , temos  $f^{-1}(X) \subset f^{-1}(Y)$ .  $\square$

**Proposição 1.10.** *Seja  $f : A \rightarrow B$  uma função bijetiva e  $X, Y \subset B$ . Temos  $f^{-1}(X) = f^{-1}(Y) \iff X = Y$ .*

*Proof.* Se  $X = Y$  é direto. Supondo  $f^{-1}(X) = f^{-1}(Y)$ . Se  $x \in X$ , existe  $a \in A$  tal que  $f(a) = x$ . Logo  $a \in f^{-1}(X)$ . Portanto  $a \in f^{-1}(Y)$ . Logo  $x = f(a) \in Y$ . Temos  $x = f(a) \in X \implies x = f(a) \in Y$ . Para  $y \in Y$  é análogo. Logo temos  $X = Y$ .  $\square$

**Proposição 1.11.** *Se existe a bijeção  $f : \{a\} \rightarrow X$ , então  $X = \{b\}$  para algum  $b$ .*

*Proof.* Seja  $b = f(a) \in X$ . Seja  $c \in X$ . Como  $f$  é sobrejetiva, existe  $k \in \{a\}$  tal que  $f(k) = c$ . Temos obrigatoriamente que  $k = a$ , logo  $b = f(a) = c$ . Logo  $X = \{b\}$ .  $\square$

**Proposição 1.12.** *Se  $f : A \rightarrow B$  e  $g : C \rightarrow D$  são bijeções, então  $h : A \times B \rightarrow B \times D$ ,  $h(a, c) = (f(a), g(c))$  é uma bijeção.*

*Proof.* Seja  $(b, d) \in B \times D$ . Como  $f$  e  $g$  são sobrejetivas, existem  $a \in A$  e  $c \in C$  tal que  $f(a) = b$  e  $g(c) = d$ . Logo existe  $(a, c) \in A \times C$  tal que  $h(a, c) = (f(a), g(c)) = (b, d)$ . Logo  $h$  é sobrejetiva.

Suponha  $h((a, b)) = h((c, d)) \iff (f(a), g(b)) = (f(c), g(d)) \iff f(a) = f(c) \wedge g(b) = g(d)$ . Como  $f$  e  $g$  são injetivas, temos  $f(a) = f(c) \implies a = c$  e  $g(b) = g(d) \implies b = d$ . Logo  $h$  é injetiva. Como  $h$  é injetiva e sobrejetiva, temos que  $h$  é bijetiva.  $\square$

**Proposição 1.13.** *Se  $f : A \rightarrow B$  é uma bijeção, então existe uma bijeção entre  $\mathcal{F}(A, C)$  e  $\mathcal{F}(B, C)$ .*

*Proof.* Definimos  $\phi : \mathcal{F}(A, C) \rightarrow \mathcal{F}(B, C)$ , que associa  $g : A \rightarrow C$  a  $h = g \circ f^{-1} : B \rightarrow C$ . Se  $\phi(p) = \phi(q)$ , temos  $p \circ f^{-1} = q \circ f^{-1}$ , logo  $(p \circ f^{-1}) \circ f = (q \circ f^{-1}) \circ f \implies p = q$ , logo  $\phi$  é injetiva. Seja  $p \in \mathcal{F}(B, C)$ . Seja  $h = p \circ f : A \rightarrow C$ . Temos  $h \in \mathcal{F}(A, C)$  com  $\phi(h) = (p \circ f) \circ f^{-1} = p$ , logo  $\phi$  é sobrejetiva.  $\square$

**Proposição 1.14.** *Se  $f : A \rightarrow B$  é uma bijeção, então existe uma bijeção entre  $\mathcal{F}(C, A)$  e  $\mathcal{F}(C, B)$ .*

*Proof.* Definimos  $\phi : \mathcal{F}(C, A) \rightarrow \mathcal{F}(C, B)$ , que associa  $g : C \rightarrow A$  a  $h = f \circ g : C \rightarrow B$ . Se  $\phi(p) = \phi(q)$ , temos  $f \circ p = f \circ q$ , logo  $f^{-1} \circ (f \circ p) = f^{-1} \circ (f \circ q) \implies p = q$ , logo  $\phi$  é injetiva. Seja  $p \in \mathcal{F}(C, B)$ . Seja  $h = f^{-1} \circ p : C \rightarrow A$ . Temos  $h \in \mathcal{F}(C, A)$  com  $\phi(h) = f \circ (f^{-1} \circ p) = p$ , logo  $\phi$  é sobrejetiva.  $\square$

**Proposição 1.15.** *Não existe sobrejeção entre  $X$  e  $\mathcal{P}(X)$ .*

*Proof.* Suponha que exista a sobrejeção  $f : X \rightarrow \mathcal{P}(X)$ . Seja  $A = \{x \in X \mid x \notin f(x)\}$ . Temos  $A \in \mathcal{P}(X)$ . Como  $f$  é sobrejetiva, existe  $p \in X$  tal que  $f(p) = A$ . Temos  $p \in A$  ou  $p \notin A$ . Se  $p \in A$ , obtemos uma contradição, pois  $x \in A \iff x \notin f(x)$  e  $f(p) = A$ . Se  $p \notin A$ , temos  $p \in A$ , pela definição de  $A$ . Em ambos os casos, obtemos uma contradição. Logo não existe sobrejeção entre  $X$  e  $\mathcal{P}(X)$ .  $\square$

**Proposição 1.16.** *Existe injeção entre  $X$  e  $\mathcal{P}(X)$ .*

*Proof.* Seja  $f : X \rightarrow \mathcal{P}(X)$ ,  $f(x) = \{x\}$ . Temos  $f(x) = f(y) \iff \{x\} = \{y\} \iff x = y$ . Logo  $f$  é injetiva.  $\square$

## 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  $s : \mathbb{N} \rightarrow \mathbb{N}$ . Para cada  $n \in \mathbb{N}$ , o número  $s(n)$  é o sucessor de  $n$ . Temos os axiomas:

**Axioma 1.**  $s : \mathbb{N} \rightarrow \mathbb{N}$  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 2.1.** *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  $n \in \mathbb{N} - s(\mathbb{N})$ . Mas  $\mathbb{N} - s(\mathbb{N}) = \{1\}$ . Logo  $n = 1$ . Contradição. Logo existe  $n_0 \in \mathbb{N}$  tal que  $s(n_0) = n$ .  $\square$

*Observação 2.1.* Observe que a função  $s : \mathbb{N} \rightarrow \mathbb{N} \setminus \{1\}$  é injetiva por definição e sobrejetiva pela proposição 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 2.2** (Associatividade da Soma). *Para todos  $p, m, n \in \mathbb{N}$ , temos  $m + (n + p) = (m + n) + p$ .*

*Proof.* Seja  $X = \{p \in \mathbb{N} \mid \forall m, n \in \mathbb{N} : m + (n + p) = (m + n) + p\}$ . 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.  $\square$

**Lema 4** (Comutatividade da soma com o 1). *Para todo  $m \in \mathbb{N}$ , temos  $m + 1 = 1 + m$ .*

*Proof.* Seja  $X = \{m \in \mathbb{N} \mid m + 1 = 1 + m\}$ . 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  $X = \mathbb{N}$ .  $\square$

**Proposição 2.3** (Comutatividade da soma). *Para todos  $m, n \in \mathbb{N}$ , temos  $m + n = n + m$ .*

*Proof.* Seja  $X = \{m \in \mathbb{N} \mid \forall n \in \mathbb{N} : m + n = n + m\}$ . Temos  $1 \in X$  pelo Lema 4. 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 2.4** (Lei do corte). *Para todos  $m, n, p \in \mathbb{N}$ , temos  $m + n = m + p \implies n = p$ .*

*Proof.* Seja  $X = \{m \in \mathbb{N} \mid \forall n \in \mathbb{N} \forall p \in \mathbb{N} : m + n = m + p \implies n = p\}$ . 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

$$s(m) + n = s(m) + p \implies$$

$$n + s(m) = p + s(m) \implies$$

$$s(n + m) = s(p + m) \implies$$

$$n + m = p + m \implies$$

$$m + n = m + p \implies$$

$$n = p.$$

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 5** (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  $m, p$ .  $\square$

**Lema 6** (Unicidade da Tricotomia). *Dados dois naturais  $m$  e  $n$ , apenas uma das 3 possibilidades ocorre:*

$$\left\{ \begin{array}{l} m = n \\ \exists p \in \mathbb{N} : m = n + p \\ \exists q \in \mathbb{N} : n = m + q \end{array} \right.$$

*Proof.* Pelo lema 5, 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 5 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 5.  $\square$

**Proposição 2.5** (Tricotomia). *Dados dois naturais  $m$  e  $n$ , exatamente uma das 3 possibilidades ocorre:*

$$\left\{ \begin{array}{l} m = n \\ \exists p \in \mathbb{N} : m = n + p \\ \exists q \in \mathbb{N} : n = m + q \end{array} \right.$$

*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 6, apenas uma das possibilidades ocorre.  $\square$

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

*Proof.* Como  $n \neq 1$ , temos pela proposição 2.1 que  $n$  possui um antecessor. Logo existe  $n_0$  tal que  $s(n_0) = n \implies n = 1 + n_0$ . Logo  $1 < n$ .  $\square$

**Definição 2.3** ( $\leq$ ).

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

**Proposição 2.7** (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  $m < p$ .  $\square$

**Proposição 2.8** (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 2.5.  $\square$

**Proposição 2.9.**

$$p \leq q \wedge q \leq p \iff p = q$$

*Proof.* Supondo  $p = q$ , temos  $p \leq q$  e  $q \leq p$ .

Supondo  $p \leq q \wedge q \leq p$ . Se  $p = q$ , acabou a demonstração. Supondo  $p \neq q$ . Logo devemos ter  $p < q$  e  $q < p$  (contradição). Logo devemos ter  $p = q$ .  $\square$

**Proposição 2.10.** *Dados  $m, n, p$  naturais, temos*

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

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

**Lema 7.**

$$m < n + 1 \iff m \leq n$$

*Proof.* Supondo  $m < n + 1$ . Logo existe  $q \in \mathbb{N}$  tal que  $n + 1 = m + q$ . Se  $q = 1$ , temos  $n + 1 = m + 1 \implies n = m \implies m \leq n$ . Se  $q \neq 1$ , existe  $q_0$  tal que  $s(q_0) = q$ . Logo  $n + 1 = m + s(q_0) = m + q_0 + 1 \implies n = m + q_0 \implies m < n \implies m \leq n$ .

Se  $m \leq n$ , temos  $m \leq n < n + 1 \implies m < n + 1$ .  $\square$

**Definição 2.4** (Multiplicação). Para todo  $m \in \mathbb{N}$ , seja  $f_m : \mathbb{N} \rightarrow \mathbb{N}$  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 8** (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  $m \cdot (n + 1) = (f_m)^n(m) = (f_m)^{s(n_0)}(m) = f_m((f_m)^{n_0}(m)) = f_m(m(n_0 + 1)) = f_m(m \cdot n) = mn + m$ .  $\square$

**Proposição 2.11** (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 2.12** (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  $1 \in X$ , pois  $(m + n) \cdot 1 = m + n = m \cdot 1 + n \cdot 1$ . 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 2.13** (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  $X = \mathbb{N}$ . □

**Lema 9** (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  $X = \mathbb{N}$ . □

**Proposição 2.14** (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 9. 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  $X = \mathbb{N}$ . □

**Proposição 2.15** (Monotonicidade).

$$m < n \implies mp < np$$

*Proof.* Supondo  $m < n$ . Logo  $n = m + q$  com  $q \in \mathbb{N}$ . Logo  $np = (m + q)p = mp + qp$ . Como  $qp \in \mathbb{N}$ , temos  $mp < np$ . □

**Proposição 2.16** (Lei do cancelamento).

$$mp < np \implies m < n$$

*Proof.* Supondo  $mp < np$ . Pela tricotomia, temos  $n < m$ ,  $m = n$ , ou  $m < n$ . Se  $n < m$ , temos  $np < mp$  (contradição). Se  $m = n$ , temos  $mp = np$  (contradição). Logo devemos ter  $m < n$ . □

**Definição 2.5** (Elemento Mínimo). Dado  $X \subset \mathbb{N}$ , dizemos que  $p \in X$  é o menor elemento (ou elemento mínimo) de  $X$  se  $\forall n \in X : p \leq n$ .

*Observação 2.3.* Como  $\forall n \in \mathbb{N} : 1 \leq n$ , temos que  $1 \in X$  implica 1 menor elemento de  $X$ .

**Proposição 2.17.** O elemento mínimo de um conjunto  $X \subset \mathbb{N}$ , quando existir, é único.

*Proof.* Suponha que dado um conjunto  $X \subset \mathbb{N}$ , existam  $p, q \in X$  elementos mínimos. Logo  $p \leq q$  e  $q \leq p$ . Logo  $p = q$ . □

**Definição 2.6** (Maior elemento). Dado  $X \subset \mathbb{N}$ , dizemos que  $p \in X$  é o maior elemento (ou elemento máximo) de  $X$  se  $\forall n \in X : p \geq n$ .

**Proposição 2.18.** *Os naturais não possuem maior elemento.*

*Proof.* Suponha que  $x \in \mathbb{N}$  seja o maior elemento de  $\mathbb{N}$ . Teríamos  $s(x) \in \mathbb{N}$  e  $x < s(x)$  (contradição). Logo os naturais não possuem maior elemento.  $\square$

**Proposição 2.19.** *O elemento máximo de um conjunto  $X \subset \mathbb{N}$ , quando existir, é único.*

*Proof.* Exercício.  $\square$

**Definição 2.7** ( $I_n$ ).

$$I_n := \{x \in \mathbb{N} \mid x \leq n\}$$

**Lema 10.**

$$I_{n+1} = I_n \cup \{n+1\}$$

*Proof.*

$$\begin{aligned} x \in I_{n+1} &\iff \\ x \leq n+1 &\iff \\ x < n+1 \vee x = n+1 &\iff \\ x \leq n \vee x = n+1 &\iff \\ x \in I_n \vee x \in \{n+1\} &\iff \\ x \in I_n \cup \{n+1\} & \end{aligned}$$

$\square$

**Teorema 1** (Princípio da boa Ordenação). *Todo subconjunto  $A \neq \emptyset$  dos naturais admite menor elemento.*

*Proof.* Dado  $A \subset \mathbb{N}$  não vazio. Se  $1 \in A$ , temos 1 menor elemento.

Supondo  $1 \notin A$ . Logo  $1 \in \mathbb{N} - A$ . Seja  $X = \{x \in \mathbb{N} \mid I_x \subset \mathbb{N} - A\}$ . Como  $1 \in \mathbb{N} - A$ , temos  $I_1 = \{1\} \subset \mathbb{N} - A$ , logo  $1 \in X$ . Como  $A$  é não vazio, existe  $a \in A$ . Logo  $a \notin \mathbb{N} - A$ . Temos  $a \leq a \implies a \in I_a$ . Logo  $I_a \not\subset \mathbb{N} - A$ . Logo  $a \notin X$ . Temos  $1 \in X$  e  $X \neq \mathbb{N}$ , logo o axioma da indução deve falhar. Logo deve existir  $n \in X$  com  $n+1 = s(n) \notin X$ .

Afirmo que  $n+1$  é o menor elemento de  $A$ . Como  $n \in X$ , temos  $I_n \subset \mathbb{N} - A$ , logo  $x \leq n \implies x \in \mathbb{N} - A$ . Como  $n+1 \notin X$ , temos  $I_{n+1} \not\subset \mathbb{N} - A$ . Logo existe um  $m \in I_{n+1}$  com  $m \notin \mathbb{N} - A \implies m \in A$ . Observe que  $m \in I_{n+1} \implies m \leq n+1 \implies m = n+1 \vee m < n+1$ . Se  $m < n+1$ , temos pelo Lema 7 que  $m \leq n$ , que implica  $m \in I_n$ , logo  $m \in \mathbb{N} - A$  (contradição). Logo devemos ter  $m = n+1$ . Temos portanto que  $n+1 \in A$ .

Suponha que exista  $p \in A$  tal que  $p < n+1$ . Teríamos  $p \leq n \implies p \in I_n \implies p \in \mathbb{N} - A \implies p \notin A$ . Contradição. Logo temos  $n+1 \leq p$  para todo  $p \in A$ . Logo  $n+1$  é o menor elemento de  $A$ .  $\square$

**Teorema 2** (Indução completa). *Seja  $X \subset \mathbb{N}$  tal que  $(\forall m \in \mathbb{N} : m < n \implies m \in X) \implies n \in X$ . Então  $X = \mathbb{N}$*

*Proof.* Temos  $1 \in X$ , pois  $1 \notin X$  implicaria na existência de um  $m < 1$  com  $m \notin X$ . Supondo  $X \neq \mathbb{N}$  e  $A = \mathbb{N} - X$ . Como  $X \neq \mathbb{N}$ , temos  $A \neq \emptyset$ . Logo  $A$  possui um menor elemento  $a \in A$ . Se  $p \in \mathbb{N}$  com  $p < a$ , então  $p \notin A$ , logo  $p \in X$ . Como  $\forall p \in \mathbb{N} : p < a \implies p \in X$ , temos  $a \in X$ . Contradição. Logo  $A$  é vazio. Logo  $X = \mathbb{N}$ .  $\square$

### 3 Conjuntos Finitos e Infinitos

**Definição 3.1** ( Conjuntos finitos). Um conjunto  $X$  é finito quando for vazio ou quando existir para algum  $n \in \mathbb{N}$  uma bijeção  $\phi : I_n \rightarrow X$

**Definição 3.2** (Tamanho de um conjunto). Dado um conjunto finito. Dizemos que ele tem zero elementos se for vazio e que ele tem  $n$  elementos se tiver bijeção com  $I_n$ .

*Observação 3.1.* O conjunto  $I_n$  é finito e possui  $n$  elementos.

*Observação 3.2.* Denota-se  $|A|$  como o tamanho do conjunto  $A$ .

**Proposição 3.1.** *Se  $f : X \rightarrow Y$  é uma bijeção, então  $X$  é finito se, e somente se,  $Y$  for finito.*

*Proof.* Se  $X$  for finito, então existe um bijeção  $\phi : I_n \rightarrow X$ . A composição  $(\phi \circ f) : I_n \rightarrow Y$  é uma bijeção, logo  $Y$  é finito. O caso  $Y$  finito é análogo.  $\square$

**Teorema 3.** *Seja  $A \subset I_n$  não vazio. Se existe uma bijeção  $f : I_n \rightarrow A$ , então  $A = I_n$ .*

*Proof.* Seja  $X = \{n \in \mathbb{N} \mid \forall A \subset I_n : (\text{Existe uma bijeção } f : I_n \rightarrow A) \implies A = I_n\}$ . Temos  $1 \in X$ , pois  $I_1 = \{1\}$  e  $A \subset I_1 \implies A = \{1\} = I_1$ . Supondo  $n \in X$ . Seja  $A \subset I_{n+1}$  com uma bijeção  $f : I_{n+1} \rightarrow A$ . Restringindo  $f$  a  $I_n$ , obtemos  $f' : I_n \rightarrow A - \{f(n+1)\}$ , que é uma bijeção pela proposição 1.7.

Se  $A - \{f(n+1)\} \subset I_n$ , temos por  $n \in X$  que  $A - \{f(n+1)\} = I_n$ . Como o contra-domínio de  $f$  é  $A$  e  $A \subset I_{n+1}$ , temos que  $f(n+1) \in A \implies f(n+1) \in I_{n+1} \implies f(n+1) \in I_n \vee f(n+1) \in \{n+1\}$ . Se  $f(n+1) \in I_n$ , temos  $f(n+1) \notin A - \{f(n+1)\}$ , logo  $A - \{f(n+1)\} \neq I_n$  (contradição). Logo temos  $f(n+1) = n+1$ . Logo  $f(n+1) = n+1 \in A$ . Como  $A - \{n+1\} = A - \{f(n+1)\} = I_n$ , temos  $(A - \{n+1\}) \cup \{n+1\} = I_n \cup \{n+1\} \implies A \cup \{n+1\} = I_{n+1} \implies A = I_{n+1}$ . Logo temos  $A = I_{n+1}$ .

Se  $A - \{f(n+1)\} \not\subset I_n$ . Logo existe  $a \in A$  tal que  $a \notin I_n$  e  $a \neq f(n+1)$ . Mas  $A \subset I_{n+1}$ . Logo  $a \in I_{n+1} = I_n \cup \{n+1\}$ . Logo devemos ter  $a = n+1$ . Como  $f$  é sobrejetiva, existe  $m \in I_{n+1}$  tal que  $f(m) = n+1$ . Definindo a função

$$g : I_{n+1} \rightarrow A, \text{ como } g(x) = \begin{cases} f(x), & x \neq f(n+1) \wedge x \neq n+1 \\ n+1, & x = n+1 \\ f(n+1), & x = m \end{cases}. \text{ Temos } g$$

uma bijeção. Logo a restrição  $g' : I_n \rightarrow A - \{g(n+1)\}$  é uma bijeção com  $A - \{g(n+1)\} \subset I_n$ . Portanto temos  $A - \{g(n+1)\} = I_n$  com  $A = I_{n+1}$ .  $\square$

**Proposição 3.2.** *Se existe uma bijeção  $f : I_n \rightarrow I_m$ , então  $I_m = I_n$ .*

*Proof.* Se  $m \leq n$ , então existe uma bijeção  $f : I_n \rightarrow I_m$  com  $I_m \subset I_n$ . Logo pelo teorema anterior, temos  $I_m = I_n$ . Se  $n > m$ , temos a bijeção  $f^{-1} : I_m \rightarrow I_n$  com  $I_n \subset I_m$ . Logo pelo teorema anterior  $I_m = I_n$ .  $\square$

**Proposição 3.3.** *Não existe uma bijeção  $f : X \rightarrow Y$  entre um conjunto finito  $X$  e uma parte própria  $Y \subset X$ .*

*Proof.* Como  $X$  é finito, existe uma bijeção  $g : I_n \rightarrow X$ . Suponha que exista uma bijeção  $f : X \rightarrow Y$ . Como  $Y$  é parte própria, existe um  $x \in X - Y$ . Tome  $A = g^{-1}(Y) \subset g^{-1}(X) = I_n$ . Temos  $g^{-1}(x) \notin A$ , logo  $A$  é uma parte própria de  $I_n$ . Queremos achar uma bijeção  $h : I_n \rightarrow A$ . Restringindo  $g$  a  $A$ , obtendo a bijeção  $g' : A \rightarrow Y$ . Definindo a bijeção  $h = (g') \circ f \circ g : I_n \rightarrow A$ . Pelo teorema 3, temos que  $A = I_n$ . Uma contradição, pois  $A$  é parte própria de  $I_n$ . Logo não existe bijeção entre um conjunto finito  $X$  e uma parte própria  $Y \subset X$ .  $\square$

**Lema 11.** *Todo subconjunto  $A$  de  $I_n$  é finito e temos  $|A| \leq n$*

*Proof.* Seja  $X = \{n \in \mathbb{N} \mid A \subset I_n \implies A \text{ finito} \wedge |A| \leq n\}$ . Temos  $1 \in X$ , pois os subconjuntos de  $I_1 = \{1\}$  são  $\{\}$  e  $\{1\} = I_1$ , ambos finitos.

Suponha  $n \in X$ . Seja  $A \subset I_{n+1} = I_n \cup \{n+1\}$ . Se  $n+1 \notin A$ , então temos  $A \subset I_n$ . Pela hipótese de indução, temos  $A$  finito e  $|A| \leq n < n+1$ .

Supondo  $n+1 \in A$ . Se  $A = \{n+1\}$ , temos  $A$  finito e  $|A| = 1 \leq n$ . Supondo  $A \neq \{n+1\}$ , temos  $B = A - \{n+1\} \neq \emptyset$  e  $B \subset I_n$ . Logo  $B$  é finito e temos  $k = |B| \leq n$ . Como  $B$  é finito, existe a bijeção  $f : I_k \rightarrow B$ . Definindo a bijeção  $f' : I_{k+1} \rightarrow A$  pondo  $f'(x) = f(x)$  para  $x \in I_k$  e  $f'(k+1) = n+1$ . Logo  $A$  é finito e temos  $|A| = k+1 \leq n+1$ .  $\square$

**Lema 12.** *Seja  $A \subset I_n$ . Temos  $|A| = n \iff A = I_n$ .*

*Proof.* Se  $|A| = n$ , existe a bijeção  $f : I_n \rightarrow A$ , com  $A \subset I_n$ , logo  $A = I_n$ .  $\square$

**Teorema 4.** *Todo subconjunto  $Y$  de um conjunto finito  $X$  é finito e  $|Y| \leq |X|$ , com  $|Y| = |X| \iff X = Y$ .*

*Proof.* Se  $X$  é finito, existe uma bijeção  $f : I_n \rightarrow X$ . Seja  $A = f^{-1}(Y) \subset I_n$  e seja a bijeção  $f' : A \rightarrow Y$  a restrição de  $f$  a  $A$ . Como  $A \subset I_n$ , temos  $A$  finito e  $|A| \leq n$ . Logo  $Y$  é finito e  $|Y| = |A| \leq n$ . Temos  $|Y| = |A| = n = |X| \iff |A| = I_n$ . Logo  $f^{-1}(Y) = I_n = f^{-1}(X)$ . Logo  $X = Y$ .  $\square$

**Proposição 3.4.** *Seja  $f : X \rightarrow Y$  uma função injetiva. Se  $Y$  é finito, então  $X$  é finito e  $|X| \leq |Y|$ .*

*Proof.* Como existe a injeção  $f : X \rightarrow Y$ , temos a bijeção  $f' : X \rightarrow f(X)$ , com  $f(X) \subset Y$ . Como  $Y$  é finito, temos  $f(X)$  finito e  $|f(X)| \leq |Y|$ . Como existe a bijeção  $f' : X \rightarrow f(X)$ , temos  $|X| = |f(X)| \leq |Y|$ .  $\square$

**Proposição 3.5.** *Seja  $f : X \rightarrow Y$  uma função sobrejetiva. Se  $X$  é finito, então  $Y$  é finito e  $|Y| \leq |X|$ .*

*Proof.* Como  $f$  é sobrejetiva, ela admite inversa à direita. Seja  $g : Y \rightarrow X$  a inversa à direita de  $f$ . Se  $g(y) = g(y')$ , temos  $f(g(y)) = f(g(y'))$ , logo  $y = y'$ . Logo  $g$  é injetiva. Pela proposição anterior, temos  $Y$  finito com  $|Y| \leq |X|$ .  $\square$

**Definição 3.3** (Conjunto infinito). Um conjunto é infinito quando não for finito.

*Observação 3.3.* A função sucessor com o contradomínio reduzido é uma bijeção entre uma parte dos naturais com os naturais:

$$s : \mathbb{N} \rightarrow \mathbb{N} - \{1\}$$

Logo os naturais são infinitos.

**Definição 3.4** (Conjunto limitado). Um conjunto  $X \subset \mathbb{N}$  é limitado quando existe  $p \in \mathbb{N}$  tal que  $\forall n \in X : n \leq p$ .

**Teorema 5.** *Seja  $X \subset \mathbb{N}$  não vazio. As seguintes afirmações são equivalentes:*

- $X$  é finito.
- $X$  é limitado.
- $X$  possui maior elemento.

*Proof.* (a)  $\implies$  (b)

Seja  $A = \{n \in \mathbb{N} \mid |X| = n \implies X \text{ limitado}\}$ . Se  $|X| = 1$ , temos que  $X = \{a\}$  para algum  $a \in \mathbb{N}$ . Logo  $X$  é limitado pelo  $a$ , pois  $a \leq a$ . Supondo  $n \in X$ . Seja  $|X| = n + 1$ . Logo existe uma bijeção  $f : I_{n+1} \rightarrow X$ . Tomando a bijeção  $f' : I_n \rightarrow X - \{f(n+1)\}$ . Logo  $X - \{f(n+1)\}$  tem tamanho  $n$ . Pela hipótese de indução, temos  $X - \{f(n+1)\}$  limitado por um  $p \in \mathbb{N}$ , ou seja:  $\forall t \in X - \{f(n+1)\} : t \leq p$ . Se  $f(n+1) \leq p$ , temos que  $p$  limita  $X$ . Se  $p \leq f(n+1)$ , temos para todo  $t \in X - \{f(n+1)\}$  que  $t \leq p \leq f(n+1)$  e  $f(n+1) \leq f(n+1)$ , logo  $f(n+1)$  limita  $X$ .

Como  $1 \in A$  e  $n \in A \implies n+1 \in A$ , temos  $A = \mathbb{N}$

(a)  $\implies$  (b) [Outra forma]

Seja  $X = \{x_1, x_2, \dots, x_n\}$ , defina  $a = x_1 + x_2 + \dots + x_n$ . Temos  $x \leq a$  para todo  $x \in X$ , logo  $X$  é limitado.

(b)  $\implies$  (c)

Como  $X$  é limitado, existe um  $p \in \mathbb{N}$  tal que  $\forall n \in X : n \leq p$ . É natural pensar que o maior elemento será o menor dos "limitadores". Logo seja  $A = \{p \in \mathbb{N} \mid \forall n \in X : n \leq p\}$ .  $A$  é não vazio, logo é limitado inferiormente por um  $a \in A$ . Se  $a \in X$ ,  $a$  é o maior elemento de  $X$ . Supondo  $a \notin X$ . Logo temos para todo  $n \in X$  que  $n \leq a$ , mas nunca  $n = a$ , logo temos  $n < a$ . Se  $a = 1$ , temos  $n < 1$  (contradição). Se  $a \neq 1$ , existe  $a_0$  tal que  $a_0 + 1 = a$ . Pelo lema



7, obtemos  $n < a_0 + 1 \implies n \leq a_0$  para todo  $n \in X$ . Uma contradição, pois  $a_0 \in A$  com  $a_0 < a$  ( $a$  é o menor elemento de  $A$ ). Logo devemos ter  $a \in X$ . Logo  $X$  possui maior elemento.

(c)  $\implies$  (a)

Seja  $p \in X$  o maior elemento de  $X$ . Conjecturo que  $|X| \leq p$ . Vamos mostrar que  $X \subset I_p$ . Seja  $x \in X$ . Como  $p$  é o maior elemento de  $X$ , temos  $x \leq p$ . Como  $X \subset \mathbb{N}$ , temos  $x \in \mathbb{N}$ . Como  $x \in \mathbb{N}$  e  $x \leq p$ , temos  $x \in I_p$ . Como  $x \in X \implies x \in I_p$ , temos  $X \subset I_p$ . Logo  $X$  é finito e  $|X| \leq p$ .  $\square$

**Teorema 6.** *Sejam  $X, Y$  conjuntos finitos disjuntos, então  $X \cup Y$  é finito e  $|X \cup Y| = |X| + |Y|$ .*

*Proof.* Sejam  $f_x : I_n \rightarrow X$  e  $f_y : I_m \rightarrow Y$  bijeções. Seja  $f_{xy} : I_{n+m} \rightarrow X \cup Y$  definida como:

$$f_{xy}(p) = \begin{cases} f_x(p), & p \leq n \\ f_y(r), & n < p \leq n + m \end{cases}$$

Se  $n < p$ , existe  $r \in \mathbb{N}$  tal que  $p = n + r$ . Como  $p \leq n + m$ , temos  $r \leq m$ .

Supondo  $f_{xy}(p) = f_{xy}(q)$  com  $p \neq q$ . Logo  $p < q$  ou  $q < p$ . Supondo sem perda de generalidade que  $p < q$ . Se  $n < q \leq n + m$  e  $p \leq n$ , temos  $f_x(p) = f_y(q)$ , mas  $X$  e  $Y$  são disjuntos, logo devemos ter ou  $p < q \leq n$  ou  $n < p < q \leq n + m$ . Se  $p < q \leq n$ , temos  $f_x(p) = f_x(q) \implies p = q$  ( $f_x$  injetiva). O caso  $n < p < q \leq n + m$  é análogo. Logo  $f_{xy}(p) = f_{xy}(q) \implies p = q$  (contradição). Logo devemos ter  $p = q$ . Logo  $f_{xy}$  é injetiva.

Seja  $p \in X \cup Y$ . Logo  $p \in X$  ou  $p \in Y$ . Supondo  $p \in X$ . Como  $f_x$  é sobrejetiva, existe  $n_x \in I_n$  tal que  $f_x(n_x) = p$ . Como  $n_x \leq n$ , temos  $f_{xy}(n_x) = f_x(n_x) = p$ . Se  $p \in Y$ . Como  $f_y$  é sobrejetiva, existe  $n_y \in I_m$  tal que  $f_y(n_y) = p$ . Como  $n_y \leq m$ , temos  $n < n + n_y \leq n + m$  e  $f_{xy}(n + n_y) = f_y(n_y) = p$  ( $n_y = r$ ). Logo  $f_{xy}$  é sobrejetiva.

Logo  $f_{xy}$  é bijetiva.

Logo  $X \cup Y$  é finito e tem tamanho  $n + m = |X| + |Y|$ .  $\square$

**Proposição 3.6.** *Sejam  $X, Y$  conjuntos finitos, então  $X \cup Y$  é finito e  $|X \cup Y| \leq |X| + |Y|$ .*

*Proof.* Sejam  $f_x : I_n \rightarrow X$  e  $f_y : I_m \rightarrow Y$  bijeções. Seja  $f_{xy} : I_{n+m} \rightarrow X \cup Y$  definida como:

$$f_{xy}(p) = \begin{cases} f_x(p), & p \leq n \\ f_y(r), & n < p \leq n + m \end{cases}$$

Se  $n < p$ , existe  $r \in \mathbb{N}$  tal que  $p = n + r$ . Como  $p \leq n + m$ , temos  $r \leq m$ .

Seja  $p \in X \cup Y$ . Logo  $p \in X$  ou  $p \in Y$ . Supondo  $p \in X$ . Como  $f_x$  é sobrejetiva, existe  $n_x \in I_n$  tal que  $f_x(n_x) = p$ . Como  $n_x \leq n$ , temos  $f_{xy}(n_x) = f_x(n_x) = p$ . Se  $p \in Y$ . Como  $f_y$  é sobrejetiva, existe  $n_y \in I_m$  tal que  $f_y(n_y) = p$ .

Como  $n_y \leq m$ , temos  $n < n + n_y \leq m$  e  $f_{xy}(n + n_y) = f_y(n_y) = p(n_y = r)$ . Logo  $f_{xy}$  é sobrejetiva.

Logo  $X \cup Y$  é finito e  $|X| + |Y| \leq |X| + |Y|$ . □

**Proposição 3.7.** *Temos para todos  $m, n \in \mathbb{N}$  que  $I_n \times I_m$  é finito e  $|I_n \times I_m| = n \cdot m$ .*

*Proof.* Seja  $X = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : |I_n \times I_m| = n \cdot m\}$ . Temos  $1 \in X$ , pois para qualquer  $m \in \mathbb{N}$ , existe uma bijeção entre  $I_m$  e  $I_m \times I_1$ , logo  $I_m \times I_1$  é finito e  $|I_m \times I_1| = |I_m| = m = 1 \cdot m$ .

Supondo  $n \in X$ . Dado  $m \in \mathbb{N}$ , seja  $I_m \times I_{n+1} = I_m \times (I_n \cup \{n+1\}) = (I_m \times I_n) \cup (I_m \times \{n+1\})$ . Temos  $(I_m \times I_n)$  finito e  $|I_m \times I_n| = m \cdot n$  (hipótese de indução) e  $I_m \times \{n+1\}$  finito com  $|I_m \times \{n+1\}| = m$ . Logo  $|I_m \times I_{n+1}| = |(I_m \times I_n) \cup (I_m \times \{n+1\})| = mn + m = m \cdot (n+1)$ .

Como  $1 \in X$  e  $n \in X \implies n+1 \in X$ , temos  $X = \mathbb{N}$ . □

**Proposição 3.8.** *Sejam  $X, Y$  conjuntos finitos, então  $X \times Y$  é finito e  $|X \times Y| = |X| \times |Y|$ .*

*Proof.* Sejam  $f_x : I_n \rightarrow X$  e  $f_y : I_m \rightarrow Y$  bijeções. Logo  $g : I_n \times I_m \rightarrow X \times Y$ , definida por  $g(p, q) = (f_x(p), f_y(q))$  é uma bijeção. Logo  $|X \times Y| = |I_n \times I_m| = m \cdot n = |X| \times |Y|$ . □

**Proposição 3.9.** *Temos para todos  $m, n \in \mathbb{N}$  que  $\mathcal{F}(I_n, I_m)$  é finito e  $|\mathcal{F}(I_n, I_m)| = m^n$ .*

*Proof.* Seja  $X = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : |\mathcal{F}(I_n, I_m)| = m^n\}$ . Temos  $1 \in X$ , pois para qualquer  $m \in \mathbb{N}$ , existe uma bijeção entre  $I_m$  e  $\mathcal{F}(I_1, I_m)$ , logo  $\mathcal{F}(I_1, I_m)$  é finito e  $|\mathcal{F}(I_1, I_m)| = |I_m| = m = m^1$ .

Supondo  $n \in X$ . Temos  $\mathcal{F}(I_{n+1}, I_m) = \mathcal{F}(I_n \cup \{n+1\}, I_m)$ . Existe uma bijeção entre  $\mathcal{F}(I_n \cup \{n+1\}, I_m)$  e  $\mathcal{F}(I_n, I_m) \times \mathcal{F}(\{n+1\}, I_m)$ . Existe uma bijeção entre  $\mathcal{F}(\{n+1\}, I_m)$  e  $\mathcal{F}(I_1, I_m)$ . Logo existe uma bijeção entre  $\mathcal{F}(I_n, I_m) \times \mathcal{F}(\{n+1\}, I_m)$  e  $\mathcal{F}(I_n, I_m) \times \mathcal{F}(I_1, I_m)$ . Como  $\mathcal{F}(I_n, I_m)$  é finito e possui tamanho  $m^n$  e  $\mathcal{F}(I_1, I_m)$  é finito e possui tamanho  $m^1$ , temos  $\mathcal{F}(I_n, I_m) \times \mathcal{F}(I_1, I_m)$  finito e de tamanho  $m^n \cdot m = m^{n+1}$ . Como existe uma bijeção entre  $\mathcal{F}(I_n, I_m) \times \mathcal{F}(I_1, I_m)$  e  $\mathcal{F}(I_{n+1}, I_m)$ , temos  $\mathcal{F}(I_{n+1}, I_m)$  finito e de tamanho  $m^{n+1}$ .

Como  $n \in X \implies n+1 \in X$  e  $1 \in X$ , temos  $X = \mathbb{N}$ . □

**Definição 3.5** (Conjunto Enumerável). Um conjunto é dito enumerável se é finito ou se existe uma bijeção  $f : \mathbb{N} \rightarrow X$ .

**Proposição 3.10.** *Se existe uma injeção  $f : \mathbb{N} \rightarrow Y$ , então  $f(\mathbb{N})$  é contável.*

*Proof.* Definindo a bijeção  $f' : \mathbb{N} \rightarrow f(\mathbb{N})$ ,  $f'(x) = f(x)$ . Temos  $f(\mathbb{N})$  contável. □

**Proposição 3.11.** *Todo conjunto infinito  $X$  tem um subconjunto contável.*

*Proof.* Basta construir uma injeção  $f : \mathbb{N} \rightarrow X$ . Seja  $A = \mathcal{P}(X) - \emptyset$ . Temos  $\bigcup A = X$  e  $\emptyset \notin A$ . Seja  $g : A \rightarrow X$  a função escolha aplicada em  $A$ . Logo temos  $g(a) \in X$  para todo  $a \in A$ . Seja  $f : \mathbb{N} \rightarrow X$  definida indutivamente por

$$f(n) = \begin{cases} g(A), & n = 1 \\ g(A - \{f(1), f(2), \dots, f(n_0)\}), & n \neq 1 \end{cases}$$

onde  $n_0$  é o sucessor de  $n$ . Se para algum  $n \in \mathbb{N}$  tivermos  $A - \{f(1), f(2), \dots, f(n_0)\} = \emptyset$ , teríamos  $A = \{f(1), \dots, f(n_0)\}$ , logo  $A$  □