

$X \neq \mathbb{N}$ . Logo a conclusão do axioma 3 não é válida. Segue-se que deve existir  $n \in X$  tal que  $n + 1 \notin X$ . Então  $I_n = \{1, 2, \dots, n\} \subset \mathbb{N} - A$  mas  $n_0 = n + 1 \in A$ . Portanto  $n_0$  é o menor elemento do conjunto  $A$ , pois não existe número natural entre  $n$  e  $n + 1$ .

## 2 Conjuntos finitos

Continuaremos usando a notação  $I_n = \{p \in \mathbb{N}; p \leq n\}$ .

Um conjunto  $X$  diz-se *finito* quando é vazio ou então existem  $n \in \mathbb{N}$  e uma bijeção  $f: I_n \rightarrow X$ . Escrevendo  $x_1 = f(1), x_2 = f(2), \dots, x_n = f(n)$  temos então  $X = \{x_1, x_2, \dots, x_n\}$ . A bijeção  $f$  chama-se uma *contagem* dos elementos de  $X$  e o número  $n$  chama-se o *número de elementos*, ou *número cardinal* do conjunto finito  $X$ . O Corolário 1 abaixo prova que o número cardinal está bem definido, isto é, não depende da particular contagem  $f$ .

**Lema.** *Se existe uma bijeção  $f: X \rightarrow Y$  então, dados  $a \in X$  e  $b \in Y$ , existe também uma bijeção  $g: X \rightarrow Y$  tal que  $g(a) = b$ .*

**Demonstração:** Seja  $b' = f(a)$ . Como  $f$  é sobrejetiva, existe  $a' \in X$  tal que  $f(a') = b$ . Definamos  $g: X \rightarrow Y$  pondo  $g(a) = b, g(a') = b'$  e  $g(x) = f(x)$  se  $x \in X$  não é igual a  $a$  nem a  $a'$ . É fácil ver que  $g$  é uma bijeção.  $\square$

**Teorema 1.** *Se  $A$  é um subconjunto próprio de  $I_n$ , não pode existir uma bijeção  $f: A \rightarrow I_n$ .*

**Demonstração:** Suponha, por absurdo, que o teorema seja falso e considere  $n_0 \in \mathbb{N}$ , o menor número natural para o qual existem um subconjunto próprio  $A \subset I_{n_0}$  e uma bijeção  $f: A \rightarrow I_{n_0}$ . Se  $n_0 \in A$  então, pelo Lema, existe uma bijeção  $g: A \rightarrow I_{n_0}$  com  $g(n_0) = n_0$ . Neste caso, a restrição de  $g$  a  $A - \{n_0\}$  é uma bijeção do subconjunto próprio  $A - \{n_0\}$  sobre  $I_{n_0-1}$ , o que contraria a minimalidade de  $n_0$ . Se, ao contrário, tivermos  $n_0 \notin A$  então tomamos  $a \in A$  com  $f(a) = n_0$  e a restrição de  $f$  ao subconjunto próprio  $A - \{a\} \subset I_{n_0-1}$  será uma bijeção sobre  $I_{n_0-1}$ , o que novamente vai contrariar a minimalidade de  $n_0$ .  $\square$

**Corolário 1.** *Se  $f: I_m \rightarrow X$  e  $g: I_n \rightarrow X$  são bijeções então  $m = n$ .*

Com efeito, se fosse  $m < n$  então  $I_m$  seria um subconjunto próprio de  $I_n$ , o que violaria o Teorema 1, pois  $g^{-1} \circ f: I_m \rightarrow I_n$  é uma bijeção. Analogamente se mostra que não é possível  $n < m$ . Logo  $m = n$ .  $\square$

**Corolário 2.** *Seja  $X$  um conjunto finito. Uma aplicação  $f: X \rightarrow X$  é injetiva se, e somente se, é sobrejetiva.*

Com efeito, existe uma bijeção  $\varphi: I_n \rightarrow X$ . A aplicação  $f: X \rightarrow X$  é injetiva ou sobrejetiva se, e somente se,  $\varphi^{-1} \circ f \circ \varphi: I_n \rightarrow I_n$  o é. Logo podemos considerar  $f: I_n \rightarrow I_n$ . Se  $f$  for injetiva então pondo  $A = f(I_n)$ , teremos uma bijeção  $f^{-1}: A \rightarrow I_n$ . Pelo Teorema 1,  $A = I_n$  e  $f$  é sobrejetiva. Reciprocamente, se  $f$  for sobrejetiva, formemos um conjunto  $A \subset I_n$  escolhendo, para cada  $y \in I_n$ , um elemento  $x \in I_n$  tal que  $f(x) = y$ . Então a restrição  $f: A \rightarrow I_n$  é uma bijeção. Pelo Teorema 1, temos  $A = I_n$ . Isto significa que, para cada  $y \in I_n$ , é único o  $x$  tal que  $f(x) = y$ , ou seja,  $f$  é injetiva.  $\square$

**Corolário 3.** *Não pode existir uma bijeção entre um conjunto finito e uma sua parte própria.*

Com efeito, sejam  $X$  finito e  $Y \subset X$  uma parte própria. Existem  $n \in \mathbb{N}$  e uma bijeção  $\varphi: I_n \rightarrow X$ . Então o conjunto  $A = \varphi^{-1}(Y)$  é uma parte própria de  $I_n$ . Chamemos de  $\varphi_A: A \rightarrow Y$  a bijeção obtida por restrição de  $\varphi$  a  $A$ . Se existisse uma bijeção  $f: Y \rightarrow X$ , a composta  $g = \varphi^{-1} \circ f \circ \varphi_A: A \rightarrow I_n$  seria também uma bijeção, contrariando o Teorema 1.  $\square$

O Corolário 3 é uma mera reformulação do Teorema 1.

**Teorema 2.** *Todo subconjunto de um conjunto finito é finito.*

**Demonstração:** Provaremos inicialmente o seguinte caso particular: se  $X$  é finito e  $a \in X$  então  $X - \{a\}$  é finito. Com efeito, existe uma bijeção  $f: I_n \rightarrow X$  a qual, pelo Lema, podemos supor que cumpre  $f(n) = a$ . Se  $n = 1$  então  $X - \{a\} = \emptyset$  é finito. Se  $n > 1$ , a restrição de  $f$  a  $I_{n-1}$  é uma bijeção sobre  $X - \{a\}$ , logo  $X - \{a\}$  é finito e tem  $n - 1$  elementos. O caso geral se prova por indução no número  $n$  de elementos de  $X$ . Ele é evidente quando  $X = \emptyset$  ou  $n = 1$ . Supondo o Teorema verdadeiro para conjuntos com  $n$  elementos, sejam  $X$  um conjunto com  $n + 1$  elementos e  $Y$  um subconjunto de  $X$ . Se  $Y = X$ , nada há o que provar. Caso contrário, existe  $a \in X$  com  $a \notin Y$ . Então, na realidade,  $Y \subset X - \{a\}$ . Como  $X - \{a\}$  tem  $n$  elementos, segue-se que  $Y$  é finito.  $\square$

**Corolário 1.** *Dada  $f: X \rightarrow Y$ , se  $Y$  é finito e  $f$  é injetiva então  $X$  é finito; se  $X$  é finito e  $f$  é sobrejetiva então  $Y$  é finito.*

Com efeito, se  $f$  é injetiva então ela é uma bijeção de  $X$  sobre um subconjunto  $f(X)$  do conjunto finito  $Y$ . Por outro lado, se  $f$  é sobrejetiva e  $X$  é finito então, para cada  $y \in Y$  podemos escolher um  $x = g(y) \in X$  tal que  $f(x) = y$ . Isto define uma aplicação  $g: Y \rightarrow X$  tal que  $f(g(y)) = y$  para todo  $y \in Y$ . Segue-se que  $g$  é injetiva logo, pelo que acabamos de provar,  $Y$  é finito.  $\square$

Um subconjunto  $X \subset \mathbb{N}$  diz-se *limitado* quando existe  $p \in \mathbb{N}$  tal que  $x \leq p$  para todo  $x \in X$ .

**Corolário 2.** *Um subconjunto  $X \subset \mathbb{N}$  é finito se, e somente se, é limitado.*

Com efeito, se  $X = \{x_1, \dots, x_n\} \subset \mathbb{N}$  é finito, pondo  $p = x_1 + \dots + x_n$  vemos que  $x \in X \Rightarrow x \leq p$  logo  $X$  é limitado. Reciprocamente, se  $X \subset \mathbb{N}$  é limitado então  $X \subset I_p$  para algum  $p \in \mathbb{N}$ , segue-se pois do Teorema 2 que  $X$  é finito.  $\square$

### 3 Conjuntos infinitos

Diz-se que um conjunto é *infinito* quando não é finito. Assim,  $X$  é infinito quando não é vazio nem existe, seja qual for  $n \in \mathbb{N}$ , uma bijeção  $f: I_n \rightarrow X$ .

Por exemplo, o conjunto  $\mathbb{N}$  dos números naturais é infinito, em virtude do Corolário 2 do Teorema 2. Pelo mesmo motivo, se  $k \in \mathbb{N}$  então o conjunto  $k \cdot \mathbb{N}$  dos múltiplos de  $k$  é infinito.

**Teorema 3.** *Se  $X$  é um conjunto infinito, então existe uma aplicação injetiva  $f: \mathbb{N} \rightarrow X$ .*

**Demonstração:** Para cada subconjunto não-vazio  $A \subset X$ , escolhamos um elemento  $x_A \in A$ . Em seguida, definimos  $f: \mathbb{N} \rightarrow X$  indutivamente. Pomos  $f(1) = x_X$  e, supondo já definidos  $f(1), \dots, f(n)$ , escrevemos  $A_n = X - \{f(1), \dots, f(n)\}$ . Como  $X$  é infinito,  $A_n$  não é vazio. Definimos então  $f(n+1) = x_{A_n}$ . Isto completa a definição de  $f$ . Para provar que  $f$  é injetiva, sejam  $m, n \in \mathbb{N}$ , digamos com  $m < n$ . Então  $f(m) \in \{f(1), \dots, f(n-1)\}$  enquanto  $f(n) \in X - \{f(1), \dots, f(n-1)\}$ . Logo  $f(m) \neq f(n)$ .  $\square$

**Corolário.** *Um conjunto  $X$  é infinito se, e somente se, existe uma bijeção  $\varphi: X \rightarrow Y$  sobre um subconjunto próprio  $Y \subset X$ .*

Com efeito, sejam  $X$  infinito e  $f: \mathbb{N} \rightarrow X$  uma aplicação injetiva. Escrevamos, para cada  $n \in \mathbb{N}$ ,  $f(n) = x_n$ . Consideremos o subconjunto próprio  $Y = X - \{x_1\}$ . Definamos a bijeção  $\varphi: X \rightarrow Y$  pondo  $\varphi(x) = x$  se  $x$  não é um dos  $x_n$  e  $\varphi(x_n) = x_{n+1}$  ( $n \in \mathbb{N}$ ). Reciprocamente, se existe uma bijeção de  $X$  sobre um seu subconjunto próprio então  $X$  é infinito, em virtude do Corolário 3 do Teorema 1.  $\square$

Se  $\mathbb{N}_1 = \mathbb{N} - \{1\}$  então  $\varphi: \mathbb{N} \rightarrow \mathbb{N}_1$ ,  $\varphi(n) = n+1$ , é uma bijeção de  $\mathbb{N}$  sobre seu subconjunto  $\mathbb{N}_1 = \{2, 3, \dots\}$ . Mais geralmente, fixando  $p \in \mathbb{N}$  podemos considerar  $\mathbb{N}_p = \{p+1, p+2, \dots\}$  e definir a bijeção  $\varphi: \mathbb{N} \rightarrow \mathbb{N}_p$ ,  $\varphi(n) = n+p$ . Fenômenos desse tipo já tinham sido observados por Galileu, que foi o primeiro a notar que “há tantos números pares quantos números naturais”, mostrando que se  $P = \{2, 4, 6, \dots\}$  é o conjunto dos números pares então  $\varphi: \mathbb{N} \rightarrow P$ , dada por  $\varphi(n) = 2n$ , é uma bijeção. Evidentemente, se  $I = \{1, 3, 5, \dots\}$  é o conjunto dos números ímpares, então  $\psi: \mathbb{N} \rightarrow I$ , com  $\psi(n) = 2n-1$ , também é uma bijeção. Nestes dois últimos exemplos,  $\mathbb{N} - P = I$  e  $\mathbb{N} - I = P$  são infinitos, enquanto  $\mathbb{N} - \mathbb{N}_p = \{1, 2, \dots, p\}$  é finito.

### 4 Conjuntos enumeráveis

Um conjunto  $X$  diz-se *enumerável* quando é finito ou quando existe uma bijeção  $f: \mathbb{N} \rightarrow X$ . Neste caso,  $f$  chama-se uma *enumeração* dos elementos de  $X$ . Escrevendo  $f(1) = x_1, f(2) = x_2, \dots, f(n) = x_n, \dots$  tem-se então  $X = \{x_1, x_2, \dots, x_n, \dots\}$ .

**Teorema 4.** *Todo subconjunto  $X \subset \mathbb{N}$  é enumerável.*

**Demonstração:** Se  $X$  é finito, nada há para demonstrar. Caso contrário, enumeramos os elementos de  $X$  pondo  $x_1 =$  menor elemento de  $X$ , e supondo definidos  $x_1 < x_2 < \dots < x_n$ , escrevemos  $A_n = X - \{x_1, \dots, x_n\}$ . Observando que  $A_n \neq \emptyset$ , pois  $X$  é infinito, definimos  $x_{n+1} =$  menor elemento de  $A_n$ . Então  $X = \{x_1, x_2, \dots, x_n, \dots\}$ . Com efeito, se existisse algum elemento  $x \in X$  diferente de todos os  $x_n$ , teríamos  $x \in A_n$  para todo  $n \in \mathbb{N}$ , logo  $x$  seria um número natural maior do que todos os elementos do conjunto infinito  $\{x_1, \dots, x_n, \dots\}$ , contrariando o Corolário 2 do Teorema 2.  $\square$

**Corolário 1.** *Seja  $f: X \rightarrow Y$  injetiva. Se  $Y$  é enumerável então  $X$ , também é. Em particular, todo subconjunto de um conjunto enumerável é enumerável.*

Com efeito, basta considerar o caso em que existe uma bijeção  $\varphi: Y \rightarrow \mathbb{N}$ . Então  $\varphi \circ f: X \rightarrow \mathbb{N}$  é uma bijeção de  $X$  sobre um subconjunto de  $\mathbb{N}$ , o qual é enumerável, pelo Teorema 4. No caso particular de  $X \subset Y$ , tomamos  $f: X \rightarrow Y$  igual à aplicação de inclusão.  $\square$

**Corolário 2.** *Seja  $f: X \rightarrow Y$  sobrejetiva. Se  $X$  é enumerável então  $Y$  também é.*

Com efeito, para cada  $y \in Y$  podemos escolher um  $x = g(y) \in X$  tal que  $f(x) = y$ . Isto define uma aplicação  $g: Y \rightarrow X$  tal que  $f(g(y)) = y$  para todo  $y \in Y$ . Segue-se daí que  $g$  é injetiva. Pelo Corolário 1,  $Y$  é enumerável.  $\square$

**Corolário 3.** *O produto cartesiano de dois conjuntos enumeráveis é um conjunto enumerável.*

Com efeito, se  $X$  e  $Y$  são enumeráveis então existem sobrejeções  $f: \mathbb{N} \rightarrow X$  e  $g: \mathbb{N} \rightarrow Y$ , logo  $\varphi: \mathbb{N} \times \mathbb{N} \rightarrow X \times Y$ , dada por  $\varphi(m, n) = (f(m), g(n))$  é sobrejetiva. Portanto, basta provar que  $\mathbb{N} \times \mathbb{N}$  é enumerável. Para isto, consideremos a aplicação  $\psi: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ , dada por  $\psi(m, n) = 2^m \cdot 3^n$ . Pela unicidade da decomposição de um número em fatores primos,  $\psi$  é injetiva. Segue-se que  $\mathbb{N} \times \mathbb{N}$  é enumerável.  $\square$

**Corolário 4.** *A reunião de uma família enumerável de conjuntos enumeráveis é enumerável.*

Com efeito, dados  $X_1, X_2, \dots, X_n, \dots$  enumeráveis, existem sobrejeções  $f_1: \mathbb{N} \rightarrow X_1, f_2: \mathbb{N} \rightarrow X_2, \dots, f_n: \mathbb{N} \rightarrow X_n, \dots$ . Tomando  $X = \bigcup_{n=1}^{\infty} X_n$ , definimos a sobrejeção  $f: \mathbb{N} \times \mathbb{N} \rightarrow X$  pondo  $f(m, n) = f_n(m)$ . O caso de uma reunião finita  $X = X_1 \cup \dots \cup X_n$  reduz-se ao anterior porque então  $X = X_1 \cup \dots \cup X_n \cup X_n \cup \dots$ .  $\square$

O Teorema 3 acima significa que o enumerável é o “menor” dos infinitos. Com efeito, ele pode ser reformulado assim:

*Todo conjunto infinito contém um subconjunto infinito enumerável.*

**Exemplo 1.** O conjunto  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$  dos números inteiros é enumerável. Uma bijeção  $f: \mathbb{N} \rightarrow \mathbb{Z}$  pode ser definida pondo  $f(n) = (n-1)/2$  para  $n$  ímpar e  $f(n) = -n/2$  para  $n$  par.

**Exemplo 2.** O conjunto  $\mathbb{Q} = \{m/n; m, n \in \mathbb{Z}, n \neq 0\}$  dos números racionais é enumerável. Com efeito, escrevendo  $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ , podemos definir uma função sobrejetiva  $f: \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}$  pondo  $f(m, n) = m/n$ .

**Exemplo 3.** (Um conjunto não-enumerável.) Seja  $S$  o conjunto de todas as seqüências infinitas, como  $s = (01100010\dots)$ , formadas com os símbolos 0 e 1. Noutras palavras,  $S$  é o conjunto de todas as funções  $s: \mathbb{N} \rightarrow \{0, 1\}$ . Para cada  $n \in \mathbb{N}$ , o valor  $s(n)$ , igual a 0 ou 1, é o  $n$ -ésimo termo da seqüência  $s$ . Afirmamos que nenhum subconjunto enumerável  $X = \{s_1, s_2, \dots, s_n, \dots\} \subset S$  é igual a  $S$ . Com efeito, dado  $X$ , indiquemos com  $s_{nm}$  o  $n$ -ésimo termo da seqüência  $s_m \in X$ . Formamos uma nova seqüência  $s^* \in S$  tomando o  $n$ -ésimo termo de  $s^*$  igual a 0 se for  $s_{nn} = 1$ , ou igual a 1 se for  $s_{nn} = 0$ . A seqüência  $s^*$  não pertence ao conjunto  $X$  porque seu  $n$ -ésimo termo é diferente do  $n$ -ésimo termo de  $s_n$ . (Este raciocínio, devido a G. Cantor, é conhecido como “método da diagonal”.)

No capítulo seguinte mostraremos que o conjunto  $\mathbb{R}$  dos números reais não é enumerável.

## 5 Exercícios

### Seção 1: Números naturais

1. Usando indução, prove:

$$(a) \quad 1 + 2 + \dots + n = n(n+1)/2;$$

$$(b) \quad 1 + 3 + 5 + \dots + 2n - 1 = n^2.$$

2. Dados  $m, n \in \mathbb{N}$  com  $n > m$ , prove que ou  $n$  é múltiplo de  $m$  ou existem  $q, r \in \mathbb{N}$  tais que  $n = mq + r$  e  $r < m$ . Prove que  $q$  e  $r$  são únicos com esta propriedade.

3. Seja  $X \subset \mathbb{N}$  um subconjunto não-vazio tal que  $m, n \in X \Leftrightarrow m, m+n \in X$ . Prove que existe  $k \in \mathbb{N}$  tal que  $X$  é o conjunto dos múltiplos de  $k$ .

4. Prove que, no segundo axioma de Peano, a palavra “único” é redundante (admitindo-se, naturalmente, os demais axiomas).

5. Prove o princípio de indução como uma conseqüência do princípio da boa ordenação.

6. Prove a lei de corte para a multiplicação:  $mp = np \Rightarrow m = n$ .

**Seção 2: Conjuntos finitos**

1. Indicando com  $\text{card } X$  o número de elementos do conjunto finito  $X$ , prove:

- (a) Se  $X$  é finito e  $Y \subset X$  então  $\text{card } Y \leq \text{card } X$ .  
 (b) Se  $X$  e  $Y$  são finitos então  $X \cup Y$  é finito e

$$\text{card}(X \cup Y) = \text{card } X + \text{card } Y - \text{card}(X \cap Y).$$

- (c) Se  $X$  e  $Y$  são finitos então  $X \times Y$  é finito e

$$\text{card}(X \times Y) = \text{card } X \cdot \text{card } Y.$$

2. Seja  $\mathcal{P}(X)$  o conjunto cujos elementos são os subconjuntos de  $X$ . Prove por indução que se  $X$  é finito então  $\text{card } \mathcal{P}(X) = 2^{\text{card } X}$ .  
 3. Seja  $\mathcal{F}(X; Y)$  o conjunto das funções  $f: X \rightarrow Y$ . Se  $\text{card } X = m$  e  $\text{card } Y = n$ , prove que  $\text{card } \mathcal{F}(X; Y) = n^m$ .  
 4. Prove que todo conjunto finito não-vazio  $X$  de números naturais contém um elemento máximo (isto é, existe  $x_0 \in X$  tal que  $x \leq x_0 \forall x \in X$ ).  
 5. Prove o Princípio das Casas de Pombo: se  $m > n$  não existe função injetiva  $f: I_m \rightarrow I_n$ . (quando  $m > n$ , para alojar  $m$  pombos em  $n$  casas é preciso que pelo menos uma casa abrigue mais de um pombo).

**Seção 3: Conjuntos infinitos**

1. Dada  $f: X \rightarrow Y$ , prove:  
 (a) Se  $X$  é infinito e  $f$  é injetiva então  $Y$  é infinito.  
 (b) Se  $Y$  é infinito e  $f$  é sobrejetiva, então  $X$  é infinito.  
 2. Sejam  $X$  um conjunto finito e  $Y$  um conjunto infinito. Prove que existe uma função injetiva  $f: X \rightarrow Y$  e uma função sobrejetiva  $g: Y \rightarrow X$ .  
 3. Prove que o conjunto  $\mathcal{P}$  dos números primos é infinito.  
 4. Dê exemplo de uma seqüência decrescente  $X_1 \supset X_2 \supset \dots \supset X_n \supset \dots$  de conjuntos infinitos cuja interseção  $\bigcap_{n=1}^{\infty} X_n$  seja vazia.

5. Prove que o conjunto  $X$  é infinito se, e somente se, não é vazio nem existe, seja qual for  $n \in \mathbb{N}$ , uma aplicação sobrejetiva  $f: I_n \rightarrow X$ .

**Seção 4: Conjuntos enumeráveis**

1. Defina  $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  pondo  $f(1, n) = 2n - 1$  e  $f(m + 1, n) = 2^m(2n - 1)$ . Prove que  $f$  é uma bijeção.  
 2. Prove que existe  $g: \mathbb{N} \rightarrow \mathbb{N}$  sobrejetiva tal que  $g^{-1}(n)$  é infinito, para cada  $n \in \mathbb{N}$ .  
 3. Exprima  $\mathbb{N} = \mathbb{N}_1 \cup \mathbb{N}_2 \cup \dots \cup \mathbb{N}_n \cup \dots$  como união infinita de subconjuntos infinitos, dois a dois disjuntos.  
 4. Para cada  $n \in \mathbb{N}$ , seja  $\mathcal{P}_n = \{X \subset \mathbb{N}; \text{card } X = n\}$ . Prove que  $\mathcal{P}_n$  é enumerável. Conclua que o conjunto  $\mathcal{P}_f$  dos subconjuntos finitos de  $\mathbb{N}$  é enumerável.  
 5. Prove que o conjunto  $\mathcal{P}(\mathbb{N})$  de todos os subconjuntos de  $\mathbb{N}$  não é enumerável.  
 6. Sejam  $Y$  enumerável e  $f: X \rightarrow Y$  tal que, para cada  $y \in Y$ ,  $f^{-1}(y)$  é enumerável. Prove que  $X$  é enumerável.