

CAPÍTULO 2. O SISTEMA DE NÚMEROS NATURAIS

SUMÁRIO

1. Axiomas de Peano	1
2. Adição e multiplicação	3
3. Relação de ordem	5
4. Boa ordenação e o segundo princípio de indução	6
5. Conjuntos finitos e infinitos	8
Conjuntos infinitos	12
6. Números inteiros	13

Intuitivamente, os números naturais são: 0, o que vem a seguir de 0 chamado 1, depois de 1 a seguir é 2, ... e assim por diante ...

Formalmente, o conjunto de números naturais é definido pelos axiomas de Peano.

1. AXIOMAS DE PEANO

Um conjunto $\mathbb{N}$, junto com uma função $s: \mathbb{N} \rightarrow \mathbb{N}$ (chamada sucessor) representa um sistema de números naturais se as seguintes propriedades (axiomas) são satisfeitas:

P1. Existe um único elemento, denotado por 0, que não é o sucessor de nenhum outro elemento, ou seja,

$$s(n) \neq 0 \quad \text{para todo } n \in \mathbb{N},$$

$$\text{e para todo } m \neq 0 \text{ existe } n \in \mathbb{N} \text{ tal que } s(n) = m.$$

P2. s é injetiva, ou seja, se $s(m) = s(n)$ então $m = n$. Em outras palavras, dois números que têm o mesmo sucessor são iguais.

P3. (Princípio da indução) Se $X \subset \mathbb{N}$ é um subconjunto tal que:

- $0 \in X$,
 - se para todo $n \in X$ tem-se também que $s(n) \in X$
- então $X = \mathbb{N}$.

Lema 1.1. Para todo $n \in \mathbb{N}$, $s(n) \neq n$, ou seja, todo número natural é diferente do seu sucessor.

Demonstração. Seja

$$X = \{n \in \mathbb{N} : s(n) \neq n\}.$$

- $0 \in X$ já que 0 não é o sucessor de nenhum número, e em particular, $s(0) \neq 0$.
- Suponha que $n \in X$, ou seja, $s(n) \neq n$.

Como S é injetiva, segue que

$$s(s(n)) \neq s(n),$$

portanto $s(n) \in X$.

Pelo princípio da indução, $X = \mathbb{N}$, ou seja, $s(n) \neq n$ para todo $n \in \mathbb{N}$. □

Observação 1.1. O princípio da indução pode ser enunciado da seguinte maneira equivalente.

Seja $P(n)$ uma propriedade que se refere aos números naturais. Suponha que as seguintes afirmações sejam válidas:

- Base de indução (ou 1º passo)

$P(0)$ é verdadeira

- Passo indutivo

Suponha que $P(n)$ seja verdadeira (hipótese de indução).

A partir dessa hipótese, prova-se que $P(s(n))$ seja verdadeira.

Então pelo princípio da indução, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

De fato, se definimos

$$X = \{n \in \mathbb{N} : P(n) \text{ é verdadeira}\},$$

tem-se:

- $0 \in X$
- Se $n \in X$ então $s(n) \in X$.

Logo, pelo princípio da indução, $X = \mathbb{N}$, ou seja, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Exemplo 1.2. Prove que se $x \neq 1$,

$$1 + x + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1} \quad \forall n \in \mathbb{N}.$$

Ou seja, prove que a propriedade/fórmula $P(n)$:

$$\sum_{k=0}^n x^k = \frac{x^{n+1} - 1}{x - 1}$$

vale para todo $n \in \mathbb{N}$.

Demonstração. Usamos o princípio da indução.

- 1º passo, ou seja, o caso $n = 0$.

A propriedade $P(0)$ significa $1 = \frac{x - 1}{x - 1}$, que é claramente válida se $x \neq 1$.

- Passo indutivo.

Suponha que $P(n)$ valha, ou seja

$$\sum_{k=0}^n x^k = \frac{x^{n+1} - 1}{x - 1}.$$

Vamos provar que $P(n + 1)$ vale também. Tem-se

$$\begin{aligned} \sum_{k=0}^{n+1} x^k &= \sum_{k=0}^n x^k + x^{n+1} \\ &= \frac{x^{n+1} - 1}{x - 1} + x^{n+1} \quad (\text{pela hipótese indutiva}) \\ &= \frac{x^{n+1} - 1}{x - 1} + \frac{x^{n+1}(x - 1)}{x - 1} \\ &= \frac{x^{n+1} - 1 + x^{n+2} - x^{n+1}}{x - 1} \\ &= \frac{x^{n+2} - 1}{x - 1}, \end{aligned}$$

provando que $P(n + 1)$ é válida.

Pelo princípio da indução, a fórmula $P(n)$ vale para todo $n \in \mathbb{N}$. □

2. ADIÇÃO E MULTIPLICAÇÃO

Dado um número natural m , definimos a soma $m + 0$ como sendo m , a soma $m + 1$ como sendo o sucessor $s(m)$ de m , a soma $m + 2$ como sendo o sucessor de $m + 1$ e assim por diante.

Formalmente, a adição por n é definida por indução.

Definição 2.1. Seja $m \in \mathbb{N}$. Então

- $m + 0 = m$.
- Se $m + n$ foi definido, então $m + s(n) = s(m + n)$.

Observe que $m + 1 = m + s(0) = s(m)$, isto é, $m + 1$ é o sucessor de m . Então em argumentos por indução, em geral escreveremos $m + 1$ em vez de $s(m)$.

A adição de números naturais satisfaz as seguintes propriedades.

Proposição 2.1. Sejam $m, p, n \in \mathbb{N}$.

- (i) (associatividade) $(m + p) + n = m + (p + n)$.
- (ii) (comutatividade) $m + n = n + m$.
- (iii) Se $m + n = p + n$ então $m = p$.

Demonstração. Vamos provar (i) e (iii). O item (ii) é exercício.

(i) Fixemos $m, p \in \mathbb{N}$ e provemos a seguinte propriedade para todo $n \in \mathbb{N}$.

$$P(n): \quad (m + p) + n = m + (p + n).$$

Usamos indução matemática.

■ Base da indução: seja $n = 0$. Então $(m + p) + 0 = m + p = m + (p + 0)$, logo $P(0)$ vale.

■ Passo de indução: suponha que $P(n)$ seja verdadeiro, isto é,

$$(m + p) + n = m + (p + n).$$

Vamos provar $P(s(n))$. De fato,

$$\begin{aligned} (m + p) + s(n) &= s((m + p) + n) \quad (\text{pela definição da adição}) \\ &= s(m + (p + n)) \quad (\text{pela hipótese de indução}) \\ &= m + s(p + n) \quad (\text{pela definição da adição}) \\ &= m + (p + s(n)) \quad (\text{de novo pela definição da adição}) \end{aligned}$$

o que estabelece $P(s(n))$.

Pelo princípio da indução, $(m + p) + n = m + (p + n)$ vale para todo $n \in \mathbb{N}$.

(iii) Fixamos $m, p \in \mathbb{N}$ e vamos provar por indução em $n \in \mathbb{N}$ que

$$\text{se } m + n = p + n \text{ então } m = p.$$

■ Base de indução: $n = 0$.

Se $m + 0 = p + 0$ então claramente $m = p$.

■ Passo de indução: suponha a afirmação verdadeira para $n \in \mathbb{N}$, ou seja, se $m + n = p + n$ então $m = p$.

Vamos provar a afirmação para $s(n)$. De fato, se

$$m + s(n) = p + s(n),$$

então pela definição da adição tem-se $s(m + n) = s(p + n)$.

Mas como a função sucessão é injetiva, segue que

$m + n = p + n$, e pela hipótese de indução concluímos que $m = p$.

Pelo princípio de indução, a conclusão segue. □

Seja m um número natural. Definimos $m \cdot 0 = 0$, $m \cdot 1 = m$, $m \cdot 2 = m + m$, $m \cdot 3 = m + m + m$ e etc. Formalmente, a multiplicação de números naturais é definida por indução como seguinte.

Definição 2.2. Seja $m \in \mathbb{N}$. Então,

- $m \cdot 0 = 0$
- Se $m \cdot n$ já foi definido então definimos $m \cdot s(n) = m \cdot n + m$.

Como $s(n) = n + 1$, temos que $m \cdot (n + 1) = m \cdot n + m$.

Em particular, $m \cdot 1 = m \cdot 0 + m = 0 + m = m$, $m \cdot 2 = m \cdot 1 + m = m + m$ e etc., como intuitivamente esperado.

A multiplicação de números naturais satisfaz as seguintes propriedades.

Proposição 2.2. Sejam $m, p, n \in \mathbb{N}$.

- (i) (distributividade) $m \cdot (p + n) = m \cdot p + m \cdot n$
- (ii) (associatividade) $m \cdot (p \cdot n) = (m \cdot p) \cdot n$
- (iii) (comutatividade) $m \cdot n = n \cdot m$
- (iv) Se $m \cdot p = n \cdot p$ e $p \neq 0$ então $m = n$.

Demonstração. Vamos provar a distributividade e deixar as outras propriedades como exercícios.

(i) Fixamos $m, p \in \mathbb{N}$ e vamos provar por indução que $\forall n \in \mathbb{N}$,

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

■ Base de indução: $n = 0$. Temos

$$m \cdot (p + 0) = m \cdot p = m \cdot p + m \cdot 0.$$

■ Passo de indução: suponha que

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

Vamos provar a mesma propriedade para $s(n)$. De fato,

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

Pelo princípio da indução, a distributividade vale para todo $n \in \mathbb{N}$. □

Observação 2.1. Pelo princípio da indução, dada uma propriedade $P(n)$ que se refere aos números naturais, para provar que ela seja verdadeira para todo $n \geq n_0$ basta provar as seguintes afirmações:

- 1) Base de indução. $P(n_0)$ é verdadeira.
- 2) Passo indutivo. Suponha que $P(n)$ seja verdadeira para algum $n \geq n_0$. Então $P(s(n))$ é verdadeira.

De fato, podemos definir o conjunto

$$X = \{m \in \mathbb{N} : P(n_0 + m) \text{ é verdadeira}\}.$$

Temos que:

- $0 \in X$ já que $P(n_0)$ é verdadeira (pela base de indução).
- Se $m \in X$, então para $n := n_0 + m$ temos que $P(n) = P(n_0 + m)$ é verdadeira. Então, pelo passo indutivo, $P(n + 1) = P(n_0 + m + 1)$ é verdadeira, ou seja, $m + 1 \in X$.

Logo, $X = \mathbb{N}$, ou seja, $P(n)$ é verdadeira para todo $n \geq n_0$.

Exemplo 2.1. Para todo $n \geq 1$,

$$1 + 2 + \dots + n = \frac{n \cdot (n + 1)}{2}.$$

Na verdade deveríamos escrever a fórmula acima como

$$2 \cdot (1 + 2 + \dots + n) = n \cdot (n + 1),$$

já que ainda não definimos frações.

Demonstração. Base de indução: começamos com $n = 1$. A fórmula se torna $2 \cdot 1 = 1 \cdot 2$ que evidentemente vale.

Passo de indução: suponha que

$$2 \cdot (1 + 2 + \dots + n) = n \cdot (n + 1)$$

e vamos provar o mesmo para $n + 1$. De fato,

$$\begin{aligned} 2 \cdot (1 + 2 + \dots + n + (n + 1)) &= 2 \cdot (1 + 2 + \dots + n) + 2 \cdot (n + 1) \\ &= n \cdot (n + 1) + 2 \cdot (n + 1) \quad (\text{pela hipótese de indução}) \\ &= (n + 2) \cdot (n + 1) = (n + 1) \cdot (n + 2). \end{aligned}$$

Pelo princípio da indução, a fórmula vale para todo $n \geq 1$. □

3. RELAÇÃO DE ORDEM

Intuitivamente, dados dois números naturais m e n , temos que $m \leq n$ se m vem antes de n na enumeração

$$0, 1, 2, \dots, m, \dots, n, \dots$$

dos números naturais, ou seja, se $n = m$ ou se n é o sucessor de m , ou se n é o sucessor do sucessor de m , ou ... Formalmente,

Definição 3.1. $m \leq n$ se existe $k \in \mathbb{N}$ tal que $n = m + k$.

Além disso, escrevemos $m < n$ se $m \leq n$ e $m \neq n$. Então $m < n$ se e somente se existe $k \neq 0$ tal que $n = m + k$.

Ademais, $n \geq m$ significa $m \leq n$ enquanto $n > m$ significa $m < n$.

Proposição 3.1. A relação $\leq$ é uma relação de ordem em $\mathbb{N}$.

Demonstração. Vamos verificar as três propriedades de uma relação de ordem.

1) Reflexividade: para todo $n \in \mathbb{N}$, tem-se $n \leq n$ já que $n = n + 0$.

2) Antissimetria: temos que provar que se $m \leq n$ e $n \leq m$ então $m = n$.

Como $m \leq n$, existe $k \in \mathbb{N}$ tal que $n = m + k$.

Como $n \leq m$, existe $l \in \mathbb{N}$ tal que $m = n + l$.

Portanto

$$n = m + k = (n + l) + k = n + (l + k),$$

e daí, $k + l = 0$.

Mas neste caso $l = 0$. De fato, se $l \neq 0$ então l é o predecessor de algum número natural p , isto é, $l = s(p)$, então

$$0 = k + l = k + s(p) = s(k + p),$$

contradição com o primeiro axioma de Peano.

Portanto $l = 0$ e daí $m = n + 0 = n$.

3) Transitividade: Sejam $m, n, p \in \mathbb{N}$ e suponha que $m \leq n$ e $n \leq p$. Então existem $k, l \in \mathbb{N}$ tais que $n = m + k$ e $p = n + l$. Portanto

$$p = n + l = (m + k) + l = m + (k + l),$$

mostrando que $m \leq p$. □

A relação de ordem é compatível com as operações algébricas, no sentido que

$$\text{se } m \leq n \text{ então } m + p \leq n + p \text{ e } m \cdot p \leq n \cdot p.$$

De fato, $m \leq n$ implica a existência de $k \in \mathbb{N}$ tal que $n = m + k$. Logo

$$n + p = (m + k) + p = (m + p) + k,$$

mostrando que $m + p \leq n + p$.

Deixamos a outra relação como exercício.

A relação de ordem em $\mathbb{N}$ é total, no sentido que quaisquer dois números naturais são comparáveis (um é menor do que ou igual ao outro). Isto não é verdadeiro para qualquer relação de ordem (por exemplo a inclusão de conjuntos não é uma ordem total: dados dois conjuntos A e B , é possível que $A \not\subset B$ e $B \not\subset A$).

Lema 3.1. *Sejam $m, n \in \mathbb{N}$. Então $m \leq n$ ou $n \leq m$.*

Demonstração. Fixemos $m \in \mathbb{N}$ e provemos por indução que todo número natural n é comparável com m .

■ 1º passo: $n = 0$. Claramente $0 \leq m$ porque $m = 0 + m$.

■ Passo indutivo: suponha que para um número natural n , temos $m \leq n$ ou $n \leq m$. Vamos provar o mesmo para $s(n) = n + 1$.

Se $m \leq n$, como $n < n + 1$, por transitividade temos $m \leq n + 1$.

Se $n \leq m$, podemos supor que $n \neq m$ (o caso $n = m$ já foi tratado acima).

Logo existe $k \neq 0$ tal que $m = n + k$.

Como $k \neq 0$, existe $l \in \mathbb{N}$ tal que $k = s(l) = l + 1$.

Então

$$m = n + (l + 1) = (n + 1) + l,$$

mostrando que $n + 1 \leq m$.

Pelo princípio de indução, $m \leq n$ ou $n \leq m$ para todo $n \in \mathbb{N}$. □

4. BOA ORDENAÇÃO E O SEGUNDO PRINCÍPIO DE INDUÇÃO

Seja $X \subset \mathbb{N}$ um subconjunto de números naturais.

Definição 4.1. Um número natural p é um mínimo de X se $p \in X$ e $p \leq n$ para todo $n \in X$.

Observe que se X admite um mínimo, ele é único. De fato, se p, q são mínimos de X , então $p \leq q$ (porque o número $q \in X$) e $q \leq p$ (porque $p \in X$), logo $p = q$.

Exemplo 4.1. 0 é claramente o mínimo de $\mathbb{N}$.

7 é claramente o mínimo de $\{7, 10, 13\}$.

Similarmente, p é um máximo de X se $p \in X$ e $p \geq n$ para todo $n \in X$. O máximo de um conjunto, se existir, deve ser único.

Exemplo 4.2. Claramente 13 é o máximo de $\{7, 10, 13\}$.

O conjunto de todos os números naturais $\mathbb{N}$ não admite um máximo.

De fato, suponha por contradição que $n \in \mathbb{N}$ seja o máximo de $\mathbb{N}$. Mas $n + 1 \in \mathbb{N}$ e $n + 1 > n$ (claramente $n + 1 \geq n$ e como foi provado no início do capítulo, $n + 1 = s(n) \neq n$). Chegamos a uma contradição com o fato do número n ser o máximo de $\mathbb{N}$. Logo $\mathbb{N}$ não tem máximo.

Enquanto subconjuntos de números naturais podem não admitir um máximo, o mínimo sempre existe, e esse resultado se chama o “Princípio da Boa Ordenação” dos números naturais.

Teorema 4.3 (O princípio da boa ordenação). *Todo subconjunto não vazio $A \subset \mathbb{N}$ possui um mínimo.*

Ideia da prova: vamos pensar num algoritmo para encontrar o mínimo de A .

- Se $0 \in A$, então 0 deve ser o mínimo de A .
- Se $0 \notin A$, o algoritmo verifique se $1 \in A$ ou $1 \notin A$. No primeiro caso, 1 deve ser o mínimo de A .
- Se $1 \notin A$ mas $2 \in A$ então 2 é o mínimo de A (já que $0 \notin A$ e $1 \notin A$).
- $\vdots$
- Se $0 \notin A, 1 \notin A, \dots, n \notin A$, verificamos se $n + 1 \in A$ ou $n + 1 \notin A$ e assim por diante.

O algoritmo tem que parar; se não, esgotamos todos os números naturais. Este procedimento leva à seguinte prova formal.

Demonstração. Suponha por contradição que A não possui mínimo. Vamos provar por indução que para todo $n \in \mathbb{N}$,

$P(n) : 0 \notin A, 1 \notin A, \dots, n \notin A$.

1º passo: $n = 0$. $0 \notin A$ porque se $0 \in A$ então 0 seria o mínimo de A .

Passo indutivo: Suponha que $P(n)$ valha, i.e.,

$0 \notin A, 1 \notin A, \dots, n \notin A$.

Neste caso, se $n + 1 \in A$ então $n + 1$ seria o mínimo de A , já que todos os números menores do que $n + 1$ não são elementos de A . Mas supomos que A não tenha mínimo, então $n + 1 \notin A$.

Logo $0 \notin A, 1 \notin A, \dots, n \notin A$ e $n + 1 \notin A$, ou seja, $P(n + 1)$ vale.

Pelo princípio de indução, $P(n)$ vale para todo $n \in \mathbb{N}$. Em particular, $n \notin A \forall n \in \mathbb{N}$, isto é, $A = \emptyset$, uma contradição.

Logo, A possui um mínimo. □

Usando o princípio da boa ordenação derivaremos um princípio de indução mais forte.

Teorema 4.4 (O segundo princípio de indução). *Seja $X \subset \mathbb{N}$ e suponha que*

- $0 \in X$,
- se $0 \in X, \dots, n \in X$ então $n + 1 \in X$.

Nestas condições, $X = \mathbb{N}$.

Em outras palavras, o segundo princípio de indução nos permite trabalhar com uma hipótese de indução mais forte, a saber, em vez de apenas supor que $n \in X$, supomos que todos os números naturais menores do que ou iguais a n pertençam a X .

Demonstração. Claramente $X = \mathbb{N}$ sse $X^c = \mathbb{N} \setminus X = \emptyset$.

Suponha por contradição que $X^c \neq \emptyset$. Então, pelo princípio da boa ordenação, existe um mínimo m de X^c .

Como $0 \in X$, tem-se $0 \notin X^c$ então $m \neq 0$.

Logo $m = n + 1$ para algum $n \in \mathbb{N}$.

Como $n + 1$ é o mínimo de X^c , então necessariamente $0 \notin X^c, 1 \notin X^c, \dots, n \notin X^c$, ou seja, $0 \in X, \dots, n \in X$.

Mas neste caso, pela hipótese de indução, $n + 1 \in X$, em contradição com o fato de que $n + 1 \in X^c$.

Portanto $X^c = \emptyset$ e daí $X = \mathbb{N}$. $\square$

O segundo princípio de indução nos permite definir objetos por recorrência que depende de mais de um termo.

Exemplo 4.5 (A sequência de Fibonacci). Definimos $F_0 = 0$, $F_1 = 1$ e para todo $n \geq 1$, $F_{n+1} = F_n + F_{n-1}$.

Em outras palavras, $\{F_n\}_{n \geq 0}$ é definida por uma recorrência de ordem 2. Similarmente podemos definir recorrências de qualquer ordem.

Definição 4.2. Um número natural p é primo se $p \neq 1$ e p não se pode escrever como $p = m \cdot n$ com $m, n \in \mathbb{N}$, e $m < p$, $n < p$.

Por exemplo 2, 3, 5, 7, 11, 13 e etc. são números primos, mas $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $12 = 3 \cdot 4$ e etc. não são primos.

Teorema 4.6. *Todo número natural $n \geq 2$ ou é primo ou pode ser escrito como um produto de números primos.*

Demonstração. Seja

$$X = \{n \geq 2: n \text{ é primo ou pode ser decomposto como produto de primos}\}.$$

Vamos provar por indução que X é o conjunto de todos os números naturais $n \geq 2$.

■ 1º passo: $n = 2$ já é primo, então $2 \in X$.

■ Passo indutivo: suponha que $2, \dots, n \in X$, ou seja, para todo $k \leq n$, $k \in X$.

Vamos provar que $n + 1 \in X$.

Se $n + 1$ é primo, automaticamente $n + 1 \in X$.

Se $n + 1$ não é primo, então existem $k, l \in \mathbb{N}$, $k < n + 1$, $l < n + 1$ tais que $n + 1 = k \cdot l$.

Logo $k \leq n$, $l \leq n$, e pela hipótese indutiva, k e l são produtos de primos. Logo $n + 1 = k \cdot l$ também é um produto de primos.

Pelo 2º princípio de indução, todo número $n \geq 2$ é primo ou produto de primos. $\square$

5. CONJUNTOS FINITOS E INFINITOS

Intuitivamente, um conjunto X é finito se existe uma contagem $x_1, x_2, \dots, x_n$ dos seus elementos. Dado $n \in \mathbb{N}$, $n \geq 1$, denotemos por

$$I_n := \{1, 2, \dots, n\}$$

o conjunto dos primeiros n números naturais sem zero.

Definição 5.1. Um conjunto X é finito se ele é vazio ou existem $n \geq 1$ e uma função bijetiva $\varphi: I_n \rightarrow X$.

Neste caso, denotando, para todo $k \in I_n$, $\varphi(k) = x_k$, os elementos $x_1, x_2, \dots, x_n$ são diferentes entre si (porque φ é injetiva) e para todo $x \in X$ existe $k \in I_n$ tal que $\varphi(k) = x$ (porque φ é sobrejetiva). Portanto

$$X = \{x_1, x_2, \dots, x_n\},$$

mostrando que a definição formal corresponde à definição intuitiva do conceito de conjunto finito.

Vamos mostrar que se $\varphi: I_n \rightarrow X$ e $\psi: I_m \rightarrow X$ são funções bijetivas para alguns $n, m \geq 1$ então $n = m$. Esta afirmação vai ser uma consequência simples do seguinte teorema.

Teorema 5.1. *Sejam $n \geq 1$ e $A \subset I_n$. Se existe $\varphi: I_n \rightarrow A$ bijetiva então $A = I_n$.*

Demonstração. Vamos provar por indução em $n \geq 1$ a seguinte afirmação.

$P(n)$: se $A \subset I_n$ e $\varphi : I_n \rightarrow A$ é bijetiva então $A = I_n$.

■ 1º passo: $n = 1$. Se $A \subset I_1 = \{1\}$ então $A = \emptyset$ (impossível, neste caso não existe nenhuma função $\varphi : I_1 \rightarrow \emptyset$) ou $A = \{1\} = I_1$, o que queríamos mostrar.

■ Passo indutivo. Suponha $P(n)$ verdadeira.

Sejam $A \subset I_{n+1}$, $\varphi : I_{n+1} \rightarrow A$ bijetiva e $a := \varphi(n+1) \in A$.

Analise os dois casos.

1) Se $A \setminus \{a\} \subset I_n$, a restrição $\tilde{\varphi} : I_n \rightarrow A \setminus \{a\}$, $\tilde{\varphi}(k) = \varphi(k)$ para todo $k \in I_n$, claramente é bijetiva, e como $A \setminus \{a\} \subset I_n$, a hipótese de indução é aplicável e temos que

$$A \setminus \{a\} = I_n.$$

Mas $A \subset I_{n+1}$, então necessariamente $a = n+1$ e daí $A = I_{n+1}$.

2) $A \setminus \{a\} \not\subset I_n$.

Como $A \subset I_{n+1}$, segue que $n+1 \in A \setminus \{a\}$.

A função φ sendo sobrejetiva, existe $p \in I_n$ tal que $\varphi(p) = n+1$.

Definimos a função $\tilde{\varphi} : I_n \rightarrow A \setminus \{a\}$ por

$$\tilde{\varphi}(p) = a$$

e $\tilde{\varphi}(j) = \varphi(j)$ para todo $j \neq p$.

É fácil verificar que $\tilde{\varphi}$ é bijetiva (usando a bijetividade de φ).

A hipótese indutiva é aplicável, já que $A \setminus \{a\} \subset I_n$.

Logo $A \setminus \{a\} = I_n$, e daí $A = I_{n+1}$.

Pelo princípio da indução concluímos a prova do teorema. $\square$

Corolário 5.2. Se $\varphi : I_n \rightarrow X$ e $\psi : I_m \rightarrow X$ são funções bijetivas para alguns $n, m \geq 1$ então $n = m$.

Demonstração. Para fixar ideias suponha que $m \leq n$. Então $I_m \subset I_n$. Temos:

$$I_n \xrightarrow{\varphi} X \xrightarrow{\psi^{-1}} I_m$$

então a função $\varphi : I_n \rightarrow I_m$

$f = \psi^{-1} \circ \varphi$ é bijetiva, com $I_m \subset I_n$. Pelo teorema anterior, $I_m = I_n$, logo $m = n$. $\square$

Corolário 5.3. Não pode existir uma bijeção $\varphi : X \rightarrow Y$ de um conjunto finito X para um subconjunto próprio $Y \subsetneq X$.

Demonstração. De fato, se $\varphi : I_n \rightarrow X$ é uma bijeção e $Y \subsetneq X$ então a pré-imagem

$$A := \varphi^{-1}(Y) \subset I_n$$

é um subconjunto próprio de I_n .

Definimos

$$g = \varphi^{-1} \circ f \circ \varphi.$$

Então a restrição $\tilde{\varphi} : A \rightarrow Y$, $\tilde{\varphi}(x) = \varphi(x)$ para todo $x \in A$ é uma bijeção.

Portanto $g : I_n \rightarrow A$ é uma bijeção. Como $A \subset I_n$, pelo teorema anterior $A = I_n$, contradição com o fato de A ser um subconjunto próprio de I_n . $\square$

Definição 5.2. Seja X um conjunto finito.

Se existem $n \geq 1$ e $f : I_n \rightarrow X$ bijetiva, então n é o número de elementos, ou a cardinalidade de X e escrevemos $\text{card } X = n$.

Se $X = \emptyset$ definimos sua cardinalidade $\text{card } X$ como 0.

Observação 5.1. Se $f : X \rightarrow Y$ é uma bijeção e X é finito, então Y é finito também e $\text{card } Y = \text{card } X$.

De fato, existem $n \geq 1$ e $\phi : I_n \rightarrow X$ é uma bijeção, então

$$I_n \xrightarrow{\phi} X \xrightarrow{f} Y,$$

logo $f \circ \phi : I_n \rightarrow Y$ é bijetiva, mostrando que Y é finito e

$$\text{card } Y = n = \text{card } X.$$

Teorema 5.4. *Todo subconjunto de um conjunto finito é finito também, ou seja, se X é finito e $Y \subset X$ então Y é finito.*

Além disso,

$$\text{card } Y \leq \text{card } X.$$

Demonstração. Basta provar o teorema para $X = I_n$, onde $n \geq 1$. Usamos indução.

$n = 1$. Se $Y \subset I_1 = \{1\}$ então $Y = \emptyset$ ou $Y = I_1$, logo Y é finito.

$n \rightarrow n + 1$. Seja $Y \subset I_{n+1}$. Analisamos dois casos.

1) $n + 1 \notin Y$. Então $Y \subset I_n$. Pela hipótese indutiva, $\text{card } Y \leq n < n + 1$.

2) $n + 1 \in Y$. Então

$$Y' = Y \setminus \{n + 1\} \subset I_n.$$

Pela hipótese indutiva, Y' é finito, e $\text{card } Y' \leq n$.

Seja $p = \text{card } Y'$. Então existe $\varphi : I_p \rightarrow Y'$ bijetiva. Considere a extensão $\tilde{\varphi} : I_{p+1} \rightarrow Y$, $\tilde{\varphi}(k) = \varphi(k)$ se $k \in I_p$ e $\tilde{\varphi}(p + 1) = n + 1$.

Então claramente $\tilde{\varphi}$ é bijetiva, logo Y é finito e

$$\text{card } Y = p + 1 \leq n + 1.$$

□

Lema 5.5. *Seja $g : X \rightarrow Y$ uma função sobrejetiva. Então existe uma função $f : Y \rightarrow X$ tal que $g \circ f = \text{id}_Y$ (a função f é uma inversa à direita de g). Em particular (por um exercício anterior), a função f é injetiva.*

Similarmente, se $g : X \rightarrow Y$ é injetiva, então existe $f : Y \rightarrow X$ tal que $f \circ g = \text{id}_X$ e em particular, f é sobrejetiva.

Demonstração. Vamos provar a primeira afirmação. A segunda é exercício.

Seja $y \in Y$. Como $g : X \rightarrow Y$ é sobrejetiva, existe um elemento $x \in X$ tal que $g(x) = y$ (poderia existir mais de um tal elemento, se g não for injetiva).

Então definimos $f(y) = x$, onde $x \in X$ é escolhido tal que $g(x) = y$.

Claramente, por essa escolha,

$$g \circ f(y) = g(f(y)) = g(x) = y,$$

mostrando que $g \circ f = \text{id}_Y$.

□

A seguir, apresentamos dois corolários do Teorema 5.4.

Corolário 5.6. *Seja $f : X \rightarrow Y$ uma função injetiva. Se Y é finito, então X também é finito e*

$$\text{card } X \leq \text{card } Y.$$

Demonstração. Considere a função $\tilde{f} : X \rightarrow f(X) \subset Y$,

$$\tilde{f}(x) = f(x),$$

isto é, a função obtida simplesmente restringindo o contradomínio de f à imagem $f(X)$.

Logo $\tilde{f}$ é sobrejetiva. Mas como f é injetiva, segue que a restrição $\tilde{f}$ é bijetiva, portanto

$$\text{card } X = \text{card } f(X).$$

Mas $f(X) \subset Y$, Y é finito, e pelo Teorema 5.4, tem-se

$$\text{card } f(X) \leq \text{card } Y,$$

portanto

$$\text{card } X = \text{card } f(X) \leq \text{card } Y,$$

e em particular X é finito. $\square$

Corolário 5.7. *Seja $g : Y \rightarrow X$ uma função sobrejetiva. Se Y é finito, então X também é finito e $\text{card } X \leq \text{card } Y$.*

Demonstração. Pelo Lema 5.5, existe $f : X \rightarrow Y$ injetiva. Pelo Corolário 5.6, $\text{card } X \leq \text{card } Y$. $\square$

Teorema 5.8. *Se X, Y são conjuntos finitos disjuntos, então $X \cup Y$ é finito e $\text{card}(X \cup Y) = \text{card } X + \text{card } Y$.*

Demonstração. Se $X = \emptyset$ ou $Y = \emptyset$ a afirmação é evidente. Então vamos supor que $X \neq \emptyset$ e $Y \neq \emptyset$ e sejam $n = \text{card } X$, $m = \text{card } Y$.

Existem $\varphi : I_n \rightarrow X$ e $\psi : I_m \rightarrow Y$ bijetivas. Definimos $f : I_{n+m} \rightarrow X \cup Y$ por

$$f(k) = \begin{cases} \varphi(k) & \text{se } k \in \{1, \dots, n\} \\ \psi(k - n) & \text{se } k \in \{n + 1, \dots, n + m\} \end{cases}$$

Claramente f é bijetiva, logo $X \cup Y$ é finito e $\text{card}(X \cup Y) = n + m$. $\square$

Corolário 5.9. *Se X, Y são conjuntos finitos (não necessariamente disjuntos), então $X \cup Y$ é finito e*

$$\text{card}(X \cup Y) \leq \text{card } X + \text{card } Y.$$

Demonstração. Sejam

$$X' = \{(x, 1) : x \in X\}$$

$$Y' = \{(y, 2) : y \in Y\}.$$

Claramente $\text{card } X' = \text{card } X$ e $\text{card } Y' = \text{card } Y$.

Mas X' e Y' são disjuntos, então pelo Teorema 5.8,

$$\begin{aligned} \text{card}(X' \cup Y') &= \text{card } X' + \text{card } Y' \\ &= \text{card } X + \text{card } Y. \end{aligned}$$

A função $f : X' \cup Y' \rightarrow X \cup Y$, definida por

$$f(x, 1) = x$$

$$f(y, 2) = y$$

é claramente sobrejetiva.

Então

$$\text{card}(X \cup Y) \leq \text{card}(X' \cup Y') = \text{card } X + \text{card } Y,$$

provando a afirmação. $\square$

Conjuntos infinitos. Um conjunto se chama infinito se ele não é finito.

O conjunto dos números naturais $\mathbb{N}$ é evidentemente infinito, o que pode ser provado de maneiras diferentes.

Por exemplo, a função $f : \mathbb{N} \rightarrow 2\mathbb{N}$, $f(n) = 2n$ é uma bijeção entre $\mathbb{N}$ e o subconjunto próprio de números pares. Logo, pelo Corolário 5.3, $\mathbb{N}$ não pode ser finito.

Além disso, a função sucessão $s : \mathbb{N} \rightarrow \{n \in \mathbb{N} : n \geq 1\}$ é bijetiva, e o contradomínio é um subconjunto próprio de $\mathbb{N}$ (ele não contém o número 0). Pelo mesmo Corolário 5.3, $\mathbb{N}$ não pode ser finito.

Um outro argumento é o seguinte. Se $p \geq 1$ e $f : I_p \rightarrow \mathbb{N}$ é uma função qualquer, então o número

$$N := \varphi(1) + \dots + \varphi(p) + 1$$

claramente satisfaz $N > \varphi(k)$ para todo $k \in I_p$.

Logo $N \neq \varphi(k)$ para todo $k \in I_p$, mostrando que φ não pode ser sobrejetiva. Então não existem $p \geq 1$ e $\varphi : I_p \rightarrow \mathbb{N}$ bijetiva, mostrando que $\mathbb{N}$ não pode ser finito, isto é, $\mathbb{N}$ é infinito.

Teorema 5.10. *Um conjunto X é infinito se e somente se existe uma função injetiva $\varphi : \mathbb{N} \rightarrow X$.*

Em outras palavras, denotando $\varphi(n) = x_n$, um conjunto X é infinito sse existem elementos *distintos*

$$x_0, x_1, \dots, x_n, \dots$$

em X .

Demonstração. A afirmação indireta é evidente. Se existir uma função injetiva $\varphi : \mathbb{N} \rightarrow X$ e se X fosse finito, pelo Corolário 5.6, o conjunto $\mathbb{N}$ seria finito, uma contradição. Portanto X é infinito.

Vamos provar a afirmação direta, ou seja, vamos supor que X seja infinito e definir uma função injetiva $f : \mathbb{N} \rightarrow X$. Vamos definir $f(n)$ por indução.

- 1º passo. Como $X \neq \emptyset$, existe um elemento $x_0 \in X$. Definimos $f(0) = x_0$.
- Passo indutivo. Dado $n \in \mathbb{N}$, suponha $f(0), \dots, f(n)$ já definidos e diferentes entre eles. Como X é infinito, tem-se

$$X \neq \{f(0), \dots, f(n)\}$$

já que $\{f(0), \dots, f(n)\}$ é um conjunto finito (com $n + 1$ elementos).

Então existe um elemento

$$x_{n+1} \in X \setminus \{f(0), \dots, f(n)\}.$$

Definimos $f(n + 1) = x_{n+1}$ e notamos que $f(n + 1) \neq f(k)$ para todo $k \in \{0, \dots, n\}$.

Pelo segundo princípio da indução, $f(n)$ é definido para todo $n \in \mathbb{N}$, então obtivemos uma função $f : \mathbb{N} \rightarrow X$.

Esta função f é claramente injetiva, já que dados $m, n \in \mathbb{N}$ com $m < n$, pela construção de f , $f(n) \neq f(m)$. □

Teorema 5.11. *Seja $X \subset \mathbb{N}$ um conjunto não vazio. Então X é finito se, e somente se, X possui máximo.*

Demonstração. A afirmação indireta é muito simples. Se X possui o máximo p , então $x \leq p$ para todo $x \in X$. Logo

$$X \subset \{0, 1, \dots, p\}.$$

Mas $\{0, 1, \dots, p\}$ é um conjunto finito, logo X também é.

Vamos provar a afirmação direta. Seja X um conjunto finito, então existe $n \geq 1$ tal que

$$X = \{x_1, \dots, x_n\}.$$

Observe que o número $N := x_1 + \dots + x_n$ claramente satisfaz a propriedade $N \geq x_k \forall k = 1, \dots, n$. Seja

$$B := \{p \in \mathbb{N} : p \geq x \text{ para todo } x \in X\}.$$

Então $N \in B$, logo $B \neq \emptyset$.

Pelo princípio da boa ordenação, B possui um mínimo p_0 .

Vamos mostrar que p_0 é o máximo de X .

Como $p_0 \in B$, tem-se $p_0 \geq x$ para todo $x \in X$.

Suponha por contradição que p_0 não seja o máximo de X . Então necessariamente $p_0 \notin X$.

Portanto $p_0 > x$ para todo $x \in X$.

Em particular $p_0 \geq x + 1$ para todo $x \in X$.

Além disso, $p_0 \neq 0$. Seja p_1 seu predecessor, então $p_1 + 1 = p_0 \geq x + 1$, logo $p_1 \geq x$ para todo $x \in X$.

Isto mostra que $p_1 \in B$. Mas $p_1 < p_0$, contradição com o fato de p_0 ser o mínimo de B .

Logo p_0 é o máximo de B . $\square$

6. NÚMEROS INTEIROS

Estendemos o conjunto de números naturais

$$\mathbb{N} = \{0, 1, 2, \dots, n, n+1, \dots\}$$

juntando um outro conjunto enumerável $\mathbb{Z}_-$ cujos elementos são denotados por

$$-1, -2, -3, \dots, -n, -(n+1), \dots$$

Seja

$$\mathbb{Z} = \mathbb{N} \cup \mathbb{Z}_- = \{\dots, -n, \dots, -1, 0, 1, \dots, n, \dots\}$$

a união entre $\mathbb{N}$ e o novo conjunto $\mathbb{Z}$.

Chamamos $\mathbb{Z}$ do conjunto de números inteiros. Estendemos as operações algébricas (adição e multiplicação) para este conjunto maior da seguinte forma.

■ **Adição.** Sejam $m, n \in \mathbb{N}$.

Se $m \geq n$ então existe $k \in \mathbb{N}$ tal que $m = n + k$.

Neste caso, definimos

$$m + (-n) = (-n) + m = k.$$

Se $m < n$ então existe $k \in \mathbb{N}$ tal que $n = m + k$.

Neste caso definimos

$$m + (-n) = (-n) + m = -k$$

Além disso, definimos

$$(-m) + (-n) = -(m + n)$$

Por exemplo, $7 + (-3) = 4$ porque $7 = 3 + 4$

e $(-7) + 3 = -4$ porque $7 = 3 + 4$

e $(-7) + (-3) = -(7 + 3) = -10$.

■ **Multiplicação.** Dados $m, n \in \mathbb{N}$, definimos

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

e

$$(-m) \cdot (-n) = m \cdot n.$$

Por exemplo, $7 \cdot (-3) = (-3) \cdot 7 = -21$

$$(-7) \cdot (-3) = 7 \cdot 3 = 21.$$

Deste modo, a adição e multiplicação são definidas para todo $m, n \in \mathbb{Z}$.

Além disso, é fácil verificar que elas satisfazem as propriedades conhecidas (associatividade, comutatividade, distributividade e que 0 e 1 têm os papéis especiais conhecidos ($n+0 = 0+n = n$, $n \cdot 1 = n$) e etc.

Ademais, estendemos a relação de ordem em $\mathbb{Z}$ pondo, para $m, n \in \mathbb{Z}$

$$-m \leq n$$

e

$$-m \leq -n \text{ se } n \leq m$$

É fácil verificar que $\leq$ é uma relação de ordem (total) em $\mathbb{Z}$, compatível com as operações algébricas, no sentido que, para $m, n, k \in \mathbb{Z}$,

$$\text{se } m \leq n \text{ então } m + k \leq n + k$$

e

$$\text{se } m \leq n \text{ e } k \geq 0 \text{ então } m \cdot k \leq n \cdot k.$$

Lema 6.1. $\mathbb{Z}$ é enumerável.

Demonstração. A função $f: \mathbb{Z} \rightarrow \mathbb{N}$,

$$f(n) = \begin{cases} 2n, & \text{se } n \geq 0, \\ 2(-n) - 1, & \text{se } n < 0 \end{cases}$$

é bijetiva. □