Elementos de Matemática

Notas de aula em construção

Fernando Manfio
ICMC – USP

Sumário

Capítulo 1

Linguagem matemática

Os assuntos abordados destas notas estão sob o seguinte critério: a Matemática fornece modelos abstratos para serem utilizados em situações concretas. Para poder empregar estes modelos é necessário verificar, em cada caso, que as hipóteses que lhe servem de base são satisfeitas. Com este espírito, daremos neste capítulo uma sucinta descrição do método axiomático.

1.1 O método axiomático

Uma definição matemática é uma convenção que consiste usar um nome, ou até mesmo uma sentença breve, para designar um objeto ou uma propriedade, cuja descrição exige normalmente o emprego de uma sentença mais longa. Vejamos alguns exemplos.

> *Ângulo* é a figura formada por duas semirretas que têm mesma origem.
>
> *Primos entre si* são dois ou mais números naturais cujo único divisor comum é a unidade.
>
> Um número inteiro x é *par* se é da forma $x = 2n$, para algum $n \in \mathbb{Z}$.
>
> Um número inteiro y é *ímpar* se é da forma $y = 2n + 1$, para algum $n \in \mathbb{Z}$.

Historicamente, nem sempre foi assim. Euclides, 325 – 265 a.C, aluno da Academia de Platão, foi o fundador da forte escola matemática de Alexandria, numa época em que Atenas passava por um momento de declínio político. Sua obra principal, os *Elementos*, consiste de treze volumes que contêm a maior parte da matemática conhecida na época. Trata-se de um texto sistemático, organizado segundo os critérios de rigor lógico-dedutivo, mas também de experiência intuitiva. Por exemplo, Euclides começa os Elementos com uma série de definições, das quais selecionamos as seguintes:

> *Linha* é um comprimento sem largura.
>
> *Superfície* é o que possui largura e comprimento somente.
>
> Quanto uma reta intercepta outra formando ângulos adjacentes iguais, cada um desses ângulos chama-se *reto* e as retas se dizem *perpendiculares*.

As quatro primeiras definições dadas acima, bem como as definições de ângulo reto e retas perpendiculares dadas por Euclides, estão corretas. Elas atendem aos padrões atuais de precisão e objetividade. No entanto, nas definições de linha e superfície, Euclides visa apenas oferecer ao leitor uma imagem intuitiva desses conceitos. Elas podem servir para ilustrar o pensamento geométrico mas não são utilizáveis nos raciocínios matemáticos porque são formuladas em termos vagos e imprecisos.

Na apresentação de uma teoria matemática, toda definição faz uso de termos específicos, os quais foram definidos usando outros termos, e assim sucessivamente. Este processo iterativo leva a três possibilidades:

(a) Continua indefinidamente, cada definição dependendo de outras anteriores, sem nunca chegar ao fim.

(b) Conduz a uma circularidade, como nos dicionários. Por exemplo: compreender $\to$ perceber, perceber $\to$ entender e entender $\to$ compreender.

(c) Termina numa palavra, ou num conjunto de palavras que não são definidas, ou seja, que são tomadas como representativas de conceitos primitivos. Por exemplo: ponto, reta, conjunto.

Evidentemente, as alternativas (a) e (b) acima citadas não nos convêm, e adotamos a alternativa (c).

Para poder empregar os conceitos primitivos adequadamente, é necessário dispor de um conjunto de princípios ou regras que disciplinem sua utilização e estabeleçam suas propriedades. Tais princípios são chamados *axiomas* ou *postulados*. Assim como os conceitos primitivos são objetos que não se definem, os axiomas são proposições que não se demonstram. Vejamos os seguintes exemplos.

> Dados quaisquer dois pontos distintos, A e B, existe uma única reta que os contém.
>
> Em cada reta existem ao menos dois pontos distintos e existem três pontos distintos que não pertencem a uma mesma reta.

Uma vez feita a lista dos conceitos primitivos e enunciado os axiomas de uma teoria matemática, todas as demais noções devem ser definidas e as afirmações seguintes devem ser demonstradas. Nisso consiste o chamado *método aximático*. As proposições a serem demonstradas chamam-se *teoremas* e suas consequências imediatas são denominadas *corolários*. Uma proposição auxiliar, usada na demonstração de um teorema, é chamada de *lema*.

Ser um axioma ou ser um teorema não é uma característica instrínsica de uma proposição. Dependendo da preferência de quem organiza a apresentação da teoria, uma determinada proposição pode ser adotada como axioma ou então provada como teorema, a partir de outra proposição que a substituiu na lista dos axiomas.

Vejamos alguns exemplos simples.

Proposição 1.1.1. A soma de dois números pares ainda é um número par.

Demonstração. Sejam $x, y \in \mathbb{Z}$ dois números pares arbitrários. Por definição, segue que $x = 2m$ e $y = 2n$, para alguns $m, n \in \mathbb{Z}$. Assim,

$$x + y = 2m + 2n = 2(m + n).$$

Como $m+n$ é um número inteiro segue, por definição, que $x+y$ é um número par, provando o resultado. □

Proposição 1.1.2. O produto de um número par com um número ímpar é um número par.

Demonstração. Sejam x um número par e y um número ímpar arbitrários. Por definição, tem-se que $x = 2m$ e $y = 2n + 1$, para alguns inteiros m e n. Então,

$$x \cdot y = 2m(2n + 1) = 4mn + 2m = 2(2mn + m).$$

Como $2mn + m$ é um número inteiro segue, por definição de número par, que $x \cdot y$ é um número par, e isso prova o resultado. □

1.2 O método de redução ao absurdo

As demonstrações nos dão segurança de que os resultados são verdadeiros. Em muitos casos elas nos dão resultados mais gerais. Um exemplo simples é o teorema de Pitágoras, que generaliza resultados que os egípcios, hindus e outros povos conheciam só casos particulares. Podemos fazer uso da tentativa e erro, cálculo de casos especiais, computadores, ou outros meios para demonstrar teoremas. O método aximático é um método de provar ue os resultados obtidos são corretos.

Em muitos casos, não é possível provar uma proposição de forma direta, como nos exemplos anteriores. Prossegue-se, então, da seguinte forma: nega-se inicialmente, supondo por absurdo, aquilo que se quer provar e, fazendo uso dos resultados e definições anteriores, chega-se a uma contradição. Se tal contradição for relativa às hipóteses da proposição ou a algum resultado já conhecido, a proposição estará provada. Tal maneira de demonstrar proposições, ou teoremas em geral, chama-se método de *redução ao absurdo*.

Vejamos alguns exemplos.

Proposição 1.2.1. Se x é um número inteiro tal que x^2 é um número par, então x também é um número par.

Demonstração. Seja x um número inteiro tal que x^2 é par, ou seja, x^2 é da forma $x^2 = 2n$, para algum $n \in \mathbb{Z}$. Suponha, por absurdo, que x não seja par. Assim, x deve ser um número ímpar e, portanto, da forma $x = 2m+1$, para algum $m \in \mathbb{Z}$. Então,

$$x^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(m^2 + 2m) + 1.$$

Como $m^2 + 2m \in \mathbb{Z}$, a última igualdade acima implica, por definição, que x^2 é um número ímpar, contradizendo a hipótese. Tal contradição surgiu de supormos que x era um número ímpar. Logo, isso não pode acontecer e, portanto, x deve ser um número par. $\square$

Teorema 1.2.2. *$\sqrt{2}$ é um número irracional.*

Demonstração. Suponha, por absurdo, que $\sqrt{2} \in \mathbb{Q}$. Assim, por definição, $\sqrt{2}$ pode ser escrito como

$$\sqrt{2} = \frac{p}{q}, \tag{1.1}$$

onde $p, q \in \mathbb{Z}$, com $q \neq 0$. Suponhamos, além disso, que a fração $\frac{p}{q}$ seja irredutível, i.e., $mdc(p,q) = 1$. Elevando ao quadrado ambos os membros da igualdade (1.1), obtemos

$$p^2 = 2q^2, \tag{1.2}$$

ou seja, o inteiro p^2 é um número par. Pela Proposição 1.2.1, segue que p também é par, ou seja, da forma $p = 2m$, para algum $m \in \mathbb{Z}$. Substituindo este valor de p em (1.2) e simplificando, obtemos $q^2 = 2m$, para algum $m \in \mathbb{Z}$. Ou seja, q^2 é um número par e, novamente pela Proposição 1.2.1, concluímos que q também é par. No entanto, p e q sendo números pares implica que a fração $\frac{p}{q}$ não é irredutível, e isso é uma contradição. Portanto, deve-se ter $\sqrt{2} \notin \mathbb{Q}$. $\square$

Capítulo 2

Conjuntos

2.1 Introdução

Os conjuntos constituem o modelo matemático para a organização do pensamento lógico, e toda a Matemática pode ser formulada na linguagem de conjuntos. Assim, a noção de conjunto é fundamental pois, além de ser uma ideia simples, a partir dela todos os conceitos matemáticos podem ser expressos. O objetivo deste capítulo é apenas introduzir a linguagem e a notação dos conjuntos, que serão suficientes para os estudos seguintes.

Em nosso estudo, aceitaremos três termos primitivos:

Conjunto, *Elemento* e *Pertinência*.

Assim, um conjunto é formado por elementos. Dados um conjunto A e um objeto qualquer a, que pode até mesmo ser outro conjunto, a única pergunta cabível em relação a eles é se a é ou não um elemento do conjunto A. No caso afirmativo, dizemos que *a pertence* ao conjunto A e escrevemos $a \in A$. Caso contrário, escrevemos $a \notin A$ e dizemos que *a não pertence* ao conjunto A. Denotaremos os conjuntos com letras maiúsculas $A, B, C, M, \ldots$ e os elementos com letras minúsculas $a, b, c, x, \ldots$.

Os conjuntos podem ser usados para substituir as propriedades e as condições. Assim, ao invés de falarmos que o objeto x possui a propriedade P, podemos escrever $x \in A$, onde A é o conjunto dos elementos que possuem a propriedade P. Nestas condições, representamos o conjunto A como sendo

$$A = \{x : x \text{ tem a propriedade } P\}.$$

A vantagem de se utilizar a linguagem e a notação de conjuntos é que entre estes existe uma álgebra, formulada sobre as operações de união e interseção, além da relação de inclusão, que passaremos a estudar.

2.2 A relação de inclusão

Dados dois conjuntos A e B, dizemos que A é *subconjunto* de B se todo elemento de A é também elemento de B. Usaremos a notação $A \subset B$ para indicar este fato. O símbolo $\subset$ é denominado *sinal de inclusão*, e a relação $A \subset B$ chama-se *relação de inclusão*. Quando A não é subconjunto de B, escrevemos $A \not\subset B$. Isto significa que existe, pelo menos, um objeto a de modo que $a \in A$ e $a \notin B$. Algumas inclusões bem naturais. Por exemplo, qualquer que seja o conjunto A, tem-se sempre $A \subset A$, pois todo elemento de A pertence ao conjunto A.

Existe um conjunto, chamado de *conjunto vazio* e denotado pelo símbolo ϕ, que é um tanto intrigante. Ele é aceito como conjunto pois cumpre a função de simplificar as proposições. Qualquer propriedade contraditória serve para defini-lo. Assim, por conjunto vazio, entenderemos o conjunto que não possui nenhum elemento. Por exemplo,

$$\phi = \{x : x \neq x\},$$

pois seja qual for o objeto x, tem-se sempre $x \notin \phi$. Observe que $\phi \subset A$, qualquer que seja o conjunto A pois, se quiséssemos mostrar que $\phi \not\subset A$, teríamos que obter um objeto x tal que $x \in \phi$ mas $x \notin A$. Como $x \in \phi$ é impossível, concluimos que $\phi \subset A$.

A relação de inclusão é uma *relação de equivalência*, ou seja, cumpre as três seguintes propriedades fundamentais:

Reflexiva: $A \subset A$,

Anti-simétrica: se $A \subset B$ e $B \subset A$ então $A = B$,

Transitiva: se $A \subset B$ e $B \subset C$ então $A \subset C$.

A verificação das propriedades acima é deixada a cargo do leitor. Quando se deseja mostrar que os conjuntos A e B são iguais prova-se, em virtude da anti-simetria, que $A \subset B$ e $B \subset A$. A propriedade transitiva da inclusão é a base do raciocínio dedutivo, sob a forma que classicamente se chama de *silogismo*. Um exemplo de silogismo é o seguinte: todo ser humano é um animal, todo animal é mortal, logo todo ser humano é mortal.

Dado um subconjunto A de um conjunto U, denotemos por A^c o *complemento* de A em relação a U, ou seja,

$$A^c = \{x \in U : x \notin A\}.$$

Fixado o subconjunto $A \subset U$ segue que, para cada elemento $x \in U$, vale somente uma das alternativas: $x \in A$ ou $x \notin A$. Este fato, de que não existe uma terceira opção, é conhecido como o *princípio do terceiro excluído*. Além disso, o fato de que as alternativas $x \in A$ e $x \notin A$ não ocorrem ao mesmo tempo chama-se o *princípio da não-contradição*.

Proposição 2.2.1. O complementar de um conjunto satisfaz as seguintes propriedades básicas:

(a) $(A^c)^c = A$, qualquer que seja o subconjunto $A \subset U$.

(b) Se $A, B \subset U$, com $A \subset B$, então $B^c \subset A^c$.

Demonstração. (a) Se $x \in (A^c)^c$, então $x \in U$ e $x \notin A^c$, ou seja, $x \in U$ e $x \in A$, logo $x \in A$. Reciprocamente, se $x \in A$, então $x \notin A^c$, logo $x \in (A^c)^c$.
(b) Dado $x \in B^c$, tem-se que $x \in U$ e $x \notin B$. Como $A \subset B$, segue que $x \notin A$, logo $x \in A^c$. Isso mostra que $B^c \subset A^c$. $\square$

A implicação

$$A \subset B \Rightarrow B^c \subset A^c$$

pode ser interpretada do ponto de vista lógico, no seguinte sentido. Suponha que os conjuntos A e B possuem propriedades p e q, respectivamente. Ou seja, o conjunto A é formado por todos os elementos de U que satisfazem a propriedade p, enquanto que os elementos de B são aqueles que têm a propriedade q. As propriedades que definem os conjuntos A^c e B^c são respectivamente as negações de p e q, denotadas por $\sim p$ e $\sim q$. Assim, dizer que um elemento x tem a propriedade $\sim p$ significa, por definição, que x não tem a propriedade p. Portanto, podemos ler a propriedade (b) da Proposição 2.2.1 como

$$\text{Se } p \Rightarrow q \text{ então } \sim q \Rightarrow \sim p.$$

A implicação $\sim q \Rightarrow \sim p$ chama-se a *contrapositiva* da implicação $p \Rightarrow q$. Note que a contrapositiva de uma implicação nada mais é do que a mesma implicação dita com outras palavras. Por exemplo, a afirmação de que todo número primo maior do que 2 é ímpar e a afirmação de que um número par maior do que 2 não é primo dizem exatamente a mesma coisa.

Finalizamos essa seção fazendo uma distinção cuidadosa sobre a idéia de *negação* e a noção não-matemática de *oposto*. Se um conceito é expresso por uma palavra, o conceito contrário é expresso pelo antônimo daquela palavra. Por exemplo, o contrário de gigantesco é minúsculo, mas a negação de gigantesco inclui outras gradações de tamanho além de minúsculo.

2.3 Operações entre conjuntos

Dados dois conjuntos A e B, a *união* $A \cup B$ é o conjunto formado pelos elementos de A mais os elementos de B. A *interseção* $A \cap B$ é o conjunto dos elementos que são ao mesmo tempo elementos de A e de B. Assim, se $x \in A \cup B$ então pelo menos uma das afirmações

$$x \in A,\ x \in B$$

é verdadeira. Por outro lado, se $x \in A \cap B$ então ambas as afirmações acima ocorrem. Mais precisamente,

$$\begin{aligned} x \in A \cup B &\Leftrightarrow x \in A \text{ ou } x \in B, \\ x \in A \cap B &\Leftrightarrow x \in A \text{ e } x \in B. \end{aligned}$$

Proposição 2.3.1. As operações de união e interseção satisfazem as seguintes propriedades:

(i) $A \cup B = B \cup A$ e $A \cap B = B \cap A$,

(ii) $(A \cup B) \cup C = A \cup (B \cup C)$ e $(A \cap B) \cap C = A \cap (B \cap C)$,

(iii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

(iv) $A \cup B = B \Leftrightarrow A \subset B \Leftrightarrow A \cap B = A$,

(v) $(A \cup B)^c = A^c \cap B^c$ e $(A \cap B)^c = A^c \cup B^c$.

A demonstração da Proposição 2.3.1 se reduz ao uso adequado dos conectivos *e* e *ou*, e será deixada a cargo do leitor.

2.4 Exercícios

2.2

1. A *diferença* entre dois conjuntos A e B, denotada por $A - B$, é conjunto definido por $A - B = \{x : x \in A \text{ e } x \notin B\}$. Mostre que:

(i) $A - B \subset A \quad \text{e} \quad (A - B) \cap B = \emptyset$,

(ii) $A - B = \emptyset \Leftrightarrow A \subset B \quad \text{e} \quad A - (A - B) = B \Leftrightarrow B \subset A$.

2.3

1. Fixados dois conjuntos A e B, considere um conjunto X com as seguintes propriedades:

(i) $A \subset X$ e $B \subset X$,

(ii) Se $A \subset Y$ e $B \subset Y$ então $X \subset Y$.

Prove que $X = A \cup B$.

Capítulo 3

Funções

3.1 Introdução

Historicamente, o termo função proporciona um exemplo interessante da tendência dos matemáticos em generalizar e ampliar os conceitos. A palavra função, na sua forma latina equivalente, foi introduzida por Liebniz em 1694, inicialmente para expressar qualquer quantidade associada a uma curva como, por exemplo, as coordenadas de um ponto da curva, a inclinação de uma curva e o raio da curvatura de uma curva.

Em torno de 1718, Bernoulli chegou a considerar função como uma expressão qualquer formada de uma variável e algumas constantes. Pouco tempo depois, Euler considerou função como uma equação ou fórmula qualquer envolvendo variáveis e constantes. O conceito de Euler se manteve inalterado até que Fourier considerou, em suas pesquisas sobre a propagação do calor, as chamadas séries trigonométricas, que envolvem uma relação mais geral entre as variáveis que as que já haviam sido estudadas anteriormente.

O conceito de função permeia grande parte da Matemática e, desde as primeiras décadas do século passado, tem sido o princípio central e unificador na organização dos cursos elementares de Matemática. O conceito parece representar um guia natural e efetivo para a seleção e desenvolvimento do material de textos de Matemática.

O objetivo desde capítulo é apenas apresentar as propriedades básicas das funções, bem como a composição de funções.

3.2 Propriedades básicas

Um par ordenado (x, y) é formado por um objeto x, chamado a *primeira coordenada*, e um objeto y, chamado a *segunda coordenada*. Dois pares ordenados (x, y) e (u, v) são iguais se $x = u$ e $y = v$. Observe que o par ordenado (x, y) não é a mesma coisa que o conjunto $\{x, y\}$, pois $\{x, y\} = \{y, x\}$ sempre, enquanto que $(x, y) = (y, x)$ somente quando $x = y$.

O *produto cartesiano* de dois conjuntos A e B é o conjunto $A \times B$ formado por todos os pares ordenados (x, y), onde $x \in A$ e $y \in B$. Simbolicamente,

$$A \times B = \{(x, y) : x \in A \text{ e } y \in B\}.$$

Definição 3.2.1. Uma *função* entre dois conjuntos A e B é uma correspondência $f : A \to B$ que associa a cada elemento $x \in A$ um único elemento $f(x) \in B$.

É usual denotarmos uma função pondo

$$x \in A \mapsto f(x) \in B.$$

O conjunto A é chamado de *domínio* da função e o conjunto B chamado de *contradomínio* da função.

O *gráfico* de uma função $f : A \to B$ é o subconjunto $Gr(f) \subset A \times B$ formado pelos pares ordenados $(x, f(x))$, onde $x \in A$. Ou seja,

$$Gr(f) = \{(x, y) \in A \times B : y = f(x)\}.$$

Duas funções $f : A \to B$ e $g : X \to Y$ são iguais se, e somente se, $A = X$, $B = Y$ e $f(x) = g(x)$, para todo $x \in A$. Portanto, elas são iguais se, e somente se, possuem o mesmo gráfico.

Definição 3.2.2. Uma função $f : A \to B$ chama-se *injetora* se para quaisquer $x, y \in A$, com $f(x) = f(y)$, tem-se $x = y$. Ou seja, $x \neq y$ em A implica $f(x) \neq f(y)$ em B.

Um exemplo simples de função injetora é a *inclusão*. Mais precisamente, se A é subconjunto de B, a inclusão de A em B é a função $i : A \to B$ dada por $i(x) = x$, para todo $x \in A$.

Definição 3.2.3. Uma função $f : A \to B$ chama-se *sobrejetora* se, para todo $y \in B$ existe ao menos um elemento $x \in A$ tal que $f(x) = y$.

As *projeções* $\pi_1 : A \times B \to A$ e $\pi_2 : A \times B \to B$ definidas por $\pi_1(a, b) = a$ e $\pi_2(a, b) = b$ são exemplos simples de funções sobrejetoras.

Exemplo 3.2.4. A função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$ não é injetora, pois $f(-3) = f(3)$, embora $-3 \neq 3$. Além disso, f também não é sobrejetora, pois não existe $x \in \mathbb{R}$ tal que $f(x) = x^2 = -1$.

Uma função $f : A \to A$ é dita ser *bijetora* se é injetora e sobrejetora ao mesmo tempo. Um exemplo simples é a função identidade $id : A \to A$, dada por $id(x) = x$, para todo $x \in A$.

Dados uma função $f : A \to B$ e um subconjunto $X \subset A$, a *imagem* de X por f é conjunto

$$f(X) = \{y \in B : y = f(x),\ x \in X\}.$$

Assim, $f(X)$ é um subconjunto de B. Para que uma função $f : A \to B$ seja sobrejetora é necessário e suficiente que $f(X) = B$. O conjunto $f(A)$ é chamado a *imagem* da função f.

Proposição 3.2.5. Dados uma função $f : A \to B$ e subconjuntos $X, Y \subset A$, valem as seguintes propriedades:

(i) $f(X \cup Y) = f(X) \cup f(Y)$,

(ii) $f(X \cap Y) \subset f(X) \cap f(Y)$,

(iii) $X \subset Y \Rightarrow f(X) \subset f(Y)$,

(iv) $f(\emptyset) = \emptyset$.

Demonstração. (i) Se $y \in f(X \cup Y)$, então existe $x \in X \cup Y$ tal que $y = f(x)$. Se $x \in X$, tem-se $y \in f(X)$ e, caso $x \in Y$, tem-se $y \in f(Y)$. Em qualquer caso, $y \in f(X) \cup f(Y)$, logo $f(X \cup Y) \subset f(X) \cup f(Y)$. Reciprocamente, seja $z \in f(X) \cup f(Y)$. Assim, $z \in f(X)$ ou $z \in f(Y)$. No primeiro caso, existe $x \in X$ tal que $z = f(x)$. No segundo, existe $y \in Y$ tal que $z = f(y)$. Em qualquer caso, existe $w \in X \cup Y$ tal que $z = f(w)$. Assim, $z \in f(X \cup Y)$, mostrando que $f(X) \cup f(Y) \subset f(X \cup Y)$. As duas inclusões provam a igualdade desejada.

(ii) Se $y \in f(X \cap Y)$, então existe $x \in X \cap Y$ tal que $y = f(x)$. O fato que $x \in X \cap Y$ significa que $x \in X$ e $x \in Y$, logo $y \in f(X)$ e $y \in f(Y)$. Portanto, $y \in f(X) \cap f(Y)$, provando a inclusão desejada.

(iii) Dado $y \in f(X)$, tem-se que existe $x \in X$ tal que $y = f(x)$. Como $X \subset Y$, tem-se $x \in Y$, logo $y = f(x) \in f(Y)$, e isso mostra a inclusão desejada.

(iv) Suponha que $f(\emptyset) \neq \emptyset$. Assim, existe ao menos um elemento y na imagem $f(\emptyset)$ de f. Isso significa que existe $x \in \emptyset$ tal que $y = f(x)$. No entanto, como $x \in \emptyset$ é impossível, concluimos que $f(\emptyset) = \emptyset$. $\square$

Exemplo 3.2.6. Seja $f : A \to B$ uma função que não é injetora. Assim, existem $x \neq y$ em A, com $f(x) = f(y)$. Sejam $X = \{x\}$ e $Y = \{y\}$. Temos $X \cap Y = \emptyset$, logo $f(X \cap Y) = \emptyset$. No entanto,

$$f(X) \cap f(Y) = \{f(x)\} \neq \emptyset,$$

mostrando que $f(X) \cap f(Y) \not\subset f(X \cap Y)$.

Dados uma função $f : A \to B$ e um subconjunto $Y \subset B$, definimos a *imagem inversa* de Y por f como o conjunto

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}.$$

Note que pode ocorrer $f^{-1}(Y) = \emptyset$, mesmo que $Y \subset B$ seja não-vazio. Por exemplo, basta escolher Y de modo que $Y \cap f(A) = \emptyset$.

Proposição 3.2.7. Dados uma função $f : A \to B$ e subconjuntos $Y, Z \subset B$, valem as seguintes propriedades:

(i) $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$,

(ii) $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$,

(iii) $f^{-1}(Y^c) = (f^{-1}(Y))^c$,

(iv) $Y \subset Z \Rightarrow f^{-1}(Y) \subset f^{-1}(Z)$,

(v) $f^{-1}(B) = A$,

(vi) $f^{-1}(\emptyset) = \emptyset$.

A demonstração da Proposição 3.2.7 é deixada a cargo do leitor.

3.3 Composição de funções

Dados duas funções $f : A \to B$ e $g : B \to C$, de modo que o domínio de g coincide com o contradomínio de f, definimos a *função composta*

$$g \circ f : A \to C$$

pondo

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

para todo $x \in A$. A composição de funções satisfaz naturalmente a propriedade associativa. De fato, dados funções $f : A \to B$, $g : B \to C$ e $h : C \to D$, temos

$$\begin{aligned} [(h \circ g) \circ f](x) &= (h \circ g)(f(x)) = h(g(f(x))) \\ &= h[(g \circ h)(x)] = [h \circ (g \circ f)](x), \end{aligned}$$

qualquer que seja o ponto $x \in A$.

Definição 3.3.1. Uma função $g : B \to A$ é dita ser uma *inversa à esquerda* para uma função $f : A \to B$ se $g \circ f = id_A$, i.e., $g(f(x)) = x$, para todo $x \in A$. Dizemos também neste caso que f possui uma inversa à esquerda.

Exemplo 3.3.2. Sejam $f : \mathbb{R}_+ \to \mathbb{R}$ dada por $f(x) = x^2$ e $g : \mathbb{R} \to \mathbb{R}_+$ definida por

$$g(y) = \begin{cases} \sqrt{y}, & \text{se} \quad y \geq 0 \\ 0, & \text{se} \quad y < 0 \end{cases} .$$

Então, para todo $x \geq 0$, tem-se

$$g(f(x)) = g(x^2) = \sqrt{x^2} = x,$$

mostrando que $g \circ f = id_{\mathbb{R}_+}$.

Proposição 3.3.3. Uma função $f : A \to B$ possui inversa à esquerda se, e somente se, é injetora.

Demonstração. Suponha que $f : A \to B$ seja injetora. Assim, para cada $y \in f(A)$, existe um único $x \in A$ tal que $y = f(x)$. Isso define uma função $g : f(A) \to A$ tal que $g(f(x)) = x$, para todo $x \in A$. Completamos a definição da função $g : B \to A$ pondo, por exemplo, $g(y) = x_0$, para todo $y \in B - f(A)$, onde x_0 é algum elemento fixado em A. Obtemos, assim, uma função $g : B \to A$ tal que $g \circ f = id_A$. Reciprocamente, seja $g : B \to A$ uma inversa à esquerda para f. Dados $a, b \in A$, com $f(a) = f(b)$, temos

$$a = g(f(a)) = g(f(b)) = b,$$

mostrando que f é injetora. □

Definição 3.3.4. Uma função $g : B \to A$ é dita ser uma *inversa à direita* para uma função $f : A \to B$ se $f \circ g = id_B$, i.e., $f(g(y)) = y$, para todo $y \in B$. Dizemos também neste caso que f possui uma inversa à direita.

Proposição 3.3.5. Uma função $f : A \to B$ possui inversa à direita se, e somente se, é sobrejetora.

Demonstração. Suponha $f : A \to B$ sobrejetora. Assim, para cada $y \in B$, tem-se $f^{-1}(y) \neq \emptyset$. Escolha, para cada $y \in B$, um elemento $x \in A$ tal que $y = f(x)$ e seja $g(y) = x$. Isso define uma função $g : B \to A$ tal que $f(g(y)) = y$. Logo, g é uma inversa à direita para f. Reciprocamente, seja $g : B \to A$ tal que $f \circ g = id_B$. Assim, para cada $y \in B$, escolhendo $x = g(y)$, temos $f(x) = f(g(y)) = y$, i.e., f é sobrejetora. $\square$

Dizemos que uma função $g : B \to A$ é uma *inversa* para uma função $f : A \to B$ se $f \circ g = id_A$ e $g \circ f = id_B$. Decorre então das Proposições 3.3.3 e 3.3.5 que uma função $f : A \to B$ possui inversa se, e somente se, f é bijetora.

3.4 Exercícios

3.2

1. Se $f : A \to B$ é uma função injetora, mostre que vale

$$f(X \cap Y) = f(X) \cap f(Y),$$

para quaisquer subconjuntos $X, Y \subset A$, com $X \cap Y \neq \emptyset$.

3.3

1. Mostre que uma função $f : A \to B$ é injetora se, e somente se, $f(A-X) = f(A) - f(X)$, qualquer que seja o subconjunto $X \subset A$.

2. Dado uma função $f : A \to B$, mostre que:

(i) $X \subset f^{-1}(f(X))$, para qualquer subconjunto $X \subset A$,

(ii) f é injetora se, e somente se, $f^{-1}(f(X)) = X$, para todo $X \subset A$.

3. Dado uma função $f : A \to B$, mostre que:

(i) $f(f^{-1}(Z)) \subset Z$, para qualquer subconjunto $Z \subset B$,

(ii) f é sobrejetora se, e somente se, $f(f^{-1}(Z)) \subset Z$, para todo $Z \subset B$.

Capítulo 4

Números naturais

4.1 Axiomas de Peano

Nesta seção apresentaremos a teoria dos números naturais que será deduzida de três axiomas, conhecidos como *axiomas de Peano*. Consideraremos, como termos primitivos, um conjunto $\mathbb{N}$, cujos elementos são chamados de *números naturais*, e uma função $s : \mathbb{N} \to \mathbb{N}$ que associa, a cada natural n, outro número natural $s(n)$ chamado o *sucessor* de n.

Axioma 1 (Axiomas de Peano)**.** A função $s : \mathbb{N} \to \mathbb{N}$ possui as seguintes propriedades:

(1) $s : \mathbb{N} \to \mathbb{N}$ é injetora.

(2) $\mathbb{N} - s(\mathbb{N})$ consiste de um único elemento. Ou seja, existe um único número natural, chamado *zero* e representado pelo símbolo 0, que não é sucessor de nenhum outro. Assim, qualquer que seja $n \in \mathbb{N}$, tem-se $0 \neq s(n)$. Por outro lado, se $n \neq 0$ então existe um único natural m tal que $s(m) = n$.

(3) Se $X \subset \mathbb{N}$ é um subconjunto tal que $0 \in X$ e, para todo $n \in X$ tem-se também $s(n) \in X$, então $X = \mathbb{N}$.

O axioma (3) é conhecido como *axioma da indução* que, sob a forma de propriedades ao invés de conjuntos, pode ser enunciado da seguinte forma.

Axioma 2 (Axioma da indução)**.** Seja $P(n)$ uma propriedade relativa ao número natural n de modo que:

(i) $P(0)$ é verdadeiro,

(ii) A validez de $P(n)$ implina a validez de $P(s(n))$, para todo $n \in \mathbb{N}$.

Então, $P(n)$ é verdadeiro para todo $n \in \mathbb{N}$.

Vejamos um exemplo simples de como usar o axioma da indução.

Exemplo 4.1.1. Para todo natural n, vale a fórmula

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

De fato, seja $P(n)$ a propriedade relativa ao natural n dada por

$$P(n): \ 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

Para $n = 0$, $P(0)$ se resume em afirmar que $0 = 0$. Suponhamos então verdadeira $P(n)$ e mostremos que $P(n+1)$ também é verdadeiro, i.e., mostremos que

$$P(n+1): \ 1 + 2 + 3 + \ldots + n + n + 1 = \frac{(n+1)(n+2)}{2}.$$

Para isso, basta apenas somar $n + 1$ em ambos os membros de $P(n)$ e simplificar o lado direito. Portanto, $P(n) \Rightarrow P(n+1)$, e a conclusão segue do axioma da indução.

Proposição 4.1.2. Qualquer que seja o natural n, tem-se $s(n) \neq n$.

Demonstração. Mostremos por indução. Para isso, consideremos a propriedade

$$P(n): \ s(n) \neq n.$$

$P(0)$ é verdadeiro pois, caso tivéssemos $P(0) = 0$, teríamos que o natural 0 seria sucessor do próprio 0. Suponhamos agora válido $P(n)$ e mostremos $P(s(n))$, ou seja, provemos que $s(s(n)) \neq s(n)$. De fato, caso fosse $s(s(n)) = s(n)$, concluímos que os naturais distintos, $s(n)$ e n, teriam o mesmo sucessor, contradizendo a injetividade da função s. Portanto, $P(n) \Rightarrow P(s(n))$. □

4.2 A operação de adição em $\mathbb{N}$

O que faremos agora é munir o conjunto $\mathbb{N}$ com algumas estruturas. Nesta seção definiremos a operação de adição.

Definição 4.2.1. Uma *adição* no conjunto $\mathbb{N}$ é uma função $\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ que cumpre os seguintes axiomas:

(1) $\phi(n, 0) = n$,

(2) $\phi(m, s(n)) = s(\phi(m, n))$,

para quaisquer $m, n \in \mathbb{N}$.

O número natural $\phi(m, n)$ é chamado a *soma* dos naturais m e n. A pergunta natural que se faz aqui é se existe uma função ϕ satisfazendo os axiomais (1) e (2) acima. Veremos, na verdade, que existe uma única tal função. Comecemos com algumas propriedades da adição.

Proposição 4.2.2. Se $\phi : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ é uma adição em $\mathbb{N}$, valem as seguintes propriedades básicas:

(a) $\phi(0, n) = n$,

(b) $\phi(m, s(n)) = \phi(s(m), n)$,

para quaisquer $m, n \in \mathbb{N}$.

Demonstração. Provemos por indução. Para o item (a), consideremos a propriedade

$$P(n) : \phi(0, n) = n.$$

$P(0)$ é verdadeiro, pois $\phi(0, 0) = 0$ em virtude do axioma (1) da adição. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também é verdadeiro, ou seja, provemos que $\phi(0, s(n)) = s(n)$. De fato, pelo axioma (2) da adição, temos

$$\phi(0, s(n)) = s(\phi(0, n)) = s(n),$$

como queríamos. Para o item (b), fixemos um natural arbitrário m e consideremos a propriedade

$$P(n) : \phi(m, s(n)) = \phi(s(m), n).$$

Observe que se $P(n)$ for verdadeiro para todo $n \in \mathbb{N}$, o item (b) estará provado em virtude da arbitrariedade de m. Então, $P(0)$ é verdadeiro, pois

$$\phi(m, s(0)) = s(\phi(m, 0)) = s(m)$$

e

$$\phi(s(m), 0) = s(m),$$

mostrando que $\phi(m, s(0)) = \phi(s(m), 0)$. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também é verdadeiro, ou seja, provemos que

$$\phi(m, s(s(n))) = \phi(s(m), s(n)).$$

De fato,

$$\begin{aligned} \phi(m, s(s(n))) &= s(\phi(m, s(n))) \\ &= s(\phi(s(m), n)) \\ &= \phi(s(m), s(n)), \end{aligned}$$

como queríamos. □

A Proposição seguinte garante que uma adição é sempre comutativa.

Proposição 4.2.3. Se $\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ é uma adição em $\mathbb{N}$, então

$$\phi(m, n) = \phi(n, m),$$

para quaisquer $m, n \in \mathbb{N}$.

Demonstração. Fixemos um natural arbitrário m e consideremos a propriedade

$$P(n) : \phi(m, n) = \phi(n, m).$$

Pelo axioma (1) da adição, temos $\phi(m, 0) = m$. Por outro lado, pelo item (a) da Proposição 4.2.2, temos $\phi(0, m) = m$. Assim, $\phi(m, 0) = \phi(0, m)$, mostrando que $P(0)$ é verdadeiro. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também é verdadeiro, ou seja, provemos que

$$\phi(m, s(n)) = \phi(s(n), m).$$

De fato,

$$\begin{aligned} \phi(m, s(n)) &= \phi(n, s(m)) = s(\phi(n, m)) \\ &= s(\phi(m, n)) = \phi(m, s(n)), \end{aligned}$$

como queríamos. □

O resultado seguinte garante a unicidade da adição em $\mathbb{N}$. Mais precisamente, se existe uma adição em $\mathbb{N}$, ela é única.

Proposição 4.2.4. Se $\phi, \psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ são duas adições em $\mathbb{N}$, então $\phi(m, n) = \psi(m, n)$, para quaisquer $m, n \in \mathbb{N}$.

Demonstração. Fixemos um natural arbitrário m e consideremos a propriedade

$$P(n) : \phi(m, n) = \psi(m, n).$$

$P(0)$ é verdadeiro pois, em virtude do axioma (1) da adição, temos $\phi(m, 0) = m = \psi(m, 0)$. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também o é. De fato,

$$\phi(m, s(n)) = s(\phi(m), n) = s(\psi(m, n)) = \psi(m, s(n)),$$

e isso conclui a demonstração. □

O resultado seguinte, conhecido como *teorema da recursão em* $\mathbb{N}$, garantirá que existe uma adição em $\mathbb{N}$.

Teorema 4.2.5 (Recursão em $\mathbb{N}$)**.** *Dados uma função $F : \mathbb{N} \to \mathbb{N}$ e um número natural m, existe uma única função $f_m : \mathbb{N} \to \mathbb{N}$ satisfazendo*

(a) $f_m(0) = m$,

(b) $f_m(s(n)) = F(f_m(n))$,

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

Corolário 4.2.6. Existe uma adição em $\mathbb{N}$.

Demonstração. Fixemos um natural m. Em virtude do Teorema 4.2.5, existe uma função $f_m : \mathbb{N} \to \mathbb{N}$ tal que

$$f_m(0) = m \quad \text{e} \quad f_m(s(n)) = s(f_m(n)),$$

para todo $n \in \mathbb{N}$. Definimos uma função $\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ pondo $\phi(m, n) = f_m(n)$. É imediato verificar que ϕ é uma adição em $\mathbb{N}$. □

Estabelecido a existência e unicidade da adição em $\mathbb{N}$ denotaremos, como de costume, a soma dos naturais m e n por $m + n$ ao invés de $\phi(m, n)$. Finalizaremos esta seção com mais uma propriedade da adição.

Proposição 4.2.7. Vale a lei do corte em $\mathbb{N}$, ou seja, se $m, n, p \in \mathbb{N}$ são tais que $m + n = m + p$, então $n = p$.

Demonstração. Mostremos por indução. Fixemos dois números arbitrários $m, p \in \mathbb{N}$ e consideremos a propriedade

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

A fim de mostrar que $P(0)$ é verdadeiro, suponha que $0+m=0+p$. Como $0+m=m$ e $0+p=p$, concluimos que $m=p$, mostrando que $P(0)$ é verdadeiro. Suponha agora que $P(n)$ é verdadeiro e mostremos que $P(s(n))$ também o é, ou seja, provemos que

$$s(n)+m=s(n)+p \Rightarrow m=p.$$

De fato, se $s(n)+m=s(n)+p$, então $m+s(n)=p+s(n)$. Disso decorre, em virtude do axioma (2) da adição, que $s(m+n)=s(p+n)$. Como s é injetora, segue que $m+n=p+n$. Pela hipótese indutiva, concluímos que $m=p$, como queríamos. □

4.3 A operação de multiplicação em $\mathbb{N}$

De forma semelhante à operação de adição em $\mathbb{N}$, passaremos a definir o produto dos números naturais.

Definição 4.3.1. Uma *multiplicação* em $\mathbb{N}$ é uma função $\phi:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ que cumpre os seguintes axiomas:

(1) $\phi(n,0)=0$,

(2) $\phi(m,s(n))=M=\phi(m,n)$,

para quaisquer $m,n\in\mathbb{N}$.

O número natural $\phi(m,n)$ será chamado o *produto* dos naturais m e n. Assim como feito para a adição em $\mathbb{N}$, mostraremos que existe uma única multiplicação em $\mathbb{N}$. Também aqui faremos uso de um resultado de recursão para os números naturais que difere, ligeiramente, do Teorema 4.2.5.

Teorema 4.3.2 (Recursão em $\mathbb{N}$). *Dados uma função $F:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ e um número natural m, existe uma única função $f_m:\mathbb{N}\to\mathbb{N}$ satisfazendo*

(a) $f_m(0)=0$,

(b) $f_m(s(n))=F(m,f_m(n))$,

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

Teorema 4.3.3. *Existe uma única multiplicação em $\mathbb{N}$.*

Demonstração. Fixado um natural m, seja $f_m : \mathbb{N} \to \mathbb{N}$ a função dada pelo Teorema 4.3.2 satisfazendo

$$f_m(0) = 0 \quad \text{e} \quad f_m(s(n)) = S(m, f_m(n)) = m + f_m(n),$$

para todo $n \in \mathbb{N}$, onde $S : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ é a adição em $\mathbb{N}$. Definimos então uma função $\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ pondo

$$\phi(m, n) = f_m(n),$$

para quaisquer $m, n \in \mathbb{N}$. Claramente ϕ é uma multiplicação em $\mathbb{N}$, pois

$$\phi(m, 0) = f_m(0) = 0$$

e

$$\phi(m, s(n)) = f_m(s(n)) = m + f_m(n) = m + \phi(m, n).$$

Isso mostra a existência da multiplicação em $\mathbb{N}$. Em relação à unicidade, sejam $\phi, \psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ duas multiplicações em $\mathbb{N}$. Mostremos, por indução, que $\phi = \psi$. De fato, fixado um número $m \in \mathbb{N}$, consideremos a propriedade

$$P(n) : \phi(m, n) = \psi(m, n).$$

Pelo axioma (1) da multiplicação, temos

$$\phi(m, 0) = 0 = \psi(m, 0),$$

mostrando que $P(0)$ é verdadeiro. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também o é, ou seja, provemos que

$$\phi(m, s(n)) = \psi(m, s(n)).$$

De fato,

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

como queríamos. □

A fim de simplificar a notação, denotaremos o produto dos naturais m e n pondo $m \cdot n$ ao invés de $\phi(m, n)$. Veremos a seguir algumas propriedades da multiplicação em $\mathbb{N}$.

Proposição 4.3.4. Quaisquer que sejam os naturais $m, n \in \mathbb{N}$, valem as seguintes propriedades:

(a) $0 \cdot n = 0$,

(b) $1 \cdot n = n$,

(c) $s(m) \cdot n = n + (m \cdot n)$.

Demonstração. Provemos por indução. Para o item (a), consideremos a propriedade

$$P(n) : 0 \cdot n = 0.$$

$P(0)$ é verdadeiro em virtude do axioma (1) da multiplicação. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também o é. Temos

$$0 \cdot s(n) = 0 + (0 \cdot n) = 0 + 0 = 0.$$

Para o item (b), consideremos a propriedade

$$P(n) : 1 \cdot n = n.$$

$P(0)$ é verdadeiro, pois $1 \cdot 0 = 0$ em virtude do axioma (1). Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também o é. Temos

$$1 \cdot s(n) = 1 + (1 \cdot n) = 1 + n = s(n),$$

como queríamos. Finalmente, para o item (c), fixemos um natural arbitrário $m \in \mathbb{N}$ e consideremos a propriedade

$$P(n) : s(m) \cdot n = n + (m \cdot n).$$

Note que $s(m) \cdot 0 = 0$ e $0 + (m \cdot 0) = 0 + 0 = 0$, logo $s(m) \cdot 0 = 0 + (m \cdot 0)$, mostrando que $P(0)$ é verdadeiro. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também é verdadeiro. De fato,

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

e isso finaliza a demonstração. $\square$

Proposição 4.3.5. São válidas as seguintes propriedades operatórias:

(a) Comutativa: $m \cdot n = n \cdot m$,

(b) Distributiva: $m \cdot (n + p) = (m \cdot n) + (m \cdot p)$,

(c) Associativa: $(m \cdot n) \cdot p = m \cdot (n \cdot p)$.

Demonstração. Provemos por indução. Para o item (a), fixemos um natural arbitrário m e consideremos a propriedade

$$P(n) : m \cdot n = n \cdot m.$$

$P(0)$ é verdadeiro pois $m \cdot 0 = 0$ e $0 \cdot m = 0$ em virtude do axioma (1) e da Proposição 4.3.4, respectivamente. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também o é. Temos

$$m \cdot s(n) = m + (m \cdot n) = m + (n \cdot m) = s(n) \cdot m,$$

em virtude do item (c) da Proposição 4.3.4. Para o item (b), considere a propriedade

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

Note que

$$m \cdot (p + 0) = m \cdot p \quad \text{e} \quad (m \cdot p) + (m \cdot 0) = m \cdot p + 0 = m \cdot p,$$

mostrando que $m \cdot (p + 0) = (m \cdot p) + (m \cdot 0)$, ou seja, $P(0)$ é verdadeiro. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também o é, ou seja, provemos que

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

Temos

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

Finalmente, para o item (c), consideremos a propriedade

$$P(n) : (m \cdot n) \cdot p = m \cdot (n \cdot p).$$

Note que $(m \cdot p) \cdot 0 = 0$ e $m \cdot (p \cdot 0) = m \cdot 0 = 0$, mostrando que $(m \cdot p) \cdot 0 = m \cdot (p \cdot 0)$, ou seja, $P(0)$ é verdadeiro. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também o é. Temos

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

como queríamos. □

Proposição 4.3.6. Considere dois números naturais m e n tais que $m \cdot n = 0$. Então, $m = 0$ ou $n = 0$.

Demonstração. Suponhamos, por exemplo, que $n \neq 0$ e mostremos que $m = 0$. Como $n \neq 0$, existe $p \in \mathbb{N}$ tal que $n = s(p)$. Assim, pela hipótese, temos que $m \cdot s(p) = 0$. Por outro lado, como $m \cdot s(p) = m + (m \cdot p)$, segue que $m + (m \cdot p) = 0$. Disso decorre, em virtude do Exercício 4.2.2, que $m = 0$ e $m \cdot p = 0$. Em particular, tem-se $m = 0$, como queríamos. □

Proposição 4.3.7. Sejam $m, n \in \mathbb{N}$ tais que $m \cdot n = 1$. Então, $m = 1$ e $n = 1$.

Demonstração. Observe, inicialmente, que se $n = 0$, então

$$m \cdot n = m \cdot 0 = 0 \neq 1.$$

Assim, $n \neq 0$ e, da mesma forma, temos $m \neq 0$. Portanto, existe $a \in \mathbb{N}$ tal que $n = a + 1$. Substituindo, obtemos

$$m \cdot n = m \cdot (a + 1) = m \cdot a + m,$$

ou seja, $m \cdot a + m = 1$. Disso decorre que $m \leq 1$. Como $m \in \mathbb{N}$, tem-se $m = 0$ ou $m = 1$. Como $m \neq 0$, temos $m = 1$. Além disso, como $1 \cdot n = 1 = 1 \cdot 1$, tem-se $n = 1$ em virtude da lei do corte. □

4.4 A relação de ordem em $\mathbb{N}$

Dados $m, n \in \mathbb{N}$, dizemos que m é *menor do que* n, e escrevemos $m < n$, se existe $p \in \mathbb{N}$ tal que $n = m + p$. Nas mesmas condições, dizemos que n é *maior do que* m, e escrevemos $n > m$. A notação $m \leq n$ sigfinica que m é *menor do que ou igual* a n.

Proposição 4.4.1. A relação $\leq$ possui as seguintes propriedades:

(a) Reflexiva: $n \leq n$, para todo $n \in \mathbb{N}$.

(b) Simétrica: $m \leq n$ e $n \leq m \Rightarrow m = n$.

(c) Transitiva: $m \leq n$ e $n \leq p \Rightarrow m \leq p$.

(d) Monotonicidade da adição: se $m \leq n$, então $m + p \leq n + p$, para todo $p \in \mathbb{N}$.

Demonstração. (a) Seja $n \in \mathbb{N}$. Como $n + 0 = n$, tem-se $n \leq n$.

(b) Por hipótese, temos que existem $p, q \in \mathbb{N}$ tais que $n = m+p$ e $m = n+q$. Disso decorre que $m = (m+p)+q$, ou seja, $m+0 = m+(p+q)$. Isso implica que $p + q = 0$ e, pelo Exercício 4.2.2, concluímos que $m = n$.

(c) As relações $m \leq n$ e $n \leq p$ significam que existem $r, s \in \mathbb{N}$ tais que $n = m + r$ e $p = n + s$. Disso decorre que

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

ou seja, $m \leq p$.

(d) A relação $m \leq n$ significa que existe $q \in \mathbb{N}$ tal que $n = m + q$. Então, $n + p = (m + q) + p$, para todo $p \in \mathbb{N}$, ou seja, $n + p = (m + p) + q$, para todo $p \in \mathbb{N}$, mostrando que $m + p \leq n + p$. $\square$

Proposição 4.4.2 (Tricotomia)**.** Dados quaisquer $m, n \in \mathbb{N}$, vale somente uma das três seguintes alternativas: $m = n$, ou $m < n$ ou $n < m$.

Demonstração. Pela definição da relação $\leq$, basta provar que, para quaisquer $m, n \in \mathbb{N}$, tem-se $m \leq n$ ou $n \leq m$. Dado um número $p \in \mathbb{N}$, consideremos o conjunto

$$C_p = \{m \in \mathbb{N} : m \leq p \text{ ou } p \leq m\}.$$

A fim de provar o resultado basta, em virtude da arbitrariedade de p, mostrar que $C_p = \mathbb{N}$. Provaremos por indução. Para isso, consideremos a propriedade

$$P(n) : C_n = \mathbb{N}.$$

Qualquer que seja $m \in \mathbb{N}$, tem-se $0 \leq m$, pois $0 + m = m$. Assim, $C_0 = \mathbb{N}$, mostrando que $P(0)$ é verdadeiro. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(s(n))$ também o é, ou seja, provemos que $C_{n+1} = \mathbb{N}$. Como $C_{n+1} \subset \mathbb{N}$, resta mostrar que $\mathbb{N} \subset C_{n+1}$. Seja $m \in \mathbb{N}$. Pela hipótese indutiva, temos que $m \in C_n$. Suponhamos, inicialmente, que $m \leq n$. Como

$m \leq n$ e $n < n+1$, temos que $m \leq n+1$ e, portanto, $m \in C_{n+1}$ Por outro lado, suponha $n \leq m$. Temos duas situações aqui. Se $n < m$, então $n+1 \leq m$ e, assim, $m \in C_{n+1}$. Caso $n = m$, então $m \leq n+1$ e, portanto, $m \in C_{n+1}$. Em qualquer caso, provamos que $\mathbb{N} \subset C_{n+1}$, e isso finaliza a demonstração. □

Proposição 4.4.3 (Lei do corte)**.** Considere números $m, n, p \in \mathbb{N}$ tais que $m \cdot p = n \cdot p$. Se $p \neq 0$, então $m = n$.

Demonstração. Suponhamos, inicialmente, que $m \leq n$. Assim, existe $a \in \mathbb{N}$ tal que $n = m + a$. Da igualdade $m \cdot p = n \cdot p$, temos que $m \cdot p = (m + a) \cdot p$, ou seja, $m \cdot p = m \cdot p + a \cdot p$. Disso decorre que $a \cdot p = 0$. Como $p \neq 0$, concluímos que $a = 0$ e, portanto, $m = n$. O caso $n \leq m$ se prova de forma inteiramente análoga. □

Dado um subconjunto $X \subset \mathbb{N}$, dizemos que um natural $p \in X$ é o *menor elemento* de X se $p \leq n$, para todo $n \in X$. Por exemplo, 0 é o menor elemento do conjunto dos naturais $\mathbb{N}$. Além disso, qualquer que seja o subconjunto $X \subset \mathbb{N}$, com $0 \in X$, 0 é o menor elemento de X.

O menor elemento de um conjunto $X \subset \mathbb{N}$ é único. De fato, sejam $p, q \in X$ menores elementos de X. Assim, temos $p \leq q$ e $q \leq p$, logo $p = q$.

De forma análoga, se $X \subset \mathbb{N}$, dizemos que um natural $p \in \mathbb{N}$ é o *maior elemento* de X se $n \leq p$, para todo $n \in X$. Note que nem todo subconjunto de $\mathbb{N}$ possui maior elemento. O próprio conjunto $\mathbb{N}$ não tem maior elemento pois, qualquer que seja $n \in \mathbb{N}$, tem-se $n < n + 1$. Além disso, se $X \subset \mathbb{N}$ admite um maior elemento, então ele é único.

Teorema 4.4.4 (Princípio da boa ordenação)**.** *Todo subconjunto não-vazio $A \subset \mathbb{N}$ possui um menor elemento.*

Demonstração. Dado $n \in \mathbb{N}$, denotemos por

$$I_n = \{p \in \mathbb{N} : 0 \leq p \leq n\}.$$

Consideremos o subconjunto $X \subset \mathbb{N}$ formado pelos naturais n de modo que $I_n \subset \mathbb{N} - A$. Assim, se $n \in X$, então $n \notin A$ e todos os naturais menores do que n também não pertencem a A. Se tivermos $0 \in A$, o teorema estará provado pois 0 será o menor elemento de A. Se $0 \notin A$, então $0 \in X$. Por outro lado, como $X \subset \mathbb{N} - A$ e $A \neq \emptyset$, temos que $X \neq \mathbb{N}$. Assim, o conjunto X cumpre a primeira hipótese do axioma da indução, pois contém 0, mas não satisfaz a conclusão, pois não é igual a $\mathbb{N}$. Dessa forma, não pode cumprir a segunda parte da hipótese. Isso significa que existe algum $n \in X$ tal que

$n+1 \notin X$. Seja $a = n+1$. Então, todos os naturais de 0 até n pertencem ao complementar de A, mas $a = n+1$ pertence a A, mostrando que a é o menor elemento do conjunto A, como queríamos. $\square$

Corolário 4.4.5 (Segundo princípio da indução)**.** Seja $X \subset \mathbb{N}$ um conjunto com a seguinte propriedade: dado $n \in \mathbb{N}$, se X contém todos os números naturais m tais que $m < n$, então $n \in X$. Nestas condições, tem-se $X = \mathbb{N}$.

Demonstração. Seja $Y = \mathbb{N} - X$. Mostrar que $X = \mathbb{N}$ equivale a mostrar que $Y = \emptyset$. Se $Y \neq \emptyset$ então, pelo princípio da boa ordenação, Y possui um menor elemento p. Então, para todo natural $m < p$, tem-se $m \in X$. Pela hipótese feita sobre X, temos $p \in X$, o que é uma contradição. Portanto, devemos ter que $X = \mathbb{N}$. $\square$

Uma aplicação simples do segundo princípio da indução é provar que todo natural se decompõe como produto de números primos. Lembremos que um número natural p chama-se *primo* quando $p > 1$ e não existe uma decomposição de p da forma $p = m \cdot n$, com $m < p$ e $n < p$.

Proposição 4.4.6. Todo número natural maior do que 1 se decompõe como produto de fatores primos.

Demonstração. Dado um número natural $n > 1$, suponhamos que todo número natural menor do que n possa ser decomposto como produto de fatores primos. Caso n seja primo, n é, trivialmente, um produto de fatores primos. Caso contrário, n é da forma $n = m \cdot k$, com $m < n$ e $k < n$. Pela hipótese de indução, m e k são produtos de fatores primos, logo n também o é. Portanto, pelo segundo princípio da indução, concluímos que todo número natural é produto de fatores primos. $\square$

4.5 Exercícios

4.1

1. Usando o axioma da indução, prove que:

$$1 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

2. Usando o axioma da indução, prove que:

$$1 + 2^3 + 3^3 + \ldots + n^3 = \frac{1}{4}n^2(n+1)^2.$$

3. Usando o axioma da indução, prove que:

$$\left(\frac{n+1}{n}\right)^n \leq n,$$

para todo $n \geq 3$.

4.2

1. Considere um número $a \in \mathbb{N}$ tal que $n + a = n$, para todo $n \in \mathbb{N}$. Mostre que $a = 0$.

2. Se $m, n \in \mathbb{N}$ são tais que $m + n = 0$, mostre que $m = 0$ e $n = 0$.

4.4

1. Mostre que, qualquer que seja $n \in \mathbb{N}$, tem-se $n < n + 1$.

2. Sejam $m, n \in \mathbb{N}$ tais que $m < n$. Mostre que $m + 1 \leq n$.

3. Sejam $m, n \in \mathbb{N}$ tais que $m \leq n$. Mostre que $m \cdot p \leq n \cdot p$, para todo $p \in \mathbb{N}$.

4. Dado um número $n \in \mathbb{N}$, mostre que não existe $p \in \mathbb{N}$ tal que $n < p$ e $p < n + 1$.

Capítulo 5

Números inteiros

5.1 Relações de equivalência

Uma *relação* entre dois conjuntos X e Y, denotada por $\sim$, é simplesmente um subconjunto do produto cartesiano $X \times Y$. Se um par (x, y) pertence à relação $\sim$, dizemos que o elemento x *está relacionado* com o elemento y, e escrevemos $x \sim y$. Quando $X = Y$, diremos simplesmente que $\sim$ é uma relação no conjunto X.

Definição 5.1.1. Uma relação $\sim$ em um conjunto X é dita ser uma *relação de equivalência* se cumpre as seguintes propriedades:

(1) Reflexiva: $x \sim x$, para todo $x \in X$.

(2) Simétrica: $x \sim y \Rightarrow y \sim x$.

(3) Transitiva: $x \sim y$ e $y \sim z \Rightarrow x \sim z$.

Exemplo 5.1.2. A *igualdade* é, trivialmente, uma relação de equivalência em qualquer conjunto X. De fato, para todo $x \in X$, tem-se $x = x$. Temos também que se $x = y$ então $y = x$. Além disso, se $x = y$ e $y = z$, então $x = z$.

Exemplo 5.1.3. Dado uma função $f : X \to Y$, consideremos a relação $\sim$ em X dada por

$$x \sim y \Leftrightarrow f(x) = f(y).$$

Afirmamos que $\sim$ é uma relação de equivalência. De fato, para todo $x \in X$, tem-se $x \sim x$, pois $f(x) = f(x)$. Se $x \sim y$, então $f(x) = f(y)$, logo temos que $y \sim x$, pois $f(y) = f(x)$. Finalmente, se $x \sim y$ e $y \sim z$, então $f(x) = f(y)$ e $f(y) = f(z)$, logo $f(x) = f(z)$, ou seja, $x \sim z$.

Considere um conjunto X munido de uma relação de equivalência $\sim$. Dado um elemento $x \in X$, denotemos por $\overline{x}$ o conjunto

$$\overline{x} = \{y \in X : y \sim x\}.$$

O conjunto $\overline{x}$ é chamado a *classe de equivalência* do elemento x. Denotaremos por $X/\!\sim$ o conjunto constituído de todas as classes de equivalência segundo a relação $\sim$, ou seja,

$$X/\!\sim = \{\overline{x} : x \in X\}.$$

Lema 5.1.4. Seja X um conjunto munido de uma relação de equivalência $\sim$, e consideremos dois elementos $x, y \in X$. Se existe $z \in \overline{x} \cap \overline{y}$, então $\overline{x} = \overline{y}$.

Demonstração. Dado um elemento $a \in \overline{x}$, tem-se $a \sim x$. Por outro lado, como $z \in \overline{x}$, tem-se $z \sim x$, logo $a \sim z$. Além disso, como $z \in \overline{y}$, tem-se $z \sim y$. Assim, pela transitividade, concluímos que $a \sim y$. Isso mostra que $a \in \overline{y}$ e, portanto, $\overline{x} \subset \overline{y}$. De forma análoga se mostra que $\overline{y} \subset \overline{x}$. □

Dado uma função $f : X \to Y$, considere a relação de equivalência $\sim$ dada como no Exemplo 5.1.3. Definimos uma função $\overline{f} : X/\!\sim \to Y$ pondo

$$\overline{f}(\overline{x}) = f(x). \tag{5.1}$$

Proposição 5.1.5. A função $\overline{f}$, dada em (5.1), está bem definida e é injetora.

Demonstração. Mostremos, inicialmente, que $\overline{f}$ está bem definida, ou seja, independe da escolha do representante da classe de equivalência. Dado um elemento $a \in \overline{x}$, tem-se $a \sim x$, logo $f(a) = f(x)$. Portanto, qualquer que seja o representante da classe $\overline{x}$, tem-se $\overline{f}(\overline{x}) = f(x) = f(a)$. Finalmente, sejam $\overline{x}, \overline{y} \in X/\!\sim$ tais que $\overline{f}(\overline{x}) = \overline{f}(\overline{y})$. Isso significa que $f(x) = f(y)$, ou seja, $x \sim y$. Disso decorre que $x \in \overline{y}$ e, pelo Lema 5.1.4, tem-se $\overline{x} = \overline{y}$. □

5.2 O conjunto dos números inteiros

Iniciaremos esta seção considerando uma relação $\sim$ no conjunto $\mathbb{N} \times \mathbb{N}$ dada por

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c, \tag{5.2}$$

com $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$.

Proposição 5.2.1. A relação dada em (5.2) é uma relação de equivalência no conjunto $\mathbb{N} \times \mathbb{N}$.

Demonstração. Dado um elemento $(a,b) \in \mathbb{N} \times \mathbb{N}$, temos que $a+b=b+a$, logo $(a,b) \sim (a,b)$. Sejam agora $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$ tais que $(a,b) \sim (c,d)$, ou seja, $a+d=b+c$. Isso é a mesma coisa que $c+b=d+a$. i.e., $(c,d) \sim (a,b)$. Finalmente, sejam $(a,b),(c,d),(e,f) \in \mathbb{N} \times \mathbb{N}$ tais que $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$, ou seja, $a+d=b+c$ e $c+f=d+e$. Assim,

$$a+d+f=b+c+f \quad \text{e} \quad c+f+b=d+e+b.$$

Dessa forma, obtemos que $a+d+f=d+e+b$, logo $a+f=b+e$, ou seja, $(a,b) \sim (e,f)$, e isso finaliza a demonstração. $\square$

Definição 5.2.2. O conjunto quociente $\mathbb{N} \times \mathbb{N}/\sim$, onde $\sim$ é a relação de equivalência dada em (5.2), será denotado por $\mathbb{Z}$ e chamado de *conjunto dos números inteiros*. Cada elemento de $\mathbb{Z}$ será chamado de *número inteiro*.

Definiremos a operação de *adição* em $\mathbb{Z}$ da seguinte forma. Dados dois elementos $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$, definimos a *soma* $\overline{(a,b)} + \overline{(c,d)}$ pondo

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c,b+d)}. \tag{5.3}$$

Devemos provar que a operação em (5.3) está bem definida no sentido de que independe da escolha dos representantes. Ou seja, devemos mostrar que se $(a,b) \sim (x,y)$ e $(c,d) \sim (z,w)$, então

$$(a+c,b+d) \sim (x+z,y+w).$$

De fato, temos que $a+y=b+x$ e $c+w=d+z$. Assim,

$$\begin{aligned} (a+c)+(y+w) &= (a+y)+(c+w) \\ &= (b+x)+(d+z) \\ &= (b+d)+(x+z), \end{aligned}$$

como queríamos.

Proposição 5.2.3. A operação da adição em $\mathbb{Z}$ satisfaz as seguintes propriedades:

(a) Comutativa: $\overline{(a,b)} + \overline{(c,d)} = \overline{(c,d)} + \overline{(a,b)}$,

(b) Associativa: $\left(\overline{(a,b)} + \overline{(c,d)}\right) + \overline{(e,f)} = \overline{(a,b)} + \left(\overline{(c,d)} + \overline{(e,f)}\right)$,

(c) Elemento neutro: $\overline{(a,b)} + \overline{(0,0)} = \overline{(a,b)}$, para todo $\overline{(a,b)} \in \mathbb{Z}$,

(d) Lei do corte: se $\overline{(a,b)} + \overline{(x,y)} = \overline{(c,d)} + \overline{(x,y)}$, então $\overline{(a,b)} = \overline{(c,d)}$.

Demonstração. (a) Dados $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$, temos:

$$\begin{aligned}
\overline{(a,b)} + \overline{(c,d)} &= \overline{(a+c, b+d)} \\
&= \overline{(c+a, d+b)} \\
&= \overline{(c,d)} + \overline{(a,b)},
\end{aligned}$$

mostrando a comutatividade da adição.

(b) Dados $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{Z}$, temos:

$$\begin{aligned}
\big(\overline{(a,b)} + \overline{(c,d)}\big) + \overline{(e,f)} &= \overline{(a+c, b+d)} + \overline{(e,f)} \\
&= \overline{((a+c)+e, (b+d)+f)} \\
&= \overline{(a+(c+e), b+(d+f))} \\
&= \overline{(a,b)} + \overline{(c+e, d+f)} \\
&= \overline{(a,b)} + \big(\overline{(c,d)} + \overline{(e,f)}\big).
\end{aligned}$$

(c) Dado um elemento $\overline{(a,b)} \in \mathbb{Z}$, temos

$$\overline{(a,b)} + \overline{(0,0)} = \overline{(a+0, b+0)} = \overline{(a,b)}.$$

(c) Por hipótese, temos que $\overline{(a+x, b+y)} = \overline{(c+x, d+y)}$. Isso significa que

$$a + x + d + y = b + y + c + x,$$

ou seja, $(a+d) + (x+y) = (b+c) + (x+y)$. Pela lei do corte em $\mathbb{N}$, temos $a + d = b + c$, i.e., $(a,b) \sim (c,d)$. Logo, temos que $\overline{(a,b)} = \overline{(c,d)}$. $\square$

Definiremos agora a operação de *multiplicação* em $\mathbb{Z}$. Dados dois elementos $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$, definimos o *produto* $\overline{(a,b)} \cdot \overline{(c,d)}$ pondo

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}. \tag{5.4}$$

Da mesma forma como na adição, devemos provar que a operação em (5.4) está bem definida. Ou seja, devemos mostrar que se $(a,b) \sim (x,y)$ e $(c,d) \sim (z,w)$, então

$$(ac+bd, ad+bc) \sim (xz+yw, xw+yz).$$

Proposição 5.2.4. A operação da multiplicação em $\mathbb{Z}$ satisfaz as seguintes propriedades:

(a) Comutativa: $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(c,d)} \cdot \overline{(a,b)}$,

(b) Associativa: $\big(\overline{(a,b)} \cdot \overline{(c,d)}\big) \cdot \overline{(e,f)} = \overline{(a,b)} \cdot \big(\overline{(c,d)} \cdot \overline{(e,f)}\big)$,

(c) Elemento neutro: $\overline{(1,0)} \cdot \overline{(a,b)} = \overline{(a,b)}$, para todo $\overline{(a,b)} \in \mathbb{Z}$,

(d) Distributiva: $\overline{(x,y)}\big(\overline{(a,b)} + \overline{(c,d)}\big) = \overline{(x,y)} \cdot \overline{(a,b)} + \overline{(x,y)} \cdot \overline{(c,d)}$.

5.3 Relação de ordem em $\mathbb{Z}$

Veremos nesta seção que todo número inteiro pode ser representado em uma forma mais simples, o que nos auxiliará em várias situações.

Proposição 5.3.1. Dado um elemento $\overline{(a,b)} \in \mathbb{Z}$, existe um único $n \in \mathbb{N}$ tal que $\overline{(a,b)} = \overline{(n,0)}$ ou $\overline{(a,b)} = \overline{(0,n)}$.

Demonstração. Se $a = b$, basta considerar $n = 0$ e $\overline{(a,b)} = \overline{(0,0}$. Se $a < b$, então existe $n \in \mathbb{N}$ tal que $b = a+n$. Assim, neste caso, tem-se $(a,b) \sim (0,n)$, logo $\overline{(a,b)} = \overline{(0,n)}$. Caso $b < a$, então existe $n \in \mathbb{N}$ tal que $a = b+n$. Assim, $(a,b) \sim (n,0)$, logo $\overline{(a,b)} = \overline{(n,0)}$. Quanto à unicidade, suponha que existam $m,n \in \mathbb{N}$ tais que $\overline{(a,b)} = \overline{(m,0)}$ e e$\overline{(a,b)} = \overline{(n,0)}$. Disso decorre, em particular, que $(m,0) \sim (n,0)$, logo $m = n$. Analogamente para o outro caso. □

Em virtude da Proposição 5.3.1, diremos que um elemento de $\mathbb{Z}$ está escrito na *forma canônica* se ele está na forma $\overline{(n,0)}$ ou $\overline{(0,n)}$, para algum $n \in \mathbb{N}$.

Proposição 5.3.2. Sejam $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$ tais que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(0,0)}$. Então, $\overline{(a,b)} = \overline{(0,0)}$ ou $\overline{(c,d)} = \overline{(0,0)}$.

Demonstração. Sejam $m,n \in \mathbb{N}$ tais que $\overline{(a,b)} = \overline{(m,0)}$ ou $\overline{(a,b)} = \overline{(0,m)}$, e $\overline{(c,d)} = \overline{(n,0)}$ ou $\overline{(c,d)} = \overline{(0,n)}$. Suponhamos, inicialmente, que $\overline{(a,b)} = \overline{(m,0)}$ e $\overline{(c,d)} = \overline{(n,0)}$. Em virtude de (5.4), temos que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(m \cdot n,0)}$. Da igualdade $\overline{(m \cdot n,0)} = \overline{(0,0)}$ concluímos, em virtude da unicidade da forma canônica, que $m \cdot n = 0$. Isso implica que $m = 0$ ou $n = 0$ e, portanto, $\overline{(a,b)} = \overline{(0,0)}$ ou $\overline{(c,d)} = \overline{(0,0)}$. Os demais casos são inteiramente análogos. □

Dados dois números $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$, consideremos $m,n \in \mathbb{N}$ tais que

$$\begin{aligned} \overline{(a,b)} = \overline{(m,0)} \quad &\text{ou} \quad \overline{(a,b)} = \overline{(0,m)}, \\ \overline{(c,d)} = \overline{(n,0)} \quad &\text{ou} \quad \overline{(c,d)} = \overline{(0,n)}. \end{aligned} \tag{5.5}$$

Definição 5.3.3. Dizemos que $\overline{(a,b)}$ é *menor do que ou igual a* $\overline{(c,d)}$ se um dos seguintes casos ocorrer:

(i) $\overline{(a,b)} = \overline{(m,0)}$, $\overline{(c,d)} = \overline{(n,0)}$ e $m \leq n$,

(ii) $\overline{(a,b)} = \overline{(0,m)}$, $\overline{(c,d)} = \overline{(n,0)}$,

(iii) $\overline{(a,b)} = \overline{(m,0)}$, $\overline{(c,d)} = \overline{(0,n)}$ e $n \leq m$.

Proposição 5.3.4. A relação $\leq$, dada pela Definição 5.3.3, satisfaz a propriedade da tricotomia. Ou seja, para quaisquer $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$, tem-se $\overline{(a,b)} \leq \overline{(c,d)}$ ou $\overline{(c,d)} \leq \overline{(a,b)}$.

Demonstração. Sejam $m, n \in \mathbb{N}$ como em (5.5) e consideremos a situação em que $\overline{(a,b)} = \overline{(m,0)}$ e $\overline{(c,d)} = \overline{(n,0)}$. Se $m \leq n$, então $\overline{(a,b)} \leq \overline{(c,d)}$. Caso contrário, temos $n \leq m$ e, assim, $\overline{(c,d)} \leq \overline{(a,b)}$. Os demais casos seguem de forma inteiramente análoga. $\square$

A partir de agora um número inteiro da forma $\overline{(m,0)}$ será denotado simplesmente por m e será chamado de *positivo*. Um inteiro da forma $\overline{(0,n)}$ será denotado por $-n$ e será chamado de *negativo*. Dessa forma, a notação $m + (-n)$ corresponde à soma $\overline{(m,0)} + \overline{(0,n)}$. Além disso, dado um número $\overline{(a,b)} \in \mathbb{Z}$, denotaremos por $-\overline{(a,b)}$ o número inteiro $\overline{(b,a)}$.

Proposição 5.3.5. Com as convenções adotadas acima, temos as seguintes propriedades:

(a) O produto de dois números positivos é um número positivo.

(b) O produto de dois números negativos é um número positivo.

(c) O produto de um número positivo com um número negativo é um número negativo.

(d) Quaisquer que sejam $m, n \in \mathbb{Z}$, temos que $-(-m) = m$ e $m \cdot (-n) = -m \cdot n$.

(d) Qualquer que seja $n \in \mathbb{N}$, temos que n é positivo se, e somente se, $-n$ é negativo.

Demonstração. Os itens (a), (b) e (c) seguem diretamente da definição, pois

$$\overline{(m,0)} \cdot \overline{(n,0)} = \overline{(m \cdot n, 0)},$$

$$\overline{(0,m)} \cdot \overline{(0,n)} = \overline{(0, m \cdot n)}$$

e

$$\overline{(m,0)} \cdot \overline{(0,n)} = \overline{(0, m \cdot n)}.$$

Para o item (d), sejam $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$ tais que $\overline{(a,b)} = m$ e $\overline{(c,d)} = n$. Então,

$$-(-m) = -(-\overline{(a,b)}) = -\overline{(b,a)} = \overline{(a,b)}$$

e

$$\begin{aligned} m\cdot(-n) &= \overline{(a,b)}\cdot(-\overline{(c,d)}) = \overline{(a,b)}\cdot\overline{(c,d)} \\ &= \overline{(ad+bc, ac+bd)} = -\overline{(ac+bd, ad+bc)} \\ &= -\overline{(a,b)}\cdot\overline{(c,d)} \\ &= -m\cdot n. \end{aligned}$$

Finalmente, para o item (e), suponha n positivo. Assim, existe $a\in\mathbb{N}$ tal que $n=\overline{(a,0)}$. Isso implica que

$$-n = -\overline{(a,0)} = \overline{(0,a)},$$

mostrando que $-n$ é negativo. A recíproca segue de forma inteiramente análoga. $\square$

5.4 Divisibilidade em $\mathbb{Z}$

O conjunto dos números inteiros $\mathbb{Z}$, apresentado nas seções anteriores, foi definido de forma que o conjunto dos números naturais seja, naturalmente, um subconjunto de $\mathbb{Z}$. Assim, a partir de agora, identificaremos o conjunto $\mathbb{N}$ com o subconjunto dos números inteiros positivos.

Definição 5.4.1. Dados dois inteiros $m,n\in\mathbb{Z}$, dizemos que m *divide* n se existe $a\in\mathbb{Z}$ tal que $n=m\cdot z$. Neste caso, denotaremos por $m|n$.

Decorre diretamente da definição que, qualquer que seja o inteiro n, tem-se $1|n$, $n|0$ e $n|n$. Além disso, vale a transitividade, ou seja, $m,n,p\in\mathbb{Z}$ são tais que $m|n$ e $n|p$, então $m|p$.

O resultado seguinte é a versão da Proposição 4.3.7 para o conjunto dos inteiros $\mathbb{Z}$.

Proposição 5.4.2. Sejam $m,n\in\mathbb{Z}$ tais que $m\cdot n=1$. Então $m=n=1$ ou $m=n=-1$.

Demonstração. Note, inicialmente, que $m\neq 0$ e $n\neq 0$ pois, do contrário, teríamos $m\cdot n=0$. Se $m>0$ $n>0$, o resultado segue diretamente da Proposição 4.3.7. Suponha agora que $m<0$ e $n<0$. Como

$$1 = m\cdot n = (-m)\cdot(-n)$$

e, $-m$ e $-n$ são positivos, tem-se que $-m=1$ e $-n=1$, logo $m=-1$ e $n=-1$. Finalmente, observe que, caso $m>0$ e $n<0$, então $m\cdot n<0$, em virtude da Proposição 5.3.5, logo esse caso não pode ocorrer. $\square$

Corolário 5.4.3. Sejam $m, n \in \mathbb{Z}$ tais que $m|n$ e $n|m$. Então, $m = n$ ou $m = -n$.

Demonstração. Podemos supor que $n \neq 0$ pois, do contrário, como $n|m$, teríamos $m = 0$ e vale o resultado. Por hipótese, existem $a, b \in \mathbb{Z}$ tais que $n = ma$ e $m = nb$. Assim,

$$n = ma = (nb)a = n(ba).$$

Pela lei do corte em $\mathbb{Z}$, segue que $ab = 1$, pois $n \neq 0$. Portanto, pela Proposição 5.4.2, segue que $a = b = 1$ ou $a = b = -1$, mostrando que $m = n$ ou $m = -n$, respectivamente. $\square$

Teorema 5.4.4 (Teorema da divisão de Euclides)**.** *Dados $a, b \in \mathbb{N}$, com $b > 0$, existem inteiros $q, r \in \mathbb{Z}$ tais que $a = bq + r$, com $0 \leq r < b$.*

Demonstração. Consideremos o conjunto

$$A = \{a - bn : n \in \mathbb{Z} \text{ e } a - bn \geq 0\}.$$

Note que, fazendo $n = 0$, temos $a - bn = a \geq 0$, logo $A \neq \emptyset$. Assim, em virtude do Teorema 4.4.4, o conjunto A admite um menor elemento r. Assim, para algum $q \in \mathbb{Z}$, tem-se que $r = a - bq$, ou seja, $a = bq + r$. Observe que, como $r \in A$, tem-se $r \geq 0$. Resta mostrar que $r < b$. Se isso não ocorre, então

$$0 \leq r - b = (a - bq) - b = a - b(q + 1).$$

Isso implica que $a - b(q + 1) \in A$. Além disso,

$$a - b(q + 1) = a - bq - b < a - bq = r,$$

uma vez que $b > 0$, e isso contradiz a minimalidade de r. Portanto, devemos ter $r < b$, e isso finaliza a demonstração. $\square$

Definição 5.4.5. Considere dois inteiros distintos $m, n \in \mathbb{Z}$. Dizemos que $d \in \mathbb{Z}$ é um *máximo divisor comum* de m e n se:

(1) $d \geq 0$,

(2) $d|m$ e $d|n$,

(3) Se $d' \in \mathbb{Z}$ satisfaz (1) e (2), então $d'|d$.

Observe que, se $d, d' \in \mathbb{Z}$ são máximos divisores comuns de m e n, segue do axioma (3) que $c|d'$ e $d'|d$, logo $d = d'$ pois ambos são positivos.

Proposição 5.4.6. O máximo divisor comum de dois inteiros distintos m e n é o elemento mínimo do conjunto

$$A = \{am + bn : a, b \in \mathbb{Z} \text{ e } am + bn > 0\}.$$

Demonstração. Observe, inicialmente, que $A \neq \emptyset$. Assim, o conjunto A admite um elemento mínimo $d > 0$. Sejam $a, b \in \mathbb{Z}$ tais que $d = am + bn$. Afirmamos que $d|m$. De fato, caso d não divida m, segue do algoritmo da divisão de Euclides que existem $q, r \in \mathbb{Z}$ tais que $m = dq + r$, com $0 < r < d$. Assim,

$$r = m - dq = m - (am + bn)q = (1 - aq)m + (-bq)n,$$

mostrando que $r \in A$. No entanto, isso contradiz a minimalidade de d. Portanto, deve-se ter que $d|m$. De forma análoga se prova que $d|n$. Portanto, a fim de verificar os axiomas da Definição 5.4.5, basta mostrar que, dado $d' \geq 0$ tal que $d'|m$ e $d'|n$, tem-se que $d'|d$. Temos que existem $p, q \in \mathbb{Z}$ tal que $m = d'p$ e $n = d'q$. Assim,

$$d = am + bn = ad'p + bd'q = d'(ap + bq),$$

mostrando que $d'|d$, como queríamos. □

Provaremos a seguir que o máximo divisor comum entre dois números inteiros é, de fato, o maior dos divisores.

Proposição 5.4.7. Sejam $m, n \in \mathbb{N}$, com $n > 0$. Se $m|n$, então $m \leq n$.

Demonstração. Por hipótese, existe $a \in \mathbb{N}$ tal que $n = m \cdot a$. Note que $a > 0$ pois, do contrário, teríamos $n = 0$. Assim, existe $b \in \mathbb{N}$ tal que $a = b + 1$. Assim,

$$n = m \cdot a = m \cdot (b + 1) = m \cdot b + m,$$

mostrando que $m \leq n$. □

Teorema 5.4.8. *Um número interiro $d \in \mathbb{Z}$ é o máximo divisor comum de dois inteiros distintos m e n se, e somente, se $d|m$, $d|n$ e se $d' \in \mathbb{Z}$ é outro inteiro tal que $d'|m$ e $d'|n$, então $d' \leq d$.*

Demonstração. Se d é o máximo divisor comum entre m e n então, pelo axioma (2) da Definição 5.4.5, temos que $d|m$ e $d|n$. Considere agora outro inteiro d' que também satisfaz $d'|m$ e $d'|n$. Se $d' < 0$, então $d' < d$, pois $d \geq 0$, em virtude do axioma (1). Caso $d' \geq 0$ então, pelo axioma (3), temos que $d'|d$ e, pela Proposição 5.4.7, concluímos que $d' \leq d$. Reciprocamente, considere um inteiro d como no enunciado. Observe, inicialmente, que $d \geq 0$ pois, do contrário, o inteiro $-d$ dividiria m e n, com $d < -d$, contradizendo as hipóteses sobre d. Assim, d satisfaz os axiomas (1) e (2) da Definição 5.4.5. Se D é o máximo divisor comum entre m e n, então $d|D$ e, pela Proposição 5.4.7, temos $d \leq D$. Por outro lado, pela hipótese sobre d, temos $D \leq d$, mostrando que $d = D$. □

A partir de agora denotaremos o máximo divisor comum entre dois inteiros distintos m e n por $\mathrm{mdc}(m, n)$. Veremos a seguir algumas consequências envolvendo números primos. Decorre da definição de número primo e da Definição 5.4.1 que um número natural $p > 1$ é primo se, e somente se, $a \in \mathbb{N}$ é tal que se $a|p$, então $a = 1$ ou $a = p$.

Corolário 5.4.9. Seja p um número primo. Se $n \in \mathbb{Z}$ é tal que p não divide n, então $\mathrm{mdc}(p, n) = 1$.

Demonstração. Seja $d = \mathrm{mdc}(p, n)$. Como $d|p$ e p é primo, tem-se $d = 1$ ou $d = p$. Porém, como p não divide n, devemos ter $d = 1$, como queríamos. □

Corolário 5.4.10. Se p é um número primo e $m, n \in \mathbb{Z}$ são tais que $p|(m \cdot n)$, então $p|m$ ou $p|n$.

Demonstração. Suponha, por exemplo, que p não divide m. Assim, pelo Corolário 5.4.9, temos que $\mathrm{mdc}(p, m) = 1$. Por outro lado, pela Proposição 5.4.6, existem $a, b \in \mathbb{Z}$ tais que $am + bp = 1$. Disso decorre que

$$n = amn + bpn. \tag{5.6}$$

Como $p|(m \cdot n)$, existe $k \in \mathbb{Z}$ tal que $mn = pk$. Substituindo em (5.6), obtemos

$$n = apk + bpn = p(ak + bn),$$

mostrando que $p|n$, como queríamos. □

O Corolário 5.4.10 pode ser visto de modo mais geral, como mostra o Exercício 5.4.1. Finalizaremos esta seção provando o teorema fundamental da Aritmética.

Teorema 5.4.11 (Fundamental da Aritmética)**.** *Todo número natural n maior do que 1 se, decompõe, de modo único, como produto de fatores primos.*

Demonstração. Em virtude da Proposição 4.4.6, resta provar a unicidade da decomposição. Sejam $p_1, \ldots, p_m, q_1, \ldots, q_k$ números primos tais que

$$n = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_k,$$

com $p_1 \leq \ldots \leq p_m$ e $q_1 \leq \ldots \leq q_k$. Observe que $p_1|(q_1 \cdot \ldots \cdot q_k)$ logo, pelo Exercício 5.4.1, existe $1 \leq j \leq k$ tal que $p_1|q_j$. Como q_j é primo, tem-se $p_1 = q_j$. Assim, aplicando a lei do corte, obtemos

$$p_2 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_k.$$

De forma análoga, podemos proceder até que sobre apenas um termo de cada lado, mostrando que $m = k$. $\square$

5.5 Congruência em $\mathbb{Z}$

Nesta seção definiremos uma relação de equivalência no conjunto $\mathbb{Z}$ da seguinte forma. Fixemos um natural $n \in \mathbb{N}$, com $n > 0$. Dados $a, b \in \mathbb{Z}$, definimos

$$a \sim b \Leftrightarrow n|(a - b). \tag{5.7}$$

Essa relação recebe o nome de *congruência módulo* n e é denotada usualmente por $\equiv (\operatorname{mod} n)$. Assim, dados $a, b \in \mathbb{Z}$, temos

$$a \equiv b(\operatorname{mod} n) \Leftrightarrow n|(a - b) \Leftrightarrow a - b = n \cdot k,$$

para algum $k \in \mathbb{Z}$. A relação (5.7) significa que $a - b$ é múltiplo inteiro de n, ou seja, $a - b$ é divisível por n.

Proposição 5.5.1. A relação (5.7) é uma relação de equivalência em $\mathbb{Z}$.

Demonstração. Qualquer que seja $a \in \mathbb{Z}$, temos $a \equiv a(\operatorname{mod} n)$, pois $a - a = 0 = n \cdot 0$, i.e., $n|(a - a)$. Sejam agora $a, b \in \mathbb{Z}$, com $a \equiv b(\operatorname{mod} n)$. Assim, existe $k \in \mathbb{Z}$ tal que $a - b = n \cdot k$. Isso implica que $b - a = n \cdot (-k)$, ou seja, $b \equiv a(\operatorname{mod} n)$. Finalmente, sejam $a, b, c \in \mathbb{Z}$ tais que $a \equiv b(\operatorname{mod} n)$ e $b \equiv c(\operatorname{mod} n)$. Assim, existem $k, l \in \mathbb{Z}$ tais que

$$a - b = n \cdot k \quad \text{e} \quad b - c = n \cdot l.$$

Disso decorre que

$$a - c = (a - b) + (b - c) = n \cdot (k + l),$$

ou seja, $a \equiv c(\operatorname{mod} n)$. $\square$

Existem várias propriedades satisfeitas pela congruência módulo n, algumas das quais contidas nos exercícios.

Proposição 5.5.2. A congruência módulo n cumpre as seguintes propriedades:

(i) $a \equiv b (\operatorname{mod} n) \Rightarrow a + c \equiv b + c (\operatorname{mod} n)$ e $a \cdot c \equiv b \cdot c (\operatorname{mod} n)$,

(ii) $a \equiv b (\operatorname{mod} n)$ e $c \equiv d (\operatorname{mod} n) \Rightarrow a + c \equiv b + d (\operatorname{mod} n)$ e $ac \equiv bd (\operatorname{mod} n)$,

(iii) $a \equiv b (\operatorname{mod} n) \Rightarrow a^k \equiv b^k (\operatorname{mod} n)$, para todo $k \in \mathbb{N}$.

Demonstração. Os itens (i) e (ii) decorrem diretamente da definição e são deixados a cargo do leitor. O item (iii) pode ser provado por indução. De fato, considere a propriedade

$$P(k) : a^k \equiv b^k (\operatorname{mod} n).$$

$P(0)$ é verdadeiro, pois $1 \equiv 1 (\operatorname{mod} n)$. Suponha agora que $P(k)$ seja verdadeiro e mostremos que $P(k+1)$ também o é. Por hipótese, temos que $a^k \equiv b^k (\operatorname{mod} n)$. Como $a \equiv b (\operatorname{mod} n)$, segue do item (ii) que $a^k \cdot a \equiv b^k \cdot b (\operatorname{mod} n)$, ou seja, $a^{k+1} \equiv b^{k+1} (\operatorname{mod} n)$, como queríamos. $\square$

Dados $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, com $n > 0$, considere inteiros $p, q, r, s \in \mathbb{Z}$ dados pelo algorítmo da divisão de Euclides

$$a = np + r \quad \text{e} \quad b = nq + s. \tag{5.8}$$

Proposição 5.5.3. $a \equiv b \mod \Leftrightarrow r = s$.

Demonstração. Se $a \equiv b (\operatorname{mod} n)$, então existe $k \in \mathbb{Z}$ tal que $a - b = n \cdot k$. Suponha, por absurdo, que $s < r$. Assim,

$$\begin{aligned} r - s &= (a - np) - (b - nq) \\ &= (a - b) + n(q - p) \\ &= nk + n(q - p) \\ &= n(k + q - p). \end{aligned}$$

Disso decorre que $n|(r - s)$. Como $r - s > 0$, decorre da Proposição 5.4.7 que $n \leq r - s$. Por outro lado, como $0 \leq r < n$ e $0 \leq s < n$, temos que $0 \leq r - s < n$, o que é uma contradição. Portanto, devemos ter $r = s$. O caso $r < s$ se prova de forma análoga. Reciprocamente, se $r = s$, decorre de (5.8) que $a - b = n(p - q)$, ou seja, $a \equiv b (\operatorname{mod} n)$. $\square$

Uma aplicação simples da congruência módulo n é verificar se um determinado número é divisível por outro.

Exemplo 5.5.4. Verifiquemos se o número $30^{99} + 61^{100}$ é divisível por 31. Para isso, observe que $30 \equiv -1 (\bmod 31)$, pois $30 - (-1) = 31$. Assim, pelo item (iii) da Proposição 5.5.2, temos

$$30^{99} \equiv (-1)^{99} (\bmod 31) \equiv -1 (\bmod 31).$$

Da mesma forma, temos $61 \equiv -1 (\bmod 31)$, logo

$$61^{100} \equiv (-1)^{100} (\bmod 31) \equiv 1 (\bmod 31).$$

Portanto, do item (i) da Proposição 5.5.2, temos

$$30^{99} + 61^{100} \equiv (-1 + 1) (\bmod 31),$$

ou seja, $30^{99} + 61^{100} \equiv 0 (\bmod 31)$. Isso significa que $30^{99} + 61^{100}$ é divisível por 31.

Exemplo 5.5.5. Calculemos o resto da divisão de $(116+17^{17})^{21}$ por 8. Para isso, observe que

$$116 \equiv 4 (\bmod 8) \quad \text{e} \quad 17 \equiv 1 (\bmod 8).$$

Assim, $17^{17} \equiv 1 (\bmod 8)$, logo $(116 + 17^{17}) \equiv 5 (\bmod 8)$. Além disso,

$$(116 + 17^{17})^2 \equiv 25 (\bmod 8) \quad \text{e} \quad 25 \equiv 1 (\bmod 8).$$

Assim, $(116 + 17^{17})^2 \equiv 1 (\bmod 8)$ e, portanto,

$$\begin{aligned} (116 + 17^{17})^{21} &\equiv (116 + 17^{17})^{20} \cdot (116 + 17^{17}) (\bmod 8) \\ &\equiv 1 \cdot 5 (\bmod 8) \\ &\equiv 5 (\bmod 8). \end{aligned}$$

Disso decorre que o resto da divisão é igual a 5.

5.6 Exercícios

5.1

1. Considere duas funções $f : X \to Y$ e $g : Y \to Z$ tais que f é sobrejetora e g injetora. No conjunto X, considere a relação $\sim$ dada por

$$x \sim y \Leftrightarrow g(f(x)) = g(f(y)).$$

Mostre que $\sim$ é uma relação de equivalência e que existe uma bijeção entre os conjuntos $X/\!\sim$ e Y.

5.2

1. Mostre que se $\overline{(a,b)} = \overline{(c,b)}$ então $a = c$.

2. Prove a unicidade dos elementos neutros da soma e produto em $\mathbb{Z}$.

3. Seja $\overline{(a,b)} \in \mathbb{Z}$. Mostre que $\overline{(a,b)} = \overline{(0,0)}$ se, e somente se, $a = b$.

5.3

1. Prove que:

(i) $(-1) \cdot (-1) = 1$,

(ii) $-n = (-1) \cdot n$, para todo $n \in \mathbb{Z}$,

(ii) $m \cdot n = (-m) \cdot (-n)$, para quaisquer $m, n \in \mathbb{Z}$.

2. Prove a lei do corte relativa ao produto em $\mathbb{Z}$.

3. Considere dois números $m, n \in \mathbb{Z}$ tais que $m \leq n$. Prove que existe um inteiro positivo $a \in \mathbb{Z}$ tal que $n = m + a$.

4. Prove as seguintes propriedades a respeito dos inteiros $m, n, p \in \mathbb{Z}$:

(a) $m \leq n \Rightarrow m + p \leq n + p$,

(b) $m \leq n$ e $p \geq 0 \Rightarrow m \cdot p \leq n \cdot p$,

(c) $m \leq n$ e $p \leq 0 \Rightarrow n \cdot p \leq m \cdot p$.

5.4

1. Sejam p um número primo e $a_1, \ldots, a_n \in \mathbb{Z}$ tais que $p|(a_a \cdot \ldots \cdot a_n)$. Mostre que existe $1 \leq j \leq n$ tal que $p|a_j$.

2. Sejam $m, n \in \mathbb{Z}$ tais que $m|n$. Prove que $\mathrm{mdc}(m, n) = |m|$.

3. Dado um inteiro $n > 1$, mostre que existe um primo p tal que $p|n$.

4. Se $p, q \in \mathbb{N}$ são números primos, mostre que p e q não dividem $p \cdot q + 1$.

5.5

1. Mostre que se $n \in \mathbb{N}$ é ímpar, então $2^n + 1$ é divisível por 3.

2. Calcule o resto da divisão de 4^{555} por 10, e de $2^{70} + 3^{70}$ por 13.

Capítulo 6

Conjuntos enumeráveis

6.1 Conjuntos finitos

Fixado um número $n \in \mathbb{N}$, denotemos por I_n o conjunto

$$I_n = \{k \in \mathbb{N} : 1 \leq k \leq n\}.$$

A proposição seguinte estabelece uma relação de ordem nestes conjuntos.

Proposição 6.1.1. Considere dois números $m, n \in \mathbb{N}$. Então, $n \leq m$ se, e somente se, $I_n \subset I_m$. Além disso, se $n < m$, então $I_n \subset I_m$, mas $I_n \neq I_m$.

Demonstração. Suponha $n \leq m$ e considere um elemento $a \in I_n$. Temos então que $a \leq n \leq m$, ou seja, $a \in I_m$, mostrando que $I_n \subset I_m$. Reciprocamente, se $I_n \subset I_m$ segue da definição que todo natural $a \leq n$ satisfaz $a \leq m$. Em particular para $a = n$. Isso mostra que $n \leq m$. Finalmente, se $n < m$, então $m = n + a$, para algum $a > 0$. Como $n < n + 1$, segue que $n + a = m \in I_m$, mas $m \notin I_n$. $\square$

Definição 6.1.2. Um conjunto não-vazio X será chamado *finito* se existir uma função injetora $f : X \to I_n$, para algum $n \in \mathbb{N}$.

Dado um conjunto finito X, denotemos por U_X o conjunto formado por todos os $n \in \mathbb{N}$ para os quais existe uma função injetora $f : X \to I_n$. Note que, como X é finito, $U_X \neq \emptyset$. O menor elemento do conjunto U_X será chamado a *cardinalidade* de X e será denotado por $\text{card}(X)$. Por definição, temos $\text{card}(\emptyset) = 0$.

Proposição 6.1.3. Considere dois conjuntos finitos X e Y. Se existe uma função injetora $f : X \to Y$, então $\text{card}(X) \leq \text{card}(Y)$. Se existe uma função sobrejetora $f : X \to Y$, então $\text{card}(Y) \leq \text{card}(X)$.

Demonstração. Suponha que exista uma função injetora $f : X \to Y$ e seja $n = \mathrm{card}(Y)$. Sabemos que existe uma função injetora $g : Y \to I_n$. Assim, a composição $g \circ f : X \to I_n$ também é uma função injetora, donde concluímos que $\mathrm{card}(X) \leq n = \mathrm{card}(Y)$. Suponha agora que exista uma função sobrejetora $f : X \to Y$ e seja $g : X \to I_n$ uma função injetora, com $n = \mathrm{card}(X)$. Isso significa que, para cada elemento $y \in Y$, o conjunto

$$S_y = \{k \in I_n : \text{existe } x \in X \text{ tal que } g(x) = k \text{ e } f(x) = y\}$$

é não-vazio. Defina então uma função $h : Y \to I_n$ pondo

$$h(y) = \min S_y.$$

Note que h está bem definida, pois S_y é um subconjunto não-vazio de $\mathbb{N}$. Afirmamos que h é uma função injetora. De fato, sejam $y_1, y_2 \in Y$ tais que $h(y_1) = h(y_2)$. Assim, $S_{y_1} \cap S_{y_2} \neq \emptyset$, já que os dois conjuntos têm o mesmo menor elemento. Disso decorre que existe $x \in X$ com $f(x) = y_1$ e $f(x) = y_2$, donde concluímos que $y_1 = y_2$. Assim, sendo $h : Y \to I_n$ injetora, concluímos que $\mathrm{card}(Y) \leq n = \mathrm{card}(X)$. □

Corolário 6.1.4. Se $f : X \to Y$ é uma função bijetora entre os conjuntos finitos X e Y, então $\mathrm{card}(X) = \mathrm{card}(Y)$.

Demonstração. Da Proposição 6.1.3 concluímos que $\mathrm{card}(X) \leq \mathrm{card}(Y)$ e $\mathrm{card}(Y) \leq \mathrm{card}(X)$, donde segue a igualdade. □

Proposição 6.1.5. Considere um número $n \in \mathbb{N}$ tal que existe um subconjunto não-vazio $A \subset I_n$, com $A \neq I_n$. Então, $\mathrm{card}(A) < n$.

Demonstração. Observe, inicialmente, que devemos ter $n > 1$ pois, caso fosse $n = 1$, não seria possível ter um subconjunto não-vazio $A \subset I_n$, com $A \neq I_n$. Assim, existe $m \in \mathbb{N}$ com $n = m + 1$. Considere agora um elemento $r \in I_n - A$ e defina uma função $f : I_n \to I_n$ pondo

$$f(k) = \begin{cases} k, & \text{se } \quad k \notin \{n, r\} \\ r, & \text{se } \quad k = n \\ n, & \text{se } \quad k = r \end{cases}.$$

A função f troca r e n de posição e mantém todos os outros elementos de I_n fixados. Assim, por construção, f é uma bijeção, logo sua restrição $f|_A$ é injetora. Além disso, o conjunto imagem $f(A)$ está contido em $I_m \subset I_n$ pois, para todo $a \in A$, com $a \neq r$, tem-se $f(a) \neq f(r) = n$, implicando que $f(a) \in I_n - \{n\} = I_m$. Assim, a restrição $f|_A$ pode ser considerada como uma função injetora $f : A \to I_m$, logo $\mathrm{card}(A) \leq m < n$. □

Proposição 6.1.6. Qualquer que seja $n \in \mathbb{N}$, tem-se $\text{card}(I_n) = n$.

Demonstração. Provemos por indução. Para isso, considere o conjunto

$$A = \{n \in \mathbb{N} : \text{card}(I_n) = n\}.$$

Observe que $1 \in A$, pois $I_1 = \{1\}$, logo $\text{card}(I_1) = 1$. Seja agora $n \in A$ e mostremos que $n+1 \in A$. Como $n+1 > n$, tem-se $I_n \subset I_{n+1}$, mas $n+1 \notin I_n$. A função $f : I_n \to I_{n+1}$ dada por $f(k) = k$ é injetora, mas não é sobrejetora, logo $n = \text{card}(I_n) < \text{card}(I_{n+1})$. Disso decorre que

$$n + 1 \leq \text{card}(I_{n+1}). \tag{6.1}$$

Por outro lado, a função $g : I_{n+1} \to I_{n+1}$ dada por $g(k) = k$ é injetora, logo

$$\text{card}(I_{n+1}) \leq n + 1. \tag{6.2}$$

Segue então de (6.1) e (6.2) que $\text{card}(I_{n+1}) = n+1$, provando que $n+1 \in A$. Portanto, pelo axioma da indução, concluímos que $A = \mathbb{N}$. $\square$

Corolário 6.1.7. Considere um subconjunto $A \subset I_n$. Se existir uma bijeção $f : A \to I_n$, então $A = I_n$.

Demonstração. Como f é bijetora, segue do Corolário 6.1.4 e da Proposição 6.1.6 que $\text{card}(A) = \text{card}(I_n) = n$. Por outro lado, caso tivéssemos $A \subset I_n$ e $A \neq I_n$, a Proposição 6.1.5 implicaria que $\text{card}(A) < n$, contradição. $\square$

Teorema 6.1.8. *Um conjunto finito X tem cardinalidade igual a n se, e somente se, existe uma bijeção entre X e I_n.*

Demonstração. Suponhamos $\text{card}(X) = n$. Assim, existe uma função injetora $f : X \to I_n$. Denotemos por $A = f(X)$ a imagem de f. Afirmamos que $A = I_n$, o que significa que f é sobrejetora e, portanto, uma bijeção. De fato, suponha por absurdo que $A \neq I_n$. Como $A \subset I_n$, segue da Proposição 6.1.5 que $\text{card}(A) < n$, de modo que existe uma função injetora $g : A \to I_m$, para algum $m < n$. Defina uma função $\xi : X \to I_m$ pondo $\xi(x) = g(f(x))$. Como f e g são injetoras, o mesmo ocorre com ξ, logo $\text{card}(X) \leq m < n$, contradizendo a hipótese de que $\text{card}(X) = n$. Portanto, devemos ter $A = I_n$, ou seja, $f : X \to I_n$ é uma bijeção. Reciprocamente, suponha que exista uma bijeção entre X e I_n. Disso decorre, em particular, que X é finito, e pelos Corolário 6.1.4 e Proposição 6.1.6, concluímos que $\text{card}(X) = \text{card}(I_n) = n$. $\square$

Corolário 6.1.9. Não existe uma bijeção $f : Y \to X$ entre um conjunto finito X e um subconjunto próprio $Y \subset X$.

Demonstração. Suponha que exista uma bijeção $f : Y \to X$. Sendo X finito, existe uma bijeção $g : X \to I_n$, para algum $n \in \mathbb{N}$. Seja $A = g(Y)$. Então, A é um subconjunto próprio de I_n, e a restrição de g a X fornece uma bijeção $g|_Y : Y \to A$.

$$\begin{tikzcd} Y \arrow[r, "f"] \arrow[d, "g|_Y"'] & X \arrow[d, "g"] \\ A \arrow[r, "h"] & I_n \end{tikzcd}$$

Assim, a composição $h = g \circ f \circ (g|_Y)^{-1}$ é uma bijeção entre I_n e o subconjunto próprio A, contradizendo o Corolário 6.1.7. $\square$

Proposição 6.1.10. Se X é um conjunto finito, então todo subconjunto $Y \subset X$ também é finito e $\operatorname{card}(Y) \leq \operatorname{card}(X)$.

Demonstração. Como X é finito, existe uma bijeção $f : X \to I_n$, para algum $n \in \mathbb{N}$. Seja $A = f(Y) \subset I_n$. A restrição $f|_Y : Y \to A$ também é uma bijeção. Considere a função $g : A \to I_k$ definida por $g(n_k) = k$, para todo $n_k \in A$. Por construção, g é uma bijeção entre A e I_k, logo $g \circ f|_Y : Y \to I_k$ é bijeção, mostrando que Y é limitado. Disso decorre, em particular, que $\operatorname{card}(Y) = k \leq n$. $\square$

O resultado seguinte fornece condições equivalentes para que um subconjunto X de $\mathbb{N}$ seja finito.

Teorema 6.1.11. *Seja $X \subset \mathbb{N}$ um subconjunto não-vazio. As seguintes afirmações são equivalentes:*

(a) X é finito,

(b) X é limitado,

(c) X possui um maior elemento.

Demonstração. $(a) \Rightarrow (b)$ Seja $X = \{x_1, x_2, \ldots, x_n\}$ e considere o elemento $p = x_1 + x_2 + \ldots + x_n$. Temos que $x < p$, para todo $x \in X$, mostrando que X é limitado.

$(b) \Rightarrow (c)$ Se $X \subset \mathbb{N}$ é limitado, então o conjunto

$$A = \{p \in \mathbb{N} : n \leq p, \text{ para todo } n \in X\}$$

é não-vazio. Assim, A admite um menor elemento $p_0 \in A$. Afirmamos que $p_0 \in X$. De fato, suponha que $p_0 \notin X$. Assim, $p_0 > n$, para todo $n \in X$. Como $X \neq \emptyset$, isso obriga $p_0 > 1$, donde $p_0 = p_1 + 1$. Se existir algum $n \in X$, com $p_1 < n$, então $p_0 = p_1 + 1 \leq n$ e $p_0 < n$, o que é uma contradição. Logo, temos que $p_1 \geq n$, para todo $n \in X$. Mas isso significa que $p_1 \in A$, o que é um absurdo pois $p_1 < p_0$ e p_0 é o menor elemento de A. Portanto, devemos ter $p_0 \in X$. Como $p_0 \geq n$, para todo $n \in X$, concluímos que p_0 é o maior elemento do conjunto X.

$(c) \Rightarrow (a)$ Seja $p \in X$ o maior elemento de X. Assim, temos que $X \subset I_p$, logo X é finito pela Proposição 6.1.10. □

Proposição 6.1.12. Considere dois conjuntos finitos e disjuntos X e Y, com $\text{card}(X) = m$ e $\text{card}(Y) = n$. Então, a união $X \cup Y$ é um conjunto finito e $\text{card}(X \cup Y) = m + n$.

Demonstração. Considere bijeções $f : I_m \to X$ e $g : I_n \to Y$, e defina a função $h : I_{m+n} \to X \cup Y$ pondo

$$h(k) = \begin{cases} f(k), & \text{se} \quad 1 \leq k \leq m \\ g(k-m), & \text{se} \quad m+1 \leq k \leq m+n \end{cases}.$$

Como f e g são bijeções e $X \cap Y = \emptyset$, segue que h também é bijeção, mostrando que $X \cup Y$ é finito, com $\text{card}(X \cup Y) = m + n$. □

Definição 6.1.13. Dado um conjunto X, definimos o conjunto $\mathcal{P}(X)$, chamado o *conjunto das partes de* X, como sendo o conjunto formado por todos os subconjuntos de X.

Por exemplo, se $X = \{a, b, c\}$, então

$$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, X\}.$$

Proposição 6.1.14. Se $\text{card}(X) = n$, então $\text{card}(\mathcal{P}(X)) = 2^n$.

Demonstração. Provaremos por indução. Para isso, consideremos a propriedade relativa ao natural n dada por

$$P(n) : \text{card}(X) = n \Rightarrow \text{card}(\mathcal{P}(X)) = 2^n.$$

Se $n = 0$, então $X = \emptyset$. Como $\emptyset \subset \emptyset$, concluímos que $\mathcal{P}(X) = \{\emptyset\}$, ou seja, $\text{card}(\mathcal{P}(X)) = 1 = 2^0$, como queríamos. Suponhamos agora $P(n)$ verdadeiro e mostremos que $P(n+1)$ também o é. Consideremos então um conjunto X, com $\text{card}(X) = n + 1$. Fixado um elemento arbitrário $a \in X$, consideremos os conjuntos

$$X_a = \{A \subset X : a \notin A\} \quad \text{e} \quad X^a = \{A \subset X : a \in A\}.$$

Note que $X_a = \mathcal{P}(X - \{a\})$. Como $\text{card}(X - \{a\}) = n$ segue, pela hipótese de indução, que $\text{card}(X_a) = 2^n$. Por outro lado, consideremos a função $f : X_a \to X^a$ definida por

$$f(A) = A \cup \{a\}.$$

Claramente f é uma bijeção, logo $\text{card}(X^a) = \text{card}(X_a) = 2^n$. Como $\mathcal{P}(X) = X_a \cup X^a$ e $X_a \cap X^a = \emptyset$, concluímos que

$$\text{card}(\mathcal{P}(X)) = \text{card}(X_a) + \text{card}(X^a) = 2^n + 2^n = 2^{n+1},$$

como queríamos. □

6.2 Conjuntos enumeráveis

Nesta seção estudaremos o conceito de enumerabilidade, estendendo a noção de conjunto finito. Aqui, convém deixar claro a negação de conjunto finito. Um conjunto X chama-se *infinito* quando não é finito. Mais precisamente, X é infinito se não é vazio e, além disso, qualquer que seja $n \in \mathbb{N}$, não existe bijeção $f : X \to I_n$. O conjunto dos números naturais $\mathbb{N}$, por exemplo, é um conjunto infinito (cf. Exercício 6.1.1).

Definição 6.2.1. Um conjunto X é dito ser *enumerável* se é finito ou se existe uma bijeção $f : \mathbb{N} \to X$.

Uma bijeção $f : \mathbb{N} \to X$ é usualmente chamada uma *enumeração* dos elementos do conjunto X.

Exemplo 6.2.2. O exemplo trivial de conjunto enumerável é o próprio $\mathbb{N}$, pois a função identidade de $\mathbb{N}$ em $\mathbb{N}$ é bijetora. Se $\mathcal{P}$ denota o subconjunto de $\mathbb{N}$ constituído dos números pares, a função $f : \mathbb{N} \to \mathcal{P}$ dada por $f(n) = 2n$ é uma bijeção, logo $\mathcal{P}$ é enumerável. De forma análoga, se $\mathcal{I}$ denota o subconjunto de $\mathbb{N}$ constituído dos números ímpares, a função $f : \mathbb{N} \to \mathcal{I}$ dada por $f(n) = 2n + 1$ é bijetora.

O Exemplo 6.2.2 é, na realidade, um caso particular de uma situação mais geral.

Proposição 6.2.3. Todo subconjunto $X \subset \mathbb{N}$ é enumerável.

Demonstração. Se X é um conjunto finito, então é enumerável por definição. Suponhamos então que X seja infinito. Assim, se retirarmos um número finito de elementos de X, o conjunto restante será não-vazio. Definiremos uma bijeção $f : \mathbb{N} \to X$ de forma indutiva. Definimos $f(1)$ como o menor elemento do conjunto X, $f(2)$ como o menor elemento de $A_1 = X - \{f(1)\}$, $f(3)$ o menor elemento de $A_2 = X - \{f(1), f(2)\}$ e, de forma análoga, definimos $f(n)$ como o menor elemento de $A_{n-1} = X - \{f(1), \ldots, f(n-1)\}$. Como A_{n-1} é não-vazio, pomos $f(n+1)$ como o menor elemento do conjunto $A_n = X - \{f(1), \ldots, f(n)\}$. Como $f(n) < f(n+1)$, segue que f é injetora. A função f também é sobrejetora pois, se existisse algum $x \in \mathbb{N} - f(\mathbb{N})$, teríamos $x \in A_n$, para todo n e, portanto, $f(n) < x$, para todo $n \in \mathbb{N}$. Mas isso implicaria que o conjunto infinito $f(\mathbb{N}) \subset \mathbb{N}$ seria limitado, contradizendo o Teorema 6.1.11. □

Corolário 6.2.4. Se $f : A \to B$ é uma função bijetora, onde B é um subconjunto de $\mathbb{N}$, então A é enumerável.

Demonstração. Como $B \subset \mathbb{N}$, segue da Proposição 6.2.3 que existe uma bijeção $g : B \to \mathbb{N}$. Assim, a composta $g \circ f : A \to \mathbb{N}$ também é bijetora, e isso mostra que A é enumerável. □

Corolário 6.2.5. Se B é um conjunto enumerável e $f : A \to B$ é uma função injetora, então A também é enumerável.

Demonstração. Por hipótese, existe uma bijeção $g : B \to \mathbb{N}$. Assim, a composta $h = g \circ f : A \to \mathbb{N}$ é injetora, logo é uma bijeção sobre sua imagem. O conjunto imagem $h(A)$, por ser subconjunto de $\mathbb{N}$, é enumerável, em virtude da Proposição 6.2.3. Portanto, pelo Corolário 6.2.4, segue que A é enumerável. □

Corolário 6.2.6. Todo subconjunto de um conjunto enumerável também é enumerável.

Demonstração. Sejam B um conjunto enumerável e A um subconjunto de B. A função $f : A \to B$, dada por $f(x) = x$, para todo $x \in A$, é injetora logo, pelo Corolário 6.2.5, segue que A é enumerável. □

Corolário 6.2.7. Se A é um conjunto enumerável e $f : A \to B$ é uma função sobrejetora, então B também é enumerável.

Demonstração. Por hipótese, temos que dado $b \in B$, existe $a \in A$ tal que $f(a) = b$. Isso permite-nos definir uma funcção $g : B \to A$ pondo $g(b) = a$, donde $f(g(b)) = f(a) = b$, para todo $b \in B$. Dados $b_1, b_2 \in B$, com $b_1 \neq b_2$, então $g(b_1) \neq g(b_2)$. De fato, caso fosse $g(b_1) = g(b_2)$, então

$$b_1 = f(g(b_1)) = f(g(b_2)) = b_2,$$

contradizendo a hipótese $b_1 \neq b_2$. Portanto, g é injetora, e como A é enumerável, segue do Corolário 6.2.5 que B é enumerável. □

Exemplo 6.2.8. O produto cartesiano $\mathbb{N} \times \mathbb{N}$ é enumerável. De fato, considere a função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $f(m, n) = 2^m \cdot 3^n$. Pela unicidade da decomposição de um número natural em fatores primos (cf. Teorema 5.4.11), segue que f é injetora logo, pelo Corolário 6.2.5, concluímos que $\mathbb{N} \times \mathbb{N}$ é enumerável.

Exemplo 6.2.9. De forma mais geral que o Exemplo 6.2.8, o produto cartesiano de dois conjuntos enumeráveis também é enumerável. De fato, dados dois conjuntos enumeráveis X e Y, considere bijeções $f : \mathbb{N} \to X$ e $g : \mathbb{N} \to Y$. Defina uma função $h : \mathbb{N} \times \mathbb{N} \to X \times Y$ pondo

$$h(m, n) = (f(m), g(n)).$$

Como f e g são sobrejetoras, o mesmo ocorre com h. Assim, como $\mathbb{N} \times \mathbb{N}$ é enumerável, segue do Corolário 6.2.7 que $X \times Y$ é enumerável.

Na Proposição 6.1.14 vimos que se X é finito, com $\text{card}(X) = n$, então o conjunto das partes $\mathcal{P}(X)$ é finito e tem-se $\text{card}(\mathcal{P}(X)) = 2^n$. Uma pergunta que podemos fazer aqui é se o conjunto das partes de $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, é enumerável.

Proposição 6.2.10. O conjunto $\mathcal{P}(\mathbb{N})$ não é enumerável.

Demonstração. Suponhamos que exista uma bijeção $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$, e consideremos o conjunto

$$A = \{n \in \mathbb{N} : n \notin f(n)\}.$$

Como f é bijetora e $A \in \mathcal{P}(\mathbb{N})$, segue que existe $n \in \mathbb{N}$ tal que $f(n) = A$. Note que, se $n \in A$, então $n \in f(n)$ e, portanto, $n \notin A$. Por outro lado, se $n \notin A$ então $n \notin f(n)$, logo $n \in A$. Em qualquer caso, obtemos uma contradição. Portanto, não existe bijeção entre $\mathbb{N}$ e o conjunto das partes $\mathcal{P}(\mathbb{N})$. □

6.3 O conjunto dos números racionais

Na seção 5.4 vimos que a equação $m \cdot n = 1$ em $\mathbb{Z}$ admite como solução $m = n = 1$ ou $m = n = -1$. O que faremos agora é ampliar essa situação. Mais precisamente, definiremos um conjunto, contendo o conjunto dos números inteiros $\mathbb{Z}$, de modo que se $m \in \mathbb{Z}$ e $m \neq 0$, então existe $n \in \mathbb{Z}$ tal que $m \cdot n = 1$. Além disso, tal conjunto também será enumerável.

Para isso, consideremos o conjunto

$$A = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : b \neq 0\}$$

e definimos a seguinte relação em A:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc. \tag{6.3}$$

Proposição 6.3.1. A relação $\sim$ definida em (6.3) é uma relação de equivalência.

Demonstração. As propriedades reflexiva e simétrica seguem diretamente de (6.3). Sejam agora $(a,b), (c,d), (e,f) \in A$ tais que $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$, ou seja,

$$ad = bc \quad \text{e} \quad cf = de. \tag{6.4}$$

Multiplicando a primeira equação em (6.4) por f e a segunda equação por b, obtemos

$$adf = bcf \quad \text{e} \quad bcf = bde,$$

donde $adf = bde$. Como $d \neq 0$, concluímos que $af = be$, o que significa que $(a,b) \sim (e,f)$, e isso mostra a propriedade transitiva. $\square$

O conjunto quociente $A/{\sim}$ será denotado por $\mathbb{Q}$ e será chamado de conjunto dos *números racionais*.

Definição 6.3.2. Dados dois números $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Q}$, definimos a *soma* de $\overline{(a,b)}$ e $\overline{(c,d)}$ pondo

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad + bc, bd)}. \tag{6.5}$$

Devemos verificar que a operação em (6.5) está bem definida. Observe, inicialmente, que $(ad + bc, bd) \in A$ pois, como $b \neq 0$ e $d \neq 0$, então $bd \neq 0$. Considere então $(x,y), (z,w) \in A$ tais que

$$(a,b) \sim (x,y) \quad \text{e} \quad (c,d) \sim (z,w).$$

Devemos mostrar que $(ad + bc, bd) \sim (xw + yz, yw)$, ou seja,

$$(ad + bc)yw = bd(xw + yz).$$

Por hipótese, temos $ay = bx$ e $cw = dz$. Assim,

$$\begin{aligned} (ad + bc)yw &= adyw + bcyw = aydw + bycw \\ &= bxdw + bydz = bdxw + bdyz \\ &= bd(xw + yz), \end{aligned}$$

como queríamos.

Definição 6.3.3. Dados dois números $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Q}$, definimos o *produto* de $\overline{(a,b)}$ e $\overline{(c,d)}$ pondo

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}. \tag{6.6}$$

Da mesma forma como na soma, devemos mostrar que a operação em (6.6) está bem definida. Como $bd \neq 0$, temos que $(ac, bd) \in A$. Além disso, sejam $(x,y), (z,w) \in A$ tais que

$$(a,b) \sim (x,y) \quad \text{e} \quad (c,d) \sim (z,w).$$

Devemos mostrar que $(ac, bd) \sim (xz, yw)$. Por hipótese, temos $ay = bx$ e $cw = dz$. Assim,

$$acyw = aycw = bxdz = bdxz,$$

mostrando o que queríamos.

Um elemento $\overline{(a,b)} \in \mathbb{Q}$ é dito estar na *forma canônica* se $b > 0$.

Proposição 6.3.4. Todo número racional admite uma representação na forma canônica.

Demonstração. Seja $\overline{(a,b)} \in \mathbb{Q}$. Se $b > 0$, não há nada a que se fazer. Caso $b < 0$, então $\overline{(-a,-b)} = \overline{(a,b)}$, pois $-ab = -ba$. Como $-b > 0$, isso mostra que $\overline{(-a,-b)}$ está na forma canônica. $\square$

Definição 6.3.5. Sejam $p, q \in \mathbb{Q}$, com $p = \overline{(a,b)}$ e $q = \overline{(c,d)}$ estando na forma canônica. Dizemos que p é *menor do que ou igual a* q, e escrevemos $p \leq q$, se $ad \leq bc$.

Devemos mostrar que a relação $\leq$, dada na Definição 6.3.5, está bem definida. Ou seja, devemos provar que se $\overline{(a,b)} = \overline{(x,y)}$, $\overline{(c,d)} = \overline{(z,w)}$ e $\overline{(a,b)} \leq \overline{(c,d)}$, então $\overline{(x,y)} \leq \overline{(z,w)}$. As duas primeiras equações significam que

$$ay = bx \quad \text{e} \quad cw = dz. \tag{6.7}$$

A condição $\overline{(a,b)} \leq \overline{(c,d)}$ significa que $ad \leq bc$. Multiplicando esta última desigualdade por $yw \geq 0$, obtemos

$$adyw \leq bcyw. \tag{6.8}$$

Substituindo (6.7) em (6.8), a desigualdade torna-se

$$bxdw \leq bydz. \tag{6.9}$$

Como $bd \geq 0$, podemos cancelar este termo em (6.9), obtendo $xw \leq yz$, como queríamos.

Dado um número racional $\overline{(a,b)} \in \mathbb{Q}$, escrito na forma canônica, a partir de agora o denotaremos por $\frac{a}{b}$. Quando $b = 1$, denotaremos $\overline{(a,b)}$ simplesmente por a. Observe que essa identificação é coerente com as notações usuais no sentido de que

$$\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = a + b,$$

onde o último termo acima é uma soma em $\mathbb{Z}$.

Proposição 6.3.6. Dado um número $p \in \mathbb{Q}$, com $p \neq 0$, existe $q \in \mathbb{Q}$ tal que $p \cdot q = 1$.

Demonstração. Observe que, pela identificação acima, temos

$$1 = \frac{1}{1} \sim \overline{(1,1)} = \overline{(n,n)},$$

com $n \neq 0$. Assim, dado $p = \overline{(a,b)}$, tome $q = \overline{(b,a)}$. Portanto,

$$p \cdot q = \overline{(a,b)} \cdot \overline{(b,a)} = \overline{(ab,ba)} = \overline{(1,1)},$$

como queríamos. $\square$

O elemento $q \in \mathbb{Q}$, dado na Proposição 6.3.6, é chamado o *elemento inverso* de p relativo à operação de produto.

Finalizeremos esta seção mostrando a enumerabilidade de $\mathbb{Q}$.

Proposição 6.3.7. O conjunto dos números racionais $\mathbb{Q}$ é enumerável.

Demonstração. Considere a função $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ dada por

$$f\left(\frac{a}{b}\right) = (a, b).$$

Claramente, f é injetora. Observe que, em virtude do Exercício 6.3.1 e do Exemplo 6.2.9, o conjunto $\mathbb{Z} \times \mathbb{Z}$ é enumerável. Portanto, pelo Corolário 6.2.5, concluímos que $\mathbb{Q}$ é enumerável. $\square$

6.4 Exercícios

6.1

1. Prove que $\mathbb{N}$ não é um conjunto finito.

2. Sejam X e Y conjuntos finitos. Prove que

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

Deduza daí que $\operatorname{card}(X \cup Y) \leq \operatorname{card}(X) + \operatorname{card}(Y)$.

3. Se X e Y são conjuntos finitos, com $\operatorname{card}(X) = m$ e $\operatorname{card}(Y) = n$, mostre que $X \times Y$ é finito, com $\operatorname{card}(X \times Y) = m \cdot n$.

4. Sejam X e Y conjuntos finitos, com $\operatorname{card}(X) = m$ e $\operatorname{card}(Y) = n$. Mostre que o conjunto $\mathcal{F}(X, Y)$ de todas as funções $f : X \to Y$ é finito, com $\operatorname{card}(\mathcal{F}(X, Y)) = n^m$.

5. Seja X um conjunto finito, com $\operatorname{card}(X) = n$. Use indução para provar que o conjunto das bijeções $f : X \to X$ é finito com cardinalidade igual a $n!$

6. Para cada caso abaixo, determine o conjunto $\mathcal{P}(X)$:

(a) $X = \{a, b, c, d\}$,

(b) $X = \emptyset$,

(c) $X = \{\emptyset\}$,

(d) $X = \mathcal{P}(\{a, b\})$.

6.2

1. Prove que o conjunto dos inteiros $\mathbb{Z}$ é enumerável.

2. Considere dois conjuntos X e Y, de forma que Y não seja enumerável. Prove que se existir uma função sobrejetora $f : X \to Y$, então X também não é enumerável.

3. Seja $f : X \to X$ uma função injetora que não é sobrejetora. Escolhendo um elemento $x \in X - f(X)$, mostre que os elementos $x, f(x), f(f(x)), \ldots$ são dois a dois disjuntos.

4. Sejam X um conjunto infinito e Y um conjunto finito. Mostre que existe uma função sobrejetora $f : X \to Y$ e uma função injetora $g : Y \to X$.

6.3

1. Mostre que as propriedades associativa, comutativa e distributiva são válidas para as operações da soma e produto em $\mathbb{Q}$.

2. Mostre que o elemento inverso do produto em $\mathbb{Q}$ é único.

Referências Bibliográficas

[1] L. F. Aurichi, *Elementos de Matemática*, Notas de Aula.

[2] A. Caminha, *Tópicos de Matemática Elementar*, vol. 5, Teoria dos Números, Coleção do Professor de Matemática, SBM, 2013.

[3] P. R. Halmos, *Naive set theory*, The University Series in Undergraduate Mathematics, Princeton, 1960.

[4] E. L. Lima, et al, *A Matemática do Ensino Médio*, vol. 1, Coleção do Professor de Matemática, SBM, 2016.

[5] E. L. Lima, *Curso de Análise*, vol. 1, IMPA, Projeto Euclides, 2016.

[6] G. P. Novaes, *Introdução à Teoria dos Conjuntos*, Coleção do Professor de Matemática, SBM, 2018.