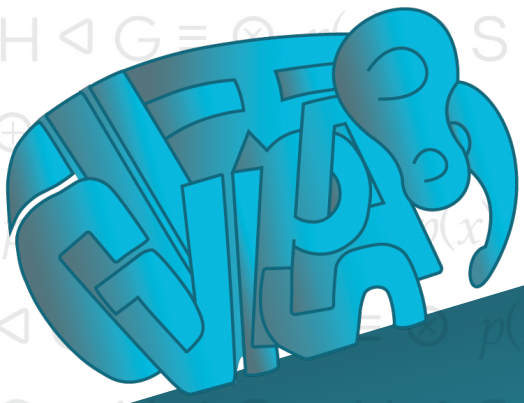
Jhone Caldeira Silva
Olimpio Ribeiro Gomes

Estruturas Algébricas para Licenciatura

Elementos de Álgebra Moderna



Blucher

vol. 3

Jhone Caldeira Silva
Olimpio Ribeiro Gomes

ESTRUTURAS ALGÉBRICAS PARA LICENCIATURA

VOLUME 3

ELEMENTOS DE ÁLGEBRA MODERNA

Estruturas algébricas para licenciatura: volume 3 – Elementos de Álgebra Moderna

Editora Edgard Blücher Ltda.

Arte da capa: Éric Flávio de Araújo, Ana Paula Chaves, Selma Alves Costa e Jhone Caldeira Silva

Blucher

Rua Pedroso Alvarenga, 1245, 4º andar
04531-934 – São Paulo – SP – Brasil
Tel.: 55 11 3078-5366
contato@blucher.com.br
www.blucher.com.br

Segundo Novo Acordo Ortográfico, conforme 5. ed. do *Vocabulário Ortográfico da Língua Portuguesa*, Academia Brasileira de Letras, março de 2009.

FiCHA CATALOGRÁFICA

Silva, Jhone Caldeira
Estruturas algébricas para licenciatura : volume 3 : Elementos de Álgebra Moderna / Jhone Caldeira Silva, Olimpio Ribeiro Gomes. — São Paulo : Blucher, 2020.
510 p. : il.

Bibliografia
ISBN 978-85-212-1853-1 (impresso)
ISBN 978-85-212-1854-8 (e-book)

1. Álgebra 2. Matemática – Estudo e ensino I. Título. II. Gomes, Olimpio Ribeiro.

19-1596 CDD 512

Índice para catálogo sistemático:
1. Álgebra

CONTEÚDO

CAPÍTULO 1
TÓPICOS PRELIMINARES

Neste primeiro capítulo apresentamos as principais ferramentas que serão utilizadas ao longo do livro. A abordagem aqui será bastante sucinta – apenas o suficiente para fixar a notação e relembrar o leitor das técnicas subjacentes a tais ferramentas. Caso o leitor deseje ou sinta necessidade de uma leitura mais profunda, encontrará uma exposição bem mais detalhada em [13] e [14].

1.1 CONJUNTOS, SUBCONJUNTOS E SEUS ELEMENTOS

Consideraremos como conceitos primitivos e, portanto, não definiremos formalmente as noções de conjunto, elemento, relação de pertinência, relação de igualdade, par ordenado e número de elementos de um conjunto. Para representar que x é um elemento do conjunto X, usaremos a notação $x \in X$, que é lida assim: "x pertence a X". A negação dessa proposição é representada por $x \notin X$, que se lê como "x não pertence a X".

SUBCONJUNTOS E CONJUNTO DAS PARTES DE UM CONJUNTO

Definição 1.1.1

Dizemos que o conjunto X é um *subconjunto* (ou uma *parte*) do conjunto Y se todo elemento de X é também elemento de Y.

- **Notação**: Escrevemos $X \subset Y$ quando o conjunto X é um subconjunto do conjunto Y.

- **O conjunto vazio.** Usamos a notação Ø para indicar um conjunto que não possui nenhum elemento. Ele é chamado de *conjunto vazio* e tem a propriedade de ser um subconjunto de qualquer conjunto. De fato, se houvesse algum conjunto X do qual Ø não fosse subconjunto, então o conjunto Ø deveria ter algum elemento que não pertencesse a X, o que é impossível, por Ø não possuir nenhum elemento.

É importante que o leitor relembre a diferença entre *ser elemento* e *ser subconjunto*. Veja o exemplo:

Exemplo 1.1.2

Considere A o conjunto das vogais da palavra *paralelepípedo* e o conjunto $B = \{a, e, \{i,o\}\}$.

(a) O conjunto $\{a,e\}$ é um subconjunto dos conjuntos A e B, pois $a \in A$ e $e \in A$, $a \in B$ e $e \in B$. Escrevemos $\{a,e\} \subset A$ e $\{a,e\} \subset B$.

(b) O conjunto $\{i,o\}$ é um subconjunto de A, pois $i \in A$ e $o \in A$, mas não é um subconjunto de B, pois $i \notin B$ (também $o \notin B$, porém basta ver que um elemento de $\{i,o\}$ não é elemento de B). Escrevemos $\{i,o\} \subset A$ e $\{i,o\} \not\subset B$. Apesar disso, $\{i,o\}$ é um elemento de B.

(c) O conjunto $\{a,o\}$ é um subconjunto de A, pois $a \in A$ e $o \in A$, mas não é um subconjunto de B, pois, como já observamos, $o \notin B$. Escrevemos $\{a,o\} \subset A$ e $\{a,o\} \not\subset B$.

A lista de todos os subconjuntos de B é $\{a,e,\{i,o\}\}$, $\{a,e\}$, $\{a,\{i,o\}\}$, $\{e,\{i,o\}\}$, $\{a\}$, $\{e\}$, $\{\{i,o\}\}$ e $\varnothing$.

A lista de todos os subconjuntos de um dado conjunto recebe um nome especial, como veremos a seguir.

Definição 1.1.3

O *conjunto das partes* de X, indicado por $\wp(X)$, é o conjunto de todos os subconjuntos de X.

Em outros termos, os elementos do conjunto $\wp(X)$ são partes do conjunto X. Assim, afirmar que $A \in \wp(X)$ é equivalente a dizer que $A \subset X$. Em palavras, A é um elemento de $\wp(X)$ se, e somente se, A é um subconjunto de X. É importante notar que X e Ø sempre são elementos de $\wp(X)$.

Por exemplo, para o conjunto $B = \{a, e, \{i,o\}\}$, temos

$$\wp(B) = \{\{a,e,\{i,o\}\}, \{a,e\}, \{a,\{i,o\}\}, \{e,\{i,o\}\}, \{a\}, \{e\}, \{\{i,o\}\}, \varnothing\}.$$

ALGUNS CONJUNTOS NUMÉRICOS CONHECIDOS

Indicando o conjunto de todos os números naturais[1] por

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, \ldots\}$$

e o conjunto dos números inteiros por

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\},$$

vemos que $\mathbb{N} \subset \mathbb{Z}$. E mais, se

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \text{ e } b \neq 0 \right\}$$

denota o conjunto de todos os números racionais, $\mathbb{R}$ o conjunto dos reais e

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ e } i = \sqrt{-1}\}$$

o conjunto dos números complexos, temos a seguinte cadeia de *inclusões*:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

- **Notação:** No caso em que o número zero é elemento do conjunto X, representamos por X^* o conjunto formado por todos os elementos de X excluindo-se o zero. Assim, para os conjuntos numéricos bem conhecidos, $\mathbb{N}^*$, $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$ denotam, respectivamente, os conjuntos dos números naturais não nulos, inteiros não nulos, racionais não nulos, reais não nulos e complexos não nulos.

Definição 1.1.4

Consideremos dois conjuntos X e Y. Dizemos que X é *igual* a Y se todo elemento de Y é também elemento de X e se todo elemento de X é também elemento de Y.

---

[1] Historicamente falando, o número zero surgiu bem depois dos outros naturais. Entretanto, atualmente, considerá-lo ou não como um número natural é uma questão de conveniência. Nesta coleção, optamos por incluir o zero como um número natural por simplicidade e padronização de notação. Acerca desse assunto, fornece-se uma explicação plausível em [9].

- **Notação:** Escrevemos $X = Y$ quando os conjuntos X e Y são iguais.

A notação introduzida logo após a Definição 1.1.1 fornece um critério para demonstrar a igualdade de conjuntos: dois conjuntos X e Y são iguais se, e somente se, $X \subset Y$ e $Y \subset X$. Em símbolos:

$$X = Y \Leftrightarrow X \subset Y \text{ e } Y \subset X .$$

1.2 OPERAÇÕES DE UNIÃO, INTERSEÇÃO E COMPLEMENTAR EM CONJUNTOS

UNIÃO DE CONJUNTOS

Definição 1.2.1

Sejam X e Y partes de um conjunto U. A *união* dos conjuntos X e Y, indicada por $X \cup Y$, é o conjunto $\{x \in U \mid x \in X \text{ ou } x \in Y\}$.

Exemplo 1.2.2

Sejam A o conjunto das vogais da palavra *paralelepípedo* e B o conjunto $B = \{a, e, \{i,o\}\}$. A união $A \cup B$ é o conjunto $A \cup B = \{a, e, i, o, \{i,o\}\}$.

[Vale lembrar que o conectivo *ou* que aparece na Definição 1.2.1 não é exclusivo, ou seja, nada impede que um elemento que esteja simultaneamente em certos conjuntos X e Y pertença à união $X \cup Y$, como é o caso dos elementos *a* e *e*, pertencentes a ambos os conjuntos A e B dados.]

- ***Observação:*** segue diretamente da Definição 1.2.1 que, dada uma parte X de U, tem-se $X \subset X \cup Y$, para qualquer parte Y de U (convidamos o leitor a escrever uma justificativa para esse fato).

INTERSEÇÃO DE CONJUNTOS

Definição 1.2.3

Sejam X e Y partes de um conjunto U. A *interseção* dos conjuntos X e Y, indicada por $X \cap Y$, é o conjunto $\{x \in U \mid x \in X \text{ e } x \in Y\}$.

Exemplo 1.2.4

Voltando aos conjuntos A e B do Exemplo 1.2.2, vemos que $A \cap B$ é o conjunto $A \cap B = \{a, e\}$.

- ***Observações***

  (i) Conjuntos cuja interseção é o conjunto vazio são chamados *disjuntos*.

  (ii) Segue diretamente da Definição 1.2.3 que, dadas duas partes X e Y de U, tem-se $X \cap Y \subset X$ e $X \cap Y \subset Y$ (convidamos o leitor a escrever uma justificativa para esse fato).

COMPLEMENTAR DE CONJUNTOS

Definição 1.2.5

Seja X uma parte de um conjunto U. O *complementar* de X em U, indicado por $C_U X$, é o conjunto $\{x \in U \mid x \notin X\}$.

O conjunto U a que se refere a definição é comumente chamado de conjunto *universo*. A noção de complementar de um conjunto X depende fortemente do universo onde X está inserido. Veja o exemplo a seguir.

Exemplo 1.2.6

Seja $U = \{a,e,i,o,u\}$ o conjunto das vogais de nosso alfabeto. Considerando novamente A o conjunto das vogais da palavra *paralelepípedo*, temos $C_U A = \{u\}$. Mas, se considerarmos U como sendo formado por todas as letras de nosso alfabeto, teremos

$$C_U A = \{b,c,d,f,g,h,j,k,l,m,n,p,q,r,s,t,u,v,w,x,y,z\}.$$

PROPRIEDADES

A seguir, enunciamos as principais propriedades das operações entre conjuntos. Convidamos o leitor a demonstrá-las.

Teorema 1.2.7

Sejam X, Y e Z partes de um conjunto U.

(1) $C_U\left(C_U X\right) = X$

(2) $X \cap X = X$

(3) $X \cap Y = Y \cap X$

(4) $\left(X \cap Y\right) \cap Z = X \cap \left(Y \cap Z\right)$

(5) $X \cap U = X$

(6) $X \cap \varnothing = \varnothing$

(7) $X \cup X = X$

(8) $X \cup Y = Y \cup X$

(9) $\left(X \cup Y\right) \cup Z = X \cup \left(Y \cup Z\right)$

(10) $X \cup U = U$

(11) $X \cup \varnothing = X$

(12) $X \cap \left(Y \cup Z\right) = \left(X \cap Y\right) \cup \left(X \cap Z\right)$

(13) $X \cup \left(Y \cap Z\right) = \left(X \cup Y\right) \cap \left(X \cup Z\right)$

(14) $C_U\left(X \cap Y\right) = C_U X \cup C_U Y$

(15) $C_U\left(X \cup Y\right) = C_U X \cap C_U Y$

(16) Se $X \subset Y$, então $C_U Y \subset C_U X$.

1.3 PRODUTOS CARTESIANOS E RELAÇÕES EM CONJUNTOS

PRODUTOS CARTESIANOS

Dissemos antes que consideramos o conceito de par ordenado como primitivo. Pois bem, é importante que se tenha em mente quando dois pares ordenados são iguais: os pares ordenados (a,b) e (c,d) são considerados iguais se, e somente se, $a = c$ e $b = d$. Também é importante que se faça distinção entre o par ordenado (a,b) e o conjunto $\{a,b\}$. Por exemplo, em contraste com a diferença entre os pares ordenados $(1,3) \neq (3,1)$, temos a igualdade entre os conjuntos $\{1,3\} = \{3,1\}$. Além disso, enquanto $(4,4)$ é um par ordenado em que o primeiro elemento (chamado de *abscissa* do par) e o segundo elemento (chamado de *ordenada* do par) são iguais, $\{4,4\}$ é um conjunto com apenas um elemento, pois $\{4,4\} = \{4\}$.

Definição 1.3.1

Sejam X e Y dois conjuntos. O *produto cartesiano* de X por Y, indicado por $X \times Y$, é o conjunto $\{(x,y) \mid x \in X \text{ e } y \in Y\}$.

Exemplo 1.3.2

Consideremos o caso em que $X = \{a,b,c\}$ e $Y = \{m,n\}$. Como o produto cartesiano $X \times Y$ é o conjunto de todos os pares ordenados com abscissa em X e ordenada em Y, temos

$$X \times Y = \{(a,m), (a,n), (b,m), (b,n), (c,m), (c,n)\}.$$

Notemos que o par (n,a) não pertence a $X \times Y$. Contudo, se escrevermos o produto cartesiano $Y \times X$, então teremos o conjunto de todos os pares ordenados com abscissa em Y e ordenada em X e, assim,

$$Y \times X = \{(m,a), (n,a), (m,b), (n,b), (m,c), (n,c)\}.$$

Note que, como ilustrado neste exemplo, em geral, $X \times Y \neq Y \times X$.

Também podemos escrever o produto cartesiano $X \times X$, em que todos os pares ordenados têm abscissa e ordenada em X:

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

RELAÇÕES

Os subconjuntos de um produto cartesiano recebem um nome especial:

Definição 1.3.3

Sejam X e Y dois conjuntos. Todo subconjunto R de $X \times Y$ é chamado de *relação de X em Y*.

Quando $X = Y$, dizemos que R é uma *relação sobre X* (veremos que relações desse tipo têm interesse especial). Note que uma relação de X em Y é um conjunto de pares ordenados. Também observe que $X \times Y$ e Ø sempre são relações de X em Y (por serem subconjuntos de $X \times Y$).

Os pares ordenados que são elementos de uma relação podem ser tratados de diferentes maneiras. A título de linguagem matemática, podemos dizer que: "o par ordenado (x, y) pertence à relação R"; "x está relacionado com y pela relação R"; ou simplesmente "x se relaciona com y", quando não há risco de confusão quanto à relação utilizada.

Em símbolos, escrevemos: $(x, y) \in R$ e $(t, z) \notin R$ quando o par (x, y) pertence à relação R e o par (t, z) não pertence.

Exemplo 1.3.4

Consideremos o caso em que $X = \{a,b,c\}$ e $Y = \{m,n\}$. Vimos que

$$X \times Y = \{(a,m), (a,n), (b,m), (b,n), (c,m), (c,n)\}.$$

Dessa forma, algumas relações de X em Y são:

$$R_1 = \{(a,m)\},\ R_2 = \{(b,n)\},\ R_3 = \{(b,m),\ (c,n)\} \text{ e } R_4 = \{(a,m), (b,n), (c,n)\}.$$

Notemos que $(b,m) \in R_3$, enquanto $(a,n) \notin R_4$. Para listar todas as relações de X em Y, basta lembrar a discussão que fizemos para as partes de um conjunto. Assim, todas as relações de $X \times Y$ podem ser encontradas no conjunto $\wp(X \times Y)$, que possui $2^6 = 64$ elementos.

DOMÍNIO E IMAGEM DE UMA RELAÇÃO

Nos exemplos anteriores é possível ver que nem todos os elementos dos conjuntos X e Y formam par numa relação. Aqueles que formam pertencem a subconjuntos de X e Y que, por isso, recebem nomes especiais.

Definição 1.3.5

Sejam X e Y dois conjuntos e R uma relação de X em Y. O *domínio* e a *imagem* de R são, respectivamente, os conjuntos

$$D(R) = \{x \in X \mid (x,y) \in R \text{ para algum } y \in Y\}$$

e

$$\text{Im}(R) = \{y \in Y \mid (x,y) \in R \text{ para algum } x \in X\}.$$

Vale notar que o domínio de uma relação de X em Y é um subconjunto de X, enquanto a imagem é um subconjunto de Y.

Exemplo 1.3.6

Sejam $X = \{x,y,z\}$ e $Y = \{a,b\}$, consideremos as seguintes relações de X em Y:

$$R_1 = \{(x,a), (y,a), (z,a)\} \text{ e } R_2 = \{(x,a), (x,b), (y,b)\}.$$

Temos

$$D(R_1) = \{x,y,z\},\ \text{Im}(R_1) = \{a\} \text{ e } D(R_2) = \{x,y\},\ \text{Im}(R_2) = \{a,b\}.$$

1.4 RELAÇÕES DE EQUIVALÊNCIA

Vimos que é natural definir uma relação R de um conjunto X nele mesmo. Algumas relações desse tipo merecem destaque e serão discutidas a partir de agora. Nosso interesse aqui é descrever um tipo bastante especial de relação: a relação de equivalência. O conceito de relação de equivalência aparece numa posição de grande destaque na Matemática.

Definição 1.4.1

Dizemos que a relação R sobre um dado conjunto não vazio X é uma *relação de equivalência* sobre X se R satisfaz as propriedades a seguir.

(*i*) $(x,x) \in R$, para todo $x \in X$ (*propriedade reflexiva*).

(*ii*) Se x e y são elementos de X tais que $(x,y) \in R$, então $(y,x) \in R$ (*propriedade simétrica*).

(*iii*) Se x, y e z são elementos de X tais que $(x,y) \in R$ e $(y,z) \in R$, então $(x,z) \in R$ (*propriedade transitiva*).

Qual é o domínio de uma relação que satisfaz as condições da Definição 1.4.1? Com um olhar na Definição 1.3.5, a propriedade reflexiva fornece a resposta: $D(R) = X$. Da mesma maneira, $\text{Im}(R) = X$.

Exemplo 1.4.2

Consideremos o caso em que X é o conjunto dos inteiros não nulos e

$$R = \left\{ (x,y) \in \mathbb{Z}^* \times \mathbb{Z}^* \;\middle|\; \text{existe algum } n \in \mathbb{Z} \text{ tal que } \frac{x}{y} = 2^n \right\}.$$

Nossa intenção é mostrar que R é uma relação de equivalência sobre $\mathbb{Z}^*$.

(*i*) Para verificar a propriedade reflexiva, temos de escolher um elemento $x \in \mathbb{Z}^*$ qualquer e mostrar que $(x,x) \in R$, ou seja, que existe um inteiro n tal que $\frac{x}{x} = 2^n$. Como $\frac{x}{x} = 1$, vemos que basta tomar $n = 0$.

(*ii*) Para verificar a propriedade simétrica, supomos inicialmente que $(x,y) \in R$, o que significa que existe um inteiro, digamos n_0, tal que $\frac{x}{y} = 2^{n_0}$. Nosso objetivo é verificar que $(y,x) \in R$, o que é feito encontrando-se um inteiro n tal que $\frac{y}{x} = 2^n$. Observando que $\frac{y}{x} = \left(\frac{x}{y}\right)^{-1} = \left(2^{n_0}\right)^{-1} = 2^{-n_0}$, vemos que basta tomar $n = -n_0$. Assim, a relação é simétrica.

(*iii*) Para verificar a propriedade transitiva, supomos inicialmente que $(x, y) \in R$ e que $(y, z) \in R$, o que significa que existem n_0, $n_1 \in \mathbb{Z}$ tais que

$$\frac{x}{y} = 2^{n_0} \text{ e } \frac{y}{z} = 2^{n_1}.$$

Devemos mostrar que $(x, z) \in R$, o que significa encontrar um inteiro n tal que $\frac{x}{z} = 2^n$. Multiplicando-se as duas igualdades anteriores, obtemos $\frac{x}{y} \cdot \frac{y}{z} = 2^{n_0} \cdot 2^{n_1}$, de onde $\frac{x}{z} = 2^{n_0+n_1}$. Assim, basta tomar $n = n_0 + n_1$ e concluir que a relação é transitiva e, portanto, uma relação de equivalência sobre $\mathbb{Z}^*$.

- **Notação:** Para representar o fato de que o par (x, y) está na relação de equivalência R sobre o conjunto X, é comum usarmos a notação $x \equiv y \pmod{R}$, que é lida assim: *x* é *equivalente* a *y módulo R*, ou simplesmente *x* é *equivalente* a *y*.

  No Exemplo 1.4.2, vemos que os números 48 e 3 são equivalentes, pois $\frac{48}{3} = 16 = 2^4$, então escrevemos $48 \equiv 3 \pmod{R}$.

Exemplo 1.4.3

Consideremos o caso em que X é o conjunto dos inteiros não nulos e $R = \{(x, y) \in \mathbb{Z}^* \times \mathbb{Z}^* \mid mdc(x, y) = 1\}$, em que $mdc(x, y)$ representa o máximo divisor comum dos elementos *x* e *y*.

É fácil ver que a relação R é simétrica, pois $mdc(x, y) = mdc(y, x)$ (assim, se $x, y \in \mathbb{Z}^*$ satisfazem $mdc(x, y) = 1$, então $mdc(y, x) = 1$). Mas a relação não é reflexiva: basta notar que, por exemplo, $mdc(7,7) \neq 1$; também não é transitiva, pois, embora $mdc(10,21) = 1$ e $mdc(21,55) = 1$, temos $mdc(10,55) = 5 \neq 1$. Assim, R não é uma relação de equivalência sobre $\mathbb{Z}^*$.

Definição 1.4.4

Seja R uma relação de equivalência sobre o conjunto não vazio X e seja $x \in X$. A *classe de equivalência* de *x* segundo a relação R, denotada por $C_R(x)$, é o conjunto $\{y \in X \mid y \equiv x \pmod{R}\}$.

Em palavras, $C_R(x)$ é o conjunto de todos os elementos de X que são equivalentes a *x* segundo a relação R, ou ainda o conjunto de todos os elementos de X que se relacionam com *x* pela relação R. Outra maneira de escrever esse conjunto é da forma

$$C_R(x) = \{y \in X \mid (y, x) \in R\}.$$

Definição 1.4.5

O conjunto formado pelas classes de equivalência módulo R é chamado de *conjunto quociente de X por R* e denotado por X / R.

Exemplo 1.4.6

Voltando à relação de equivalência dada no Exemplo 1.4.2, vamos encontrar todos os elementos da classe de equivalência do número 3, ou seja, determinaremos o conjunto $C_R(3) = \{y \in X \mid y \equiv 3 \pmod{R}\}$. Já vimos que 48 é um elemento de $C_R(3)$; pela propriedade reflexiva, também o é o próprio número 3. Um número inteiro não nulo y está em $C_R(3)$ se, e somente se, $\frac{y}{3} = 2^n$ para algum inteiro n, ou, equivalentemente, se $y = 3 \cdot 2^n$ para algum n. Fazendo n percorrer o conjunto dos inteiros, obtemos todos os elementos de $C_R(3) = \{3,6,12,24,48,\ldots\}$.

E a classe de equivalência do número 2? Um procedimento análogo mostra que $C_R(2) = \{1,2,4,8,16,\ldots\}$ é o conjunto das potências de 2. O leitor pode observar que os elementos de $C_R(3)$ podem ser obtidos multiplicando-se cada elemento de $C_R(2)$ por 3. Isso é verdade também para a classe de equivalência do 5 ($C_R(5) = \{5,10,20,40,80,\ldots\}$), do 7 ($C_R(7) = \{7,14,28,56,112,\ldots\}$), e de qualquer outro número. Observemos ainda que $C_R(4)$ é igual a $C_R(2)$ e que $C_R(2)$ e $C_R(5)$ não têm nem mesmo um só elemento em comum.

Listando mais classes de equivalência, podemos observar que, se um número já ocorreu em uma das classes, então a sua classe é exatamente igual àquela em que ele ocorreu; também notamos que classes distintas não possuem elementos comuns – elas são sempre disjuntas. Mais ainda, se reunirmos todas as classes de equivalência, teremos todo o conjunto $\mathbb{Z}^*$. Esses fatos são casos particulares do teorema a seguir.

Teorema 1.4.7 (*Teorema Fundamental das Relações de Equivalência*)

Sejam X um conjunto não vazio e R uma relação de equivalência sobre X. Então:

(a) $C_R(x) \neq \varnothing$, para todo $x \in X$.

(b) Se $y \in C_R(x)$, então $x \in C_R(y)$.

(c) Dados dois elementos $x, y \in X$, ou $C_R(x) = C_R(y)$, ou $C_R(x) \cap C_R(y) = \varnothing$.

(d) $X = \bigcup_{x \in X} C_R(x)$.

Demonstração

Algumas verificações são bastante simples.

(a) Basta notar que, pela propriedade reflexiva, dado qualquer $x \in X$, pelo menos o próprio x está em $C_R(x)$, donde $C_R(x) \neq \varnothing$, para todo $x \in X$.

(b) É consequência imediata da definição de classe de equivalência e da propriedade simétrica que, uma vez que $y \in C_R(x)$, por definição, $y \equiv x \pmod{R}$, ou seja, $(y,x) \in R$ e, pela simetria, $(x,y) \in R$, donde $x \equiv y \pmod{R}$ e $x \in C_R(y)$.

(c) Provaremos que, se $C_R(x) \cap C_R(y) \neq \varnothing$, então $C_R(x) = C_R(y)$. Supondo $C_R(x) \cap C_R(y) \neq \varnothing$, podemos tomar um elemento $a \in C_R(x) \cap C_R(y)$. Como a está em $C_R(x)$ e em $C_R(y)$, concluímos que a é equivalente tanto a x quanto a y módulo R. Pela simetria e pela transitividade de R, temos $x \equiv y \pmod{R}$. Escolhamos agora um elemento $b \in C_R(x)$ qualquer. Então, $b \equiv x \pmod{R}$; e, como $x \equiv y \pmod{R}$, usamos novamente a transitividade para concluir que $b \equiv y \pmod{R}$, de modo que $b \in C_R(y)$, o que mostra que $C_R(x) \subset C_R(y)$. Seguindo um raciocínio completamente análogo, mostramos que $C_R(y) \subset C_R(x)$, o que nos dá $C_R(x) = C_R(y)$, como queríamos.

(d) A notação $\bigcup_{x \in X} C_R(x)$ representa a união das classes de equivalência de todos os elementos de X, sendo assim $\bigcup_{x \in X} C_R(x)$ um subconjunto de X. Como cada elemento de X está em alguma classe, a união $\bigcup_{x \in X} C_R(x)$ contém todos os elementos de X. Portanto, $X = \bigcup_{x \in X} C_R(x)$. ▪

Uma observação final: os itens (c) e (d) do Teorema 1.4.7 mostram que, eliminando as classes de equivalência que são iguais na união $\bigcup_{x \in X} C_R(x)$, podemos escrever o conjunto X como união disjunta de classes de equivalência. Esse fato é de grande importância, conforme a experiência mostrará ao leitor. Isso será formalizado a seguir.

PARTIÇÃO DE UM CONJUNTO

Definição 1.4.8

Seja X um conjunto não vazio. Dizemos que uma classe F de subconjuntos não vazios de X é uma *partição* de X quando:

(*i*) dois membros quaisquer de F ou são iguais ou são disjuntos;

(*ii*) a união de todos os membros de F é igual a X.

Exemplo 1.4.9

$F = \{\{0,1,3\},\{4\},\{5,6\}\}$ é uma partição do conjunto $X = \{0,1,3,4,5,6\}$.

Exemplo 1.4.10

Para a relação de equivalência do Exemplo 1.4.2, no Exemplo 1.4.6, listamos alguns elementos da partição que ela estabelece sobre $\mathbb{Z}^*$. Foram as classes $C_R(2)$, $C_R(3)$,

$C_R(5)$ e $C_R(7)$. Convidamos o leitor a determinar os elementos de outras classes. O que você observa? Consegue ter uma ideia de uma partição definida por aquela relação?

Um fato bem interessante é que uma relação de equivalência definida sobre um conjunto não vazio X sempre determina uma partição desse conjunto. Esse será um resultado bastante utilizado neste livro e, por isso, o registraremos a seguir. Também é verdade que, dada uma partição do conjunto X, é possível estabelecer sobre X uma relação de equivalência associada a essa partição (para uma demonstração, veja [13]).

Teorema 1.4.11

Se R é uma relação de equivalência definida sobre um conjunto não vazio X, então o conjunto quociente X / R é uma partição de X.

Demonstração

Isso é exatamente o que demonstramos nos itens (c) e (d) do Teorema 1.4.7. ▪

1.5 A RELAÇÃO DE CONGRUÊNCIA MÓDULO *m*

Nesta seção apresentamos um tipo bastante especial e importante de relação de equivalência, a relação de congruência módulo m. Trata-se de uma relação definida sobre o conjunto dos números inteiros e, assim, precisaremos utilizar conceitos, notações e teoremas relacionados com esse conjunto numérico, como a noção de divisibilidade e o Algoritmo da Divisão. Para esta seção, supomos que o leitor possui familiaridade com a teoria de divisibilidade de números inteiros e nos limitaremos aqui a enunciar os principais resultados à medida que forem sendo aplicados. O leitor que sentir necessidade de rever os conceitos e as notações relacionados, ou desejar analisar as demonstrações dos resultados aplicados, poderá encontrá-los em [14], que apresenta uma exposição detalhada.

Definição 1.5.1

Sejam a e b dois inteiros e m um inteiro maior que 1. Dizemos que a é *congruente* a b módulo m se m divide a diferença $a - b$.

- **Notação:** Escrevemos $a \equiv b \pmod{m}$ para representar a afirmação "a é congruente a b módulo m".

Observemos que o fato de a ser *congruente* a b módulo m pode ser escrito nas seguintes formas:

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b) \Leftrightarrow \text{existe } q \in \mathbb{Z} \text{ tal que } a - b = mq.$$

No caso em que m não divide a diferença $a - b$, dizemos que "*a não é congruente* a b módulo m" ou que "a é *incongruente* a b módulo m" e usamos a notação $a \not\equiv b \pmod{m}$. Por exemplo, $18 \not\equiv 4 \pmod{3}$, pois 3 não divide 18 – 4 = 14.

Exemplo 1.5.2

Consideremos $m = 9$ e notemos que 61 é congruente a 43 módulo 9, pois 61 – 43 = 18, que é divisível por 9. Também é verdade que 61 ≡ 7 (mod 9), pois 61 – 7 = 54, que é múltiplo de 9. Ainda, ao se efetuar a divisão de 61 por 9, obtemos resto 7, e isso nos dá uma indicação do resultado enunciado na próxima proposição.

A demonstração de tal proposição faz uso do Algoritmo da Divisão:

Teorema (*Algoritmo da Divisão*). Se a e m são dois inteiros quaisquer, com $m \neq 0$, então existem, e são únicos, os inteiros q e r que satisfazem as seguintes condições: $a = mq + r$ e $0 \leq r < |m|$.

Com exceção das considerações sobre o sinal, o Algoritmo da Divisão se baseia no fato de que, necessariamente, o número inteiro a está compreendido entre os dois múltiplos consecutivos de m. Veja os detalhes em [14].

Proposição 1.5.3

Sejam a um inteiro qualquer, r um inteiro não negativo e m um inteiro maior que 1. Se r é o resto da divisão euclidiana de a por m, então

$$a \equiv r \pmod{m}.$$

Demonstração

Aplicando o Algoritmo da Divisão, podemos afirmar que existe um inteiro q tal que

$$a = mq + r.$$

Portanto,

$$a - r = mq.$$

Essa igualdade significa que m divide $a - r$. Logo, pela Definição 1.5.1, $a \equiv r \pmod{m}$, como queríamos. ▪

A definição de congruência de números inteiros define uma relação de equivalência muito interessante sobre $\mathbb{Z}$, e dessa relação vem o aparato básico para compreendermos as definições e propriedades das operações módulo *m* apresentadas no Capítulo 2.

Proposição 1.5.4

Se *m* é um inteiro maior que 1, então o conjunto

$$R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \pmod{m}\}$$

é uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração

É necessário demonstrar que *R* satisfaz as propriedades *reflexiva*, *simétrica* e *transitiva* em $\mathbb{Z}$, que, no caso em questão, se escrevem, respectivamente:

(*i*) $a \equiv a \pmod{m}$, para qualquer inteiro *a*.

(*ii*) Se *a* e *b* são inteiros tais que $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

(*iii*) Se *a*, *b* e *c* são inteiros tais que $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Para mostrarmos a propriedade reflexiva, precisamos verificar, segundo a Definição 1.5.1, que $a - a$ é múltiplo de *m*. Basta ver que $a - a$ é igual a zero, múltiplo de *m*.

Para a propriedade simétrica, temos como premissa $a \equiv b \pmod{m}$, ou seja, *m* divide $a - b$, ou ainda, existe um inteiro *q* tal que $a - b = mq$. Multiplicando essa igualdade por –1, obtemos $b - a = m(-q)$, donde *m* divide $b - a$, ou seja, $b \equiv a \pmod{m}$.

Na propriedade transitiva, temos por premissa $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, de onde existem inteiros q_1 e q_2 tais que $a - b = mq_1$ e $b - c = mq_2$. Adicionando-se essas igualdades, obtemos $a - c = m(q_1 + q_2)$, donde *m* divide $a - c$, ou seja, $a \equiv c \pmod{m}$. ▪

Exemplo 1.5.5

Consideremos o caso em que $m = 7$. Quais são os inteiros congruentes a 6 módulo 7? Em outras palavras, qual a classe de equivalência do número 6 módulo 7? Para responder a essa pergunta, devemos encontrar todos os elementos do conjunto

$$C_7(6) = \{x \in \mathbb{Z} \mid x \equiv 6 \pmod{7}\}.$$

Ora, a propriedade reflexiva afirma que pelo menos o próprio número 6 está nessa classe, pois $6 \equiv 6 \pmod{7}$. Uma inspeção entre os números inteiros mostra que $13 \equiv 6$

(mod 7), $20 \equiv 6 \pmod 7$, $27 \equiv 6 \pmod 7$, $-1 \equiv 6 \pmod 7$ e $-8 \equiv 6 \pmod 7$, de modo que 13, 20, 27, –1 e –8 também estão na classe $C_7(6)$. Escrevendo de forma mais completa, temos

$$C_7(6) = \{\ldots, -22, -15, -8, -1, 6, 13, 20, 27, 34, 41, \ldots\}.$$

Notemos que a classe contém infinitos elementos. Além disso, na ordem em que colocamos os números, temos uma espécie de progressão aritmética de razão 7, ou seja, os números aumentam de 7 em 7. O leitor certamente notará outras características nessa classe, principalmente se compará-la com as outras classes módulo 7, que apresentamos a seguir.

$$C_7(0) = \{\ldots, -28, -21, -14, -7, 0, 7, 14, 21, 28, 35, \ldots\}$$

$$C_7(1) = \{\ldots, -27, -20, -13, -6, 1, 8, 15, 22, 29, 36, \ldots\}$$

$$C_7(2) = \{\ldots, -26, -19, -12, -5, 2, 9, 16, 23, 30, 37, \ldots\}$$

$$C_7(3) = \{\ldots, -25, -18, -11, -4, 3, 10, 17, 24, 31, 38, \ldots\}$$

$$C_7(4) = \{\ldots, -24, -17, -10, -3, 4, 11, 18, 25, 32, 39, \ldots\}$$

$$C_7(5) = \{\ldots, -23, -16, -9, -2, 5, 12, 19, 26, 33, 40, \ldots\}$$

Listamos as classes de equivalência módulo 7 dos números de 0 a 6. Qual seria, por exemplo, a classe de equivalência módulo 7 do número –1? E do número 7? Podemos verificar rapidamente que $C_7(-1) = C_7(6)$ e que $C_7(7) = C_7(0)$. E qual a classe de equivalência módulo 7 do número 1.798? Afirmamos que é uma daquelas listadas e, para saber qual, usamos a Proposição 1.5.3: o resto da divisão euclidiana de 1.798 por 7 é 6. Logo, $C_7(1.798) = C_7(6)$.

Em outras palavras, o que estamos tentando dizer é que, quando olhamos módulo 7, qualquer inteiro estará em uma das classes de $C_7(0)$ a $C_7(6)$, ou seja, a união dessas classes esgota o conjunto dos números inteiros. Além disso, duas classes distintas não têm nem mesmo um só elemento em comum. Isso nos mostra que determinamos uma partição de $\mathbb{Z}$. Lembrando que o conjunto quociente de $\mathbb{Z}$ pela relação de congruência é formado por todas as classes de equivalência que a relação determina sobre $\mathbb{Z}$, temos, no caso da relação de congruência módulo 7, que o conjunto quociente de $\mathbb{Z}$ por essa relação é dado por

$$\mathbb{Z}/R = \{C_7(0), C_7(1), C_7(2), C_7(3), C_7(4), C_7(5), C_7(6)\}$$

e isso significa que

$$\mathbb{Z} = C_7(0) \cup C_7(1) \cup C_7(2) \cup C_7(3) \cup C_7(4) \cup C_7(5) \cup C_7(6).$$

Propriedades naturais estão claramente expostas nos conjuntos que formam as classes de equivalência obtidas: primeiro, quaisquer dois elementos em uma mesma classe são congruentes módulo 7 e, segundo, se tomarmos quaisquer dois elementos em classes distintas, eles não são congruentes módulo 7. É importante notar ainda que há exatamente 7 classes de equivalência distintas módulo 7. E perguntamos: o que o número 7 tem de especial nesta história? Nada! Note que, se tomarmos qualquer outro inteiro maior que 1 para o módulo, todas essas características poderão ser observadas. Que tal o leitor tentar encontrar todas as classes de equivalência módulo 8 para verificar? Escreva o conjunto quociente para esse caso.

- ***Observações***

  (i) A classe de equivalência de $x \in \mathbb{Z}$ módulo m é conhecida como a *classe de congruência de* $x \in \mathbb{Z}$ *módulo* m.

  (ii) Vale notar que dois inteiros são congruentes módulo m se, e somente se, deixam o mesmo resto na divisão euclidiana por m. Uma maneira de demonstrar isso é obter essa propriedade como consequência da Proposição 1.5.3, das propriedades simétrica e transitiva e do item (i) da Proposição 1.5.6 a seguir.

A próxima proposição lista algumas das principais propriedades da relação de congruência módulo m. Essas propriedades nos permitem operar no conjunto quociente que a relação de congruência define sobre o conjunto $\mathbb{Z}$ quase da mesma maneira que operamos com os números inteiros.

Proposição 1.5.6

Seja m um inteiro maior que 1.

(a) Se a e b são inteiros tais que $a \equiv b \pmod{m}$, então $a - b \equiv 0 \pmod{m}$.

(b) Se a, b, c e d são inteiros tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

(c) Se a, b, c e d são inteiros tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a - c \equiv b - d \pmod{m}$.

(d) Se a, b, c e d são inteiros tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.

(e) Se a e b são inteiros tais que $a \equiv b \pmod{m}$, então $ax \equiv bx \pmod{m}$, para todo inteiro x.

(f) Seja d um inteiro tal que $mdc(d,m) = 1$. Se a e b são inteiros tais que $ad \equiv bd \pmod{m}$, então $a \equiv b \pmod{m}$.

(g) Se a, b e d são inteiros tais que $ad \equiv bd \pmod{md}$, então $a \equiv b \pmod{m}$.

(h) Se a, b, c e d são inteiros tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ax \equiv c \pmod{m}$ se, e somente se, $bx \equiv d \pmod{m}$, para todo inteiro x.

(i) Sejam a e b inteiros tais que $0 \leq a \leq m-1$ e $0 \leq b \leq m-1$. Se $a \equiv b \pmod{m}$, então $a = b$.

(j) Se a e b são inteiros tais que $a \equiv b \pmod{m}$, então $a^x \equiv b^x \pmod{m}$, para todo número natural x.

Demonstração

Demonstraremos alguns itens e outros deixaremos como exercícios ao leitor.

(b) As premissas nos dizem que m divide $a - b$ e m divide $c - d$. Assim, existem inteiros q_1 e q_2 tais que $a - b = mq_1$ e $c - d = mq_2$, de onde concluímos que $(a - b) + (c - d) = m(q_1 + q_2)$. Reagrupando as parcelas dessa última soma, obtemos que m divide $(a + c) - (b + d)$, que é exatamente a conclusão desejada.

(d) Das hipóteses, existem inteiros q_1 e q_2 tais que $a - b = mq_1$ e $c - d = mq_2$. Multiplicando-se os dois membros da primeira igualdade por c e os dois membros da segunda igualdade por b, obtemos $ac - bc = mq_1c$ e $bc - bd = mq_2b$. Adicionando-se essas últimas igualdades, obtemos $(ac - bc) + (bc - bd) = mq_1c + mq_2b$, o que nos dá $ac - bd = m(q_1c + q_2b)$. Com isso, m divide $ac - bd$, o que é equivalente a afirmar que $ac \equiv bd \pmod{m}$.

(f) Para a demonstração desta parte precisamos do seguinte resultado da teoria de divisibilidade de inteiros:

Proposição. Sejam $a,b,c \in \mathbb{Z}$ tais que a e b são primos entre si. Se $a \mid bc$, então $a \mid c$.

[Sua veracidade se baseia no fato de que podemos sempre escrever o número 1 como combinação linear entre números primos entre si; veja os detalhes em [14].]

Quanto à demonstração da parte (f), como $mdc(d,m) = 1$, d e m são primos entre si. Por outro lado, como $ad \equiv bd \pmod{m}$, temos que m divide $ad - bd = d(a - b)$. Aplicando a proposição mencionada, vemos que m divide $a - b$, o que é equivalente a $a \equiv b \pmod{m}$.

(g) A hipótese implica que existe um inteiro q tal que $ad - bd = mdq$. Aplicando a Lei do Cancelamento da Multiplicação a essa igualdade, temos $a - b = mq$. Isso conduz à conclusão $a \equiv b \pmod{m}$.

(h) Aqui, demonstraremos a parte *se* da proposição e deixaremos a parte *somente se* como um exercício. Além das hipóteses $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, temos ainda a premissa $ax \equiv c \pmod{m}$. Usando a parte (e) e o fato de a congruência ser uma relação de equivalência, obtemos: $ax \equiv bx \pmod{m}$ e $bx \equiv ax \equiv c \equiv d \pmod{m}$.

(i) Como $0 \le a \le m-1$ e $0 \le b \le m-1$, obtemos

$$\begin{cases} 0 & \le & a & \le & m-1 \\ -(m-1) & \le & -b & \le & 0 \end{cases}.$$

Adicionando-se essas desigualdades, obtemos

$$-(m-1) \le a-b \le m-1.$$

Por outro lado, da hipótese $a \equiv b \pmod{m}$, vemos que $a - b$ é múltiplo de m. Agora, o único múltiplo de m entre $-(m-1)$ e $m-1$ é zero (justifique!). Assim, $a - b = 0$, ou seja, $a = b$. Isso finaliza a demonstração de (i).

[Vale comentar o significado da contrarrecíproca (contrapositiva) da propriedade (i): ela nos diz que, tomados dois inteiros distintos no conjunto $\{0,1,2,\ldots,m-1\}$, eles são incongruentes módulo m. Ou seja, não existem dois inteiros distintos não negativos menores que m que são congruentes módulo m.]

(j) Basta aplicarmos repetidas vezes a parte (d) já provada. ▪

Algumas considerações sobre a Proposição 1.5.6 são bastante pertinentes:

(*i*) As partes (b), (c) e (d) nos dizem que adicionando, subtraindo ou multiplicando elementos congruentes aos dois membros de uma congruência ela se mantém verdadeira.

(*ii*) Casos particulares das partes (b) e (c) surgem quando utilizamos a propriedade reflexiva da relação de congruência e, da mesma forma, podemos ver a parte (e) como um caso particular da parte (d): uma vez que $c \equiv c \pmod{m}$ para qualquer $c \in \mathbb{Z}$, então $a \equiv b \pmod{m}$ implica

$$a + c \equiv b + c \pmod{m},\ a - c \equiv b - c \pmod{m} \text{ e } ac \equiv bc \pmod{m}.$$

(*iii*) As partes (f) e (g), cada uma a seu modo, nos dizem que a *Lei do Cancelamento* vale para as congruências.

1.6 EQUAÇÕES DE CONGRUÊNCIAS LINEARES

Nosso interesse aqui está voltado ao estudo (no caso linear) de equações envolvendo uma congruência. Chamamos de *equação de congruência linear* toda equação da forma $ax \equiv b \pmod{m}$, em que $a, b, m \in \mathbb{Z},\ m > 1$ e x é uma incógnita que deve assumir valores inteiros (quando possível). Dizemos proceder à *resolução* da equação quando

investigamos a possível existência de inteiros x que a satisfaçam, sendo tais valores chamados *soluções* da equação.

Sempre que resolver equações de congruências lineares, o leitor poderá recorrer às Proposições 1.5.3, 1.5.4 e 1.5.6 para tentar simplificar a equação a ser resolvida. Assim, é desejável que o leitor adquira destreza para operar com as propriedades das congruências listadas nessas proposições. No exemplo a seguir, deixamos parte das justificativas de cada simplificação a cargo do leitor para que possa treinar o uso das proposições. Este exemplo tem também a função de preparar o espírito do leitor para a demonstração do próximo teorema.

Exemplo 1.6.1

Consideremos o problema de resolver a seguinte equação de congruência linear: $77x + 8 \equiv 106 \pmod{28}$. Temos as seguintes simplificações:

- $77x \equiv 98 \pmod{28}$, pela Proposição 1.5.6(c).
- $21x \equiv 14 \pmod{28}$, pelas Proposições 1.5.3 e 1.5.6(h).
- $3x \equiv 2 \pmod{4}$, pela Proposição 1.5.6(g) .

Agora, se existir um inteiro x_0 que satisfaça a última equação, então 4 divide o número $3x_0 - 2$. Mas isso significa que existe um inteiro y_0 tal que $3x_0 - 2 = 4y_0$, o que nos dá $3x_0 - 4y_0 = 2$. Em outras palavras, o problema de resolver a equação de congruência $3x \equiv 2 \pmod{4}$ é equivalente ao de resolver a equação diofantina linear[2] $3x - 4y = 2$. Um olhar atento a $3x - 4y = 2$ nos mostra que $x_0 = 2$ e $y_0 = 1$ formam uma solução. Logo, $x_0 = 2$ é uma solução de $3x \equiv 2 \pmod{4}$ e, portanto, de $77x + 8 \equiv 106 \pmod{28}$.

As Proposições 1.5.3, 1.5.4 e 1.5.6 permitem escrever qualquer equação de congruência linear na forma $ax \equiv b \pmod{m}$. O Teorema 1.6.2, a seguir, fornece uma maneira de se verificar se a equação tem solução. A demonstração lembrará muito a discussão do exemplo anterior, e se baseia em um importante resultado da teoria de divisibilidade:

Teorema. A equação diofantina linear $ax + by = c$, de incógnitas x e y, tem solução se, e somente se, $mdc(a,b)$ divide c.

[Sua veracidade se baseia no fato de que podemos sempre escrever o máximo divisor comum entre dois inteiros como combinação linear entre esses inteiros; veja os detalhes em [14].]

[2] Uma equação diofantina linear a duas variáveis é uma equação da forma $ax + by = c$, com a, b e c coeficientes inteiros, para a qual se deseja conhecer soluções constituídas por pares ordenados (x, y) de números inteiros.

Teorema 1.6.2

Sejam a e b inteiros e m um inteiro maior que 1. A equação $ax \equiv b \pmod{m}$ tem solução se, e somente se, $mdc(a,m)$ divide b.

Demonstração

Se existir um inteiro x_0 que satisfaça a equação $ax \equiv b \pmod{m}$, então teremos m dividindo $ax_0 - b$. Isso significa a existência de um inteiro y_0 tal que $ax_0 - b = my_0$, ou seja, tal que $ax_0 - my_0 = b$. Dito de outra maneira, o problema de resolver a equação de congruência linear $ax \equiv b \pmod{m}$ com incógnita x é equivalente ao de resolver a equação $ax + (-my) = b$ com incógnitas x e y. Pelo teorema citado há pouco, essa equação tem solução se, e somente se, $mdc(a,-m) = mdc(a,m)$ divide b. Isso é exatamente o que queríamos demonstrar. ▪

- ***Observação:*** seja x_0 uma solução particular da equação de congruência linear $ax \equiv b \pmod{m}$, isto é, $ax_0 \equiv b \pmod{m}$, e suponhamos que x_1 seja um inteiro tal que $x_1 \equiv x_0 \pmod{m}$. Então, x_1 também é solução de $ax \equiv b \pmod{m}$, pois

$$x_1 \equiv x_0 \pmod{m} \Leftrightarrow ax_1 \equiv ax_0 \pmod{m} \Leftrightarrow ax_1 \equiv b \pmod{m}.$$

Portanto, se um elemento de uma classe de congruência módulo m é solução de $ax \equiv b \pmod{m}$, então todo elemento da referida classe também é solução. Neste momento é razoável perguntar: serão essas todas as soluções?

A proposição a seguir nos mostra uma maneira de encontrar todas as soluções de uma equação de congruência linear. Sua demonstração será omitida porque futuramente, neste livro, estaremos interessados apenas em saber se uma equação desse tipo admite ou não solução e conhecer uma solução em particular (aplicaremos isso no estudo de elementos simétricos de um grupo). Uma discussão mais detalhada a respeito do conjunto de todas as soluções pode ser encontrada em [14].

Proposição 1.6.3

Sejam a e b inteiros e m um inteiro maior que 1. Se a equação de congruência linear $ax \equiv b \pmod{m}$ possui solução x_0, então a equação possui infinitas soluções e o conjunto de todas as soluções é

$$S = \left\{ x_0 + \frac{m}{d}t \;\middle|\; t \in \mathbb{Z} \right\},$$

onde $d = mdc(a,m)$.

Exemplo 1.6.4

Determinemos o conjunto de todas as soluções da equação de congruência linear: $77x + 8 \equiv 106 \pmod{28}$.

Vimos no Exemplo 1.6.1 que essa equação é equivalente a $77x \equiv 98 \pmod{28}$ e que $x_0 = 2$ é uma solução particular. Sendo $mdc(77,28) = 7$, pela Proposição 1.6.3, temos que $S = \{2 + 4t \mid t \in \mathbb{Z}\}$ é o conjunto de todas as soluções da equação. Note que esse conjunto é exatamente a classe de congruência $C_4(2)$.

Para finalizarmos nossa discussão a respeito das soluções de uma equação de congruência, voltemos à pergunta apresentada na observação anterior. Com o que mostramos lá, sabemos que todo elemento da classe $C_{28}(2)$ é uma solução da equação, no entanto vemos que essa classe não contém todas as soluções. Note que $C_{28}(2) \subset C_4(2)$.

1.7 O CONCEITO DE FUNÇÃO

Agora estudaremos um importante tipo de relação entre dois conjuntos: as funções. Trata-se de um dos mais importantes conceitos da Matemática, uma vez que encontra utilizações nas mais diversas áreas do conhecimento humano, fornecendo uma poderosa ferramenta para a modelagem de situações. Abordaremos as funções como tipos especiais de relações em conjuntos, ou seja, como subconjuntos especiais do produto cartesiano entre dois conjuntos para os quais definimos relações entre seus elementos.

Definição 1.7.1

Sejam X e Y dois conjuntos e $f \subset X \times Y$ uma relação. Dizemos que a relação f é uma *função de X em Y* se valem as propriedades a seguir.

(*i*) Para cada elemento $x \in X$ dado, existe um elemento $y \in Y$ tal que $(x, y) \in f$.

(*ii*) Se $x \in X$ e $y, z \in Y$ são elementos tais que $(x, y) \in f$ e $(x, z) \in f$, então $y = z$.

No caso em que $X = Y$ na Definição 1.7.1, dizemos que definimos uma função sobre o conjunto X. O item (*i*) da definição significa que a relação definida é *total* e o item (*ii*) significa que a relação é *unívoca*. Note que a definição apresentada tem uma universalidade impressionante, pois os conjuntos X e Y podem ser, a princípio, quaisquer conjuntos.

Exemplo 1.7.2

Consideremos $X = \mathbb{Z}$, $Y = \mathbb{Q}$ e a seguinte relação de X em Y:

$$f = \left\{ (x, y) \in \mathbb{Z} \times \mathbb{Q} \;\middle|\; y = \frac{2x - 1}{3} \right\}.$$

Mostremos que essa relação é uma função de X em Y. Para verificar a propriedade (*i*) da Definição 1.7.1, basta notar que, para todo inteiro x_0, o número $\frac{2x_0 - 1}{3}$ é racional e forma par com x_0 na relação f. Para a propriedade (*ii*), devemos mostrar que, se $(x_0, y) \in f$ e $(x_0, z) \in f$, então $y = z$. De fato, $(x_0, y) \in f$ implica $y = \frac{2x_0 - 1}{3}$ e $(x_0, z) \in f$ implica $z = \frac{2x_0 - 1}{3}$, de modo que $y = z$. Temos, assim, uma função de $\mathbb{Z}$ em $\mathbb{Q}$.

É importante notar que as propriedades da definição de função são independentes, ou seja, é possível que uma relação cumpra uma das propriedades, mas não a outra. Naturalmente, pode não cumprir nenhuma das duas.

DOMÍNIO E CONTRADOMÍNIO DE UMA FUNÇÃO

No caso em que a relação f de X em Y é uma função, a propriedade (*i*) da Definição 1.7.1 nos diz que $D(f) = X$, ou seja, o domínio de uma função de X em Y é o conjunto X. O conjunto Y é chamado de *contradomínio* de f. É importante notar também que as duas propriedades (*i*) e (*ii*) da definição são equivalentes a esta outra:

- para cada elemento $x \in X$ dado, existe um único elemento $y \in Y$ tal que $(x, y) \in f$.

- **Notação:** Usamos a notação $f : X \to Y$ para expressar o fato de que a relação f de X em Y é uma função. Além disso, dado $x \in X$, o único elemento $y \in Y$ tal que $(x_0, y) \in f$ é chamado de *imagem* de x pela função f e será representado por $y = f(x)$. Nesse caso, dizemos que x é a *variável independente* e y é a *variável dependente*.

Com essas notações, a função f é o seguinte subconjunto de $X \times Y$:

$$f = \{(x, f(x)) \in X \times Y \mid x \in X\}.$$

Exemplo 1.7.3

Para o Exemplo 1.7.2, $D(f) = \mathbb{Z}$ e o contradomínio é o conjunto dos números racionais $\mathbb{Q}$.

IMAGEM DE UMA FUNÇÃO

Seja f uma função de X em Y. Como $D(f) = X$, voltando à Definição 1.3.5, vemos que a *imagem* de f, que é um subconjunto do contradomínio Y, é definida pelo conjunto

$$\text{Im}(f) = \{y \in Y \mid (x, y) \in f, \text{ com } x \in X\}.$$

Segundo a notação anterior, podemos escrever

$$\mathrm{Im}(f) = \{ f(x) \mid x \in X \}.$$

Exemplo 1.7.4

Para o Exemplo 1.7.2, $\mathrm{Im}(f)$ é o conjunto formado por todos os números racionais que se expressam na forma $y = \frac{2x-1}{3}$, com $x \in \mathbb{Z}$. Verifiquemos que esse conjunto não é igual a $\mathbb{Q}$. Seja $y_0 \in \mathbb{Q}$ um elemento qualquer. Devemos verificar se é possível escrevê-lo na forma $y_0 = \frac{2x_0 - 1}{3}$ para algum $x_0 \in \mathbb{Z}$. Assim, teríamos $y_0 = \frac{2x_0 - 1}{3}$, que é equivalente a $3y_0 = 2x_0 - 1$ e equivalente a $x_0 = \frac{3y_0 + 1}{2}$. Observe que este último não necessariamente é um número inteiro, por exemplo, no caso de $y_0 = 0$ teríamos $x_0 = \frac{1}{2}$.

Alguns elementos de $\mathrm{Im}(f)$ são $\frac{-7}{3}, \frac{-5}{3}, -1, \frac{-1}{3}, \frac{1}{3}, 1, \frac{5}{3}, \frac{7}{3}$. Certamente o leitor consegue ter uma ideia de todos os elementos de $\mathrm{Im}(f)$.

IGUALDADE DE FUNÇÕES

Os elementos necessários para construir uma função são dois conjuntos *X* e *Y* para formarem o domínio e o contradomínio, respectivamente, e uma regra que permita relacionar a cada elemento de *X* um único elemento de *Y*. Há situações em que, apesar de as regras usadas para relacionar os elementos do domínio e do contradomínio de duas funções *f* e *g* serem iguais, não podemos afirmar que essas funções são iguais por seus domínios serem diferentes. Para o caso em que os domínios e os contradomínios de duas funções são iguais, as notações introduzidas anteriormente permitem deduzir um critério para decidirmos a igualdade dessas duas funções. O teorema a seguir fornece tal critério, sendo uma ótima oportunidade para relembrar como demonstramos a igualdade dos conjuntos *f* e *g*, em que $f \subset X \times Y$ e $g \subset X \times Y$.

- **Notação:** Escrevemos $f = g$ para indicar que as funções *f* e *g* são iguais.

Teorema 1.7.5

As funções $f : X \to Y$ e $g : X \to Y$ são iguais se, e somente se, $f(x) = g(x)$, para todo $x \in X$.

Demonstração

Como se trata de um teorema do tipo "se, e somente se", temos duas tarefas a cumprir.

Primeiro, supomos que as funções $f : X \to Y$ e $g : X \to Y$ sejam iguais, o que significa que $f = g$ como conjuntos (ou seja, $f \subset X \times Y$ e $g \subset X \times Y$ têm exatamente os mesmos elementos). Assim, se $x \in X$, a propriedade (*i*) da Definição 1.7.1 garante que existem $f(x) \in Y$ e $g(x) \in Y$ tais que $\big(x, f(x)\big) \in f$ e $\big(x, g(x)\big) \in g$. Como $f = g$, todo elemento de g está em f, de modo que $\big(x, g(x)\big) \in f$. Portanto, tendo $\big(x, f(x)\big) \in f$ e $\big(x, g(x)\big) \in f$, a propriedade (*ii*) garante que $f(x) = g(x)$.

Agora, supomos que $f(x) = g(x)$, para todo $x \in X$. Primeiro, se o par (x, y) é um elemento de f, então temos $y = f(x)$, de modo que $y = g(x)$ e, assim, o par (x, y) está também em g. Isso mostra que $f \subset g$. Segundo, se o par (x, y) é um elemento de g, então $y = g(x)$, de modo que $y = f(x)$, donde o par (x, y) está também em f. Assim, $g \subset f$. Logo, as duas inclusões nos dão $f = g$. ▪

É importante enfatizar que as funções f e g do Teorema 1.7.5 estão definidas para o mesmo domínio e o mesmo contradomínio. Se fosse diferente, já não faria sentido pensar na igualdade das funções. Em resumo: para que duas funções f e g sejam iguais, elas devem possuir mesmo domínio e mesmo contradomínio, além de satisfazer $f(x) = g(x)$, para todo elemento x do domínio.

- **Notação:** Quando se fizer necessário, utilizaremos a notação $\mathbb{R} \setminus \{a, b, c, \ldots\}$ para denotar o conjunto dos números reais, excluindo-se os elementos $a, b, c, \ldots$

Exemplo 1.7.6

Consideremos as seguintes relações do conjunto dos números reais não negativos em $\mathbb{R}$:

$$f = \left\{ (x, y) \in \mathbb{R}_+ \times \mathbb{R} \;\middle|\; y = \frac{x^2 + 5x + 6}{x + 3} \right\}$$

e

$$g = \left\{ (x, y) \in \mathbb{R}_+ \times \mathbb{R} \;\middle|\; y = \frac{x^2 + 7x + 10}{x + 5} \right\}.$$

De modo semelhante ao que fizemos no Exemplo 1.7.2, podemos mostrar que essas relações são funções $f : \mathbb{R}_+ \to \mathbb{R}$ e $g : \mathbb{R}_+ \to \mathbb{R}$ dadas por

$$f(x) = \frac{x^2 + 5x + 6}{x + 3} \quad \text{e} \quad g(x) = \frac{x^2 + 7x + 10}{x + 5}$$

(esse é um bom exercício para o leitor). Como o domínio dessas funções é o conjunto $\mathbb{R}_+$, temos que os valores que a variável x pode assumir nessas expressões são diferentes de –3 e –5. Assim, podemos realizar simplificações nas expressões e, para todo $x \in \mathbb{R}_+$, obtemos

$$\frac{x^2+5x+6}{x+3} = \frac{(x+2)(x+3)}{x+3} = x+2$$

e

$$\frac{x^2+7x+10}{x+5} = \frac{(x+2)(x+5)}{x+5} = x+2.$$

Portanto, para todo $x \in \mathbb{R}_+$ temos $f(x) = g(x)$, de modo que, no domínio dos números reais não negativos, as funções f e g são iguais.

Vale observar que poderíamos redefinir

$$f = \left\{ (x,y) \in \mathbb{R} \setminus \{-3\} \times \mathbb{R} \;\middle|\; y = \frac{x^2+5x+6}{x+3} \right\}$$

e

$$g = \left\{ (x,y) \in \mathbb{R} \setminus \{-5\} \times \mathbb{R} \;\middle|\; y = \frac{x^2+7x+10}{x+5} \right\},$$

de modo que não teríamos funções iguais.

1.8 FUNÇÕES INJETORAS, SOBREJETORAS E BIJETORAS

É oportuno enfatizar que, para uma dada relação $f \subset X \times Y$ ser uma função de X em Y, cada elemento x de X deve estar associado a um único elemento y de Y. Mas bem pode acontecer que elementos distintos x_1 e x_2 de X estejam associados ao mesmo elemento y de Y. As funções em que isso *não* ocorre recebem um nome especial.

Definição 1.8.1

Dizemos que a função $f : X \to Y$ é *injetora* se $x_1, x_2 \in X$ são tais que $x_1 \neq x_2$, então $f(x_1) \neq f(x_2)$. Equivalentemente,

$$\text{se } x_1, x_2 \in X \text{ são tais que } f(x_1) = f(x_2), \text{ então } x_1 = x_2.$$

Exemplo 1.8.2.

(a) Consideremos a função $f:\mathbb{R}\setminus\{2\}\to\mathbb{R}$ dada por $f(x)=\dfrac{5x-3}{x-2}$. Mostremos que essa função é injetora. De fato, se $x_1,x_2\in\mathbb{R}\setminus\{2\}$ são tais que $f(x_1)=f(x_2)$, então

$$\frac{5x_1-3}{x_1-2}=\frac{5x_2-3}{x_2-2}.$$

Assim,

$$(5x_1-3)(x_2-2)=(5x_2-3)(x_1-2).$$

Efetuando os produtos,

$$5x_1x_2-10x_1-3x_2+6=5x_2x_1-10x_2-3x_1+6.$$

Agrupando os termos semelhantes,

$$10x_2-3x_2=10x_1-3x_1,$$

ou seja, $7x_2=7x_1$. Logo, $x_2=x_1$.

Isso mostra que a única possibilidade para que dois elementos tenham a mesma imagem é que esses elementos sejam iguais.

(b) Consideremos a função $f:\mathbb{R}\to\mathbb{R}$ dada por $f(x)=|x|$. Este é um exemplo simples de uma função que não é injetora, pois, se $x_1,x_2\in\mathbb{R}$ são tais que $f(x_1)=f(x_2)$, então $|x_1|=|x_2|$, o que não significa que $x_1=x_2$ (por exemplo, podemos tomar $x_1=1$ e $x_2=-1$). Observamos que, resolvendo a igualdade $|x_1|=|x_2|$, chegaríamos a $x_1=\pm x_2$.

Também é importante enfatizar que, em uma função $f:X\to Y$, cada elemento de X tem de estar associado a algum (na verdade, um único) elemento de Y. Mas pode acontecer que algum elemento de Y não se associe a nenhum elemento de X. As funções em que todos os elementos de Y estão associados a elementos de X também recebem nome especial:

Definição 1.8.3

Dizemos que a função $f:X\to Y$ é *sobrejetora* quando, para cada elemento $y_0\in Y$ dado, existe um elemento $x_0\in X$ tal que $y_0=f(x_0)$, ou seja, quando $\mathrm{Im}(f)=Y$.

Em outros termos, para mostrar que uma dada função $f : X \to Y$ é sobrejetora, devemos verificar que, para cada elemento $y_0 \in Y$ dado, a equação $y_0 = f(x)$, de incógnita *x*, possui pelo menos uma solução x_0 em *X*. Ou seja, a função $f : X \to Y$ é sobrejetora se, e somente se, a imagem de *f*, $\mathrm{Im}(f)$, é igual ao contradomínio *Y*.

Exemplo 1.8.4

(a) Voltemos ao Exemplo 1.8.2(a). A fim de verificarmos se a função $f : \mathbb{R} \setminus \{2\} \to \mathbb{R}$ dada por $f(x) = \dfrac{5x-3}{x-2}$ é sobrejetora, devemos encontrar solução para a equação $y_0 = f(x)$, qualquer que seja $y_0 \in \mathbb{R}$. Para resolvermos uma equação, o método mais comum é aquele em que isolamos a incógnita. Vejamos:

$$\begin{aligned} y_0 = \frac{5x-3}{x-2} &\Leftrightarrow y_0(x-2) = 5x-3 \\ &\Leftrightarrow y_0x - 2y_0 = 5x-3 \\ &\Leftrightarrow y_0x - 5x = 2y_0 - 3 \\ &\Leftrightarrow x(y_0-5) = 2y_0 - 3\,. \end{aligned}$$

Agora, para determinar o valor de *x*, somente podemos efetuar a divisão por $y_0 - 5$ quando y_0 for diferente de 5. Mas, então, não conseguimos resolver a equação $y_0 = f(x)$ para $y_0 = 5$, de modo que a função não é sobrejetora.

Com isso, vemos que o contradomínio de *f* possui um elemento que não é imagem de nenhum elemento do domínio. Agora, se o contradomínio da função fosse o conjunto $\mathbb{R} \setminus \{5\}$, teríamos uma função sobrejetora. Assim, a função $g : \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{5\}$ dada por $g(x) = \dfrac{5x-3}{x-2}$ é sobrejetora. Como isso em nada muda o procedimento que apresentamos no Exemplo 1.8.2(a), temos definida uma função *g* que é ao mesmo tempo injetora e sobrejetora. Funções com essa propriedade recebem nome especial, como veremos na Definição 1.8.5.

(b) Voltando ao Exemplo 1.8.2(b), é fácil notar que a função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = |x|$ não é sobrejetora. Basta escolher um número real negativo y_0 e ver que y_0 não pertence à imagem de *f*.

Definição 1.8.5

Dizemos que a função $f : X \to Y$ é *bijetora* se é simultaneamente injetora e sobrejetora.

Talvez o exemplo mais conhecido de função bijetora seja o de função polinomial do primeiro grau, o que apresentamos no próximo exemplo.

Exemplo 1.8.6

Sejam $a, b \in \mathbb{R}$, com $a \neq 0$, e consideremos a função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = ax + b$. Para mostrar que *f* é injetora, sejam $x_1, x_2 \in \mathbb{R}$ tais que $f(x_1) = f(x_2)$. Então

$$ax_1 + b = ax_2 + b \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2,$$

em que última implicação decorre do fato de que $a \neq 0$. Para mostrar que *f* é sobrejetora, seja $y_0 \in \mathbb{R}$ e vamos resolver a equação $y_0 = f(x)$ de incógnita *x*. Temos:

$$ax + b = y_0 \Leftrightarrow ax = y_0 - b \Leftrightarrow x = \frac{y_0 - b}{a},$$

onde novamente usamos o fato de que $a \neq 0$. Assim, $x_0 = \dfrac{y_0 - b}{a}$ é a solução da equação e *f* é sobrejetora. Logo, *f* é uma função bijetora.

É importante que o leitor compreenda que há funções apenas injetoras, apenas sobrejetoras, bijetoras e ainda há funções que não são injetoras nem sobrejetoras.

- ***Observação*:** no caso em que a função $f : X \to Y$ é injetora, dado $y_0 \in Y$, a equação $y_0 = f(x)$ poderá não ter solução, mas, se tiver, tal solução será única. Já sabemos que a função é sobrejetora se, e somente se, a equação $y_0 = f(x)$, de incógnita *x*, possui solução para todo $y_0 \in Y$. Assim, a função $f : X \to Y$ é bijetora se, e somente se, para cada $y_0 \in Y$, a equação $y_0 = f(x)$, de incógnita *x*, possui uma única solução.

1.9 COMPOSIÇÃO DE FUNÇÕES E INVERSA DE UMA FUNÇÃO

COMPOSIÇÃO DE FUNÇÕES

Sejam *X*, *Y* e *Z* conjuntos e sejam $f : X \to Y$ e $g : Y \to Z$ duas funções. Notemos que o domínio da função *g* é o contradomínio da função *f*, de modo que, para cada elemento $x \in X$, sua imagem $y = f(x)$ está no domínio da função *g*, e então faz sentido "calcular" $g(y)$. O sentido da palavra "calcular" empregado aqui é que podemos estudar o valor da função *g* em *y*. Ou ainda, como já dissemos antes, podemos obter a imagem de *y* pela função *g*.

Definição 1.9.1

A *função composta* de $g : Y \to Z$ e $f : X \to Y$, nessa ordem, é a função $h : X \to Z$ definida por $h(x) = g\big(f(x)\big)$, para todo $x \in X$.

- **Notação:** Representamos a função composta de *g* e *f*, nessa ordem, por $g \circ f$, que se lê "*g* composta com *f*". Escrevemos:

$$(g \circ f)(x) = g(f(x)), \text{ para todo } x \in X.$$

Exemplo 1.9.2

(a) Sejam $X = \mathbb{R}$, $Y = \mathbb{R}_+$ e $Z = \mathbb{R}$. Consideremos as funções $f : X \to Y$ e $g : Y \to Z$ definidas por

$$f(x) = |x-4| \text{ e } g(y) = \sqrt{y^3+2}.$$

A função composta de *g* e *f*, $g \circ f : X \to Z$, é obtida substituindo-se a expressão $|x-4|$ da função *f* no lugar de *y* na função *g*, ou seja,

$$(g \circ f)(x) = g(f(x)) = g(|x-4|) = \sqrt{(|x-4|)^3+2}.$$

Então, a composta de *g* e *f* é a função $g \circ f : \mathbb{R} \to \mathbb{R}$ dada por

$$(g \circ f)(x) = \sqrt{(|x-4|)^3+2}.$$

Agora, a função composta de *f* e *g*, $f \circ g : Y \to Y$ (note que *Z* = *X*), é obtida calculando-se $(f \circ g)(y)$, para todo $y \in Y$. Assim, substituímos a expressão $\sqrt{y^3+2}$ da função *g* no lugar de *x* na função *f*, ou seja,

$$(f \circ g)(y) = f(g(y)) = f\left(\sqrt{y^3+2}\right) = \left|\sqrt{y^3+2}-4\right|.$$

Assim, a composta de *f* e *g* está definida e é a função $f \circ g : \mathbb{R}_+ \to \mathbb{R}_+$ dada por

$$(f \circ g)(y) = \left|\sqrt{y^3+2}-4\right|.$$

(b) Sejam $X = \mathbb{R}$, $Y = \{x \in \mathbb{R} \mid x \geq -1\}$ e $Z = \mathbb{R}_+$. Consideremos as funções $f : X \to Y$ e $g : Y \to Z$ definidas por

$$f(x) = 2^x - 1 \text{ e } g(y) = \sqrt{y+1}.$$

A função composta de *g* e *f*, $g \circ f : X \to Z$, é obtida substituindo-se a expressão $2^x - 1$ da função *f* no lugar de *y* na função *g*, ou seja,

$$\big(g \circ f\big)(x) = g\big(f(x)\big) = g\left(2^x - 1\right) = \sqrt{\left(2^x - 1\right) + 1} = \sqrt{2^x}\ .$$

Assim, a composta de *g* e *f* é a função $g \circ f : \mathbb{R} \to \mathbb{R}_+$ dada por

$$\big(g \circ f\big)(x) = \sqrt{2^x}.$$

Já a composta de *f* e *g*, que deveria ser uma função $f \circ g : Y \to Y$, não está definida. Isso porque o domínio da função *f* não coincide com o contradomínio da função *g*. Notemos que seria uma função para a qual deveríamos calcular $\big(f \circ g\big)(y) = f\big(g(y)\big)$, para todo $y \in Y$. É fato que $g(y) = \sqrt{y+1}$, pertencente a $Z = \mathbb{R}_+$, pode ser calculado para todo $y \in Y = \big\{x \in \mathbb{R} \mid x \geq -1\big\}$, donde podemos calcular $f\big(g(y)\big) = 2^{g(y)} - 1$. No entanto, *Z* não coincide com o domínio $X = \mathbb{R}$ da função *f* (ainda que $Z \subset X$) e, assim, $f \circ g$ não satisfaz a Definição 1.9.1.

Vimos com o exemplo anterior que nem sempre a igualdade $g \circ f = f \circ g$ ocorre. Em verdade, pode ocorrer que um dos membros dessa igualdade sequer esteja definido.

Quando as funções *f* e *g* são injetoras ou sobrejetoras, a função $g \circ f$ herda essas propriedades. Isso é parte do que mostramos no teorema a seguir, que resume as principais propriedades da composição de funções.

Teorema 1.9.3

Sejam *X*, *Y*, *Z* e *W* conjuntos.

(a) Se $f : X \to Y$ e $g : Y \to Z$ são funções injetoras, então $g \circ f : X \to Z$ também é uma função injetora.

(b) Se $f : X \to Y$ e $g : Y \to Z$ são funções sobrejetoras, então $g \circ f : X \to Z$ também é uma função sobrejetora.

(c) Se $f : X \to Y$ e $g : Y \to Z$ são funções bijetoras, então $g \circ f : X \to Z$ também é uma função bijetora.

(d) A composição de funções satisfaz a propriedade associativa, isto é, para quaisquer funções $f : X \to Y$, $g : Y \to Z$ e $h : Z \to W$ tem-se

$$\big(h \circ g\big) \circ f = h \circ \big(g \circ f\big).$$

(e) Sendo $f : X \to Y$ uma função, existe uma função $I_X : X \to X$ e uma função $I_Y : Y \to Y$ tais que

$$I_Y \circ f = f \text{ e } f \circ I_X = f.$$

(f) Se $f : X \to Y$ é uma função bijetora, então existe uma função bijetora $g : Y \to X$ tal que

$$g \circ f = I_X \text{ e } f \circ g = I_Y.$$

Demonstração

(a) Consideremos $x_1, x_2 \in X$ e sejam $y_1, y_2 \in Y$ as imagens de x_1 e x_2 pela função *f*, respectivamente. Escrevemos $y_1 = f(x_1)$ e $y_2 = f(x_2)$. Para verificar que $g \circ f$ é injetora, suponhamos $(g \circ f)(x_1) = (g \circ f)(x_2)$. Assim, $g(f(x_1)) = g(f(x_2))$, ou seja, $g(y_1) = g(y_2)$. Como *g* é injetora, isso implica que $y_1 = y_2$, o que nos dá $f(x_1) = f(x_2)$. Mas agora o fato de que *f* também é injetora garante que $x_1 = x_2$. Isso mostra que a única possibilidade para que dois elementos tenham a mesma imagem pela função $g \circ f$ é que estes sejam iguais. Logo, $g \circ f$ é injetora.

(b) Como já observamos antes, para mostrarmos que a função $g \circ f : X \to Z$ é sobrejetora, dado qualquer elemento $z_0 \in Z$, devemos mostrar que a equação $(g \circ f)(x) = z_0$, de incógnita *x*, tem pelo menos uma solução em *X*. Mas, por ser sobrejetora a função *g*, a equação $g(y) = z_0$, de incógnita *y*, possui uma solução $y_0 \in Y$, ou seja, $g(y_0) = z_0$. E, por ser sobrejetora a função *f*, a equação $f(x) = y_0$, de incógnita *x*, tem uma solução $x_0 \in X$, isto é, $f(x_0) = y_0$. Logo, $(g \circ f)(x_0) = g(f(x_0)) = g(y_0) = z_0$, de modo que x_0 é solução da equação $(g \circ f)(x) = z_0$.

(c) Este item é consequência imediata dos itens (a) e (b).

(d) Primeiramente, note que as funções $(h \circ g) \circ f$ e $h \circ (g \circ f)$ possuem os mesmos domínio e contradomínio, estando ambas definidas de *X* em *W*. Pelo Teorema 1.7.5, para mostrarmos a igualdade entre essas funções, devemos mostrar que, para todo $x \in X$, vale a igualdade

$$[(h \circ g) \circ f](x) = [h \circ (g \circ f)](x).$$

Para isso, sejam $f(x) = y$, $g(y) = z$ e $h(z) = t$, com $x \in X$, $y \in Y$, $z \in Z$ e $t \in W$. Então,

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = (h \circ g)(y) = h(g(y)) = h(z) = t$$

e

$$[h \circ (g \circ f)](x) = h((g \circ f)(x)) = h(g(f(x))) = h(g(y)) = h(z) = t,$$

donde temos a igualdade desejada.

(e) Definamos duas funções $I_X : X \to X$ e $I_Y : Y \to Y$ por: $I_X(x) = x$, para todo $x \in X$, e $I_Y(y) = y$, para todo $y \in Y$. Então, escolhendo $x \in X$ e escrevendo $f(x) = y$, temos

$$\big(I_Y \circ f\big)(x) = I_Y\big(f(x)\big) = I_Y\big(y\big) = y = f(x)$$

e

$$\big(f \circ I_X\big)(x) = f\big(I_X(x)\big) = f(x).$$

Uma vez que as funções f e $I_Y \circ f$ possuem os mesmos domínio e contradomínio, e isso também é verdade para as funções f e $f \circ I_X$, pelo Teorema 1.7.5, segue que $I_Y \circ f = f$ e $f \circ I_X = f$.

(f) Seja $g = \big\{(y,x) \in Y \times X \mid y = f(x)\big\}$. Primeiramente, mostremos que g é uma função. Já tivemos a oportunidade de comentar com o leitor que a função $f : X \to Y$ é bijetora se, e somente se, para cada $y_0 \in Y$, a equação $y_0 = f(x)$, de incógnita x, possui uma única solução $x_0 \in X$. Sendo f bijetora por hipótese, para cada $y_0 \in Y$, existe e é único o elemento $x_0 \in X$ tal que o par (y_0, x_0) está em g. Isso é suficiente para mostrarmos que g cumpre as duas condições da Definição 1.7.1. Pela notação introduzida antes do Exemplo 1.7.3, temos que $x_0 = g(y_0)$ é equivalente a $(y_0, x_0) \in g$, que, pela definição de g, é o mesmo que $(x_0, y_0) \in f$, ou seja, $y_0 = f(x_0)$. Com isso, temos:

(*i*) a igualdade $\big(g \circ f\big)(x_0) = g\big(f(x_0)\big) = g(y_0) = x_0 = I_X(x_0)$ verdadeira para todo $x_0 \in X$;

(*ii*) a igualdade $\big(f \circ g\big)(y_0) = f\big(g(y_0)\big) = f(x_0) = y_0 = I_Y(y_0)$ verdadeira para todo $y_0 \in Y$.

Observando que $g \circ f$ e I_X têm os mesmos domínio e contradomínio e isso também vale para $f \circ g$ e I_Y, o Teorema 1.7.5 nos dá $g \circ f = I_X$ e $f \circ g = I_Y$. ▪

FUNÇÃO IDENTIDADE E INVERSA DE UMA FUNÇÃO

As funções I_X e I_Y apresentadas na parte (e) do Teorema 1.9.3 recebem o nome de *função identidade* em X e Y, respectivamente, dado o fato de que a imagem de um elemento é o próprio. Já a função g que aparece na parte (f) recebe o nome de *função inversa* de f e geralmente é representada por f^{-1}. Quando uma função possui uma inversa, o procedimento geralmente usado para encontrar f^{-1} é escrever $y = f(x)$ e isolar a variável x (isso porque $y = f(x)$ é equivalente a $f^{-1}(y) = f^{-1}\big(f(x)\big)$, que é equivalente a $x = f^{-1}(y)$). Esse método é ilustrado no próximo exemplo.

Exemplo 1.9.4

No Exemplo 1.8.4(a) já tivemos a oportunidade de mostrar que a função $g:\mathbb{R}\setminus\{2\}\to\mathbb{R}\setminus\{5\}$ dada por $g(x)=\dfrac{5x-3}{x-2}$ é bijetora. Encontremos sua inversa. Fazendo $y=g(x)$ e isolando a variável x, temos

$$\begin{aligned} y=\frac{5x-3}{x-2} &\Rightarrow y(x-2)=5x-3\\ &\Rightarrow yx-2y=5x-3\\ &\Rightarrow yx-5x=2y-3\\ &\Rightarrow x(y-5)=2y-3\\ &\Rightarrow x=\frac{2y-3}{y-5}. \end{aligned}$$

Assim, a função $g^{-1}:\mathbb{R}\setminus\{5\}\to\mathbb{R}\setminus\{2\}$ dada por $g^{-1}(y)=\dfrac{2y-3}{y-5}$ é a inversa procurada. De fato, verifiquemos o item (f) do Teorema 1.9.3:

$$\left(g^{-1}\circ g\right)(x)=g^{-1}\left(g(x)\right)=\frac{2\left(g(x)\right)-3}{g(x)-5}=\frac{2\left(\dfrac{5x-3}{x-2}\right)-3}{\dfrac{5x-3}{x-2}-5}$$

$$=\frac{\dfrac{10x-6}{x-2}-3}{\dfrac{5x-3}{x-2}-5}=\frac{\dfrac{10x-6}{x-2}-\dfrac{3(x-2)}{x-2}}{\dfrac{5x-3}{x-2}-\dfrac{5(x-2)}{x-2}}$$

$$=\frac{(10x-6)-(3x-6)}{(5x-3)-(5x-10)}=\frac{7x}{7}=x=I_X(x).$$

Agora,

$$\left(g\circ g^{-1}\right)(y)=g\left(g^{-1}(y)\right)=\frac{5\left(g^{-1}(y)\right)-3}{g^{-1}(y)-2}=\frac{5\left(\dfrac{2y-3}{y-5}\right)-3}{\dfrac{2y-3}{y-5}-2}$$

$$=\frac{\dfrac{10y-15}{y-5}-3}{\dfrac{2y-3}{y-5}-2}=\frac{\dfrac{10y-15}{y-5}-\dfrac{3(y-5)}{y-5}}{\dfrac{2y-3}{y-5}-\dfrac{2(y-5)}{y-5}}$$

$$= \frac{(10y-15)-(3y-15)}{(2y-3)-(2y-10)} = \frac{7y}{7} = y = I_Y(y).$$

EXERCÍCIOS PROPOSTOS

SEÇÃO 1.2

1. Considerando X um conjunto com 3 elementos, determine quantos elementos tem $\wp(X)$. No caso em que X tem 4 elementos, quantos elementos tem $\wp(X)$? E no caso em que X tem 5 elementos? Generalize para X um conjunto com n elementos.
2. *Diferença de conjuntos.* Sejam X e Y subconjuntos de um conjunto U. Definimos o *conjunto diferença* de X por Y como $X \setminus Y = \{x \in X \mid x \notin Y\}$ (esse conjunto também pode ser representado por $X - Y$). Mostre que, se X e Y são ambos subconjuntos de um mesmo conjunto U, então $X \setminus Y = X \cap C_U Y$.
3. *Diferença simétrica de conjuntos.* Sendo A e B duas partes do conjunto U, definimos a *diferença simétrica* de A e B por $A \Delta B = (A \setminus B) \cup (B \setminus A)$. Demonstre que:
   a) $A \Delta B = B \Delta A$
   b) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$
   c) $A \Delta \varnothing = A$
   d) $A \Delta A = \varnothing$
   e) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$ [*Sugestão*: utilize o Exercício 2.]
4. Responda os itens a seguir.
   a) Se A e B são subconjuntos de U, demonstre que as seguintes condições são equivalentes entre si:
      1. $A \subset B$ 2. $A \cap B = A$ 3. $A \cup B = B$
      4. $A \cap C_U B = \varnothing$ 5. $C_U B \subset C_U A$
   b) Demonstre as propriedades listadas no Teorema 1.2.7.

SEÇÃO 1.3

5. Mostre as igualdades de conjuntos a seguir:
   a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
   b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$
   c) $A \times B = \varnothing \Leftrightarrow A = \varnothing$ ou $B = \varnothing$

6. Determine todas as relações de E em E, e todas as relações de E em F, com $E=\{1,2\}$ e $F=\{3,4,5\}$. Para cada uma delas, determine o domínio e a imagem.

SEÇÃO 1.4

7. Responda os itens a seguir.

   a) Sejam X o conjunto dos inteiros e

$$R=\left\{(x,y)\in\mathbb{Z}\times\mathbb{Z} \;\middle|\; \text{existe } n\in\mathbb{Z} \text{ tal que } \frac{x}{y}=3^n\right\}.$$

   Mostre que R satisfaz as propriedades simétrica e transitiva, mas não a reflexiva (atenção: o problema não é o número 3 na base da potência).

   b) Sejam X um conjunto não vazio e R uma relação sobre X que satisfaça as propriedades simétrica e transitiva. O raciocínio a seguir "demonstra" que uma relação que seja simétrica e transitiva é também reflexiva.

   "Sejam $x,y\in X$; se $(x,y)\in R$, pela propriedade simétrica, concluímos que $(y,x)\in R$. Usando agora a propriedade transitiva com os pares $(x,y)\in R$ e $(y,x)\in R$, vemos que $(x,x)\in R$. Assim, R é reflexiva."

   O item (a) desta questão é um exemplo de que esse raciocínio está errado. Encontre o erro.

8. Dados os conjuntos X e $R\subset X\times X$ a seguir, demonstre que R é uma relação de equivalência sobre X ou explique qual a propriedade que falha para não ser uma relação de equivalência.

   a) $X=\mathbb{Z},\ R=\{(a,b)\in X\times X \mid a-b \text{ é múltiplo de } m\},\ m\in\mathbb{Z}^*$

   b) $X=\{\text{retas de um plano dado}\},\ R=\{(a,b)\in X\times X \mid a \text{ é paralela a } b\}$

   c) $X=\{\text{retas de um plano dado}\},\ R=\{(a,b)\in X\times X \mid a \text{ é perpendicular a } b\}$

   d) $X=\{\text{conjunto qualquer}\},\ R=\{(a,b)\in X\times X \mid a=b\}$

   e) $X=\mathbb{R}$ e $R=\{(a,b)\in X\times X \mid a=\pm b\}$

   f) $X=\mathbb{Z},\ R=\{(a,b)\in X\times X \mid \text{existem inteiros } x \text{ e } y \text{ tais que } ay-bx=0\}$

9. Em algumas ocasiões, utilizamos a expressão *relação binária* com o mesmo sentido de *relação* dado pela definição. Seja $X=\{a,b,c,d\}$. Consideremos as seguintes relações binárias definidas sobre X:

$$R_1=\{(a,b),(a,a),(b,b),(b,a),(c,c),(d,d)\}$$
$$R_2=\{(a,a),(b,b),(c,c),(a,b),(b,c),(d,c)\}$$
$$R_3=\{(a,a),(b,b),(a,b),(b,c),(c,a)\}$$

$R_4 = \{(a,b),(a,a),(b,b),(b,a),(c,c),(d,c),(c,d)\}$

$R_5 = \{(a,a),(b,b),(b,c),(c,b),(a,c),(c,a),(d,d)\}$

$R_6 = X \times X$

$R_7 = \varnothing$

a) Determine o domínio e a imagem de cada uma dessas relações.

b) Quais dessas relações são reflexivas? Simétricas? Transitivas?

c) Quais relações são de equivalência?

10. Considere a relação R sobre $\mathbb{N} \times \mathbb{N}$ definida por $(x, y)\ R\ (z, t)$ se, e somente se, $x + y = z + t$. Mostre que R é uma relação de equivalência.

11. Considere o conjunto $X = \{x \in \mathbb{Z} \mid 0 \leq x \leq 50\}$. Defina sobre X a seguinte relação:

$$R = \{(a,b) \in X \times X \mid a - b \text{ é múltiplo de } 4\}.$$

a) Mostre que R é uma relação de equivalência.

b) Descreva as classes de equivalência e o conjunto quociente X/R.

12. Seja R uma relação de equivalência definida sobre um conjunto não vazio X. Sejam $x, y \in X$. Demonstre que as afirmações a seguir são equivalentes:

1. x se relaciona com y pela relação R.

2. $x \in C_R(y)$

3. $y \in C_R(x)$

4. $C_R(x) = C_R(y)$

13. *Inversa de uma relação.* Sejam X e Y dois conjuntos e R uma relação de X em Y. Definimos a relação inversa de R, denotada R^{-1}, pela seguinte relação:

$$R^{-1} = \{(y,x) \in Y \times X \mid (y,x) \in R\}.$$

a) Para $X = \{a,b,c\}$ e $Y = \{m,n\}$, determine a inversa da relação de X em Y dada por $R = \{(a,m), (b,n), (c,m), (c,n)\}$.

b) Para $X = Y = \mathbb{R}$, determine a inversa da relação sobre $\mathbb{R}$ dada por $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y = 5x\}$.

c) Mostre que $D(R^{-1}) = \text{Im}(R)$, $\text{Im}(R^{-1}) = D(R)$ e $(R^{-1})^{-1} = R$.

d) Argumente contra ou a favor da seguinte afirmação: se R é uma relação reflexiva sobre um conjunto X, então R^{-1} também é reflexiva sobre X.

e) Argumente contra ou a favor da seguinte afirmação: se R é uma relação simétrica sobre um conjunto X, então R^{-1} também é simétrica sobre X.

f) Argumente contra ou a favor da seguinte afirmação: se R é uma relação transitiva sobre um conjunto X, então R^{-1} também é transitiva sobre X.

SEÇÃO 1.5

14. Faça o que se pede em cada item a seguir.

a) Mostre que dois números inteiros são sempre congruentes módulo 1. Determine todas as classes de congruência módulo 1.

b) Mostre que dois números inteiros pares são sempre congruentes módulo 2. Determine todas as classes de congruência módulo 2.

c) Mostre que dois números inteiros ímpares são sempre congruentes módulo 2.

d) Mostre que, se dois números inteiros são congruentes módulo 0, então esses números são iguais. Determine todas as classes de congruência módulo 0.

e) Considere sobre $\mathbb{Z}$ a relação de congruência definida para $m < 0$. O que você observa?

15. Faça o que se pede em cada item a seguir.

a) Encontre todos os números inteiros entre 0 e 30 que são congruentes a 4 módulo 5.

b) Encontre todos os números inteiros entre –10 e 40 que são congruentes a 3 módulo 7.

c) Que padrão você observa? Esse padrão pode ser usado para descrever todos os números inteiros (positivos e negativos) que são congruentes a 8 módulo 11?

d) Determine todas as classes de congruência módulo m, quando $m = 5, 7, 8, 11$ e 20.

16. Para cada par de inteiros a e m a seguir, encontre um inteiro r tal que $a \equiv r \pmod{m}$ e $0 \leq r < m$.

a) $a = 2.351$ e $m = 2$ b) $a = 50.121$ e $m = 13$

c) $a = 321.671$ e $m = 14$ d) $a = -2.351$ e $m = 2$

e) $a = -50.121$ e $m = 13$ f) $a = -321.671$ e $m = 14$

17. Faça o que se pede em cada item a seguir.

a) Encontre o menor inteiro não negativo x tal que $x \equiv 1.789 \pmod{30}$.

b) Encontre o menor inteiro não negativo x tal que $x \equiv -1.789 \pmod{30}$.

c) Como a Proposição 1.5.3 pode ajudar a resolver os itens (a) e (b)?

18. Demonstre as propriedades (a), (c) e (e) e a parte *somente se* da propriedade (h) da Proposição 1.5.6.

19. Sejam $a, b \in \mathbb{Z}$ e seja m um inteiro maior que 1.

    a) Argumente contra ou a favor da seguinte afirmação: se $ad \equiv bd \pmod{m}$, então $a \equiv b \pmod{m}$, para todo $d \in \mathbb{Z}$. (A questão aqui é verificar a validade da recíproca da propriedade (e) da Proposição 1.5.6.)

    b) Argumente contra ou a favor da seguinte afirmação: se $a^n \equiv b^n \pmod{m}$, então $a \equiv b \pmod{m}$, para todo número natural n. (A questão aqui é verificar a validade da recíproca da propriedade (j) da Proposição 1.5.6.)

    c) Argumente contra ou a favor da seguinte afirmação: se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{n}$, então $ac \equiv bd \pmod{mn}$, para todos $c, d \in \mathbb{Z}$ e n inteiro maior que 1. (Compare essa afirmação com a propriedade (d) da Proposição 1.5.6.)

    d) Argumente contra ou a favor da seguinte afirmação: se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m^n}$, para todo número natural n. (Compare essa afirmação com a propriedade (j) da Proposição 1.5.6.)

20. Sejam $a, b \in \mathbb{Z}$ tais que $0 \leq a < 10$ e $0 \leq b < 10$. Demonstre que, se $a \equiv b \pmod{10}$, então $a = b$. Generalize!

21. Sejam a, b e m inteiros, m maior que 1. Mostre que a e b são congruentes módulo m se, e somente se, deixam o mesmo resto na divisão euclidiana por m.

SEÇÃO 1.6

22. Encontre, quando existir, todas as soluções das equações de congruências lineares a seguir.

    a) $7x + 2 \equiv 0 \pmod{4}$ b) $35x - 1 \equiv 54 \pmod{15}$

    c) $52x + 4 \equiv 110 \pmod{46}$ d) $112x - 7 \equiv 273 \pmod{24}$

    e) $524x + 6 \equiv 360 \pmod{98}$ f) $60x - 2 \equiv 280 \pmod{42}$

23. Encontre todos os inteiros a para os quais a equação $ax \equiv 1 \pmod{11}$ tem solução.

24. Encontre todos os inteiros a para os quais a equação $ax \equiv 1 \pmod{12}$ tem solução. Compare os resultados deste exercício com o anterior.

25. Sejam $a \in \mathbb{Z}$ e m um inteiro maior que 1.

    a) Demonstre que a equação $ax \equiv 1 \pmod{m}$ tem solução se, e somente se, a e m são coprimos.

    b) Demonstre que, se a e m são coprimos, então a equação $ax \equiv b \pmod{m}$ tem solução para qualquer inteiro b.

SEÇÃO 1.7

26. Dados os conjuntos X e Y, verifique, em cada caso, se a relação $f \subset X \times Y$ é uma função.

a) X e Y são ambos iguais ao conjunto dos números inteiros e $f = \{(x, y) \in X \times Y \mid x^2 + y^2 = 25\}$

b) X e Y são ambos iguais ao conjunto dos números naturais e $f = \{(x, y) \in X \times Y \mid x = y^2\}$

c) X e Y são ambos iguais ao conjunto dos números reais e $f = \{(x, y) \in X \times Y \mid y = x^2\}$

d) X e Y são ambos iguais ao conjunto dos números reais e $f = \{(x, y) \in X \times Y \mid x = y^2\}$

e) X e Y são ambos iguais ao conjunto dos números reais e $f = \{(x, y) \in X \times Y \mid x^2 = y^2\}$

f) X e Y são ambos iguais ao conjunto dos números reais e $f = \{(x, y) \in X \times Y \mid x^2 = y^3\}$

g) X e Y são ambos iguais ao conjunto dos números reais e $f = \{(x, y) \in X \times Y \mid x^3 = y^2\}$

27. Para os itens a seguir, considere a relação de $\mathbb{Q}$ em $\mathbb{N}$ dada por

$$f = \{(x, y) \in \mathbb{Q} \times \mathbb{N} \mid y \text{ é o numerador de uma fração que representa } x\}.$$

a) Verifique se a relação f satisfaz a seguinte propriedade:

$$\forall x \in \mathbb{Q},\ \exists y \in \mathbb{N} \mid (x, y) \in f.$$

b) Verifique se a relação f satisfaz a seguinte propriedade:

Se $y_1, y_2 \in \mathbb{N}$ são tais que $(x, y_1) \in f$ e $(x, y_2) \in f$

para algum $x \in \mathbb{Q}$, então $y_1 = y_2$.

c) Argumente contra ou a favor da seguinte afirmação: a relação f é uma função de $\mathbb{Q}$ em $\mathbb{N}$.

28. Faça o que se pede em cada item a seguir.

a) Encontre todas as funções com domínio no conjunto $X = \{1, 2, 3\}$ e contradomínio no conjunto $Y = \{a, b\}$.

b) Encontre todas as funções com domínio no conjunto $X = \{1, 2\}$ e contradomínio no conjunto $Y = \{a, b, c\}$.

29. Para as funções *f* e *g* dadas em cada item a seguir, determine $D(f)$ e $D(g)$, escolha contradomínios para *f* e g, determine Im(*f*) e Im(*g*), e discuta se é verdade que $f = g$.

a) $f(x) = x$ e $g(x) = \dfrac{x^2}{x}$

b) $f(x) = x$ e $g(x) = \sqrt{|x^2|}$

c) $f(x) = x$ e $g(x) = \left(\sqrt[3]{x}\right)^3$

d) $f(x) = \dfrac{x^2 - 16}{x + 4}$ e $g(x) = x - 4$

e) $f(x) = \dfrac{x^2 - 2x + 1}{x - 1}$ e $g(x) = x - 1$

30. *Soma e produto de funções.* Sejam $f : X \to Y$ e $g : Z \to W$ duas funções. Definimos a função soma $f + g : X \cap Z \to T$ e a função produto $f \cdot g : X \cap Z \to U$ mediante:

$$\left(f + g\right)(x) = f(x) + g(x) \text{ e } \left(f \cdot g\right)(x) = f(x) \cdot g(x).$$

[As operações definidas impõem que $D\left(f + g\right) = D\left(f \cdot g\right) = D(f) \cap D(g)$ e que os contradomínios de $f + g$ e de $f \cdot g$, denotados por *T* e *U*, respectivamente, sejam conjuntos contendo os elementos $f(x) + g(x)$ e $f(x) \cdot g(x)$, para todo $x \in D(f) \cap D(g)$, respectivamente.]

Determine a soma e o produto das funções dadas a seguir, exibindo o domínio e o contradomínio.

a) $f : \mathbb{R} \to \mathbb{R}_+$, $x \mapsto x^3 + 4$ e $g : \mathbb{Q}_+ \to \mathbb{R}$, $x \mapsto \sqrt{x}$

b) $f : \mathbb{N} \to \mathbb{Q}$, $x \mapsto \dfrac{x}{9}$ e $g : \mathbb{N} \to \mathbb{N}$, $x \mapsto 9x$

c) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2 + 3x - 1$ e $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3 - 5x^2 + 8x$

SEÇÃO 1.8

31. Sejam $E = \{1, 2, 3\}$ e $F = \{a, b, c, d\}$.

a) Determine o número de funções injetoras de *E* em *F*.

b) Determine o número de funções sobrejetoras de *E* em *F*.

32. Demonstre que a função $g : \mathbb{Z} \to \mathbb{R}$ definida por $g(x) = \dfrac{x}{\pi^x}$ é injetora.

Sugestão: π^x é irracional para todo $x \in \mathbb{Z}^*$.

33. Considere a função $f:\mathbb{N}\to\mathbb{R}$ definida por $f(x)=\dfrac{x}{\sqrt{2}^{\,x}}$.
    a) Calcule $f(2)$ e $f(4)$.
    b) Prove ou refute: a função f é injetora.
    c) Mostre que a equação $f(x)=2$ não possui solução.
    d) Prove ou refute: a função f é sobrejetora.
34. Sejam $a,b,c\in\mathbb{R}$, com $a\neq 0$. Mostre que a função $f:\mathbb{R}\setminus\{b\}\to\mathbb{R}\setminus\{a\}$ dada por $f(x)=\dfrac{ax+c}{x-b}$ é bijetora.
35. Mostre que é bijetora a função $f:\mathbb{N}\to\mathbb{Z}$ dada por

$$f(x)=\begin{cases}-\dfrac{x}{2}, & \text{se } x \text{ é par}\\[2ex] \dfrac{x+1}{2}, & \text{se } x \text{ é ímpar}\end{cases}.$$

36. Como todo número natural x pode ser escrito de modo único na forma $x=2^k\cdot m$, com $k\in\{0,1,2,3,\ldots\}$ e m ímpar, definimos a função $f:\mathbb{N}\to\mathbb{Q}$ por $f(x)=\dfrac{k}{m}$.
    a) Encontre uma solução para a equação $f(x)=\dfrac{6}{5}$.
    b) Mostre que a equação $f(x)=\dfrac{5}{6}$ não possui solução e justifique por que a função *f* não é sobrejetora.
    c) Sendo $x_1=2^2\cdot 3$ e $x_2=2^6\cdot 9$, calcule $f(x_1)$ e $f(x_2)$ e justifique por que a função *f* não é injetora.

SEÇÃO 1.9

37. Dê exemplos de funções $f:X\to Y$ e $g:Y\to Z$ tais que:
    a) uma das funções compostas $f\circ g$ e $f\circ g$ esteja definida e a outra não;
    b) $g\circ f$ e $f\circ g$ estejam definidas, mas sejam distintas;
    c) $g\circ f$ e $g\circ f$ estejam definidas e sejam iguais.
38. Considere a função $f:\mathbb{R}\setminus\{4\}\to\mathbb{R}\setminus\{1\}$ definida por $f(x)=\dfrac{1}{x-4}$.
    a) Encontre a função inversa de *f*.
    b) Se *g* denota a inversa de *f*, encontre a função composta $f\circ g$. O que dizer da função composta $g\circ f$?

39. Considere a função *f* definida por $f(x)=\dfrac{(2x-4)^{2/3}}{5x+3}$.

a) Determine o domínio de *f*.

b) Determine $f \circ f$.

40. Considere as funções $f:\mathbb{R}\to\mathbb{R}$ e $g:\mathbb{R}\to\mathbb{R}$ definidas por $f(x)=\sqrt[3]{x-5}$ e $g(x)=x^3+5$, para todo $x\in\mathbb{R}$.

a) Determine as funções compostas $f \circ g$ e $g \circ f$.

b) *f* é inversa da função *g*? Justifique.

41. Considere as funções $f:\mathbb{R}\setminus\{0\}\to\mathbb{R}\setminus\{1\}$ e $g:\mathbb{R}\setminus\{1\}\to\mathbb{R}\setminus\{0\}$ definidas por $f(x)=1-\dfrac{1}{x}$ e $g(x)=\dfrac{1}{1-x}$.

a) Determine as funções compostas $f \circ g$ e $g \circ f$.

b) *f* é inversa da função *g*? Justifique.

42. Sejam $f:X\to Y$ e $g:Y\to Z$ funções tais que $f^{-1}:Y\to X$, $g^{-1}:Z\to Y$ e $g\circ f:X\to Z$ estejam definidas. Mostre que $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

O ensino de estruturas algébricas na Licenciatura em Matemática é essencial

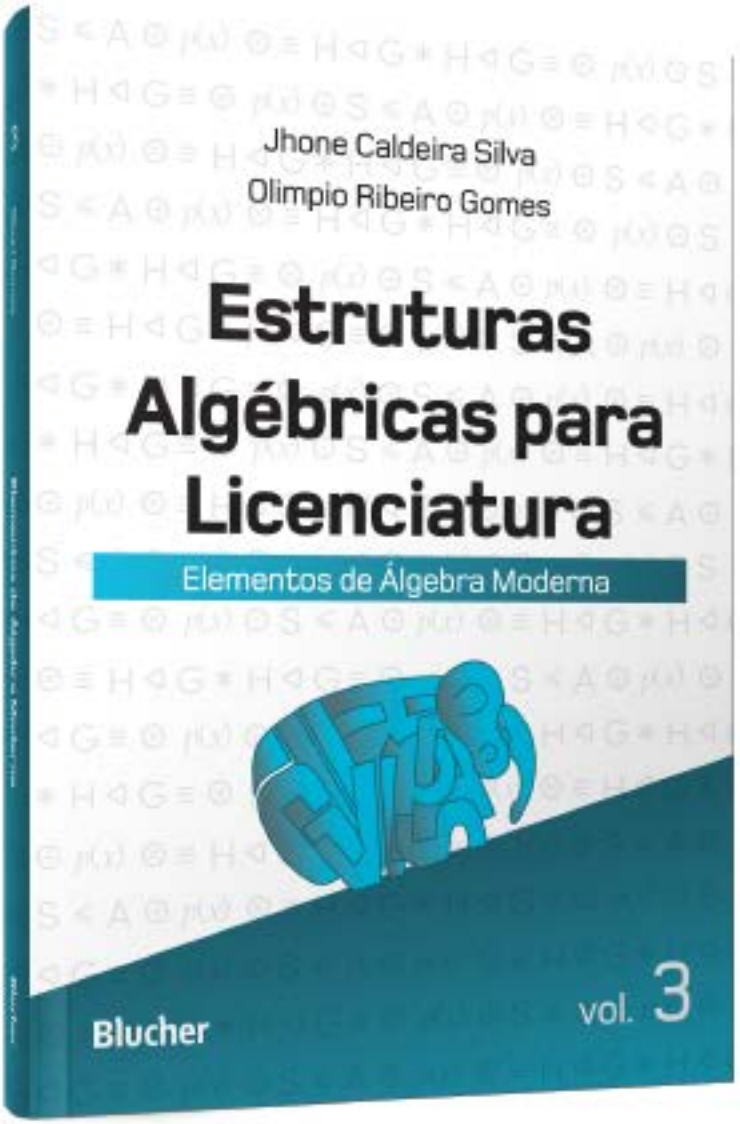
Estruturas Algébricas para Licenciatura é um conjunto de obras que visa auxiliar professores e alunos no processo de ensino e aprendizagem de fundamentos básicos de Matemática, da teoria de conjuntos e das principais estruturas algébricas. Buscamos sanar dificuldades relacionadas à linguagem e ao conteúdo, oferecendo textos dialogados e ricos em detalhes. As demonstrações são desenvolvidas com clareza; exemplos e exercícios são apresentados com o intuito de facilitar o entendimento e a aplicação dos resultados. Ao final de cada livro, apresentamos respostas de alguns exercícios propostos. Neste volume, *Elementos de Álgebra Moderna*, abordamos o estudo das estruturas algébricas básicas: grupos, anéis e corpos, partindo do estudo detalhado das operações binárias, passando pelos principais tópicos da Álgebra Moderna, até os anéis de polinômios.

www.blucher.com.br

ISBN 978-85-212-1853-1

9 788521 218531

Blucher



Clique aqui e:

VEJA NA LOJA

Estruturas algébricas para licenciatura - Volume 3

Elementos de Álgebra Moderna

Jhone Caldeira Silva, Olimpio Ribeiro Gomes

ISBN: 9788521218531

Páginas: 506

Formato: 17 x 24 cm

Ano de Publicação: 2020

Peso: 0.810 kg
