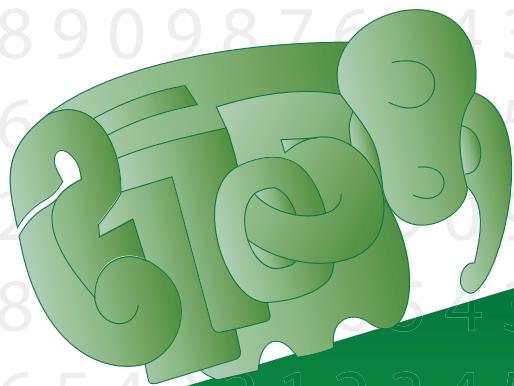


Jhone Caldeira Silva

Olimpio Ribeiro Gomes

# Estruturas Algébricas para Licenciatura

Elementos de Aritmética Superior



Blucher

vol. 2

Jhone Caldeira Silva  
Olimpio Ribeiro Gomes

# ESTRUTURAS ALGÉBRICAS PARA LICENCIATURA

VOLUME 2

ELEMENTOS DE ARITMÉTICA SUPERIOR

*Estruturas algébricas para licenciatura: volume 2 – Elementos de Aritmética Superior*

© 2018 Jhone Caldeira Silva, Olimpio Ribeiro Gomes

Editora Edgard Blücher Ltda.

*Arte da capa:* Éric Flávio de Araújo, Ana Paula Chaves 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.

É proibida a reprodução total ou parcial por  
quaisquer meios sem autorização escrita da  
editora.

---

Todos os direitos reservados pela Editora  
Edgard Blücher Ltda.

---

## FICHA CATALOGRÁFICA

---

Silva, Jhone Caldeira  
Estruturas algébricas para licenciatura : Elementos  
de Aritmética Superior – volume 2 / Jhone Caldeira  
Silva, Olimpio Ribeiro Gomes. – São Paulo : Blucher,  
2018.  
300 p. : il.

Bibliografia  
ISBN 978-85-212-1146-4

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

16-1532

CDD 510.7

---

Índice para catálogo sistemático:  
1. Matemática – Estudo e ensino

# CONTEÚDO

## **CAPÍTULO 1 – A CONSTRUÇÃO DO CONJUNTO**

### **DOS NÚMEROS NATURAIS ..... 17**

1.1	Os Axiomas de Peano.....	17
1.2	Adição de números naturais.....	21
1.3	Multiplicação de números naturais.....	26
1.4	Ordenação dos números naturais.....	31
1.5	Subtração de números naturais.....	34
1.6	Ordem estrita.....	36
1.7	O Princípio da Boa Ordenação.....	38
	O Princípio da Boa Ordenação e o Axioma de Indução Finita.....	40

Apêndice: relações em um conjunto..... 41

Apêndice: a crise dos fundamentos..... 49

Apêndice: contagem de elementos de um conjunto..... 51

Exercícios propostos..... 53

### **CAPÍTULO 2 – O CONJUNTO DOS NÚMEROS INTEIROS..... 57**

2.1	Os números inteiros.....	57
2.2	Adição e multiplicação de números inteiros.....	60
2.3	Subtração de números inteiros.....	71

2.4	Ordenação dos números inteiros .....	72
2.5	Ordem estrita .....	74
2.6	Valor absoluto .....	76
2.7	O Princípio do Menor Inteiro .....	77
2.8	Primeiro Princípio de Indução .....	80
2.9	Segundo Princípio de Indução .....	84
	Exercícios propostos .....	86

### **CAPÍTULO 3 – DIVISIBILIDADE EM $\mathbb{Z}$ E APLICAÇÕES ..... 91**

3.1	Divisibilidade em $\mathbb{Z}$ .....	91
	Múltiplos e divisores: divisão exata .....	92
3.2	O Algoritmo da Divisão .....	96
3.3	Máximo divisor comum e mínimo múltiplo comum .....	104
	O máximo divisor comum .....	104
	O Algoritmo de Euclides ou Processo das Divisões Sucessivas .....	111
	Inteiros primos entre si .....	113
	O mínimo múltiplo comum .....	117
	Exercícios propostos .....	120

### **CAPÍTULO 4 – NÚMEROS PRIMOS ..... 129**

4.1	O Teorema Fundamental da Aritmética .....	129
4.2	Fatoração-padrão ou decomposição primária .....	135
	Apêndice: números perfeitos, números de Mersenne e números de Fermat .....	145
	Exercícios propostos .....	148

### **CAPÍTULO 5 – EQUAÇÕES DIOFANTINAS E ARITMÉTICA MÓDULO $m$ .... 153**

5.1	Equações diofantinas lineares .....	153
	Equações diofantinas lineares a duas incógnitas .....	153
	Soluções com restrições .....	159
5.2	A aritmética modular .....	162
	A relação de congruência módulo $m$ .....	162
	Equações de congruências lineares .....	170
	Sistemas completos de resíduos .....	178
	Operações módulo $m$ .....	181
	Aplicações: critérios de divisibilidade .....	186

Apêndice: o Princípio da Casa dos Pombos.....	190
Exercícios propostos.....	198

**CAPÍTULO 6 – ALGUNS TEOREMAS CLÁSSICOS  
DA TEORIA DOS NÚMEROS .....209**

6.1	Funções aritméticas .....	210
	Funções aritméticas multiplicativas .....	210
	A Função $\varphi$ de Euler .....	211
	A Função $\mu$ de Möbius.....	214
6.2	Alguns teoremas clássicos.....	216
	Pequeno Teorema de Fermat .....	216
	Teorema de Euler .....	218
	Teorema de Wilson .....	220
	Teorema Chinês dos Restos.....	222
6.3	Resíduos quadráticos e a Lei da Reciprocidade Quadrática .....	231
	Resíduos quadráticos .....	231
	O Símbolo de Legendre e um Critério de Euler .....	239
	Apêndice .....	255
	Exercícios propostos.....	261

**RESPOSTAS DE ALGUNS EXERCÍCIOS .....271**

**REFERÊNCIAS BIBLIOGRÁFICAS .....299**

# CAPÍTULO 1

## A CONSTRUÇÃO DO CONJUNTO DOS NÚMEROS NATURAIS

Neste capítulo apresentamos uma construção lógico-formal do conjunto dos números naturais. Postularemos a existência de um conjunto satisfazendo certos axiomas e investigaremos que propriedades tal conjunto detém. De início, adotaremos a postura de ignorar conhecimentos que já temos a respeito da natureza desse conjunto, por exemplo, admitiremos sequer conhecer que  $2 + 2 = 4$  para a adição de naturais. A finalidade disso está em “desbravarmos” propriedades puramente por meio das ferramentas da lógica. Gradualmente, à medida que formos demonstrando tais propriedades, esse conjunto irá se tornando mais familiar.

### 1.1 OS AXIOMAS DE PEANO

Deve-se a Giuseppe Peano (1858-1932) a constatação de que se pode elaborar toda a teoria dos números naturais a partir de alguns poucos fatos básicos, conhecidos atualmente como os *Axiomas de Peano*. Trata-se de algumas propriedades fundamentais das quais resultam, como consequências lógicas, todas as afirmações verdadeiras que se podem fazer sobre esses números.

Nossa abordagem aqui segue de perto essas ideias, porém trilhamos um caminho ligeiramente diferente.

#### Postulado 1.1.1

Existem um conjunto  $\mathbb{N}$  e uma função  $s : \mathbb{N} \rightarrow \mathbb{N}$  que satisfazem os axiomas a seguir.

(i) Se  $n, m \in \mathbb{N}$  e  $n \neq m$ , então  $s(n) \neq s(m)$ .

- (ii) Existe um elemento  $0 \in \mathbb{N}$  tal que  $s(n) \neq 0$ , para todo  $n \in \mathbb{N}$ .
- (iii) Se um subconjunto  $X \subset \mathbb{N}$  é tal que  $0 \in X$  e  $s(X) \subset X$ , então  $X = \mathbb{N}$ . (Equivalentemente, se um subconjunto  $X \subset \mathbb{N}$  é tal que  $0 \in X$  e  $s(r) \in X$  sempre que  $r \in X$ , então  $X = \mathbb{N}$ .)

- **O conjunto dos números naturais:** o conjunto  $\mathbb{N}$  é chamado de *conjunto dos números naturais* e seus elementos são os *números naturais*.

Reiteramos que, apesar do nome familiar, ainda admitimos conhecer bem pouco sobre esse conjunto, conforme combinamos na introdução deste capítulo. Em verdade, tudo o que conhecemos sobre  $\mathbb{N}$  até agora é o que está estabelecido no Postulado 1.1.1: sabemos que o conjunto  $\mathbb{N}$  existe e que, segundo o conceito de função, a cada número natural  $n$  está associado um único número natural  $s(n)$ , o qual chamaremos de *sucessor de  $n$* .

O axioma (i) nos diz que números naturais distintos possuem sucessores distintos (equivalentemente, números naturais que tenham o mesmo sucessor são eles próprios iguais); (ii) nos diz que  $\mathbb{N}$  possui um elemento especial, chamado de *zero*,<sup>1</sup> que não é sucessor de nenhum número natural – apesar disso, ele possui um sucessor, pois, do contrário,  $s$  não seria uma função; já o axioma (iii), conhecido como *Axioma de Indução Finita*, nos diz que se uma coleção  $X$  de números naturais contém o zero e também o sucessor de todo elemento de  $X$ , então  $X$  coincide com o conjunto de todos os números naturais.

Mais adiante faremos uma análise mais detalhada do Axioma de Indução Finita. Por ora, nós o usaremos para provar algumas propriedades elementares do conjunto  $\mathbb{N}$ . Antes, porém, convém informar que o axioma (ii) nos diz que  $\mathbb{N} \neq \emptyset$ , pois  $0 \in \mathbb{N}$ . Em verdade, se já “soubéssemos” contar e “conhecêssemos” o número dois, poderíamos até afirmar que o conjunto dos números naturais possui pelo menos “dois” elementos: o zero e seu sucessor, que deve ser diferente do próprio zero em razão do axioma (ii). Aliás, embora isto não conste explicitamente entre os axiomas, podemos afirmar que todo número natural é diferente do seu sucessor:

### Proposição 1.1.2

$s(n) \neq n$ , para todo  $n \in \mathbb{N}$ .

<sup>1</sup> 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 nesse conjunto por simplicidade e padronização de notação e para que tenhamos um elemento neutro para a operação de adição, como ficará evidente mais adiante. [11] apresenta uma discussão interessante acerca desse assunto.



### Demonstração

Seja  $X = \{n \in \mathbb{N} \mid s(n) \neq n\}$  o conjunto formado por todos os números naturais que diferem de seu próprio sucessor. Desejamos mostrar que  $X = \mathbb{N}$ , o que é equivalente a afirmar que  $s(n) \neq n$ , para todo  $n \in \mathbb{N}$ .

Em primeiro lugar, notemos que  $0 \in X$ , pois, pelo axioma (ii), 0 não é sucessor de nenhum número natural e, em particular, não pode ser sucessor de si próprio, donde  $s(0) \neq 0$ . Em seguida, tomemos um elemento arbitrário  $r \in X$ . Pela definição do conjunto  $X$ , isso significa que  $s(r) \neq r$ , ou seja,  $r$  e seu sucessor  $s(r)$  são números naturais distintos, o que significa, em razão do axioma (i), que os sucessores desses números naturais – de  $s(r)$  e  $r$  – são também distintos, ou seja,  $s(s(r)) \neq s(r)$ . Isso significa que o número  $s(r)$  também é elemento de  $X$ .

De tudo o que foi dito, vemos que  $X$  é subconjunto de  $\mathbb{N}$  tal que  $0 \in X$  e  $s(r) \in X$  sempre que  $r \in X$ . Por força do axioma (iii), somos levados a concluir que  $X = \mathbb{N}$ , como queríamos demonstrar. ■

O axioma (ii) nos diz que o número zero não é sucessor de nenhum número natural. Perguntamos se há outro número natural com essa propriedade. A resposta está na próxima proposição:

### Proposição 1.1.3

Se  $n \in \mathbb{N}$  e  $n \neq 0$ , então existe  $a \in \mathbb{N}$  tal que  $s(a) = n$ .

### Demonstração

Seja  $X = \{0\} \cup \{n \in \mathbb{N} \mid n \neq 0 \text{ e } n = s(a), \text{ para algum } a \in \mathbb{N}\}$ , o conjunto formado pelo zero e por todos os números naturais  $n$  que são sucessores de algum outro natural  $a$ . Desejamos mostrar que  $X = \mathbb{N}$ , o que é equivalente a afirmar que todo natural diferente de zero é o sucessor de algum outro natural.

Em primeiro lugar, notemos que, pela construção do conjunto  $X$ , temos  $0 \in X$ . Em seguida, tomemos um elemento arbitrário  $r \in X$ . Se  $r = 0$ , claramente  $s(r) = s(0) \in X$  (pois  $s(0) \neq 0$ , pela Proposição 1.1.2, e  $s(0)$  é o sucessor do natural 0). Se  $r \neq 0$ , pela definição do conjunto  $X$ ,  $r = s(a)$ , para algum  $a \in \mathbb{N}$ , de modo que  $s(r) = s(s(a))$ , ou seja, também neste caso o número  $s(r)$  é elemento de  $X$ , uma vez que  $s(r) \neq 0$  e  $s(r)$  é o sucessor do natural  $s(a)$ .

De tudo o que foi dito, vemos que  $X$  é subconjunto de  $\mathbb{N}$  tal que  $0 \in X$  e  $s(r) \in X$  sempre que  $r \in X$ . Por força do axioma (iii), somos levados a concluir que  $X = \mathbb{N}$ . ■

- **Observação:** juntamente com o axioma (ii), a Proposição 1.1.3 nos diz que o número zero é o único número natural tal que, para todo  $n \in \mathbb{N}$ ,  $s(n) \neq 0$ . Em outros termos:

- O zero é o único natural que não é sucessor de outro natural.
- Todo número natural não nulo é sucessor de algum outro número natural.
- **Notação:** Façamos uma pequena pausa no desenvolvimento da teoria para estabelecer uma notação:
  - (i) Já sabemos que o sucessor de zero é diferente de zero. Usamos o símbolo 1 para representá-lo, ou seja,  $s(0) = 1$ . Tal elemento recebe o nome de *número um*.
  - (ii) O sucessor de 1 é diferente de 0 (já que zero não é sucessor de nenhum número natural) e também é diferente de 1 (por força da Proposição 1.1.2). Representamos pelo símbolo 2 – o qual chamamos de *número dois* – o sucessor de 1:  $s(1) = 2$ .
  - (iii) O sucessor de 2 é diferente de 0 (que não é sucessor de nenhum número natural), é diferente de 1 (pois 1 já é sucessor de outro número natural e o axioma (i) afirma que números naturais distintos possuem sucessores distintos), e do próprio 2 (por força da Proposição 1.1.2). Representamos pelo símbolo 3 – chamado de *número três* – o sucessor de 2.
  - (iv) Repetindo essa construção, obtemos uma sequência de números naturais

$$0, 1 = s(0), 2 = s(1), 3 = s(2), 4 = s(3), \dots$$

na qual cada elemento é diferente de todos os seus “antecessores”, sempre por uma destas razões: zero não é sucessor de nenhum número natural; e cada “antecessor” exceto o zero já é sucessor de outro número natural, e o axioma (ii) impõe que números naturais distintos possuam sucessores distintos.

Mais ainda, pela Proposição 1.1.3, todos os números naturais estarão escritos nessa lista quando a “terminarmos”. Isso nos gera um problema de ordem prática: rapidamente nossa criatividade para inventar novos símbolos para representar o sucessor de cada elemento que for surgindo em nossa lista se esgotará. Um sistema simbólico foi inventado para lidar com esse problema: o *Sistema Indo-Arábico de Numeração*, desenvolvido na Índia há mais de 1.500 anos e difundido pelos árabes, que o levaram à Europa, substituindo a escrita romana.

O sistema utiliza apenas os símbolos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9 – chamados de *algarismos* – para representar todos os números naturais e leva em consideração a posição que o algarismo ocupa – razão pela qual dizemos que trata-se de um sistema *posicional*. A ideia para conseguir isso é dar a cada algarismo um “valor” dependente de sua posição na escrita do número. O sucessor de 9 é representado por 10; o sucessor de 10 por 11; o de 11 por 12; o de 12 por 13; e assim continuamos até obtermos 19. Até este momento, já utilizamos todos os algarismos, estando o algarismo 1 ocupando a segunda posição (da direita para a esquerda); passamos então a usar o algarismo 2

na segunda posição (da direita para a esquerda), representando o sucessor de 19 por 20; o de 20 por 21; e assim até obtermos 29. Procedemos sucessivamente e, quando a primeira e a segunda posições já tiverem usado todos os algarismos, iniciamos o uso de uma terceira posição (a terceira posição da direita para a esquerda começa a ser utilizada para representar 100 como sendo o sucessor de 99, e essa etapa do processo segue até o natural 999). Isso pode ser repetido indefinidamente.

Voltemos ao desenvolvimento geral. Nosso próximo passo é definir as operações de adição e de multiplicação em  $\mathbb{N}$ .

## 1.2 ADIÇÃO DE NÚMEROS NATURAIS

Adotaremos a seguinte postura: iniciaremos definindo a operação de adição por meio de uma função que satisfaça certos axiomas, mesmo sem a garantia de que tal função exista ou que seja única; em seguida, nos preocuparemos com tais problemas; depois fixaremos alguma notação e nos dedicaremos às principais propriedades dessa operação.

### Definição 1.2.1

Chamamos de *operação de adição* em  $\mathbb{N}$  a função  $a : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  que satisfaz os axiomas a seguir.

$$(A1) \quad a(x, 0) = x, \text{ para todo } x \in \mathbb{N};$$

$$(A2) \quad a(x, s(y)) = s(a(x, y)), \text{ para todos } x, y \in \mathbb{N}.$$

Um primeiro problema que se impõe é o da existência e unicidade de uma função satisfazendo os axiomas da Definição 1.2.1, isto é, se de fato  $a(u, v)$  está definida para todos os pares de números naturais  $u$  e  $v$  e se isso se dá de modo único. Para ver que a resposta é afirmativa, façamos assim: fixado  $u \in \mathbb{N}$  escolhido arbitrariamente, consideremos o conjunto

$$X = \{v \in \mathbb{N} \mid \text{existe um único } w \in \mathbb{N} \text{ tal que } a(u, v) = w\}.$$

Notemos inicialmente que  $0 \in X$ , pois  $a(u, 0)$  existe e é único, uma vez que foi escolhido como sendo igual a  $u$  (isso é o que o axioma (A1) nos diz). Agora, tomemos um elemento arbitrário  $r \in X$ . Isso significa que existe um único  $w_0 \in \mathbb{N}$  tal que  $a(u, r) = w_0$ . O que dizer de  $a(u, s(r))$ ? Ora, pela escolha feita no axioma (A2), devemos ter  $a(u, s(r)) = s(a(u, r)) = s(w_0)$ . Como tanto  $w_0$  quanto  $s(w_0)$  existem e estão univocamente determinados, este por  $s$  ser uma função (Postulado 1.1.1), aquele pela

definição do conjunto  $X$ , o mesmo ocorre com  $a(u, s(r))$ . De tudo o que foi dito, vemos que  $X$  é subconjunto de  $\mathbb{N}$  tal que  $0 \in X$  e  $s(r) \in X$  sempre que  $r \in X$ . Por força do axioma (iii) do Postulado 1.1.1, somos levados a concluir que  $X = \mathbb{N}$ , o que garante a existência e unicidade da função que define a operação de adição.

- **Notação:** Simplificamos a representação usando a notação  $a(x, y) = x + y$ . Assim, os axiomas da Definição 1.2.1 se reescrevem como:

$$(A1)' \quad x + 0 = x, \text{ para todo } x \in \mathbb{N};$$

$$(A2)' \quad x + s(y) = s(x + y), \text{ para todos } x, y \in \mathbb{N}.$$

Em  $x + y = z$ ,  $x$  e  $y$  são chamados de *parcelas*, enquanto  $z$  é chamado de *soma* de  $x$  e  $y$ .

O axioma (A2)' nos diz que adicionar  $x$  ao sucessor de  $y$  é o mesmo que tomar o sucessor da soma de  $x$  com  $y$ .

Passemos às principais propriedades da operação de adição de naturais.

### Proposição 1.2.2

Se  $x \in \mathbb{N}$ , então  $s(x) = x + 1$ .

#### Demonstração

Basta notar que, como  $s(0) = 1$ , aplicando a definição de adição, temos

$$x + 1 = x + s(0) = s(x + 0) = s(x),$$

onde a penúltima igualdade segue do axioma (A2)' e a última do (A1)'. ■

Isso significa que adicionar 1 a um número natural  $x$  é o mesmo que tomar seu sucessor. Vejamos um exemplo.

### Exemplo 1.2.3

Vamos provar que  $2 + 2 = 4$ . Como  $s(1) = 2$ , temos  $2 + 2 = 2 + s(1)$ . Pelo axioma (A2)', temos  $2 + s(1) = s(2 + 1)$ . Agora, aplicando a Proposição 1.2.2 com  $x = 2$ , obtemos  $2 + 1 = s(2)$ . Finalmente, juntando tudo isso com os fatos de que  $s(2) = 3$  e  $s(3) = 4$ , obtemos

$$2 + 2 = 2 + s(1) = s(2 + 1) = s(s(2)) = s(3) = 4.$$

Passemos à demonstração de uma sequência de propriedades da operação de adição de números naturais. Iniciamos provando que a soma de dois números naturais é nula somente quando tais números são eles próprios nulos:

### Proposição 1.2.4 (*Lei do Anulamento da Adição*)

Se  $a, b \in \mathbb{N}$  e  $a + b = 0$ , então  $a = 0$  e  $b = 0$ .

#### *Demonstração*

Suponhamos, por contradição, que  $b \neq 0$ . Então, pela Proposição 1.1.3, existe  $u \in \mathbb{N}$  tal que  $b = s(u)$ . Assim, pela hipótese  $a + b = 0$  e pela definição de adição, obtemos

$$0 = a + b = a + s(u) = s(a + u),$$

o que contradiz o fato de zero não ser sucessor de nenhum número natural. Portanto, devemos ter  $b = 0$ , o que implica, diretamente pela hipótese, que  $a = 0$  (pois teremos  $a + 0 = 0$  e, pela definição de adição, devemos ter  $a + 0 = a$ , donde  $a = a + 0 = 0$ ). ■

A próxima proposição nos auxiliará nos cálculos que eventualmente venhamos a realizar com a adição de números naturais.

### Proposição 1.2.5

Sejam  $a, b, c \in \mathbb{N}$ . Então:

- (a)  $a + (b + c) = (a + b) + c$ ;
- (b)  $0 + a = a$ ;
- (c)  $a + b = b + a$ ;
- (d) se  $a + b = c + b$ , então  $a = c$ .

#### • *Observações*

(i) Alguns comentários acerca de cada uma das propriedades antes de demonstrá-las:

Em (a), a presença dos parênteses indica onde a adição deve ser efetuada em primeiro lugar. Assim, no primeiro membro, devemos primeiro obter a soma  $b + c$  para depois adicioná-la a  $a$ , enquanto no segundo membro devemos primeiro obter a soma  $a + b$  para depois adicionar-lhe  $c$ . Como são dois caminhos distintos, é “surpreendente” que ocorra a igualdade independentemente de quais sejam os números naturais  $a, b$  e  $c$ , o que justifica o uso de um nome especial: *propriedade associativa da adição*.

A propriedade (b) e o axioma (A1)' nos dizem que o número zero é um *elemento neutro* para a operação de adição.

A propriedade (c), conhecida como *propriedade comutativa da adição*, nos diz que a adição de  $a$  com  $b$  produz a mesma soma que a adição de  $b$  com  $a$ . Sumarizamos isso dizendo que a *ordem das parcelas não altera a soma*.

Em (d) temos a chamada Lei do Cancelamento da Adição, que tem grande utilidade quando estamos a resolver equações. É interessante notar que, em razão da propriedade em (c), temos que também vale o cancelamento: se  $b + a = b + c$ , então  $a = c$ .

(ii) No que segue, será bastante comum utilizarmos o Axioma de Indução para demonstrar algumas propriedades. A argumentação sempre objetivará concluir que o conjunto  $X$ , em que certa propriedade é verdadeira, coincide exatamente com  $\mathbb{N}$ . Isso consiste, segundo o Axioma de Indução, em mostrar que  $0 \in X$  e que  $s(r) \in X$  sempre que  $r \in X$ . No Capítulo 2, o leitor terá a oportunidade de conhecer um método de demonstração chamado Primeiro Princípio de Indução Finita, que será estabelecido para demonstrar propriedades válidas em subconjuntos do conjunto dos números inteiros e, assim, em particular, também poderá ser aplicado ao conjunto (e aos subconjuntos) dos números naturais. As argumentações feitas aqui e no Capítulo 2 com o Primeiro Princípio de Indução são praticamente idênticas sob o ponto de vista matemático, possuindo apenas roupagens diferentes. Aqui nosso objetivo é ilustrar uma argumentação (demonstração) por indução como uma aplicação de um dos Axiomas de Peano. Já no Capítulo 2, desejamos apresentar tal argumentação como uma técnica de demonstração válida em subconjuntos do conjunto dos números inteiros.

Passemos à demonstração da Proposição 1.2.5:

### *Demonstração da Proposição 1.2.5*

- (a) Considerando fixados os números  $a$  e  $b$ , definamos o seguinte conjunto:  $C = \{c \in \mathbb{N} \mid a + (b + c) = (a + b) + c\}$ . Em primeiro lugar, notemos que  $0 \in C$ , pois, fazendo uso do axioma (A1)', temos

$$a + (b + 0) = a + b = (a + b) + 0.$$

Em seguida, tomemos um elemento arbitrário  $r \in C$ . Pela definição do conjunto  $C$ , temos  $a + (b + r) = (a + b) + r$ . Usando esse fato e o axioma (A2)', obtemos

$$\begin{aligned} a + (b + s(r)) &= a + s(b + r) \\ &= s(a + (b + r)) \\ &= s((a + b) + r) \\ &= (a + b) + s(r), \end{aligned}$$

o que mostra que o número  $s(r)$  é elemento de  $C$ . Pelo Axioma de Indução, obtemos  $C = \mathbb{N}$ .

Isso significa que a igualdade  $a + (b + c) = (a + b) + c$  é válida para todo  $c \in \mathbb{N}$ , fixados os naturais  $a$  e  $b$ . Dada a arbitrariedade dos elementos fixados  $a$  e  $b$ , temos que a igualdade vale para todos  $a, b, c \in \mathbb{N}$ .

- (b) Definamos o conjunto  $A = \{a \in \mathbb{N} \mid 0 + a = a\}$ . Aplicando o axioma (A1)' com  $x = 0$ , obtemos  $0 + 0 = 0$ , o que mostra que  $0 \in A$ . Agora tomemos um elemento  $r \in A$ . Pela definição do conjunto  $A$ , temos  $0 + r = r$ . Assim, pelo axioma (A2)', temos  $0 + s(r) = s(0 + r) = s(r)$ , de modo que  $s(r) \in A$ . O Axioma de Indução nos permite concluir que  $A = \mathbb{N}$ .

Isso significa que a igualdade  $0 + a = a$  é válida para todo  $a \in \mathbb{N}$ .

- (c) A demonstração seguirá duas etapas: primeiro demonstraremos que  $a + s(b) = s(a) + b$ , para todos  $a, b \in \mathbb{N}$ . Para tanto, fixemos  $a \in \mathbb{N}$  e definamos o conjunto  $B = \{b \in \mathbb{N} \mid a + s(b) = s(a) + b\}$ . Notemos inicialmente que  $0 \in B$ , pois, pelo axioma (A2)' e pela propriedade demonstrada em (b), temos

$$a + s(0) = s(a + 0) = s(0 + a) = 0 + s(a) = s(a) + 0.$$

Agora tomemos  $r \in B$ . Isso significa que  $a + s(r) = s(a) + r$ . Temos o seguinte:

$$a + s(s(r)) = s(a + s(r)) = s(s(a) + r) = s(a) + s(r),$$

o que mostra que  $s(r) \in B$ . Pelo Axioma de Indução, concluímos que  $B = \mathbb{N}$ .

Com isso, temos que a igualdade  $a + s(b) = s(a) + b$  é válida para todo  $b \in \mathbb{N}$ , fixado o natural  $a$ . Dada a arbitrariedade do elemento fixado  $a$ , temos que a igualdade vale para todos  $a, b \in \mathbb{N}$ .

Para a próxima etapa (mostrar que  $a + b = b + a$ , para todos  $a, b \in \mathbb{N}$ ), fixado  $a \in \mathbb{N}$ , definamos o conjunto  $D = \{b \in \mathbb{N} \mid a + b = b + a\}$  e notemos que, pelo axioma (A1)' e pela propriedade demonstrada em (b), temos  $a + 0 = a = 0 + a$ , de modo que  $0 \in D$ . Tomemos  $r \in D$ . Então  $a + r = r + a$ . Portanto,

$$a + s(r) = s(a + r) = s(r + a) = r + s(a) = s(r) + a,$$

onde a última igualdade decorre do que foi demonstrado na primeira etapa. Assim,  $s(r) \in D$ , de modo que, pelo Axioma de Indução,  $D = \mathbb{N}$ .

Isso significa que a igualdade  $a + b = b + a$  é válida para todo  $b \in \mathbb{N}$ , fixado o natural  $a$ . Dada a arbitrariedade do elemento fixado  $a$ , temos que a igualdade vale para todos  $a, b \in \mathbb{N}$ .

- (d) Aqui seremos um pouco mais sucintos. Seja  $E = \{b \in \mathbb{N} \mid \text{se } a + b = c + b, \text{ então } a = c\}$  e notemos que  $0 \in E$ , pois, uma vez admitido que valha a igualdade  $a + 0 = c + 0$ , não podemos negar que também valha  $a = c$  (lembre-se da definição de adição). Tomemos  $r \in E$ . Isso significa que se  $a + r = c + r$ , então  $a = c$ . O que dizer sobre o sucessor de  $r$ ? Ora, admitindo que  $a + s(r) = c + s(r)$ , temos

$$s(a + r) = a + s(r) = c + s(r) = s(c + r),$$

e, como números naturais que têm o mesmo sucessor são eles próprios iguais, devemos ter  $a + r = c + r$ , o que nos leva a  $a = c$ , uma vez que  $r \in E$ . Daí concluímos, pelo Axioma de Indução, que  $E = \mathbb{N}$ . ■

- **Observação:** é importante evidenciar a propriedade obtida e utilizada na demonstração que acabamos de apresentar:

$$\text{dados } a, b \in \mathbb{N}, \text{ temos } a + s(b) = s(a) + b.$$

### 1.3 MULTIPLICAÇÃO DE NÚMEROS NATURAIS

Passemos à operação de multiplicação. Como fizemos para a adição, iniciaremos definindo a operação de multiplicação por meio de uma função que satisfaça certos axiomas, mesmo sem a garantia de que tal função exista ou que seja única; em seguida, nos preocuparemos com tais problemas; depois, fixaremos alguma notação e nos dedicaremos às principais propriedades.

#### Definição 1.3.1

Chamamos de *operação de multiplicação* em  $\mathbb{N}$  a função  $m: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  que satisfaz os axiomas a seguir.

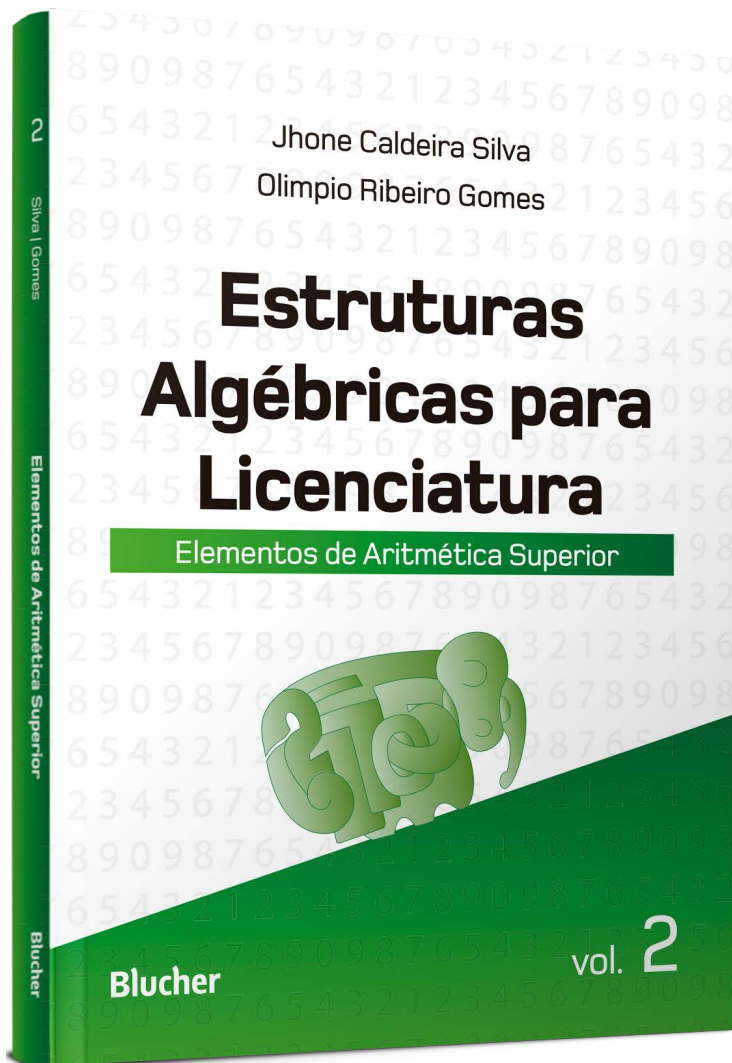
$$(M1) \quad m(x, 0) = 0, \text{ para todo } x \in \mathbb{N};$$

$$(M2) \quad m(x, s(y)) = m(x, y) + x, \text{ para todos } x, y \in \mathbb{N}.$$

Um primeiro problema que se impõe é o da existência e unicidade de uma função satisfazendo os axiomas da Definição 1.3.1, isto é, se de fato  $m(u, v)$  está definida para todos os pares de números naturais  $u$  e  $v$  e se isso se dá de modo único. Para ver que a resposta é afirmativa, façamos assim: fixado  $u \in \mathbb{N}$  escolhido arbitrariamente, consideremos o conjunto

$$X = \{v \in \mathbb{N} \mid \text{existe um único } w \in \mathbb{N} \text{ tal que } m(u, v) = w\}.$$





Clique aqui e:

[Veja na loja](#)

# Estruturas algébricas para licenciatura - Vol. 2

Jhone Caldeira Silva  
Olimpio Ribeiro Gomes

ISBN: 9788521211464

Páginas: 300

Formato: 17x42 cm

Ano de Publicação: 2018