ESTRUTURAS ALGÉBRICAS

Parham Salehyan

ESTRUTURAS ALGÉBRICAS

EDITORA UNICAMP

FICHA CATALOGRÁFICA ELABORADA PELO
SISTEMA DE BIBLIOTECAS DA UNICAMP
DIVISÃO DE TRATAMENTO DA INFORMAÇÃO
Bibliotecária: Maria Lúcia Nery Dutra de Castro – CRB-8ª / 1724

Sa32e

Salehyan, Parham
Estruturas algébricas / Parham Salehyan. – Campinas, SP : Editora da Unicamp, 2023.

1. Álgebra. 2. Grupos. 3. Anéis (Álgebra). 4. Domínios. 5. Módulos (Álgebra)

CDD – 512
– 512.2
– 512.4
– 519.76
– 512.42

ISBN 978-85-268-1617-6

Foi feito o depósito legal.

Direitos reservados a

Editora da Unicamp
Rua Sérgio Buarque de Holanda, 421 – 3º andar
Campus Unicamp
CEP 13083-859 – Campinas – SP – Brasil
Tel./Fax: (19) 3521-7718 / 7728
www.editoraunicamp.com.br – vendas@editora.unicamp.br

Sumário

Introdução

A álgebra é usada por praticamente todos os matemáticos independentemente de sua especialidade, e algum conhecimento de álgebra linear, de teoria dos grupos e dos anéis é necessário para compreender e resolver muitos problemas. Em geral, esses tópicos são introduzidos nos cursos de graduação.

Este livro é escrito para o leitor ter o primeiro contato com algumas das principais estruturas algébricas: grupos, anéis e módulos. Essas estruturas foram intensivamente estudadas nos últimos dois séculos.

O livro pode ser usado como texto para os cursos de álgebra em nível de graduação, e também como uma leitura complementar para aqueles que já conhecem esses assuntos, pois há alguns tópicos que em geral não são abordados nesses cursos.

Começaremos o livro com preliminares, uma revisão das noções básicas sobre conjuntos, relações, funções e aritmética dos inteiros. No primeiro capítulo, reunimos todos os resultados e notações que serão necessários ao longo do livro.

Em seguida, estudaremos grupos, anéis e módulos. Os exemplos são fundamentais para compreender os resultados e mostrar a necessidade das hipóteses nas proposições e nos teoremas. Por isso, em cada caso apresentaremos vários exemplos. Além disso, todos os capítulos são acompanhados de listas de exercícios com vários graus de dificuldade.

Algumas demonstrações são omitidas, pois em alguns casos são semelhantes às outras já feitas e por isso são deixadas como exercícios; ou requerem um estudo mais detalhado do assunto, e esse não é o objetivo deste livro.

Todas as referências bibliográficas utilizadas são disponibilizadas no final do livro. Nelas, o leitor pode encontrar as demonstrações omitidas e outros resultados citados ao longo do livro e também consultá-las para uma leitura complementar.

O objetivo é apresentar todos os conceitos e resultados da forma mais natural possível para que o leitor possa compreender a motivação e a razão

de existência de cada um. Além disso, sempre são colocados os dados históricos sobre os principais nomes que aparecem ao longo do texto.

Todas as sugestões e correções serão muito bem-vindas e poderão ser enviadas ao endereço *p.salehyan@unesp.br*

1. Preliminares

O objetivo deste capítulo é fazer uma breve revisão dos conceitos e resultados básicos que serão fundamentais no restante do livro. Por ser uma revisão, a maioria das demonstrações é omitida. O capítulo contém quatro seções. Na primeira, faremos uma revisão dos conceitos elementares da teoria dos conjuntos e, em seguida, da teoria elementar dos números, mais especificamente da aritmética dos inteiros. As duas últimas seções são dedicadas aos conceitos de função, relação e operações binárias.

1.1 Conjuntos

Não há uma definição para o conceito de conjunto, ou seja, não podemos defini-lo a partir de conceitos anteriormente definidos. Um conjunto é uma coleção de objetos na qual a ordem desses objetos não tem importância. Tais objetos são chamados de elementos do conjunto. Em geral, usamos letras maiúsculas para representar conjuntos e letras minúsculas para seus elementos. Se A é um conjunto e x um elemento de A, então escrevemos

$$x \in A,$$

caso contrário,

$$x \notin A.$$

Há várias maneiras de representar um conjunto. Pode ser de maneira explícita, ou seja, descrevendo todos os elementos do conjunto. Por exemplo, se os elementos de A são os números $1, 2$ e 3, então A é representado explicitamente da forma

$$A = \{1, 2, 3\}.$$

Outra forma é representar o conjunto por meio de uma condição pela qual seus elementos são identificados. Nessa representação, o conjunto A é dado por

$$A = \{x \in \mathbb{Z} \mid 1 \leq x \leq 3\},$$

onde $\mathbb{Z}$ é o conjunto dos números inteiros. Outro exemplo é o do conjunto dos números reais menores ou iguais a 2,

$$B = \{x \in \mathbb{R} \mid x \leq 2\},$$

onde $\mathbb{R}$ representa o conjunto dos números reais. São comuns representações do tipo $\{1,2,3,\ldots\}$ para o conjunto dos números inteiros positivos, ou $\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$ para o conjunto dos números inteiros.

Na descrição de um conjunto, a ordem e a repetição dos elementos não fazem diferença; por exemplo, $\{1,2,4\}$, $\{4,1,2\}$ e $\{1,2,2,1,4\}$ representam o mesmo conjunto.

Diremos que um conjunto é finito se possui um número finito de elementos; caso contrário, é infinito. As notações usuais para o número de elementos de um conjunto A são $|A|$ e $\#A$. O conjunto vazio é o conjunto que não possui nenhum elemento e é denotado[1] por $\{\}$, $\emptyset$ ou $\varnothing$.

Definição 1 Sejam A e B conjuntos. Dizemos que A é subconjunto de B e escrevemos $A \subseteq B$ se todo elemento de A pertence a B, ou seja,

$$\forall x \in A \Rightarrow x \in B.$$

Caso contrário, escrevemos $A \nsubseteq B$.

Outros termos para dizer que A é subconjunto de B são *A está contido em B*, ou *B contém o conjunto A*.

Claramente, $\varnothing \subseteq A$ e $A \subseteq A$ para todo conjunto A. Observem que a relação de inclusão entre conjuntos não satisfaz a lei de tricotomia, ou seja, nem sempre podemos dizer que num par de conjuntos um é subconjunto do outro; por exemplo, $A = \{1,2\}$ e $B = \{1,3\}$.

Definição 2 Sejam A e B conjuntos. Dizemos que eles são iguais se $A \subseteq B$ e $B \subseteq A$. Nesse caso, escrevemos $A = B$.

Se $A \subseteq B$ e $A \neq B$, então dizemos que A é um *subconjunto próprio* de B e escrevemos $A \subsetneq B$ ou $A \subsetneqq B$. É comum usar notações $B \supseteq A$ (respectivamente, $B \supsetneq A$ e $B \supsetneqq A$) em lugar de $A \subseteq B$ (respectivamente, $A \subsetneq B$ e $A \subsetneqq B$).

1.1.1 Operações entre conjuntos

Nesta seção, definiremos as principais operações entre conjuntos, isto é, a construção de conjuntos novos a partir de conjuntos já existentes.

[1] As notações $\emptyset$ ou $\varnothing$ foram inventadas por André Weil, um dos membros do grupo Bourbaki, em 1939.

Definição 3 Sejam X um conjunto e $A, B \subseteq X$. A união de A e B é o conjunto

$$A \cup B := \{x \in X \mid x \in A \text{ ou } x \in B\},$$

e a interseção de A e B é

$$A \cap B := \{x \in X \mid x \in A \text{ e } x \in B\}.$$

Se $A \cap B = \varnothing$, então dizemos que A e B são disjuntos.

A próxima proposição reúne as propriedades da união e da interseção. As demonstrações seguem diretamente da definição.

Proposição 4 Sejam $A, B, C \subseteq X$. Então,

1. $A \subseteq A \cup B$ e $B \subseteq A \cup B$.
2. $A \cap B \subseteq A$ e $A \cap B \subseteq B$.
3. Comutatividade: $A \cup B = B \cup A$ e $A \cap B = B \cap A$.
4. $A \cup \varnothing = A$ e $A \cap \varnothing = \varnothing$.
5. Associatividade:

$$A \cup (B \cup C) = (A \cup B) \cup C,$$
$$A \cap (B \cap C) = (A \cap B) \cap C.$$

6. Distributividade:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Pela propriedade (5) na proposição (4), podemos definir a união e a interseção de conjuntos $A_1, \ldots, A_n$, $n \geq 3$, por

$$A_1 \cup \cdots \cup A_n = (A_1 \cup \cdots \cup A_{n-1}) \cup A_n$$

e

$$A_1 \cap \cdots \cap A_n = (A_1 \cap \cdots \cap A_{n-1}) \cap A_n.$$

Mais geralmente podemos definir as operações acima para qualquer família de subconjuntos de X. Seja $I \neq \varnothing$ um conjunto. Para cada $i \in I$ considerem um subconjunto A_i de X. O conjunto $\{A_i \mid i \in I\}$, denotado também por $\{A_i\}_{i \in I}$, é chamado de uma família de subconjuntos de X.

Definição 5 (União e Interseção Generalizadas) Seja $\{A_i\}_{i\in I}$ uma família de subconjuntos de X. Por definição,

$$\bigcup_{i\in I} A_i = \{x \mid \exists i \text{ tal que } x \in A_i\}$$

e

$$\bigcap_{i\in I} A_i = \{x \mid \forall i,\ x \in A_i\}.$$

Definição 6 Sejam $A, B \subseteq X$. A diferença entre A e B é:

$$A \setminus B := \{x \in X \mid x \in A \text{ e } x \notin B\}.$$

O conjunto $A^c := X \setminus A$ é chamado de complementar de A em X.

Na próxima proposição, apresentaremos as propriedades de diferença.

Proposição 7 Sejam $A, B \subseteq X$.

1. $A = B \iff A^c = B^c$.
2. Leis de Morgan: $(A \cup B)^c = A^c \cap B^c$ e $(A \cap B)^c = A^c \cup B^c$.
3. $A \setminus B = A \cap B^c$.
4. $(A^c)^c = A$.
5. $X^c = \varnothing$ e $\varnothing^c = X$.
6. $A \cap A^c = \varnothing$.
7. $A \cup A^c = X$.

Prova. Como exercícios a cargo dos leitores. □

Definição 8 Sejam $A, B \subseteq X$. A diferença simétrica entre A e B é definida por

$$A\Delta B := (A \setminus B) \cup (B \setminus A).$$

Por exemplo, se $A = \{1,2,3\}$ e $B = \{3,4\}$, então $A\Delta B = \{1,2\} \cup \{4\} = \{1,2,4\}$.

Proposição 9 Sejam $A, B, C \subseteq X$. Então:

1. $A\Delta B = (A \cup B) \setminus (A \cap B)$
2. $A\Delta B = B\Delta A$

3. $A\Delta B = \varnothing \iff A = B$
4. $A\Delta B = X \iff A \cup B = X$ e $A \cap B = \varnothing$. Em particular, $A\Delta A^c = X$
5. $A\Delta(B\Delta C) = \Big(A \cup B \cup C) \setminus ((A \cap B) \cup (A \cap C) \cup (B \cap C)\Big) \cup (A \cap B \cap C)$
6. $(A\Delta B)\Delta C = A\Delta(B\Delta C)$
7. $A\Delta B = A \iff B = \varnothing$
8. $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$
9. $(A \cup B)\Delta(A \cup C) \subseteq A \cup (B\Delta C)$

Prova. Os itens 1 a 4 e 7 e 8 seguem diretamente da definição. O item 6 é consequência direta do item 5. □

A propriedade (6) da proposição (9) garante a associatividade da diferença simétrica, e por isso podemos definir a diferença simétrica dos conjuntos $A_1, A_2, \ldots, A_n$ da seguinte forma:

$$A_1\Delta\cdots\Delta A_n := (A_1\Delta\cdots\Delta A_{n-1})\Delta A_n, \;\; n \geq 3.$$

1.1.2 Produto Cartesiano

As operações definidas na seção anterior possuem um ponto em comum: a partir de dois subconjuntos de um conjunto X, fornecem um terceiro subconjunto de X, ou seja, o resultado vive no mesmo ambiente[2]. Esse é exatamente o conceito de operação que estudaremos na seção 1.4. A próxima construção possui uma natureza um pouco diferente. Primeiro temos de definir a noção de par ordenado. Essa noção foi apresentada em 1920 por Kuratowski[3].

Definição 10 Sejam X um conjunto e $A, B \subseteq X$. Dados $a \in A$ e $b \in B$, o par ordenado (a,b) é definido por

$$(a,b) := \{\{a\}, \{a,b\}\}.$$

Observem a diferença entre o par ordenado (a,b) e o conjunto $\{a,b\}$. Em geral $(a,b) \neq (b,a)$, mas $\{a,b\} = \{b,a\}$. De fato, a ideia de definir um par ordenado é essa. O intuito do Kuratowski foi introduzir a noção de ordem na teoria dos conjuntos. Vejam a próxima proposição.

[2]Comparem isso com as operações usuais entre números, entre matrizes etc.
[3]Kazimierz Kuratowski, matemático polonês, 1896-1980.

Proposição 11 Dois pares (a,b) e (c,d) são iguais, se, e somente se, $a = c$ e $b = d$.

Prova. Segue diretamente da definição. Separem os casos em que $a = b$ e $a \neq b$. □

Podemos generalizar a noção de pares ordenados para n-ulpas ordenadas para todo $n \geq 3$. O primeiro passo é definir uma tripla ordenada. A próxima proposição é necessária para isso.

Proposição 12 Sejam $A, B, C \subseteq X$ e $a \in A$, $b \in B$ e $c \in C$. Então, $(a,(b,c)) = ((a,b),c)$.

Prova. Segue diretamente da definição. □

Pela proposição (12), podemos definir uma tripla ordenada por

$$(a,b,c) = ((a,b),c),$$

e, mais geralmente, uma n-upla ordenada

$$(a_1,\ldots,a_n) := ((a_1,\ldots,a_{n-1}),a_n), \;\; n \geq 3.$$

A noção de par ordenado ou mais geralmente n-upla ordenada é o ingrediente principal para definir o produto cartesiano de conjunto. Mas antes seria interessante observar onde vive um par ordenado, ou seja, observar qual é o conjunto ao qual (a,b) pertence. Pela definição,

$$(a,b) = \{\{a\},\{a,b\}\}.$$

Os elementos a e b pertencem a A e B, respectivamente. Então, podemos considerá-los como elementos de $A \cup B$, ou seja, $\{a\},\{a,b\} \subseteq A \cup B$. Portanto, (a,b) é um conjunto cujos elementos são subconjuntos de $A \cup B$. Em outras palavras, estamos falando de um conjunto de subconjuntos de um conjunto. Essa noção é formalizada na seguinte definição:

Definição 13 Seja A um conjunto. O conjunto de todos os subconjuntos de A é chamado de conjunto das partes de A ou conjunto de potência de A e é denotado por $\mathscr{P}(A) := \{Y \mid Y \subseteq A\}$, ou 2^A.

Por exemplo, se $A = \{1,2\}$, então $\mathscr{P}(A) = \{\varnothing,\{1\},\{2\},\{1,2\}\}$.

Observações 14

- Pelo fato de que $\varnothing \subseteq A$ para todo conjunto A, concluímos que sempre $\varnothing \in \mathscr{P}(A)$, ou $\{\varnothing\} \subseteq \mathscr{P}(A)$. Isto é, $\mathscr{P}(A)$ nunca é vazio.

- Se $\#A = n$, então $\#\mathscr{P}(A) = 2^n$.

Proposição 15 Sejam A e B conjuntos. Então

$$A \subseteq B \Leftrightarrow \mathscr{P}(A) \subseteq \mathscr{P}(B).$$

Prova. Se $A \subseteq B$, então, para todo subconjunto de A é claramente subconjunto de B; logo, $\mathscr{P}(A) \subseteq \mathscr{P}(B)$. Reciprocamente, se $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, então de $A \in \mathscr{P}(A)$ concluímos que $A \in \mathscr{P}(B)$, ou seja, $A \subseteq B$. □

Agora voltamos a nossa pergunta anterior. Já observamos que (a,b) é um conjunto formado por subconjuntos de $A \cup B$. Pela definição (13), $\{a\}, \{a,b\} \in \mathscr{P}(A \cup B)$ ou $\{\{a\},\{a,b\}\} \subseteq \mathscr{P}(A \cup B)$, que por sua vez é equivalente a $\{\{a\},\{a,b\}\} \in \mathscr{P}(\mathscr{P}(A \cup B))$. Então

$$(a,b) \in \mathscr{P}(\mathscr{P}(A \cup B)).$$

Definição 16 Sejam A e B conjuntos. O produto cartesiano de A e B é

$$A \times B := \{(a,b) \mid a \in A \text{ e } b \in B\}.$$

Em geral, o produto cartesiano dos conjuntos $A_1, \ldots, A_n$ é definido por

$$A_1 \times \cdots \times A_n := \prod_{i=1}^{n} A_i = \{(a_1, \ldots, a_n) \mid a_i \in A_i, \forall i = 1, \ldots, n\}.$$

É comum denotar o produto cartesiano $\underbrace{A \times \cdots \times A}_{n \text{ vezes}}$ por A^n. O termo cartesiano vem do nome René Descartes[4], um dos inventores[5] da geometria analítica.

Por exemplo, se $A = \{a,b\}$ e $B = \{c\}$, então $A \times B = \{(a,c),(b,c)\}$. Se $A = B = \mathbb{R}$, então teremos $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, que geometricamente é o plano cartesiano que conhecemos na geometria analítica.

1.1.3 Diagrama de Venn

Uma ferramenta útil para visualizar as propriedades de conjuntos é utilizar os diagramas de Venn[6]. Sejam X um conjunto e $A, B \subseteq X$. A figura (1.1) mostra todas as configurações possíveis dos conjuntos A e B: na configuração (i) são disjuntos, em (ii) possuem elementos em comum e

[4] René Descartes, físico, filósofo e matemático francês, 1596-1650.
[5] O outro foi Pierre de Fermat, magistrado, matemática e cientista francês, 1607-1665.
[6] John Venn, matemático inglês, 1834-1923.

em (iii) um é subconjunto do outro. Vale observar que a configuração (iii) de fato tem dois casos: $A \subseteq B$ e $B \subseteq A$, e, dependendo do problema, devemos considerá-los separadamente. Ou seja, se quisermos verificar todas as possibilidades de alguma propriedade sobre dois conjuntos, deveremos considerar as quatro possibilidades, a não ser que haja simetria entre A e B na afirmação, i.e., se trocando A por B e vice-versa a afirmação continuar a mesma.

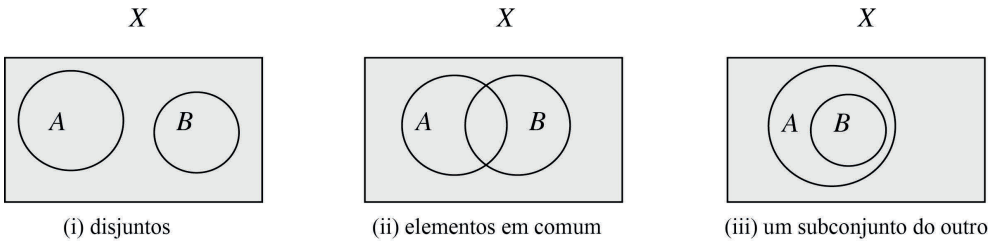

Figura 1.1: diagramas de Venn para dois conjuntos

Observem que esses diagramas não são eficientes para fazer demonstrações, pois, dependendo do número dos conjuntos, teremos muitas configurações, ou seja, muitos casos para verificar. Por exemplo, no caso de três conjuntos, a menos de simetria, há nove possibilidades.

Exercícios

1. Sejam $A, B, C \subseteq X$.

   (a) Se para todo $B \subseteq X$, $A \cap B = \varnothing$, então $A = \varnothing$.

   (b) Se para todo $B \subseteq X$, $A \cup B = X$, então $A = X$.

   (c) Se $A \Delta B = A \Delta C$, então $B = C$.

2. Sejam $A, B \subseteq X$. Provem que são equivalentes:

   (a) $A \subseteq B$

   (b) $A \cap B^c = \varnothing$

   (c) $A \cup B = B$

   (d) $B^c \subseteq A^c$

(e) $A \cap B = A$

(f) $A \cup (B \setminus A) \subseteq B$

3. Sejam $A, B \subseteq X$. Provem:

   (a) $(A\Delta B)^c = (A^c \cap B^c) \cup (A \cap B) = (A^c \cap B^c)\Delta(A \cap B)$

   (b) $A\Delta B = X \Leftrightarrow A = B^c$

   (c) $A \subseteq B \Leftrightarrow A\Delta B = B \setminus A$

4. Deem um exemplo para mostrar que no item (9) da proposição (9) a inclusão é própria, ou seja, que em geral não teremos a igualdade.

5. Mostrem que $A_1\Delta A_2\Delta\cdots\Delta A_n$ consiste em elementos que pertencem a um número ímpar dos conjuntos $A_1\Delta A_2\Delta\cdots\Delta A_n$. Usando esse fato, desenhem o diagrama de Venn de $A_1\Delta A_2\Delta A_3$ no caso em que $A_i \cap A_j \neq \varnothing$ para todo i e j. (Dica: por indução.)

6. Em cada item, determinem o conjunto da potência.

   (a) $A = \{1\}$

   (b) $D = \{\varnothing, \{\varnothing, \{\varnothing\}\}$

   (c) $B = \{1, \{1\}\}$

   (d) $E = \{\varnothing, F\}$, $F \neq \varnothing$ é um conjunto.

   (e) $C = \{\varnothing\}$

7. Sejam $A, B \subseteq X$. Mostrem que

   (a) $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$

   (b) $\mathscr{P}(A) \cup \mathscr{P}(B) \subsetneq \mathscr{P}(A \cup B)$

   (c) Verifiquem se, em geral, há alguma relação de inclusão entre $\mathscr{P}(A\Delta B)$ e $\mathscr{P}(A)\Delta\mathscr{P}(B)$.

   (d) Verifiquem se, em geral, há alguma relação de inclusão entre $\mathscr{P}(A \setminus B)$ e $\mathscr{P}(A) \setminus \mathscr{P}(B)$.

8. Sejam $\{A_i\}_{i\in I}$ uma família de subconjuntos de X. Mostrem que

   (a) $X \cap (\bigcup_{i\in I} A_i) = \bigcup_{i\in I}(X \cap A_i)$.

   (b) $X \cup (\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(X \cup A_i)$.

   (c) $X \setminus (\bigcup_{i\in I} A_i) = \bigcap_{i\in I}(X \setminus A_i)$.

   (d) $X \setminus (\bigcap_{i\in I} A_i) = \bigcup_{i\in I}(X \setminus A_i)$.

9. Sejam $A, B, C, D \subseteq X$. Provem:
   (a) $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$.
   (b) $(A \bigstar B) \times C = (A \times C) \bigstar (B \times C)$, onde $\bigstar$ é uma das operações $\cap, \cup$, $\setminus$ ou Δ.
   (c) $A \times B = \varnothing \Leftrightarrow A = \varnothing$ ou $B = \varnothing$.
   (d) $(C \times D) \setminus (A \times B) = (C \times (D \setminus B)) \cup ((C \setminus A) \times D)$.
   (e) Se $A \subseteq C$ e $B \subseteq D$, então $A \times B \subseteq C \times D$. Se $A \times B \neq \varnothing$, então vale a recíproca. Deem um exemplo para mostrar que a hipótese $A \times B \neq \varnothing$ é necessária.
   (f) Se $E \subseteq C \times D$, então existem $A \subseteq C$ e $B \subseteq D$ tais que $E = A \times B$?
   (g) Se $A \times B = C \times D \neq \varnothing$, então $A = C$ e $B = D$.
10. Desenhem, a menos de simetria, todas as configurações possíveis do diagrama de Venn para três conjuntos.
11. Sejam $A_1, A_2, \ldots$ conjuntos. Mostrem que existem conjuntos $B_1, B_2, \ldots$ dois a dois disjuntos tais que $B_i \subseteq A_i$ para todo i e $\bigcup_i A_i = \bigcup_i B_i$.

1.2 Aritmética dos Inteiros

Na teoria básica dos números, que basicamente estuda a teoria dos números no conjunto dos números inteiros, a indução finita possui um papel fundamental. Por isso, iniciaremos esta seção com esse tópico.

Usaremos as seguintes notações: $\mathbb{R}$ para o conjunto dos números reais, $\mathbb{Q}$ para o conjunto dos números racionais, $\mathbb{Z}$ para o conjunto dos números inteiros, e $\mathbb{N}$ para os números naturais, i.e., os números inteiros não negativos. Para representar os números positivos desses conjuntos, usaremos as notações $\mathbb{R}^+, \mathbb{Q}^+$ e $\mathbb{Z}^+$.

1.2.1 Indução Finita e Princípio da Boa Ordem

Uma ferramenta muito útil nas demonstrações dos resultados que envolvem números inteiros é o teorema de indução finita. O objetivo desta seção é estudar esse teorema.

Definição 17 Seja $\varnothing \neq A \subseteq \mathbb{R}$. Diremos que A é limitado inferiormente (respectivamente, superiormente), se existe $r \in \mathbb{R}$ tal que para todo $a \in A, r \leq a$ (respectivamente, $a \leq r$). Um conjunto é limitado se é limitado inferiormente e superiormente.

Por exemplo, $\mathbb{N}$ é limitado inferiormente; basta tomar $r = 0$; o intervalo $]1,2[$ é limitado inferiormente; basta tomar $r = 1$; e também superiormente; basta tomar $r = 2$. O intervalo $]-3,+\infty[$ é limitado inferiormente, mas não superiormente.

Observem que o número r na definição acima não é necessariamente um elemento de A e também não é único. Os subconjuntos limitados inferiormente ou superiormente dos números inteiros possuem uma propriedade muito importante que é formalizada na seguinte forma:

Princípio da Boa Ordem (P.B.O.) Todo subconjunto não vazio e limitado inferiormente (respectivamente, superiormente) de $\mathbb{Z}$ possui menor (respectivamente, maior) elemento.

Isto é, se $\varnothing \neq A \subseteq \mathbb{Z}$ é limitado inferiormente (respectivamente, superiormente), então

$$\exists m \in A \text{ tal que } \forall a \in A, m \leq a \text{ (respectivamente, } a \leq m).$$

É fácil verificar que nesses casos $m \in A$ é único.

Usando o P.B.O. podemos provar a indução finita. A forma mais usual da indução é dada no seguinte teorema:

Teorema 18 (Indução Finita) Seja $P(n)$ uma sentença associada a cada $n \in \mathbb{Z}$. Se

1. existe $n_0 \in \mathbb{Z}$ tal que $P(n_0)$ é verdadeira,
2. $P(k)$ é verdadeira implica que $P(k+1)$ é verdadeira, $k \geq n_0$,

então $P(n)$ é verdadeira para todo $n \in \mathbb{Z}$ tal que $n \geq n_0$.

Prova. Seja, por absurdo,

$$\exists n \in \mathbb{Z}, n > n_0, \text{ tal que } P(n) \text{ não é verdadeira.}$$

Então

$$\mathscr{V} := \{n \in \mathbb{N} \mid n > n_0 \text{ e } P(n) \text{ não é verdadeira}\} \neq \varnothing.$$

Portanto, pelo P.B.O, possui o menor elemento. Seja $m = \min \mathscr{V}$. Isto é, $m-1 \notin \mathscr{V}$, ou seja, $P(m-1)$ é verdadeira. Observem que $m > n_0$; logo, $m-1 \geq n_0$. Portanto, pela hipótese, $P((m-1)+1) = P(m)$ é verdadeira. Mas isso é absurdo. Essa contradição mostra $\mathscr{V} = \varnothing$. Então, $P(n)$ é verdadeira para todo $n \geq n_0$. □

Observações 19

- A condição (1) no teorema (18) é chamada de *primeiro passo da indução*; a validade de $P(k)$ é chamada de *hipótese da indução*; e $P(k+1)$ é a *tese da indução*.
- O teorema (18) vale se $P(n)$ for uma sentença associada a um subconjunto $A \neq \varnothing$ de $\mathbb{Z}$. Nesse caso, $n_0 \in A$.
- Outra forma de indução é dada pela substituição da condição (2) no teorema (18) por

  (2)' Dado $r > n_0$, se $P(k)$ é verdadeira para todo k, $n_0 \leq k < r$, então $P(r)$ também é verdadeira.
- O que fizemos aqui foi assumir o P.B.O e mostrar o teorema de indução. É possível fazer a recíproca, ou seja, assumir a indução como princípio e a partir disso mostrar o P.B.O. Isto é, a indução e o P.B.O são equivalentes.

Exemplos 20

1. Para todo $n \in \mathbb{N}$, $1 + \cdots + n = \frac{n(n+1)}{2}$.

   Nesse caso, o primeiro passo é óbvio: $1 = \frac{1+1}{2}$. Agora mostraremos que de $1 + \cdots + k = \frac{k(k+1)}{2}$ concluiremos $1 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2}$. Pela hipótese da indução

   $$1 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}.$$

   Portanto, pelo teorema da indução finita para todo $n \in \mathbb{N}$, $1 + \cdots + n = \frac{n(n+1)}{2}$.

2. A soma dos ângulos internos de um polígono convexo de n lados é $(n-2) \cdot 180^\circ, n \geq 3$.

   Nesse caso, $P(n)$ é a afirmação acima. O primeiro passo da indução é

   $$P(3) : \textit{soma dos ângulos internos de um triângulo é } (3-2) \cdot 180^\circ = 180^\circ.$$

   Essa afirmação é um fato conhecido da geometria euclidiana. Sejam $k \geq 3$ e $P(k)$ válida. Considerem o polígono convexo $A_1A_2 \cdots A_kA_{k+1}$