Solucionário

"Undergraduate Algebra: A Unified Approach"

Matej Brešar

Guilherme Garcia Nallin

nallinguilherme@gmail.com

Sumário

1 Glossary of Basic Algebraic Structures **2**
1.1 Binary Operations 2
1.2 Semigrupos e Monóides 6
1.3 Grupos 9

Capítulo 1

Glossary of Basic Algebraic Structures

1.1 Binary Operations

Exercício 1.17: *Let $\mathcal{P}(x)$ be the power set of the nonempty set X. The union, intersection, and set difference are binary operations on P(X). Determine which among them are associative, commutative, and have a (left or right) identity element.*

Solução: Sejam $A, B, C \in \mathcal{P}(X)$, assim, para a operação de união desses conjuntos, temos:

$$\begin{aligned}(A \cup B) \cup C &= A \cup (B \cup C)\\ (A \cup B) \cup C &= A \cup (C \cup B)\\ (A \cup B) \cup C &= (A \cup C) \cup B\end{aligned}$$

O que mostra que a operação de união é associativa. Além disso, temos que: $A \cup B = B \cup A$, o que mostra que a operação de união é comutativa. Por fim, o conjunto vazio é o elemento identidade para a operação de união, pois $A \cup \emptyset = \emptyset \cup A = A$.

Para a operação de interseção, podemos verificar a associatividade:

$$\begin{aligned}(A \cap B) \cap C &= A \cap (B \cap C)\\ (A \cap B) \cap C &= A \cap (C \cap B)\\ (A \cap B) \cap C &= (A \cap C) \cap B\end{aligned}$$

E o conjunto X é o elemento identidade para a interseção, uma vez que: $X \cap A = A \cap X = A$.

Por fim, a operação de diferença de conjuntos não é comutativa, tome o contraexemplo em que $A = \{1\}$, $B = \{1, 2\}$ e $C = \{2\}$, assim: $A - B = \emptyset$

mas $B - A = 2$. Para a associatividade, temos: $(A - B) - C = A - (B - C)$, e o conjunto vazio é o elemento identidade para a diferença de conjuntos, pois: $A - \emptyset = A$. $\square$

Exercício 1.18: *Determine which of the following binary operations on* $\mathbb{N}$ *are associative, have a (left or right) identity element, and contain two different elements that commute:*

(a) $m * n = m + 2n$;

(b) $m * n = m^2 n$;

(c) $m * n = m$;

(d) $m * n = m^n$.

Solução: Sejam $m, n, p \in \mathbb{N}$ então para o caso (a), a comutatividade é falsa, uma vez que $m * n = m + 2n \neq n + m = n + 2m$, já a associatividade falha em:

$$\begin{aligned}(m * n) * p &= (m + 2n) * p = m + 2n + 2p \\ \neq m * (n * p) &= m * (n + 2p) = m + 2n + 4p\end{aligned}$$

Vamos verificar se há elemento neutro da operação, para isso tome $e \in \mathbb{N}$, para $e = 1$:

$$\begin{aligned}&m * 1 = m + 2 \cdot 1 = m + 2 \\ &\neq 1 * m = 1 + 2m\end{aligned}$$

Se considerarmos $0 \notin \mathbb{N}$, acabou. Caso contrário, para $e = 0$:

$$\begin{aligned}&m * 0 = m + 2 \cdot 0 = m \\ &\neq 0 * m = 0 + 2m = 2m\end{aligned}$$

Assim, a operação admite elemento identidade à direita.

Para o item *(b)*, vamos verificar a comutatividade: $m * n = m^2 n \neq n * m = n^2 m$, basta tomar $m = 2$, $n = 3$ que falha. Para a associatividade falha também, basta tomar $m = 2, n = 1, m = 3$. Seja $e \in \mathbb{N}$ o elemento neutro, então $e * m = e^2 m = em = m$, no entanto $m * e = m^2 e = m^2$, o que demonstra que a operação admite identidade à esquerda.

Para o item *(c)*, vamos verificar a comutatividade: $m * n = m \neq n * m = n$, basta que $m \neq n$ para que falhe a propriedade. Vamos verificar a associatividade:

$$\begin{aligned} m * (n * p) &= m * n = m \\ &= (m * n) * p = m * p = m \end{aligned}$$

E a existência do elemento identidade segue por: $m * e = m \neq e * m = e$, porém isso implica que, sendo $e_1 = 2, e_2 = 3 \in \mathbb{N}$ temos $m * 2 = m = m * 3 \implies 2 = 3$, o que é falso, contradizendo o proposição de que, uma vez que existe elemento neutro, ele é único.

Para *(d)*, vamos verificar a comutatividade: $m * n = m^n \neq n * m = n^m$, basta tomar $m = 2$, $n = 3$ que falha. Para a associatividade falha também, basta tomar $m = 2, n = 1, p = 3$. Seja $e \in \mathbb{N}$ o elemento neutro, então $e * m = e^m = m$, no entanto $m * e = m^e = m$, o que demonstra que a operação admite identidade à esquerda.(d) $\square$

Exercício 1.19: *Let S be a set with a binary operation $*$. If subsets T and T' of S are closed under $*$, then so is their intersection $T \cap T'$. Find an example showing that this does not always hold for the union $T \cup T'$.*

Solução: Sejam $S = \mathbb{Z}, T = \{1, 0\}, T' = \{-1\}$ e a operação de adição definida em [1.1]. Assim, $1 + (-1) = 0 \notin T \cap T'$, porém $0 \in T \cup T'$.

... Procurarei um exemplo melhor.

$\square$

Exercício 1.20: *Find all finite nonempty subsets of Z that are closed under addition.*

Solução: Seja $A \subseteq \mathbb{Z}$ um subconjunto finito não vazio fechado sob adição. Vamos analisar os possíveis casos:

1. Se A contém apenas um elemento, então $A = \{a\}$ onde $a \in \mathbb{Z}$. Neste caso, A é fechado sob adição, pois $a + a = 2a \in A$ se e somente se $a = 0$. Portanto, $A = \{0\}$.

2. Se A contém mais de um elemento, seja a o menor elemento positivo em A. Como A é fechado sob adição, todos os múltiplos de a devem estar em A. No entanto, como A é finito, isso implica que A deve ser da forma $\{0, a, 2a, \ldots, ka\}$ para algum $k \in \mathbb{N}$.

3. Se A contém elementos negativos, seja $-b$ o menor elemento negativo em A. Similarmente, todos os múltiplos de $-b$ devem estar em A. Portanto, A deve ser da forma $\{-kb, \ldots, -b, 0, b, \ldots, jb\}$ para alguns $k, j \in \mathbb{N}$.

Portanto, os únicos subconjuntos finitos não vazios de $\mathbb{Z}$ que são fechados sob adição são da forma $\{0\}$ ou $\{-ka, \ldots, -a, 0, a, \ldots, ja\}$ para algum $a \in \mathbb{Z}$ e $k, j \in \mathbb{N}$. □

Exercício 1.20: *Let T be a nonempty subset of $\mathbb{Z}$. Consider the following conditions:*

(a) T is closed under subtraction.

(b) T is closed under addition.

(c) T is closed under multiplication.

Show that (a) implies both (b) and (c), whereas (b) and (c) are independent conditions (to establish the latter, find an example of a set satisfying (b) but not (c), and an example of a set satisfying (c) but not (b)). Also, find some examples of sets satisfying (a). Can you find them all?

Solução: Vamos mostrar que $(a) \implies (b)$. Tome $a \in \mathbb{Z}$,
$T = \{-ka, \ldots, -a, 0, a, \ldots, ja\}$ para algum $a \in \mathbb{Z}$ e $k, j \in \mathbb{N}$, sem perda de generalidade. Sendo assim, tome $-ka$ e ja e faça $(-ka)+(ja) = (-k+j)a = (j-k)a \in T$, pois T é fechado por subtração.

Vamos mostrar $(a) \implies (c)$. *finalizar...* □

Exercício 1.22: *How many binary operations are there on a set with n elements?*

Solução: Sejam A, B dois conjuntos finitos tais que $|A| = n$, $|B| = m$, assim, o número de mapeamentos (ou seriam funções ?) de A para B é igual a m^n, pois, para cada n-ésimo elemento de A existem m possibilidades de mapeamento em B. Este é um caso mais geral. Para a operação binária, seja S um conjunto finito tal que $|S| = n$, assim, os mapeamentos tais que $S \times S \longrightarrow S$ são $n^{n \cdot n} = n^{n^2}$. Pois, para cada elemento n-ésimo do conjunto de chegada S temos $n \cdot n$ elementos para serem escolhidos na tupla de partida que constitui $S \times S$. □

Exercício 1.23: *Let S be a set with two elements. Find a binary operation on S such that $(x * y) * z \neq x * (y * z)$ for all $x, y, z \in S$.*

Solução: *Comentário:* Note que o enunciado diz que S tem apenas dois elementos, porém em seguida ele declara três elementos x, y, z que pertencem a S. Caso forem distintos, há contradição. Caso contrário, $y = z$.

Sejam $x, y, z \in S$ e a operação binária $x * y = x + 2y$. Basta tomar $x = 1$, $y = 2, z = 1$ como exemplo. $\square$

Exercício 1.24: *Seja $f \in Map(\mathbb{Z})$ dada por $f(n) = n + 1$ para todo $n \in \mathbb{Z}$. Queremos determinar todos os elementos $g \in Map(\mathbb{Z})$ que comutam com f, ou seja, tais que:*

Solução: Seja $g \in Map(\mathbb{Z})$ tal que $g(n) = k + n$, $\forall\, k \in \mathbb{Z}$. Assim:

$$(f \circ g)(n) = k + n + 1 = (g \circ f)(n) = k + n + 1$$

$\square$

Exercício 1.25: *Denote by Inj(X) the set of all injective maps in Map(X), by Sur(X) the set of all surjective maps in Map(X), and by Bij(X) the set of all bijective maps in Map(X).*

(a) Prove that the sets Inj(X), Sur(X), Bij(X), Map$(X) \setminus$ Inj(X), and Map$(X) \setminus$ Sur(X) are closed under $\circ$.

(b) Prove that Inj(X) = Sur(X) = Bij(X) if X is a finite set.

(c) Prove that the set Map$(X) \setminus$ Bij(X) is closed under $\circ$ if and only if X is a finite set.

Solução:

$\square$

1.2 Semigrupos e Monóides

Exercício 1.40: *Show that $\mathbb{N}$ is a semigroup under the operation $m * n = max\{m, n\}$, as well as under the operation $m * n = min\{m, n\}$. Which one among them is a monoid?*

Solução: Primeiro, seja $*$ a operação tal que, dados $m, n, p \in \mathbb{N}$, então $m * n = max\{m, n\}$. Assim,

$$m * (n * p) = m * \max(n, p) = \max(m, n, p) = \max\{m, n\} * p = (m * n) * p$$

Para a operação $m * n = \min(m, n)$:

$$m * (n * p) = m * \min(n, p) = \min(m, n, p)$$
$$= \min(m, n) * p = (m * n) * p$$
$$.$$

Note que apenas no primeiro caso, podemos considerar $(\mathbb{N}, *)$ um monóide, uma vez que possui o elemento identidade $1 \in \mathbb{N}$:

$$m * 1 = \max(1, n) = \max(n, 1) = 1 * m, \, \forall m \in \mathbb{N}$$

□

Exercício 1.41: *Find all binary operations on the set $S = \{e, a\}$ for which S is a semigroup and e is a left identity element.*

Solução: Sendo e identidade à esquerda, podemos definir a operação $a * e = a$.

Para que S seja um semigrupo, a operação deve ser associativa. Vamos analisar todas as possíveis operações binárias em $S = \{e, a\}$:

1. $e * e = e$ 2. $e * a = a$ 3. $a * e = a$ 4. $a * a = x$, onde $x \in \{e, a\}$

Vamos verificar a associatividade para cada caso de $a * a$:

Caso 1: $a * a = e$

$$(a * a) * a = e * a = a \quad \text{e} \quad a * (a * a) = a * e = a$$

Neste caso, a operação é associativa.

Caso 2: $a * a = a$

$$(a * a) * a = a * a = a \quad \text{e} \quad a * (a * a) = a * a = a$$

Neste caso, a operação também é associativa.

Portanto, as operações binárias que fazem de S um semigrupo com e como identidade à esquerda são:

1. $e * e = e$, $e * a = a$, $a * e = a$, $a * a = e$ 2. $e * e = e$, $e * a = a$, $a * e = a$, $a * a = a$ □

Exercício 1.42: *Show that $\mathbb{R}$ is a semigroup under the operation $x * y = |x|y$. Does it have a left or right identity element? For each $x \in \mathbb{R}$, find all elements commuting with x.*

Solução: Devemos verificar a associatividade em $(\mathbb{R}, *)$. Para isso, tome $x, y, z \in \mathbb{R}$, daí:

$$
\begin{aligned}
x * (y * z) &= x * |y|z = |x|y||z = |xy|z \\
&= ||x|y|z = |x|y * z = (x * y) * z \\
&\implies x * (y * z) = (x * y) * z
\end{aligned}
$$

Agora, vamos determinar os elementos que comutam com x. Para $x \geq 0$, os elementos que comutam são $p \in \mathbb{R}$ tal que $p \geq 0$ e o contrário é válido. □

Exercício 1.43: *Show that* $\mathbb{Z}$ *is a monoid under the operation* $m * n = m + n + mn$. *Find all its invertible elements.*

Solução: Vamos mostrar que $(\mathbb{Z}, *)$ é um monóide. Verifiquemos a associatividade, para isso, considere $a, b, c \in \mathbb{Z}$.

$$
\begin{gathered}
a * (b * c) = a * (b + c + bc) = a + (b + c + bc) + ab + ac + abc \\
(a * b) * c = (a + b + ab) * c = (a + b + ab) + c + ac + bc + abc \\
\therefore a * (b * c) = (a * b) * c.
\end{gathered}
$$

Note que o elemento identidade da operação definida é $0 \in \mathbb{Z}$: $a * 0 = a + 0 + a0 = a = 0 + a + 0a = 0 * a$ e, pela sua existência, $(\mathbb{Z}, *)$ é monóide.

O único elemento invertível do monóide é $0 \in \mathbb{Z}$. □

Exercício 1.44: *Prove that in each monoid with identity element* e,$x * y * x = e$ *implies that* x *and* y *are invertible and* $y = x^{-2}$.

Solução: Primeiro, vamos provar que $x * y * x = e \implies \exists\ x^{-1}, y^{-1}$. Observe que $y * x$ é inversa a direita de x e $x * y$ é inversa a esquerda de x, assim, x é invertível. Para y fazemos: $x * y * x * (y * x) = y * x \implies x * y = y * x$ o que mostra que existe y^{-1}.

Segundo, vamos provar que $y = x^{-2}$. Como provamos, existe x^{-1} então:

$$
\begin{aligned}
x * y * x &= e \\
x^{-1} * x * y * x &= x^{-1} \\
y * x &= x^{-1} \\
y * x * x^{-1} &= x^{-1}x^{-1} \\
y &= x^{-2}.
\end{aligned}
$$

□

Exercício 1.45: *Determine which among the following conditions imply that an element of a monoid* S *is invertible:*

(a) There exists a $y \in S$ *such that* $x * y$ *is invertible.*

(b) There exists a $y \in S$ *commuting with* x *such that* $x * y$ *is invertible.*

(c) There exists an $n \in \mathbb{N}$ *such that* x^n *is invertible.*

Solução: Para o item (a)

Para o item (b), temos que y comuta com x, ou seja:

$$x * y = y * x$$

□

1.3 Grupos

Exercício 1.55.: *Determine which of the following sets of numbers are groups under the usual addition:*

(a) $\left\{\frac{n}{2} \mid n \in \mathbb{Z}\right\}$.

(b) $\{x \in \mathbb{R} \mid x \geq 0\}$.

(c) $\{x \in \mathbb{R} \mid x \notin \mathbb{Q}\} \cup \{0\}$.

(d) $\{z \in \mathbb{C} \mid \mathrm{Im}(z) \in \mathbb{Z}\}$.

(e) $\{z \in \mathbb{C} \mid \mathrm{Re}(z) \cdot \mathrm{Im}(z) = 0\}$.

(f) $\{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$.

Solução: (a): É um grupo. O conjunto munido da soma goza da associatividade, todo elemento tem inverso e o elemento identidade da operação é $0 \in \mathbb{Z}$.

(b): Não é um grupo. Tome $1 \in \{x \in \mathbb{R};\ x \geq 0\}$, não há elemento x nesse conjunto tal que $x + 1 = 1 + x = 0$.

(c): É um grupo. Podemos tratar o conjunto como dos números irracionais, incluindo o zero. O conjunto munido da soma goza da associatividade, todo elemento tem inverso e o elemento identidade da operação é $0 \in \mathbb{Z}$.

(d): É um grupo.

(e): Não é um grupo, pois não é fechado para a soma. Tome $z_1 = 1$, $z_2 = i, \in \mathbb{C}$, note que $z_1 + z_2 = 1 + i \notin \{z \in \mathbb{C} \mid \mathrm{Re}(z) \cdot \mathrm{Im}(z) = 0\}$, apesar de ambos os números estarem no conjunto.

(f): É um grupo. □

Exercício 1.56: *Determine which of the following sets of numbers are groups under the usual multiplication:*

(a) $\{2^n \mid n \in \mathbb{Z}\}$.

(b) $\{x \in \mathbb{R} \mid x > 0\}$.

(c) $\{x \in \mathbb{R} \mid x < 0\}$.

(d) $\{x \in \mathbb{R} \mid 0 < x < 1\}$.

(e) $\{z \in \mathbb{C} \mid |z| \geq 1\}$.

(f) $\{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\} \setminus \{0\}$.

Solução: (a): É um grupo.

(b): É um grupo.

(c): Não é um grupo. Neste conjunto munido da operação de multiplicação não há elemento identidade.

(d): Não é um grupo. Tome $0 < x < 1$, $x \in \mathbb{R}$, não há inverso multiplicativo, nem identidade neste conjunto.

(e): Não é um grupo. Tome $|z| = 2 \implies |z^{-1}| = \frac{1}{|z|} = \frac{1}{2} \leq 1$.

(f) Não é um grupo, pois não possui elemento neutro. □