Operações Binárias e Aplicações
um resumo

Guilherme Philippi

15 de fevereiro de 2021

Apresenta-se nesse texto um compilado de definições e resultados envolvendo os conceitos de operações binárias e algumas de suas aplica. Tudo que aqui se apresenta fora extraído de [1, 2, 3], principalmente de [1].

1 Operações binárias

Definição 1.1 (Operação binária)**.** Uma *operação binária* sobre um conjunto S é uma função $* : S \times S \longrightarrow S$.

Exemplo 1.1 (Produto sobre $\mathbb{R}$)**.** Seja a função $\cdot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ tal que $\cdot(x, y) = x \cdot y$, isto é, associa-se a cada par (x, y) de números reais o respectivo produto $x \cdot y$. A função $\cdot$ é a operação binária conhecida como *produto sobre* $\mathbb{R}$.

Exemplo 1.2 (Composição de funções)**.** O mapa $\circ : \mathcal{F}_{\mathbb{R}} \times \mathcal{F}_{\mathbb{R}} \longrightarrow \mathcal{F}_{\mathbb{R}}$, em que $\mathcal{F}_{\mathbb{R}}$ representa o *conjunto das funções de* $\mathbb{R}$ *em* $\mathbb{R}$, é a operação definida pela *composição de funções* $\circ(f, g) = f \circ g$ *sobre* $\mathcal{F}_{\mathbb{R}}$.

Observação 1.1 (Notação de operação)**.** Usaremos a notação $*(a, b) = a * b$, para simplificar a escrita de propriedades. Também, quando não houver ambiguidade, suprimiremos o simbolo da operação, fazendo $a * b = ab$.

Exemplo 1.3 (Adição sobre $\mathbb{R}$)**.** A função $+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ definida pela soma $x + y$ é a operação de *adição sobre* $\mathbb{R}$.

Definição 1.2. Para $a, b, c \in S$, uma operação binária $*$ é dita

- *Associativa*, se $(a * b) * c = a * (b * c)$;
- *Comutativa*, se $a * b = b * a$.

Exemplo 1.4 (Multiplicação matricial)**.** Seja $\mathbb{R}^{n \times n}$ o *conjunto das matrizes reais quadradas de ordem* n. A operação $\times : \mathbb{R}^{n\times n} \times \mathbb{R}^{n\times n} \longrightarrow \mathbb{R}^{n\times n}$ é o *produto matricial* $\times(M, N) = M \times N$ *sobre* $\mathbb{R}^{n\times n}$. Sabe-se que essa operação é associativa, visto que $(XY)Z = X(YZ),\ \forall X, Y, Z \in \mathbb{R}^{n\times n}$. Porém, como

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix} \neq \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 23 & 34 \\ 31 & 46 \end{pmatrix},$$

segue que $\times$ não pode ser comutativa.

Exemplo 1.5 (Potência em $\mathbb{N}$)**.** Seja $f(x,y) = x^y$ a operação de *potenciação sobre* $\mathbb{N}$. f não é nem associativa,

$$\text{pois } 2^{(3^4)} = 2^{81} \neq (2^3)^4 = 2^{12},$$

nem comutativa,

$$\text{pois } 2^3 = 8 \neq 3^2 = 9.$$

Exemplo 1.6 (Adição)**.** As adições sobre $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ são operações tanto associativas quanto comutativas. Deixa-se ao leitor mostrar que isso é verdade.

Proposição 1.1. *Seja uma operação associativa dada sobre o conjunto S. Há uma única forma de definir, para todo inteiro n, um produto de n elementos $a_1, \ldots, a_n \in S$ (diremos $[a_1 \cdots a_n]$) com as seguintes propriedades:*

1. *o produto $[a_1]$ de um elemento é o próprio elemento;*
2. *o produto $[a_1 a_2]$ de dois elementos é dado pela operação binária;*
3. *para todo inteiro $1 \leq i \leq n$, $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$.*

Demonstração. A demonstração dessa proposição é feita por indução em n. □

Definição 1.3. Dizemos que $e \in S$ é *identidade* para uma operação binária se $ea = ae = a$ para todo $a \in S$.

Proposição 1.2. *O elemento identidade é único.*

Demonstração. Se e, e' são identidades, já que e é identidade, então $ee' = e'$ e, como e' é uma identidade, $ee' = e$. Logo $e = e'$, isto é, a identidade é única. □

Observação 1.2. Usaremos $\vec{1}$ para representar a identidade multiplicativa e $\vec{0}$ para denotar a aditiva.

Definição 1.4 (Elemento inverso)**.** Seja uma operação binária que possua uma identidade. Um elemento $a \in S$ é chamado *invertível* se há um outro elemento $b \in S$ tal que $ab = ba = 1$. Desde que b exista, ela é única e a denotaremos por a^{-1} e a chamaremos *inversa de a*.

Proposição 1.3. *Se $a, b \in S$ possuem inversa, então a composição $(ab)^{-1} = b^{-1}a^{-1}$.*

Observação 1.3 (Potências)**.** Usaremos as seguintes notações:

- $a^n = a^{n-1}a$ é a composição de $a \cdots a$ n vezes;
- a^{-n} é a inversa de a^n;
- $a^0 = \vec{1}$.

Com isso, tem-se que $a^{r+s} = a^r a^s$ e $(a^r)^s = a^{rs}$. (Isso não induz uma notação de fração $\frac{b}{a}$ a menos que seja uma operação comutativa, visto que ba^{-1} pode ser diferente de $a^{-1}b$). Para falar de uma operação aditiva, usaremos $-a$ no lugar de a^{-1} e na no lugar de a^n.

Referências

[1] John B Fraleigh. *A First Course in Abstract Algebra*. Pearson, 2014.

[2] Michael Artin. *Algebra*. A Simon and Schuster Company, 1991.

[3] Rudolf R. Maier. *Algebra I (texto de aula)*. UFSC, 2005.