álgebra

lcc :: 2.º ano

paula mendes martins

departamento de matemática :: uminho

preliminares

Definição. Um par $(S, *)$ diz-se um *grupóide* se S é um conjunto e $*$ é uma operação binária em S, i.e., se $*$ é definida por

$$\begin{array}{rcl} * : S \times S & \longrightarrow & S \\ (x, y) & \longmapsto & x * y. \end{array}$$

Definição. Seja $(S, *)$ um grupóide. A operação $*$ diz-se *comutativa* se

$$a * b = b * a, \qquad \forall a, b \in S.$$

Nestas condições, dizemos que $(S, *)$ é *comutativo* ou *abeliano*.

Exemplo 1.

- Se $*$ é definida por $x * y = \frac{x+y}{2}$ em $S = \mathbb{R}$, então, $(S, *)$ é um grupóide abeliano.
- Se $*$ é definida por $x * y = x - y$ em $S = \mathbb{N}$, então, $(\mathbb{N}, *)$ não é um grupóide.
- Se $*$ é definida por $x * y = 3$ em $S = \mathbb{N}$, então, $(\mathbb{N}, *)$ é um grupóide comutativo.
- Se $*$ é a adição ou a multiplicação usuais de classes em $\mathbb{Z}_n$, com $n \in \mathbb{N}$, então $(\mathbb{Z}_n, *)$ é um grupóide comutativo.

Exemplo 2. Sejam $S = \{a, b, c\}$ e $*$ a operação binária definida pela seguinte tabela (à qual se chama *tabela de Cayley*):

$$\begin{array}{c|ccc} * & a & b & c \\ \hline a & a & b & b \\ b & b & a & c \\ c & b & c & a \end{array}.$$

Então, $(S, *)$ é um grupóide comutativo.

Definição. Seja $(S, *)$ um grupóide. A operação $*$ diz-se *associativa* se

$$a * (b * c) = (a * b) * c, \quad \forall a, b, c \in S.$$

Nestas condições, escrevemos apenas $a * b * c$ e dizemos que o grupóide $(S, *)$ é um *semigrupo*.

Exemplo 3. O conjunto dos números inteiros constitui um semigrupo quando algebrizado com a multiplicação usual.

Exemplo 4. O grupóide do Exemplo 2 não é um semigrupo. De facto, temos que $a * (c * c) = a * a = a$ e $(a * c) * c = c$.

Definição. Seja $(S, *)$ um grupóide. Um elemento $a \in S$ diz-se um *elemento idempotente* se $a * a = a$.

Exemplo 5. No primeiro grupóide do Exemplo 1, todos os elementos são idempotentes. De facto, para todo $x \in S$, $x * x = \frac{x+x}{2} = x$.

Definição. Seja $(S, *)$ um grupóide. Um elemento $0 \in S$ diz-se *elemento zero* ou *nulo* se

$$0 * a = a * 0 = 0, \qquad \forall a \in S.$$

Um elemento $e \in S$ diz-se *elemento neutro* ou *elemento identidade* se

$$a * e = e * a = a, \qquad \forall a \in S.$$

Observação. Um elemento neutro ou um elemento zero de um grupóide é um elemento idempotente.

Proposição. Num grupóide $(S, *)$ existe, no máximo, um elemento neutro. $\square$

Definição. Um semigrupo $(S, *)$ que admita elemento neutro diz-se um *monóide* ou um *semigrupo com identidade*. O único elemento neutro existente num monóide $(S, *)$ representa-se por 1_S.

Exemplo 6. O semigrupo $(\mathbb{N}, *)$ onde $*$ está definida por

$$a * b = 2ab, \qquad \forall a, b \in \mathbb{N},$$

não admite elemento neutro.

Exemplo 7. O semigrupo $(S, *)$, onde $S = \{a, b, c, d\}$ e $*$ é definida pela tabela

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

é um monóide, e a é o seu elemento neutro.

Definição. Sejam $(S,*)$ um semigrupo com identidade e $a \in S$. Um elemento $a' \in S$ diz-se *elemento oposto* de a se $a * a' = a' * a = 1_S$.

Proposição. Num semigrupo $(S,*)$ com identidade, um elemento $a \in S$ tem, no máximo, um elemento oposto. $\square$

Observação. Caso não haja ambiguidade quanto à operação $*$, referimo-nos muitas vezes ao grupóide (respetivamente, semigrupo, monóide) $(S,*)$ como o grupóide (respetivamente, semigrupo, monóide) S.

potência natural de um elemento num semigrupo

Para representarmos a operação binária definida num conjunto podemos usar dois tipos de linguagem: a multiplicativa e a aditiva. Nestes casos temos:

Linguagem multiplicativa	Linguagem aditiva
$a * b = ab$ (produto de a por b)	$a * b = a + b$ (a soma de a por b)
a^{-1} é o oposto ou *inverso* de a	$-a$ é o oposto ou *simétrico* de a

Dado um elemento a de um semigrupo S, utilizamos a seguinte notação para representar os seguintes produtos (ou somas):

Linguagem multiplicativa	Linguagem aditiva	
$a^2 = aa$	$2a = a + a$	
$a^3 = aaa$	$3a = a + a + a$	
$\vdots$	$\vdots$	
$a^n = \underbrace{aa \cdots aa}_{n \text{ vezes}}$	$na = \underbrace{a + a + \cdots + a + a}_{n \text{ vezes}}$	(com $n \in \mathbb{N}$)

A a^n chamamos *potência de a* e a na chamamos *múltiplo de a*.

A não ser que seja referido, trabalhamos com a linguagem multiplicativa.

Proposição. Sejam S um semigrupo, $m, n \in \mathbb{N}$ e $a \in S$. Então,

1. $a^m a^n = a^{m+n}$ $\quad$ $[\ ma + na = (m+n)\,a\ ]$;
2. $(a^m)^n = a^{mn}$ $\quad$ $[\ n\,(ma) = (nm)\,a\ ]$.

$\square$