Elementos da Teoria de Grupos

lcc :: lmat :: 2.º ano

paula mendes martins

departamento de matemática :: uminho

generalidades

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

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

Definição. Seja $(S, *)$ um grupóide. A operação $*$ diz-se *comutativa* ou *abeliana* 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, $(N, *)$ não é um grupóide.
- Se $*$ é definida por $x * y = 3$ em $S = \mathbb{N}$, então, $(N, *)$ 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.

Demonstração. Suponhamos que $(S, *)$ admite dois elementos neutros, e e e'. Então, porque e é elemento neutro,

$$e * e' = e'.$$

Por outro lado, porque e' é elemento neutro,

$$e * e' = e.$$

Logo, $e = e'$. $\square$

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.

Demonstração. Suponhamos que $a \in S$ admite dois elementos opostos, a' e a''. Então,

$$a' = a' * 1_S = a' * (a * a'') = (a' * a) * a'' = 1_S * a'' = a''.$$

Logo, quando existe, o oposto de um elemento é único. $\square$

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. $(a^m)^n = a^{mn}$ $\quad [\ n\,(ma) = (nm)\,a\ ]$.

Demonstração. Trivial, tendo em conta a associatividade da operação. $\square$

Definição. Seja G um conjunto no qual está definida uma operação binária. Então, G diz-se um *grupo* se G é um semigrupo com identidade e no qual todos os elementos admitem um único elemento oposto, i.e., G é grupo se:

G1. A operação binária é associativa em G;

G2. $(\exists e \in G)\,(\forall a \in G) \qquad ae = ea = a$;

G3. $(\forall a \in G)\,\left(\exists^! a^{-1} \in G\right) \qquad aa^{-1} = a^{-1}a = e.$

Se a operação for comutativa, o grupo diz-se *comutativo* ou *abeliano.*

Representamos a identidade do grupo G por 1_G.

Exemplo 8. $(\mathbb{R}, +)$ é grupo abeliano ($+$ é a adição usual de números reais). $(\mathbb{R}, \cdot)$ não é grupo ($\cdot$ é a multiplicação usual de números reais), mas $(\mathbb{R} \setminus \{0\}, \cdot)$ é grupo abeliano.

Exemplo 9. Seja $n \in \mathbb{N}$. Sendo $\oplus$ e $\otimes$ as operações de adição e multiplicação usuais de classes de $\mathbb{Z}_n$, temos que $(\mathbb{Z}_n, \oplus)$ é grupo e $(\mathbb{Z}_n, \otimes)$ não é grupo. Sendo $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]_n\}$, temos que $(\mathbb{Z}_n^*, \otimes)$ é grupo se e só se n é primo.

Exemplo 10. $(\mathbb{Z}, \cdot)$ não é grupo ($\cdot$ é a multiplicação usual de números inteiros), mas $(\mathbb{Z}, +)$ é grupo abeliano ($+$ é a adição usual de números inteiros).

Exemplo 11. Um conjunto singular, $\{x\}$, quando algebrizado com a única operação binária possível, $x * x = x$, é um grupo abeliano (chamado de *grupo trivial*).

Proposição. Num grupo G são válidas as leis do corte, i.e., para $x, y, a \in G$,

$$ax = ay \Rightarrow x = y \quad e \quad xa = ya \Rightarrow x = y.$$

Demonstração. Sejam $a, x, y \in G$. Então,

$$\begin{aligned} ax = ay \quad &\Longrightarrow \quad a^{-1}(ax) = a^{-1}(ay) \\ &\Rightarrow \quad \left(a^{-1}a\right)x = \left(a^{-1}a\right)y \\ &\Rightarrow \quad 1_G x = 1_G y \\ &\Rightarrow \quad x = y. \end{aligned}$$

A segunda implicação demonstra-se de modo análogo. $\square$

Observação. Existem semigrupos que não são grupos nos quais se verifica a lei do corte, como, por exemplo, $\mathbb{Z} \setminus \{0\}$ algebrizado com a multiplicação usual de inteiros. Este semigrupo comutativo com identidade satisfaz as leis do corte, mas não é um grupo, pois os únicos elementos que admitem inverso são 1 e -1.

Teorema. Num grupo G, as equações $ax = b$ e $ya = b$, admitem uma única solução, para quaisquer $a, b \in G$.

Reciprocamente, um semigrupo S no qual as equações $ax = b$ e $ya = b$ admitem soluções únicas, para quaisquer $a, b \in S$, é um grupo.

Demonstração. Suponhamos, primeiro, que G é um grupo. Então, para $a, b \in G$, os elementos $a^{-1}b$ e ba^{-1} de G são soluções das equações $ax = b$ e $ya = b$, respetivamente. A unicidade destas soluções resulta do facto de as leis de corte serem válidas em G.

Reciprocamente, sejam S um semigrupo e $a \in S$. Então, existem soluções únicas das equações $ax = a$ e $ya = a$. Sejam e e e' essas soluções, respetivamente. Então, como para todo $b \in S$ existe um único $c \in S$ tal que $b = ca$, temos que

$$be = (ca)\,e = c\,(ae) = ca = b.$$

Logo, e é elemento neutro à direita em S. De modo análogo, provamos que e' é elemento neutro à esquerda. Assim,

$$e = e'e = e'$$

e, portanto, e é elemento neutro do semigrupo S.

Seja $a \in S$. Então, existem soluções únicas das equações $ax = e$ e $ya = e$. Sejam a' e a'' essas soluções, respetivamente. Temos então que $aa' = e$ e $a''a = e$. Logo,

$$a'' = a''e = a''\left(aa'\right) = \left(a''a\right)a' = ea' = a',$$

pelo que cada elemento $a \in S$ admite um oposto $a' \in S$. Portanto, S é um grupo. $\square$

Proposição. Seja S um semigrupo finito que satisfaz as leis do corte. Então S é um grupo.

Demonstração. Seja a um elemento qualquer de S. Então, as aplicações $\rho_a, \lambda_a : S \to S$ definidas por, respetivamente, $\rho_a(x) = xa$ e $\lambda_a(x) = ax$, $x \in S$, são injetivas. De facto, para $x, y \in S$, tendo em conta as leis do corte,

$$\rho_a(x) = \rho_a(y) \Leftrightarrow xa = ya \Rightarrow x = y$$

e

$$\lambda_a(x) = \lambda_a(y) \Leftrightarrow ax = ay \Rightarrow x = y.$$

Logo, sendo S um conjunto finito, temos que as duas aplicações são também sobrejetivas, pelo que as equações $ax = b$ e $ya = b$ têm soluções únicas em S. Assim, pelo teorema anterior, o semigrupo S é um grupo. $\square$

Proposição. Seja G um grupo. Então:

1. $1_G^{-1} = 1_G$;
2. $\left(a^{-1}\right)^{-1} = a, \quad \forall a \in G$;
3. $(ab)^{-1} = b^{-1}a^{-1}, \quad \forall a, b \in G$;
4. $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$, $(\forall n \in \mathbb{N})\,(\forall a_1, a_2, \ldots, a_n \in G)$.

Dado um elemento a de um grupo G e $p \in \mathbb{Z}$, define-se

$$
\begin{aligned}
a^P &= \underbrace{aa \cdots a}_{p \text{ vezes}} && \text{se } p \in \mathbb{Z}^+;\\
a^p &= 1_G && \text{se } p = 0;\\
a^p &= \left(a^{-1}\right)^{-p} = \left(a^{-p}\right)^{-1} && \text{se } p \in \mathbb{Z}^-.
\end{aligned}
$$

Em linguagem aditiva temos

$$
\begin{aligned}
pa &= \underbrace{a + a + \cdots + a}_{p \text{ vezes}} && \text{se } \mathbb{Z}^+;\\
pa &= 1_G && \text{se } p = 0;\\
pa &= (-p)\,(-a) = -\left((-p)\,a\right) && \text{se } p \in \mathbb{Z}^-.
\end{aligned}
$$

Proposição. Sejam G um grupo, $x \in G$ e $m, n \in \mathbb{Z}$. Então,

1. $x^m x^n = x^{m+n}$ (na linguagem aditiva: $mx + nx = (m+n)x$);
2. $(x^m)^n = x^{mn}$ (na linguagem aditiva: $n(mx) = (nm)x$).

Demonstração. Temos de considerar vários casos.

Caso 1: Sejam $m, n \in \mathbb{Z}^+$. O caso resulta imediatamente da definição.

Caso 2: Sejam $m, n \in \mathbb{Z}^-$. Então, $m = -l$ e $n = -k$ com $l, k > 0$, pelo que

$$\begin{aligned} x^m x^n &= x^{-l} x^{-k} = \left(x^l\right)^{-1} \left(x^k\right)^{-1} = \left(x^k x^l\right)^{-1} \\ &= \left(x^{k+l}\right)^{-1} = x^{-(k+l)} = x^{-k-l} = x^{n+m}. \end{aligned}$$

Mais ainda,

$$\begin{aligned} (x^m)^n &= \left(x^{-l}\right)^{-k} = \left[\left(\left(x^{-1}\right)^l\right)^k\right]^{-1} = \left[\left(x^{-1}\right)^{lk}\right]^{-1} \\ &= \left[\left(x^{lk}\right)^{-1}\right]^{-1} = x^{lk} = x^{(-m)(-n)} = x^{mn}. \end{aligned}$$

Caso 3: Sejam $m, n \in \mathbb{Z}$ tais que $m > 0,\ n < 0$ e $|m| > |n|$. Então, $n = -l$ com $m > l > 0$, pelo que

$$x^m x^n = x^{m-l+l} x^{-l} = x^{m-l} x^l \left(x^l\right)^{-1} = x^{m-l} 1_G = x^{m-l} = x^{m+n},$$

o que prova **1.** Por outro lado,

$$(x^m)^n = (x^m)^{-l} = \left[(x^m)^l\right]^{-1} = \left(x^{ml}\right)^{-1} = x^{-ml} = x^{mn},$$

o que prova a condição **2.**

Caso 4. Sejam $m, n \in \mathbb{Z}$ tais que $m > 0,\ n < 0$ e $|m| < |n|$. Então, $n = -l$ com $l > m > 0$, pelo que

$$\begin{aligned} x^m x^n &= x^m x^{-l} = x^m \left(x^l\right)^{-1} = x^m \left(x^{l-m+m}\right)^{-1} = x^m \left(x^{l-m} x^m\right)^{-1} = \\ &= x^m (x^m)^{-1} \left(x^{l-m}\right)^{-1} = 1_G x^{-(l-m)} = x^{-l+m} = x^{n+m}. \end{aligned}$$

A demonstração de **2.** é igual à do Caso 3.

Os casos em que pelo menos um dos inteiros é zero são triviais e qualquer outro caso é igual aos casos 3 ou 4. $\square$