

Encerramos a aula passada definindo grupo.

Lembrando: $(G, *)$ é um grupo se a operação $*$ definida em G for associativa, possuir um neutro, e for simetrizável. Ou seja,

$\forall a, b, c \in G$, devem-se cumprir as seguintes propriedades:

(i) $a * (b * c) = (a * b) * c$ (associatividade)

(ii) $\exists e \in G$ tal que $a * e = e * a = a$,
 $\forall a \in G$ - (existência do neutro da operação $*$)

(iii) $\forall a \in G, \exists b \in G$ tal que
 $a * b = e = b * a$

(todo elemento é simetrizável.)

Neste caso, b chama-se simétrico ou inverso (aditivo ou multiplicativo) de a , e podemos, no caso multiplicativo, denotar $b = a^{-1}$, e, no caso aditivo,

podemos escrever $b = -a$

Obs: Embora não esteja declarado no conceito acima, o fechamento se cumpre; ou seja, dado $a, b \in G$, $a * b \in G$. Isto porque definiremos a operação $*$ como sendo fechada, ou seja:

$$*: G \times G \rightarrow G$$

$$(a, b) \mapsto a * b \in G.$$

Note que o neutro é serê único, e cada elemento $x \in G$, possui um único simétrico. Estes fatos já foram demonstrados ao estudar o conceito de operação na aula passada.

Ao que segue apresentaremos uma coleção de exemplos de grupos.

01) $(\mathbb{Z}, +)$ é um grupo, pois:

(i) vale a associatividade da adição em $\mathbb{Z}$:

$$a + (b + c) = (a + b) + c, \forall a, b, c \in \mathbb{Z}.$$

(ii) $\exists 0 \in \mathbb{Z}$ tal que

$$a + 0 = 0 + a = a$$

(0 zero é o neutro aditivo).

(iii) $\forall a \in \mathbb{Z}, \exists -a \in \mathbb{Z}$, tal que

$$a + (-a) = 0$$

(todo elemento é simétrico)

Além disso, $(\mathbb{Z}, +)$ é abeliano (comutativo):

$$a + b = b + a; \forall a, b \in \mathbb{Z}.$$

02) $(M_n(\mathbb{R}), +)$ - o conjunto das matrizes

quadradas de ordem n , equipadas com a adição usual de matrizes. Afirmamos que

$(M_n(\mathbb{R}), +)$ é um grupo. De fato, sabe-se da Álgebra linear, que, $\forall A, B, C \in M_n(\mathbb{R})$, tem-se que:

(i) $A + (B + C) = (A + B) + C$. (associativ.)

(ii) $\exists 0$ [matriz nula] tal que

$$A + 0 = A = 0 + A.$$

A matriz nula é o neutro aditivo.

(iii) $\forall A \in M_n(\mathbb{R})$, $\exists -A \in M_n(\mathbb{R})$

tal que $A + (-A) = (-A) + A = 0$

(ou seja, toda matriz possui um elemento simétrico)

(iv) $A + B = B + A$ (comutativa)

Ou seja, $(M_n(\mathbb{R}), +)$ é um grupo abeliano.

03) $(M_n(\mathbb{R}), \cdot)$, onde $\cdot$ denota o produto usual de matrizes, é um grupo?

Note que, neste caso, o elemento multiplicativo é a matriz identidade I_n .

O que falta é o item (iii); ou seja, nem toda matriz é invertível (no sentido de existir inverso multiplicativo), pois para poder derivarmos ter sempre que

$$A \cdot A^{-1} = I \quad (\star)$$

↪ inversa de A .

Porém, nem todas as matrizes possuem inversa

Ex: em $M_2(\mathbb{R})$; a matriz

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ não tem inversa}$$

(pois $\det A = 0$). Logo $\nexists A^{-1}$

tal que se cumpra $(\star)$

Então, $(M_n(\mathbb{R}), \cdot)$ não é um grupo.

04) $(\mathbb{C} \setminus \{0\}, \cdot)$, onde $\mathbb{C}$ é o conjunto dos números complexos:

$$\mathbb{C} = \{a+bi : a, b \in \mathbb{R} ; i = \sqrt{-1}\},$$

e $\cdot$ é o produto usual em $\mathbb{C}$:

$$(a+bi) \cdot (x+yi) = \underbrace{(a \cdot x - b \cdot y)}_{\text{PARTE REAL}} + \underbrace{(a \cdot y + b \cdot x)}_{\text{PARTE IMAGINÁRIA}} i$$

Perguntamos: $(\mathbb{C}, \cdot)$ é um grupo?

Dados $\alpha, \beta, \gamma \in \mathbb{C}$, com:

$$\alpha = a+bi ; \beta = x+yi ; \gamma = p+qi ;$$

temos:

$$\begin{aligned} (1) \quad \underline{\alpha \cdot (\beta \cdot \gamma)} &= \alpha \cdot ((x+yi) \cdot (p+qi)) = \\ &= \alpha \cdot (x \cdot p - y \cdot q + (x \cdot q + y \cdot p)i) = \\ &= (a+bi) \cdot ((xp - yq) + (xq + yp)i) = \end{aligned}$$

$$= a \cdot (x_p - y_q) - b(x_q + y_p) + [a(x_q + y_p) + b(x_p - y_q)]i$$

$$= a(x_p) - a(y_q) - b(x_q) - b(y_p) + (a x_q + a y_p + b x_p - b y_q)i$$

Por outro lado:

$$\alpha \cdot \beta \cdot \gamma = [(a+bi) \cdot (x+yi)] \cdot \gamma =$$

$$= ((a \cdot x - b \cdot y) + (a \cdot y + b \cdot x)i) \cdot (p + qi)$$

$$= (ax - by)p - (ay + bx)q + [(ax - by)q + (ay + bx)p]i$$

$$= axp - byp - ayq - bxq + (axq - byq + ay p + bxp)i$$

Comparando as igualdades (*) e (**) segue que

$$\alpha \cdot (\beta \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

(ii) neutro multiplicativo.

Dado $\alpha = a+bi$; qual é o neutro e tal que

$$\alpha \cdot e = \alpha ?$$

$$(a+bi) \cdot (\underbrace{x+yi}_e) = (a+bi)$$

$$\underbrace{ax - by}_{\text{orange}} + \underbrace{(ay + bx)i}_{\text{green}} = \underbrace{a}_{\text{orange}} + \underbrace{bi}_{\text{green}}$$

$$\Leftrightarrow \begin{cases} ax - by = a & \times a \\ ay + bx = b & \times b \end{cases}$$

$$\begin{array}{l} \begin{cases} a^2x - \cancel{aby} = a^2 \\ \cancel{aby} + b^2x = b^2 \end{cases} \\ + \\ \hline \end{array}$$

$$a^2x + b^2x = a^2 + b^2$$

$$(a^2 + b^2) \cdot x = a^2 + b^2 ; (*)$$

e como estamos em $\mathbb{C} \setminus \{0\}$; então
 a, b não são simultaneamente nulos; ou seja;
temos $a^2 + b^2 \neq 0$; e então, podemos
dividir a igualdade (*) por $a^2 + b^2$; obtendo:

$$(a^2 + b^2)x = a^2 + b^2$$

$$x = \frac{\cancel{a^2 + b^2}}{\cancel{a^2 + b^2}} \Rightarrow \boxed{x = 1}$$

E, como $ax - by = a$; para $x = 1$, vem:

$$a \cdot 1 - by = a$$

$$\cancel{a} - by = \cancel{a}$$

$$-by = 0 \Rightarrow by = 0$$

$$b = 0 \text{ ou } \underline{\underline{y = 0}}$$

Conclusão:

$$(a + bi) \cdot (x + yi) = (a + bi)$$

$$\Leftrightarrow x = 1 \text{ e } y = 0;$$

ou seja, o número complexo

$$1 + 0i = 1 \text{ e } 0$$

neutro multiplicativo em $\mathbb{C} \setminus \{0\}$.

(iii) simétrico:

Dado $\alpha = a + bi$, com a ou $b \neq 0$,
queremos obter $\beta = x + yi$ tal que

$$\alpha \cdot \beta = 1. \text{ (neutro)}$$

$$(a + bi) \cdot (x + yi) = 1 = 1 + 0i$$

$$(ax - by) + (ay + bx)i = 1 + 0i$$

$$\begin{cases} ax - by = 1 & \times (a) \\ ay + bx = 0 & \times (b) \end{cases}$$

$$\begin{aligned} \Rightarrow & \begin{cases} a^2x - \cancel{aby} = a \\ \cancel{aby} + b^2x = 0 \end{cases} \\ + & \hline & a^2x + b^2x = a \end{aligned}$$

$$(a^2 + b^2) \cdot x = a$$

$$\circ \quad x = \frac{a}{a^2 + b^2}$$

Voltando ao 1º equacionamento:

$$\begin{cases} ax - by = 1 & x(-b) \\ ay + bx = 0 & x(a) \end{cases}$$

$$\Rightarrow \begin{cases} -\cancel{ab}x + b^2y = -b \\ a^2y + \cancel{ab}x = 0 \end{cases}$$

$$a^2y + b^2y = -b$$

$$(a^2 + b^2) \cdot y = -b$$

$$\circ \quad y = -\frac{b}{a^2 + b^2}$$

conclusão: o número complexo (inverso multiplicativo de $z = a + bi$) será:

$$\beta = x + yi = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

obs.. verificação:

$$\begin{aligned} \alpha \cdot \beta &= (a + bi) \cdot \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \right) = \\ &= \left(\frac{a^2}{a^2 + b^2} + \frac{b^2}{a^2 + b^2} \right) + \left(-\frac{ab}{a^2 + b^2} + \frac{ab}{a^2 + b^2} \right) i = \\ &= \frac{a^2 + b^2}{a^2 + b^2} + 0i = 1 + 0i = \underline{1}. \end{aligned}$$

05) Seja $\text{bij}(A) = \{ f: A \rightarrow A : f \text{ é bijetiva} \}$,
onde $A \subset \mathbb{R}$ é um conjunto não vazio.

Afirmação: $(\text{bij}(A), \circ)$ onde " $\circ$ " é a
composição de funções, é um grupo.

De fato, do estudo de funções, sabemos
que; $\forall f, g, h \in \text{bij}(A)$, tem-se:

(i) $f \circ (g \circ h) = (f \circ g) \circ h$; ou seja, a composição de funções é associativa.

(ii) $\text{id}: A \rightarrow A$; $\text{id}(x) = x$ a função identidade é o neutro da operação ; ou seja:

$$f \circ \text{id} = f \quad \text{e} \quad \text{id} \circ f = f.$$

(iii) Todo elemento é invertível. De fato, $\forall f \in \text{bij}(A)$, $\exists f^{-1} \in \text{bij}(A)$,

$$\text{tal que } f \circ f^{-1} = \text{id} \quad \text{e} \quad f^{-1} \circ f = \text{id}.$$

(f^{-1} é a função inversa de f)

Portanto $(\text{bij}(A), \circ)$ é um grupo, mas não é abeliano, pois a composição de funções não comuta ; ou seja ;

$$f \circ g \neq g \circ f.$$

06) Do exemplo anterior, quando o conjunto A for finito, com n elementos, o conjunto $\text{bij}(A)$ chama-se conjunto das permutações de n elementos, e é denotada por S_n .

Na prática, sendo $A = \{1, 2, 3, \dots, n\}$ ou quaisquer outros símbolos, entre;
um elemento de S_n é representado por uma matriz como segue:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$$

Ex-1: $n = 3$; temos S_3 ; onde
temos $3! = 3 \times 2 \times 1 = 6$ elementos.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \underline{\text{id}} = ;^{\beta^2}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} ; \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} ;$$

α $\alpha \circ \beta$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} ; \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} ; \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

α^2 β α

Denote $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Então; montemos composições:

$$\alpha^2 = \alpha \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$\alpha(\alpha(1)) = 2$ $\alpha(2) = 3$

$$(\alpha \circ \alpha)(n) = \alpha(\alpha(n))$$

$$\beta^2 = \beta \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id.}$$

$\beta(\beta(1)) = 1$ $\beta(2) = 2$

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Dito, notamos que α e β geram todos os elementos de S_3 ; ou seja:

$$S_3 = \{id = \beta^2, \alpha^2, \alpha, \beta, \alpha\beta, \beta\alpha\}$$

Como α e β geram S_3 , dizemos que

S_3 é gerado por eles, e escrevemos:

$$S_3 = \langle \alpha, \beta \rangle.$$

EXERCÍCIO: Montar a tabela de composição de S_3 :

id	$id = \beta^2$	α^2	α	β	$\alpha\beta$	$\beta\alpha$
$id = \beta^2$	id	α^2	α	β	$\alpha\beta$	$\beta\alpha$
α^2	α^2	id	$\beta\alpha$	$\dots$	$\dots$	$\dots$
α	α	$\dots$	id	$\dots$	$\dots$	$\dots$
β	β	$\dots$	$\dots$	id	$\dots$	$\dots$
$\alpha\beta$	$\alpha\beta$	$\dots$	$\dots$	$\dots$	id	$\beta\alpha$
$\beta\alpha$	$\beta\alpha$	$\dots$	$\dots$	$\dots$	$\beta\alpha$	id

$$\bullet \alpha^2_0 \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha$$

$$\bullet \alpha^2_0 \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}$$

$$\bullet \alpha^1_0 \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \beta_0 \alpha$$