

Nesta aula vamos definir subgrupos de um grupo. Vamos, o resultado:

PROP.: Seja G um grupo e $H \subset G$, $H \neq \emptyset$. Então H é subgrupo de G , e escrevemos $H < G$, se e só se, $\forall \alpha, \beta \in H$; tivermos:

$$(i) \quad \alpha \cdot \beta \in H \quad (\text{fechamento de } H)$$

$$(ii) \quad \alpha \in H \Rightarrow \alpha^{-1} \in H.$$

Vamos dar exemplos. Vamos seguir com outros.

$$(c) \quad G = (S_4, \circ) ; \text{ onde}$$

$$S_4 = \{ \text{id}, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3 \}$$

$$\text{Defina } H = \langle \text{id}, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}} \rangle \subset S_4.$$

Afirmamos que $H < S_4$; ou seja, $(H, \circ)$ é um subgrupo do grupo S_4 das simetrias do triângulo.

De fato, basta observar a tabela:

o	id	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
id	id	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	id	R_3	R_1	R_2
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	id	$R_{\frac{2\pi}{3}}$	R_2	R_3	R_1
R_1	R_1	R_3	R_2	id	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$
R_2	R_2	R_1	R_3	$R_{\frac{2\pi}{3}}$	id	$R_{\frac{4\pi}{3}}$
R_3	R_3	R_2	R_1	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$	id

O bloco destacado na tabela acima é o subconjunto H , com os seus elementos operados entre si, 2 a 2. Note que:

- a operação $\circ$ é fechada em H ; ou seja, elementos de H operados entre si resultam em elementos de H .
- o neutro é a identidade, e além

Logo, o simétrico de id é ele mesmo; o simétrico de $R_{\frac{2\pi}{3}}$ é $R_{\frac{4\pi}{3}}$ e o simétrico de $R_{\frac{4\pi}{3}}$ é $R_{\frac{2\pi}{3}}$, todos em H .

Ou seja, o que mostramos acima é:

$$(i) \quad \alpha, \beta \in H \Rightarrow \alpha \circ \beta \in H$$

$$(ii) \quad \alpha \in H \Rightarrow \alpha^{-1} \in H.$$

Portanto, $H < S_4$.

Além disso, é abeliano, devido à simetria na tabela para H . (embora S_4 não seja abeliano)

(d) $(G, \cdot)$; sendo

$G = \{1, i, -1, -i\}$; i - unidade imaginária; e o produto " $\cdot$ " é o produto em $\mathbb{C}$.

H

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Tomemos a parte sombreada:

$\cdot$	1	-1
1	1	-1
-1	-1	1

$H = \{1, -1\}$
 é subgrupo de G ,
 pois é fechado;
 ou seja $a, b \in H$;
 $a \cdot b \in H$;

e também, se $a \in H \Rightarrow a^{-1} \in H$

(pois $1 \in H \Rightarrow (1)^{-1} = 1 \in H$

$-1 \in H \quad (-1)^{-1} = -1 \in H$

(e) Seja G um grupo não vazio e defina o conjunto $Z(G)$ por:

$$Z(G) = \{g \in G : x \cdot g = g \cdot x, \forall x \in G\},$$

chamado de CENTRO DE G .

Primeiramente, note que $Z(G) \neq \emptyset$.
De fato, $\forall x \in G$; temos que

$$x = x * e = e * x.$$

$$\text{Logo, } e \in Z(G)$$

$\hookrightarrow e$: neutro de G .

AF: $Z(G) < G$.

Dados $\alpha, \beta \in Z(G)$, mostraremos que:

(i) $\alpha \cdot \beta \in Z(G)$;

(ii) $\alpha \in Z(G) \Rightarrow \alpha^{-1} \in Z(G)$.

De fato:

$$(i) \quad \underbrace{(\alpha \cdot \beta) \cdot x}_{\text{ASSOC.}} = \alpha \cdot (\beta \cdot x) \underset{\beta \in Z(G)}{=} \alpha \cdot (x \cdot \beta) =$$

$$\underset{\text{ASSOC.}}{=} (\alpha \cdot x) \cdot \beta = (x \cdot \alpha) \cdot \beta \underset{\alpha \in Z(G)}{=} x \cdot (\alpha \cdot \beta) \underset{\text{ASSOC.}}{=}$$

$$\Rightarrow (\alpha \cdot \beta) \cdot x = x \cdot (\alpha \cdot \beta) ; \text{ logo,}$$

$$\alpha \cdot \beta \in Z(G)$$

$$(ii) \quad \alpha \in Z(G) \Rightarrow \alpha^{-1} \in Z(G)?$$

Precisamos mostrar que

$$\alpha^{-1} x = x \cdot \alpha^{-1}, \quad \forall x \in G.$$

Note que; como $\alpha \in Z(G)$, então.

$$\alpha x = x \alpha.$$

Multiplicando à esquerda por α^{-1} , temos:

$$\tilde{\alpha}^{-1}(\alpha\eta) = \tilde{\alpha}^{-1}(\alpha\alpha)$$

Per associatività;

$$(\underbrace{\tilde{\alpha}^{-1} \cdot \alpha}_e) \cdot \alpha = (\tilde{\alpha}^{-1} \cdot \eta) \cdot \alpha$$

$$\Rightarrow \alpha = (\tilde{\alpha}^{-1} \cdot \alpha) \cdot \alpha$$

Moltiplicando à sinistra per $\tilde{\alpha}^{-1}$, veni:

$$\alpha \cdot \tilde{\alpha}^{-1} = (\tilde{\alpha}^{-1} \cdot \alpha) \cdot \underbrace{\alpha \cdot \tilde{\alpha}^{-1}}_e$$

$$\Rightarrow \alpha \cdot \tilde{\alpha}^{-1} = \tilde{\alpha}^{-1} \cdot \alpha \quad \Rightarrow \quad \tilde{\alpha}^{-1} \in Z(G)$$

Quindi, $Z(G) < G$.



grupos cíclicos:

Não que segue, vamos apresentar o conceito de grupo cíclico. Antes, porém, definiremos potência de um elemento de um grupo.

Def: Seja $(G, \cdot)$ um grupo multiplicativo.

Definimos a potência de $g \in G$ por; $\forall m \in \mathbb{Z}$:

$$g^m = \begin{cases} e, & \text{se } m = 0 \\ (g^{m-1}) \cdot g, & \text{se } m > 0 \\ (g^{-1})^{-m}, & \text{se } m < 0 \end{cases}$$

Se o grupo $(G, +)$ for aditivo, a "potência" é definida por:

$$n \cdot g = \begin{cases} e, & \text{se } n = 0 \\ (n-1) \cdot g + g & \text{se } n > 0 \\ (-n) \cdot (-g), & \text{se } n < 0 \end{cases}$$

Dados $a, b \in (G, \cdot)$, então :

$$(a \cdot b)^n = \underbrace{(a \cdot b) \cdot (a \cdot b) \cdot \dots \cdot (a \cdot b)}_{n \text{ fatores.}}$$

Se o grupo for abeliano, então

$$(a \cdot b)^n = a^n \cdot b^n.$$

De fato :

$$(a \cdot b)^n = \underbrace{(a \cdot b) \cdot (a \cdot b) \cdot (a \cdot b) \cdot \dots \cdot (a \cdot b)}_{n \text{ fatores.}} =$$
$$= \underbrace{(b \cdot a)}_{\text{COMUTAT.}} \cdot (a \cdot b) \cdot (a \cdot b) \cdot \dots \cdot (a \cdot b) =$$

$$= b \cdot (a \cdot a) \cdot b \cdot (a \cdot b) \cdot \dots \cdot (a \cdot b) =$$

$$= b \cdot (a^2 \cdot b) \cdot (a \cdot b) \cdot \dots \cdot (a \cdot b) =$$

$$= b \cdot (b \cdot a^2) \cdot (a \cdot b) \cdot \dots \cdot (a \cdot b) =$$

$$\underbrace{(b \cdot b)}_{\text{COMUTAT.}} \cdot a^2 \cdot (a \cdot b) \cdot \dots \cdot (a \cdot b) =$$

$$= b^2 a^2 (ab) \dots (ab)$$

$$= b^2 a^3 b (ab) \dots (ab)$$

$$\vdots$$

$$= a^m \cdot b^m$$

Def. Seja $(G, \cdot)$ um grupo. Dizemos que G é cíclico se $\exists g \in G$ tal que todo elemento de G seja potência de g .

Outra seja, G é cíclico se, e só se,

$$G = \{ g^n : n \in \mathbb{Z} \}.$$

Neste caso, dizemos que $g \in G$ é um gerador do grupo G , e escrevemos

$$G = \langle g \rangle,$$

para denotar que G é gerado pelo elemento $g \in G$.

Na notação aditiva, $(G, +)$ é cíclico
se $\exists g \in G$ tal que, $\forall x \in G$,

$$x = n \cdot g.$$

Ou seja, $G = \{ n \cdot g : n \in \mathbb{Z} \}$, e
então, $G = \langle g \rangle$.

EXEMPLOS:

01) $G = (\mathbb{Z}, +)$ é um grupo cíclico,
pois, $\forall a \in \mathbb{Z}$, $a = a \cdot 1$

Analogamente, $\mathbb{Z} = \langle 1 \rangle$, ou seja,
 $1 \in \mathbb{Z}$ é um gerador de $(\mathbb{Z}, +)$.

De fato, $\forall \alpha \in \mathbb{Z}$;

$$\alpha = \alpha \cdot 1$$

Note que também -1 gera todo o $\mathbb{Z}$,
pois, $\forall \alpha \in \mathbb{Z}$ $\alpha = (\alpha) \cdot (-1)$

[um múltiplo de -1].

Assim, também se tem que $\mathbb{Z} = \langle -1 \rangle$

02) $G = (\{1, i, -1, -i\}, \cdot)$

G é cíclico, pois,

$$\left. \begin{array}{l} \bullet 1 = i^0 \\ \bullet i = i^1 \\ \bullet -1 = i^2 \\ \bullet -i = i^3 \end{array} \right\} \Rightarrow \forall x \in G: \\ x = i^m$$

Portanto, G é cíclico, com $G = \langle i \rangle$

03) $(\mathbb{Q}, +)$ não é cíclica.

De fato, se por absurdo $(\mathbb{Q}, +)$ fosse cíclica, então existiria $x = \frac{p}{q} \in \mathbb{Q}$, com $p \in \mathbb{Z}$ e $q \in \mathbb{N}$, tal que

$$Q = \langle \alpha \rangle = \langle \frac{p}{q} \rangle.$$

Logo, todo elemento de Q deve ser um múltiplo de $\frac{p}{q}$, i.e;

$$\forall \alpha \in Q;$$

$$\alpha = m \cdot \frac{p}{q} = \frac{mp}{q}$$

$$\text{Logo } \frac{mp}{q+1} \in Q; \text{ e então}$$

$$\frac{mp}{q+1} = \frac{mp}{q} = \frac{1}{q+1} = \frac{1}{q}$$

$$\Rightarrow q = q+1 \text{ (Absurdo!)}$$

Portanto, $(Q, +)$ não é cíclico.

PROPOSIÇÃO Se $(G, \cdot)$ for cíclico, então G é um grupo abeliano.

DEMONSTRAÇÃO: Seja $(G, \cdot)$ um grupo cíclico.

Então, $\exists g \in G$ tal que, $\forall x \in G$;

$$x = g^m, m \in \mathbb{Z}, \text{ i.e., } G = \langle g \rangle.$$

Dados $x, y \in G$. Então, $\exists m, n \in \mathbb{Z}$

tais que $x = g^m$ e $y = g^n$. Assim:

$$\underline{x \cdot y} = g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m = \underline{y \cdot x}$$

Logo, G é comutativo (abeliano) $\square$

obs.: Note que, c.f. o resultado acima, de forma contrapositiva, temos que S_4 não é cíclico, pois pela tabela para $(S_4, \cdot)$ vemos que o não é comutativo, logo, $(S_4, \cdot)$

não será um grupo cíclico.

$$(*) \text{ contraposição: } P \Rightarrow Q \vdash \neg Q \Rightarrow \neg P$$

obs: A recíproca da proposição acima, em geral, é falsa; ou seja, o fato de G ser abeliano não implica em G ser cíclico.

Ex: $G = (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$; onde:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$$

$\mathbb{Z}_2 \times \mathbb{Z}_2$ é abeliano, pois dados

$(\bar{a}, \bar{b}), (\bar{x}, \bar{y})$; então:

$$\begin{aligned} \underline{(\bar{a}, \bar{b}) + (\bar{x}, \bar{y})} &= (\bar{a} \oplus \bar{x}, \bar{b} \oplus \bar{y}) = \\ &= (\overline{a+x}, \overline{b+y}) = (\overline{x+a}, \overline{y+b}) = \\ &= (\bar{x} \oplus \bar{a}, \bar{y} \oplus \bar{b}) = \underline{(\bar{x}, \bar{y}) + (\bar{a}, \bar{b})} \end{aligned}$$

Logo:

$$\begin{aligned}
 (\bar{a}, \bar{b}) + (\bar{a}, \bar{b}) &= (\bar{a} \oplus \bar{a}, \bar{b} \oplus \bar{b}) = \\
 &= (\overline{a+a}, \overline{b+b}) = (\underbrace{2a}, \underbrace{2b}) \\
 &= (\bar{0}, \bar{0})
 \end{aligned}$$

DÍGITE
 EXATA
 em $\mathbb{Z}_2$

$$\Rightarrow 2 \cdot (\bar{a}, \bar{b}) = (\bar{0}, \bar{0})$$

Ou seja, nenhum $(\bar{a}, \bar{b}) \in \mathbb{Z}_2 \times \mathbb{Z}_2$;

serve como gerador para $\mathbb{Z}_2 \times \mathbb{Z}_2$, ou seja, $\mathbb{Z}_2 \times \mathbb{Z}_2$ não é cíclico.

Ex:

$$\bullet (\bar{1}, \bar{0}) + (\bar{1}, \bar{0}) = (\bar{2}, \bar{0}) = (\bar{0}, \bar{0})$$

$$\bullet (\bar{1}, \bar{1}) + (\bar{1}, \bar{1}) = (\bar{2}, \bar{2}) = (\bar{0}, \bar{0})$$

⋮

Outro exemplo para mostrar que G abeliano não implica em G cíclico é $(\mathbb{Q}, +)$ [exemplo anterior à proposição].

EXERCÍCIOS DA LISTA 01.

2. Considere a operação $\star$ em $\mathbb{R}$ definida por

$$x \star y = ax + by + cxy,$$

onde $a, b, c \in \mathbb{R}$ são números reais dados. Obtenha as condições sobre a, b, c para que $\star$ seja associativa.

Para ser associativa, dados $x, y, z \in \mathbb{R}$, devemos ter

$$(x \star y) \star z = x \star (y \star z)$$

Por um lado:

$$\begin{aligned} \underline{(x \star y) \star z} &= (ax + by + cxy) \star z = \\ &= a \cdot (ax + by + cxy) + bz + c \cdot (ax + by + cxy) \cdot z \\ &= a^2x + aby + acxy + bz + (acx + bcy + c^2xy)z \\ &= \underline{a^2x + aby + acxy + bz + acxz + bcyz + c^2xyz} \end{aligned}$$

Por outro lado:

$$\begin{aligned} \underline{x \star (y \star z)} &= x \star (a \cdot y + b \cdot z + cyz) = \\ &= a \cdot x + b \cdot (ay + bz + cyz) + c \cdot x \cdot (ay + bz + cyz) = \end{aligned}$$

$$= ax + aby + b^2z + bcyz + acxz + bcxz + c^2yz$$

Como deve ser comutativo, então:

$$\begin{aligned} a^2x + \cancel{abx} + \cancel{acx} + bz + \cancel{acz} + \cancel{bcx} + \cancel{c^2x} &= \\ = a\cancel{x} + \cancel{abx} + b^2z + \cancel{bcx} + \cancel{acz} + \cancel{bcx} + \cancel{c^2x} & \end{aligned}$$

$$\underline{a^2x} + \underline{bz} + \underline{acz} = \underline{ax} + \underline{b^2z} + \underline{bcxz}$$

Comparando, pensando em uma expressão em termos de x , z e xz , somos obrigados a concluir que

$$\begin{cases} a^2 = a \Rightarrow a = 1 \text{ ou } a = 0 \\ b = b^2 \Rightarrow b = 1 \text{ ou } b = 0 \\ ac = bc \Rightarrow \text{se } a = b = 1, \text{ então} \\ c \in \mathbb{R}. \end{cases}$$

1ª conclusão: devemos ter:

$$a = b = 1 \text{ e } c \in \mathbb{R}.$$

2ª conclusão: $a=0$; $b=0$ e $c \in \mathbb{R}$

3ª conclusão: $a=1$; $b=0$, e então
devemos ter $c=0$

4ª conclusão: $a=0$; $b=1$ e então
devemos ter $c=0$.

Res: $(a, b, c) = (1, 1, c)$; ou
 $= (0, 0, c)$ ou
 $= (1, 0, 0)$ ou
 $= (0, 1, 0)$.