

Na aula passada estudamos grupos cíclicos.

$(G, \cdot)$ é cíclico se $\exists g \in G$ tal que, $\forall x \in G$;
 $x = g^m$, para algum $m \in \mathbb{Z}$. Ou seja;

$$G = \{g^m : m \in \mathbb{Z}\} \quad (\text{na not. multiplic.})$$

Na notação aditiva, $(G, +)$ é cíclico se
 $\exists g \in G$ tal que, $\forall x \in G$; $x = m.g$; $m \in \mathbb{Z}$.

Neste caso,

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

Seja G cíclico, escrevemos

$G = \langle g \rangle$, e $g \in G$ é um
gerador de G .

SUBGRUPO GERADO POR UM CONJUNTO :

Seja $(G, \cdot)$ um grupo e seja $a \in G$.

Considere $\langle a \rangle = \{ a^m : m \in \mathbb{Z} \}$. Assuma que a não seja um gerador de G . Assim, $\langle a \rangle \neq G$.

AF: $\langle a \rangle$ é um subgrupo de G .

Note que $\langle a \rangle \neq \emptyset$, pois, por exemplo, para $m = 0$, temos $a^0 = e$.

Dados $\alpha, \beta \in \langle a \rangle$, vamos mostrar que :

- (i) $\alpha \cdot \beta \in \langle a \rangle$;
- (ii) $\alpha^{-1} \in \langle a \rangle$.

De fato, como $\alpha, \beta \in \langle a \rangle$, então $\exists p, q \in \mathbb{Z}$ tais que $\alpha = a^p$ e $\beta = a^q$. Assim:

$$(i) \quad \alpha \cdot \beta = a^p \cdot a^q = a^{p+q} \in \langle a \rangle, \text{ pois } p+q \in \mathbb{Z}.$$

$$(ii) \quad \alpha^{-1} = (a^p)^{-1} = a^{-p} \in \langle a \rangle, \text{ pois } -p \in \mathbb{Z}.$$

Portanto, $\langle a \rangle \leq G$.

Dado $(G, \cdot)$ um grupo e $S \subset G$, $S \neq \emptyset$ um conjunto não vazio em G .

Defina o subconjunto gerado pelo conjunto S por:

$$\langle S \rangle = \{ a_1 \cdot a_2 \cdots a_m : a_i \in S \text{ ou } a_i^{-1} \in S \}$$

Note que $\langle S \rangle \neq \emptyset$. De fato; por exemplo, dado $a_1 \in S$ então, pela def. de $\langle S \rangle$, segue que $a_1 \in \langle S \rangle$.

AF.: $\langle S \rangle \subset G$.

De fato, dado $x \in \langle S \rangle$, mostremos que $x \in G$. Sendo $x \in \langle S \rangle$, então,

$$x = a_1 \cdot a_2 \cdots a_m, \text{ onde } a_i \in S \text{ ou } a_i^{-1} \in S.$$

Como $S \subset G$, então cada $a_j \in S \subset G$, i, j ;
 $a_j \in G$ e a_j^{-1} também.

Como G é um grupo (e portanto, é fechado), concluímos que

$$x = \underbrace{a_1}_{\in G} \cdot \underbrace{a_2}_{\in G} \cdots \underbrace{a_m}_{\in G} \in G.$$

Dele arbitrariedade da escolha de x , concluímos que $\langle S \rangle \subset G$.

Mais que isso, o gerado por S é mais que um subconjunto, é um subgrupo de G . Ou seja, vale o seguinte resultado:

PROP.: Dado $(G, \cdot)$ um grupo e $S \subset G$ um subconjunto não vazio de G . Então,
 $\langle S \rangle < G$.

DEMONSTRA.: Sejam $\alpha, \beta \in \langle S \rangle$. A mostrar:

$$(i) \alpha \cdot \beta \in \langle S \rangle;$$

$$(ii) \alpha^{-1} \in \langle S \rangle.$$

De fato, como $\alpha, \beta \in \langle S \rangle$, então:

$$\alpha = a_1 \cdot a_2 \cdot \dots \cdot a_m : a_i \in S \text{ ou } a_i^{-1} \in S.$$

$$\beta = b_1 \cdot b_2 \cdot \dots \cdot b_k : b_j \in S \text{ ou } b_j^{-1} \in S.$$

Então:

$$\alpha \cdot \beta = a_1 \cdot a_2 \cdot \dots \cdot a_m \cdot b_1 \cdot \dots \cdot b_k ;$$

$$\text{e como } a_i \in S \text{ ou } a_i^{-1} \in S ;$$

$$b_j \in S \text{ ou } b_j^{-1} \in S ,$$

segue que $\alpha \cdot \beta \in \langle S \rangle$; provando (i).

Por fim, dado $\alpha = a_1 \cdot a_2 \cdot \dots \cdot a_m \in \langle S \rangle$,
mostramos que $\alpha^{-1} \in \langle S \rangle$. De fato:

$$\alpha^{-1} = (a_1 \cdot a_2 \cdot \dots \cdot a_m)^{-1} =$$

$$= a_m^{-1} \cdot a_{m-1}^{-1} \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1} ; \text{ com}$$

$$a_i^{-1} \in S \text{ ou } (a_i^{-1})^{-1} \in S$$

"
 a_i

$$\Rightarrow \alpha^{-1} \in \langle S \rangle.$$

□

obs: $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. (em um grupo)

De fato, dados $x, y \in G$; então

$x \cdot y \in G$. Seja $(x \cdot y)^{-1}$ o seu inverso.

Logo,

$$(x \cdot y) \cdot (x \cdot y)^{-1} = e$$

Multiplicando à esquerda por x^{-1} , vem:

$$(x^{-1} \cdot (x \cdot y)) \cdot (x \cdot y)^{-1} = x^{-1} \cdot e$$

$$\underbrace{(x^{-1} \cdot x)}_e \cdot y \cdot (x \cdot y)^{-1} = x^{-1}$$

$$\Rightarrow y \cdot (x \cdot y)^{-1} = x^{-1}$$

Multiplicando à esquerda por y^{-1} , vem:

$$\underbrace{y^{-1} \cdot (y \cdot (x \cdot y)^{-1})}_e = y^{-1} \cdot x^{-1}$$

$$\boxed{\Rightarrow (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}}$$

Ex-1: $G = \{1, i, -1, -i\}$, equipada com o produto usual em $\mathbb{C}$.

Seja $S = \{-1\}$ um subconj. não vazio de G .

$\langle S \rangle = \{ \}$ é o conj. de produtos dos elementos de S , incluindo seus inversos?

$$\langle S \rangle = \{-1, 1\} < G.$$

↑
VISTO NA ÁULA PASSADA.

PROPOSIÇÃO: Dados $(G, \cdot)$ um grupo e $S \subset G$, $S \neq \emptyset$
Então, $\langle S \rangle$ é o menor subgrupo que contém S .

DEMONSTRAR: Seja $S \subset G$ e considere $H < G$ tal que $S \subset H$. Vamos mostrar que $\langle S \rangle \subset H$.

Dado $x \in \langle S \rangle$ qualquer, vamos mostrar que $x \in H$.

Como $x \in \langle S \rangle$, então,

$$x = a_1 \cdot a_2 \cdots a_m : a_i \in S \text{ ou } a_i^{-1} \in S.$$

- se $a_i \in S$, como $S \subset H$, segue que $a_i \in H$,
e como $H < G$, segue que $a_i^{-1} \in H$,
 $\forall i \in \{1, 2, \dots, m\}$. Logo, concluir-se,
neste caso, que $x = a_1 a_2 \dots a_m \in H$.

- se $a_i^{-1} \in S$, como $S \subset H$, segue que $a_i^{-1} \in H$,
e como $H < G$, segue que $(a_i^{-1})^{-1} \in H$,
" a_i

$\forall i \in \{1, 2, \dots, m\}$. Logo, concluir-se que
 $x = a_1 a_2 \dots a_m \in H$.

Em qualquer dos casos concluímos que $x \in H$,
como queríamos mostrar.

Dele arbitrariedade da escolha de x segue que
 $\langle S \rangle \subset H$, $\forall H$ tal que $S \subset H$.

Daí se vê, $\langle S \rangle$ é o menor subgrupo de G
que contém S .

ORDEN DE UM GRUPO:

Def.: Seja G um grupo. Definimos por ordem de G , e denotamos por $o(G)$ ou $|G|$, como sendo o número de elementos de um grupo.

Quando o grupo for finito escreveremos

$$|G| < \infty;$$

e quando for infinito, escreveremos $|G| = \infty$.

EXEMPLOS:

(a) $(\mathbb{Z}, +)$ - grupo aditivo dos inteiros.

Neste caso, $|\mathbb{Z}| = \infty$.

(b) $(S_4, \circ)$; onde

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

Neste caso, $|S_4| = 6$.

(c) $(S_n, \circ)$; onde S_n é o grupo das permutações de n elementos.

Neste caso, $|S_n| = n!$

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

$$|G| = 4.$$

PROPOSIÇÃO: Seja G um grupo multiplicativo e seja $\alpha \in G$, $\alpha \neq e$. Então, são equivalentes as seguintes afirmações:

(i) $|\langle \alpha \rangle| = n < \infty$;

(ii) $\exists t \geq 1$; tal que $\alpha^t = e$.

Neste caso,

$$\langle \alpha \rangle = \{e, \alpha, \alpha^2, \dots, \alpha^{n-1}\}.$$

DEMONSTRAÇÃO:

(i) $\Rightarrow$ (ii): Seja $\alpha \neq e$, e considere

$$\langle \alpha \rangle = \{ \alpha^m : m \in \mathbb{Z} \}.$$

Como $|\langle \alpha \rangle| < \infty$ (ordem finita); então,

$\exists p, q \in \mathbb{Z}$ tais que

$$\alpha^p = \alpha^q \quad (*)$$

Sem perda de generalidade, assumo que $p > q$.

Multiplicando (*) à direita por $\alpha^{-q} \in \langle \alpha \rangle$,
obtemos:

$$\alpha^p \cdot \alpha^{-q} = \alpha^q \cdot \alpha^{-q} = \alpha^{q-q} = \alpha^0 = e$$

$$\Rightarrow \alpha^{p-q} = \alpha^p \cdot \alpha^{-q} = e,$$

com $p-q > 0$ e $p-q \in \mathbb{Z}$. Logo, $p-q \geq 1$.

Denote $t = p-q \geq 1$. Então, obtemos

$$t \geq 1, \text{ com } \alpha^t = e,$$

o que prova (ii).

($\Leftarrow$) Reciprocamente, suponha que

$$\exists t \geq 1 \text{ tal que } \alpha^t = e.$$

Vamos mostrar que

$$\langle \alpha \rangle = \{ e, \alpha, \alpha^2, \dots, \alpha^{n-1} \}$$

(ou seja, que $|\langle \alpha \rangle| = n < \infty$).

Defina o número:

$$n = \min \{ t \geq 1 : \alpha^t = e \}.$$

A.F.: $\langle \alpha \rangle = \{ e, \alpha, \alpha^2, \dots, \alpha^{n-1} \}$; onde
seus elementos são diferentes dois a dois

Isso absendo, suponha que não. Assim,
existem $p, q \in \mathbb{N}$; $0 \leq p, q < n$ tais que

$$\alpha^p = \alpha^q. \quad (**)$$

Assuma, sem perda de generalidade que $p > q$.
multiplicando (**) por α^{-q} , vem:

$$\alpha^p \cdot \alpha^{-q} = \alpha^q \cdot \alpha^{-q} = \alpha^0 = e$$

$$\Rightarrow \alpha^{p-q} = e, \text{ onde}$$

$$0 < p-q < n = \min \{ t \geq 1 : \alpha^t = e \};$$

mas isto contradiz a minimalidade de n ; ou seja, temos um absurdo!

Portanto, vale a AF; ou seja;

$\langle \alpha \rangle = \{e, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$, com todos elementos distintos entre si.

Logo, $|\langle \alpha \rangle| = n < \infty$.

□

Ex: i $G = \{1, i, -1, -i\}$, equipado com o produto em $\mathbb{C}$. Então, temos que

$$\langle -1 \rangle = \{-1, 1\}$$

$$\Rightarrow |\langle -1 \rangle| = 2 < \infty.$$

Logo, $\exists t \geq 1$ tal que $(-1)^t = e = 1$.

(no caso, $t = 2$), e temos:

$$\langle -1 \rangle = \{1=e, (-1)^1\} = \{1, -1\}$$

CLASSES LATERAIS:

Def: Seja $(G, \cdot)$ um grupo e $H < G$. Dados $x, y \in G$, dizemos que x é côngruo a y , módulo H , e escrevemos

$$x \equiv y \pmod{H},$$

$$\text{ou } x \cdot y^{-1} \in H.$$

AF-: A cônica módulo H é uma relação de equivalência.

De fato, ela é reflexiva, simétrica e transitiva. Vejamos:

(i) REFLEXIVA: $x \equiv x \pmod{H}$, pois

$$e = x \cdot x^{-1} \in H.$$

(ii) SIMÉTRICA: $x \equiv y \pmod{H} \Rightarrow y \equiv x \pmod{H}$:

Suponha $x \equiv y \pmod{H}$. Então,

$$x \cdot y^{-1} \in H.$$

Como $H < G$ (ou seja, H é subgrupo),
segue que $(x \cdot \bar{y}^{-1})^{-1} \in H$, ou seja,

$$(x \cdot \bar{y}^{-1})^{-1} = (\bar{y}^{-1})^{-1} \cdot x^{-1} \in H,$$

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

isto é,

$$y \cdot x^{-1} \in H \stackrel{\text{def.}}{\iff} y \equiv x \pmod{H}$$

(iii) TRANSITIVIDADE: $x \equiv y \pmod{H}$ e $y \equiv z \pmod{H}$,
então $x \equiv z \pmod{H}$.

De fato, suponha

$$x \equiv y \pmod{H} \text{ e } y \equiv z \pmod{H}.$$

Então,

$$x \cdot \bar{y}^{-1} \in H \text{ e } y \cdot \bar{z}^{-1} \in H.$$

Como H é um subgrupo de G , segue que o
produto de seus elementos fica em H . Assim:

$$(x \cdot \bar{y}^{-1}) \cdot (y \cdot \bar{z}^{-1}) \in H;$$

o que, por associatividade:

$$x \cdot (\underbrace{y^{-1} \cdot y}_{=e}) \cdot \bar{z}^{-1} \in H \Rightarrow x \cdot \bar{z}^{-1} \in H,$$

ou seja;

$$x \equiv z \pmod{H}.$$

Da mesma forma que a congruência módulo m estudada na Aritmética produz classes de equivalência, a congruência módulo H , com $H < G$, também define classes de equivalência como segue:

$$\begin{aligned} \bar{x} &= \{ y \in G : y \equiv x \pmod{H} \} = \\ &= \{ y \in G : y \cdot \bar{x}^{-1} \in H \} \end{aligned}$$

Desse forma:

$$\alpha \in \bar{x} \Leftrightarrow \alpha \equiv x \pmod{H} \Leftrightarrow$$

$$\Leftrightarrow \alpha \cdot \bar{x}^{-1} \in H \Rightarrow$$

$$\Leftrightarrow \alpha \bar{x}^{-1} = h : h \in H.$$

$$\Leftrightarrow \alpha \bar{x}^{-1} \cdot x = h x : h \in H$$

$$\Leftrightarrow \alpha = hx : h \in H$$

$$\Leftrightarrow \alpha = hx \in Hx,$$

onde $Hx = \{h \cdot x : h \in H\}$, e' um conjunto chamado de classe lateral à direita de H .

Ou seja:

$$\bar{x} = Hx$$

Analogamente define-se a classe lateral à esquerda.
