

No final da aula passada iniciaremos o estudo de classes laterais. Vimos que, dado $(G, \cdot)$ um grupo e $H < G$, então, $\forall x, y \in G$, definiremos a congruência módulo H por:

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

Vimos que esta congruência é uma relação de equivalência (reflexiva, simétrica e transitiva)

Vimos que

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

Analisando:

$$\begin{aligned}y \in \bar{x} &\iff y \cdot x^{-1} \in H \iff \\ &\iff \exists h \in H \text{ tal que } h = y \cdot x^{-1} \\ &\quad \text{multiplica à direita por } x \\ &\iff h \cdot x = y\end{aligned}$$

$$\Leftrightarrow y = hx \in Hx ; \text{ onde}$$

$$Hx = \{ h \cdot x : h \in H \}, \text{ e'}$$

chamada de CLASSE LATERAL À DIREITA de H .

Ou seja, temos a seguinte definição:

Def: Sejam $(G, \cdot)$ um grupo e $H < G$. Para $x \in G$,
definimos a classe lateral à direita de H

em G por:

$$Hx = \{ hx : h \in H \}.$$

Do mesmo modo definimos a classe lateral à esquerda de H em G por:

$$xH = \{ x \cdot h : h \in H \}.$$

O conjunto de todas as classes laterais à direita de $H < G$ é denotada por G/H .

$$G/H = \{ H \cdot x : x \in G \}.$$

Obs: Note que, em geral, fixado $x \in G$;

$1 \cdot x \neq x \cdot 1$ (uma classe lateral à esquerda não é necessariamente igual a uma classe lateral à direita). Se' temos $1x = x1$ se G for abeliano.

Veja'nos um exemplo para justificar este fato:

$G = S_\Delta = \{id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}$,
cuja tabela com a operação de composição
é mostrada abaixo: (não comutativa)

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

Seja o subgrupo $H = \{id, R_1\} \leq S_3$

Seja, por exemplo $x = R_2$. Vamos obter as classes laterais

$H \cdot R_2$ e $R_2 \cdot H$. Assim:

- $H \cdot R_2 = \{id \circ R_2, R_1 \circ R_2\} = \{R_2, R_{\frac{4\pi}{3}}\}.$

- $R_2 \cdot H = \{R_2 \circ id, R_2 \circ R_1\} = \{R_2, R_{\frac{2\pi}{3}}\}$

$$\Rightarrow H \circ R_2 \neq R_2 \circ H$$

(pois S_3 não é abeliano)

Def: Seja $(G, \cdot)$ um grupo e $H < G$, a cardinalidade (*) do conjunto G/H (ou seja, de todas as classes laterais de H em G) é chamada de índice de H em G , e é denotado por $(G:H)$ ou $|G/H|$.

(*) se G for finito, a cardinalidade de G corresponde ao número de elementos de G .

No que segue, queremos apresentar um importante teorema, chamado de TEOREMA DE LAGRANGE, que estabelece uma relação entre um grupo com os seus subgrupos. Antes, porém, precisaremos enunciar alguns lemas técnicos.

Dado $(G, \cdot)$ e $H < G$, vimos acima que, em geral, $\forall x \in G$ fixado, $H \cdot x \neq x \cdot H$.

(a menos que G seja abeliano). A primeira questão a pensar é: percorrendo todos os $x \in G$, será que a quantidade de classes à esquerda é igual à quantidade de classes laterais à direita, ou não?

De fato, terá mesma quantidade, ou não,

note o seguinte lema:

LEMA 1: Existe uma correspondência bijetiva entre as classes laterais à esquerda e as classes laterais à direita.

DEMONSTRA: Seja $(G, \cdot)$ um grupo e $H < G$.

Defina os conjuntos:

$A = \{ Hx : x \in G \}$ (conj. de todas as classes laterais à direita de H) ;

$B = \{ xH : x \in G \}$ (conj. de todas as classes laterais à esquerda de H)

Defina $\varphi: A \rightarrow B$ por:

$$\varphi(Hx) = x^{-1}H.$$

Note que:

- φ é injetiva ($\Rightarrow$) e está bem definida ($\Leftarrow$)

De fato, basta observar que:

$$\varphi(Hx) = \varphi(Hy) \Leftrightarrow x^{-1}H = y^{-1}H \Leftrightarrow$$

$$\Leftrightarrow x^{-1} \equiv y^{-1} \pmod{H} \Leftrightarrow (x^{-1})^{-1} \cdot y^{-1} \in H$$

↳ congruência à esquerda.

$$\Leftrightarrow x \cdot y^{-1} \in H \Leftrightarrow x \equiv y \pmod{H} \Leftrightarrow$$

↳ congruência à direita

$$\Leftrightarrow Hx = Hy.$$

• φ é surjetiva:

$$\varphi: A \rightarrow B$$

$$\varphi(Hx) = x^{-1} \cdot H$$

Dado $zH \in B$, precisamos mostrar que $\exists Hx \in A$ tal que $\varphi(Hx) = zH$. De fato, basta tomar $Hx = H\bar{z}^{-1} \in A$:

$$\varphi(Hx) = \varphi(H\bar{z}^{-1}) = (\bar{z}^{-1})^{-1}H = zH.$$

□



LEMA 02: Seja G um grupo e $H < G$. Então, para $x \in G$, a cardinalidade de H é a mesma cardinalidade de Hx . (ou xH , c.f. lema 1)

DEMONSTRA. Defina $\varphi: H \rightarrow Hx$ por:

$$\varphi(h) = hx$$

Note que:

- φ é injetiva: (obs. não precisamos verificar se φ está bem definida pois agora o domínio da função não é um conj. de classes, não havendo, portanto, problemas com diferentes representantes do mesmo objeto do domínio).

De fato:

$$\begin{aligned} \varphi(a) = \varphi(b) &\Rightarrow a \cdot x = b \cdot x \Rightarrow a \cdot \underbrace{x^{-1}}_e = b \cdot \underbrace{x^{-1}}_e \\ &\Rightarrow \underline{a = b.} \end{aligned}$$

- φ é sobrejetiva: Dado $hx \in Hx$, precisamos encontrar $\alpha \in H$ tal que $\varphi(\alpha) = hx$.

De fato, basta tomar $\alpha = h$:

$$\varphi(x) = \varphi(h) = hx.$$

Logo, φ é bijetora, e, portanto, H e Hx possuem mesma cardinalidade.

□

LEMA 03: Seja $(G, \cdot)$ um grupo e $H < G$.

Então G é uma união disjunta de todas as classes laterais à esquerda (ou à direita) de H .
Mais precisamente,

$$G = \dot{\bigcup}_{x \in G} xH.$$

DEMONSTR: Precisamos provar duas contenções para mostrar a igualdade entre conjuntos acima.

AFOL: $G \subset \dot{\bigcup}_{x \in G} xH$: como esta contenção é

"forte demais" - no sentido de grupo inteiro estar contido numa união de outros conjuntos - vamos por absurdo.

Se absurdo, suponha que $G \not\subset \dot{\bigcup}_{x \in G} xH$.

Então, $\exists g_0 \in G$ tal que $g_0 \notin \bigcup_{x \in G} xH$.

No entanto, observe que

$$\underbrace{g_0}_{\text{wavy}} = g_0 \cdot \underbrace{e}_{\substack{\uparrow \\ e \in H}} \in g_0 H \subset \underbrace{\bigcup_{x \in G} xH}_{\text{wavy}}$$

Logo, $g_0 \in \bigcup_{x \in G} xH$, mas $g_0 \notin \bigcup_{x \in G} xH$.

Absurdo! Portanto, vale a AF. 01.

AF. 02: $\bigcup_{x \in G} xH \subset G$:

Dado $w \in \bigcup_{x \in G} xH$, precisamos mostrar

que $w \in G$. Como $w \in \bigcup_{x \in G} xH$, então, $\exists x_0 \in G$

tal que $w \in x_0 H$. Logo, $\exists h \in H$ tal que

$$\underbrace{w}_{\text{wavy}} = x_0 \cdot \underbrace{h}_{\text{wavy}} \in G \quad (\text{pois } x_0 \in G \text{ e } h \in H \subset G \text{ e } G \text{ é grupo})$$

$$\Rightarrow w \in G.$$

Dele arbitrariedade da escolha de w segue a AF. 02.

Deles afirmações 01 e 02 o resultado segue. $\square$

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

$$H = \{id, R_1\} < S_4.$$

Vamos determinar as classes laterais à esquerda (todas elas) de H em G :

- $id \cdot H = H$

$$R_{\frac{2\pi}{3}} \cdot H = \{R_{\frac{2\pi}{3}} \circ id, R_{\frac{2\pi}{3}} \circ R_1\} = \{R_{\frac{2\pi}{3}}, R_2\}$$

- $R_{\frac{4\pi}{3}} H = \{R_{\frac{4\pi}{3}} \circ id, R_{\frac{4\pi}{3}} \circ R_1\} = \{R_{\frac{4\pi}{3}}, R_3\}$

- $R_1 H = \{R_1 \circ id, R_1 \circ R_1\} = \{R_1, id\} = H$

- $R_2 H = \{R_2 \circ id, R_2 \circ R_1\} = \{R_2, R_{\frac{2\pi}{3}}\}$

- $R_3 H = \{R_3 \circ id, R_3 \circ R_1\} = \{R_3, R_{\frac{4\pi}{3}}\}$

Então, desse exemplo, notamos que:

$$G = H \dot{\cup} R_{\frac{2\pi}{3}} \cdot H \dot{\cup} R_{\frac{4\pi}{3}} \cdot H,$$

ilustrando o lema 3.

Além disso, notamos que H tem 2 elementos; e qualquer uma das 3 elenes obtidas também, ilustrando o lema 2.

Com estes lemas podemos finalmente apresentar o teorema de Lagrange.

TEOREMA DE LAGRANGE: Sejam G um grupo finito e $H < G$. Então, a ordem de H divide a ordem de G , ou seja,

$$|H| \mid |G|.$$

Mais precisamente,

$$|H| \cdot |G/H| = |G|.$$

DEMONSTR.: Seja G um grupo finito e $H < G$. Considere G/H o conjunto de todas as classes laterais de H em G (à esquerda ou à direita, tanto faz). Como G é finito, então G/H também é. Suponha que $|G/H| = m$, $m \in \mathbb{N}$.

Então,

$$G/H = \{ H \cdot x_1, H \cdot x_2, \dots, H \cdot x_m \}$$

Pelo lema 3;

$$G = \bigcup_{i=1}^m H x_i.$$

(união disjunta das m classes laterais)

Então:

$$|G| = \sum_{i=1}^m |H x_i| = \sum_{i=1}^m |H|$$

$$|H x_i| = |H|$$

(pelo lema 2)

$$\Rightarrow |G| = \underbrace{|H| + |H| + \dots + |H|}_{m \text{ adições.}}$$

$$\Rightarrow |G| = m \cdot |H| \Rightarrow |H| \mid |G|.$$

Mais que isso:

$$|G| = m \cdot |H| = |G/H| \cdot |H|.$$

□

Ex: S_4 . $|S_4| = 6$.

$$H = \{id, R_2\} < G. \Rightarrow |H| = 2.$$

$$e 2 \mid 6$$

Questão: Um grupo com 12 elementos pode possuir um subgrupo com 8 elementos?

Não, pois $8 \nmid 12$ (T. de Lagrange)

Outro, pelo T. de Lagrange, um grupo com 12 elementos só pode ter subgrupos com 1 elemento (no caso, só o neutro e); com 2 elementos, com 3 elementos, com 4 elementos, com 6 elementos ou com 12 elementos. Isso porque

↳ todo o G .

$$1 \mid 12 ; 2 \mid 12 ; 3 \mid 12 ; 4 \mid 12 ; 6 \mid 12 \text{ e } 12 \mid 12.$$