Introdução a Teoria dos Grupos – MAT 113 – Pós Mat – UFABC-QS2020.2

Informações rápidas

- Página da disciplina: hostel.ufabc.edu.br/~edson.iwaki ➔procure o link da sua turma.
- Email: edson.iwaki@ufabc.edu.br
- Além de todas as informações gerais do curso, os slides das aulas serão disponibilizados na página da disciplina.
- Recorde: o site do moodle: moodle.ufabc.edu.br

DEF: UM GRUPO G É UM PAR $(G, \cdot)$

ONDE G É UM CONJUNTO E '$\cdot$' É UMA OPERAÇÃO BINÁRIA

SOBRE G SATISFAZENDO:

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\forall a, b, c \in G$ (ASSOCIATIVA)

(ii) EXISTE UM ELEMENTO $e \in G$, TAL QUE $a \cdot e = e \cdot a = a$, $\forall a \in G$.
(EXISTÊNCIA DE ELEMENTO IDENTIDADE)

(iii) PARA CADA $a \in G$, EXISTE $\bar{a}' \in G$, TAL QUE
$a \cdot \bar{a}' = \bar{a}' \cdot a = e$. (EXISTÊNCIA DE ELEMENTO INVERSO)

G É DITO SER UM GRUPO ABELIANO (OU COMUTATIVO)
SE $ab = ba$, $\forall a, b \in G$.

OBS: G NÃO É VAZIO, DEVIDO A PROPRIEDADE (ii)

EXEMPLOS:

(i) $(\mathbb{Z},+)$; $(\mathbb{Q},+)$; $(\mathbb{C},+)$ SÃO GRUPOS, $e=0$, $\bar{a}=-a$, $\forall a$

(ii) $(\mathbb{Q}^*,\cdot)$; $(\mathbb{C}^*,\cdot)$ SÃO GRUPOS, $e=1$, $\bar{a}=\frac{1}{a}$, $\forall a$

- $(\mathbb{Z}^*,\cdot)$ NÃO É GRUPO, POIS 2 NÃO POSSUI INVERSO EM $\mathbb{Z}^*=\mathbb{Z}\setminus\{0\}$.

(iii) $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+\right)$ É GRUPO, $n\in\mathbb{Z}$, $n\geq 1$, fixado

(iv) $E_n=\{\theta_n^i \mid i=0,1,2,\ldots,n-1\}$ É GRUPO, ONDE $\theta_n=\cos\theta+i\,\mathrm{sen}\,\theta$, RAIZ n-ÉSIMA DA UNIDADE

COM O PRODUTO USUAL DOS COMPLEXOS..

DEF: UM GRUPO É FINITO SE ELE POSSUIR UM NÚMERO FINITO DE ELEMENTOS. O NÚMERO DE ELEMENTOS DE UM GRUPO G É DENOMINADO <u>ORDEM</u> DO GRUPO G E É DENOTADO POR $|G|$.

<u>PROPRIEDADES</u>: <u>LEMA</u>: SEJA G GRUPO:

(i) A IDENTIDADE e DE G É ÚNICA.

(ii) PARA CADA $a \in G$, a^{-1} É ÚNICO.

(iii) $(a^{-1})^{-1} = a$. $\forall a \in G$

(iv) $(ab)^{-1} = b^{-1}a^{-1}$; $a, b \in G$

(i) SUPONHA, f, g identidades de G.

$$\left.\begin{array}{l} \Rightarrow fg = f \quad (\text{pois } f \text{ é identidade}) \\ fg = g \quad (\text{pois } g \text{ é identidade}) \end{array}\right\} \Rightarrow f = g.$$

(ii) SEJAM b, c INVERSOS PARA a; e identidade de G.

$$\therefore \begin{array}{l} ab = e \\ ca = e \end{array}$$

$$\begin{aligned} \therefore \quad c &= ce \\ &= c(ab) \\ &= (ca)b \quad (\text{ASSOCIATIVIDADE}) \\ &= eb \\ &= b \end{aligned}$$

(iii) POR DEFINIÇÃO, $\bar{a}^{-1}\cdot(\bar{a}^{-1})^{-1} = e$, MAS $\bar{a}^{-1}a = e$

$$\therefore \bar{a}^{-1}(\bar{a}^{-1})^{-1} = \bar{a}^{-1}\cdot a \Rightarrow (\bar{a}^{-1})^{-1} = a \quad (\text{MULT. } \times a \text{ À ESQUERDA})$$

$$(ab)(\bar{b}^{-1}\bar{a}^{-1}) \underset{\text{ASSOC}}{=} ((ab)b^{-1})\bar{a}^{-1} \underset{\text{ASSOC}}{=} (a(bb^{-1}))\bar{a}^{-1} = (ae)\bar{a}^{-1} = a\bar{a}^{-1} = e.$$

Analogo: $(\bar{b}^{-1}\bar{a}^{-1})(ab) = e$

$(G, \cdot)$ GRUPO

DEF: UM SUBCONJUNTO $H \subseteq G$ É DITO SER UM SUBGRUPO DE G NÃO VAZIO

SE: (i) $a, b \in H \Longrightarrow ab \in H$

(ii) $a \in H \Longrightarrow a^{-1} \in H$.

NOT: $H \leq G$

EX: (i) $2\mathbb{Z} = \{2m \mid m \in \mathbb{Z}\}$, $H = (2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$

(ii) $k \in \mathbb{Z}$ fixado, $(k\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

(iii) Seja G GRUPO, $a \in \mathbb{Z}$. ENTÃO: $A = \{a^i \mid i \in \mathbb{Z}\}$ é SUBGRUPO DE G.

$\left(\begin{array}{l} a^i \in A,\ a^j \in A \Rightarrow a^i \cdot a^j = a^{i+j} \in A \\ (a^i)^{-1} = (a^{-1})^i = a^{-i} \in A. \end{array} \right.$

A ACIMA É DENOTADO SUBGRUPO CÍCLICO GERADO POR a,

É USUAL: $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$

DEF: O SUBGRUPO <u>cíclico</u> de G GERADO POR a É O CONJUNTO $\{a^i \mid i \in \mathbb{Z}\}$, DENOTADO POR $\langle a \rangle$.

Obs: EM NOTAÇÃO ADITIVA: $\langle a \rangle = \{ia \mid i \in \mathbb{Z}\}$.

Ex: $(\mathbb{Z}, +) = \langle +1 \rangle = \langle -1 \rangle$.

Ex. DEF: UMA RELAÇÃO $\sim$ SOBRE UM CONJUNTO S É DITA SER DE <u>EQUIVALÊNCIA</u> SE ELA SATISFAZ; para todo $a, b \in S$,

(i) $a \sim a$; (REFLEXIVA)

(ii) $a \sim b \Rightarrow b \sim a$ (SIMÉTRICA)

(iii) $a \sim b$ e $b \sim c \Rightarrow a \sim c$ (TRANSITIVA)

DEF: SE $\sim$ É UMA RELAÇÃO DE EQUIVALÊNCIA SOBRE UM CONJUNTO S, ENTÃO A <u>CLASSE DE EQUIVALÊNCIA</u> DE $a \in S$, DENOTADA POR $[a] = \{b \in S \mid b \sim a\}$

TEOREMA: SE $\sim$ É UMA RELAÇÃO DE EQUIVALÊNCIA SOBRE S ENTÃO $S = \bigcup [a]$, ONDE A UNIÃO VARRE UM ELEMENTO DE CADA CLASSE, E ONDE $[a] \neq [b]$ IMPLICA QUE $[a] \cap [b] = \phi$. ISTO É, $\sim$ PARTICIONA S EM CLASSES DE EQUIVALÊNCIA.

EX. DEF: UMA RELAÇÃO $\sim$ SOBRE UM CONJUNTO S É DITA SER DE **EQUIVALÊNCIA** SE ELA SATISFAZ; para todo $a, b \in S$,

(i) $a \sim a$; (REFLEXIVA)

(ii) $a \sim b \Rightarrow b \sim a$ (SIMÉTRICA)

(iii) $a \sim b$ e $b \sim c \Rightarrow a \sim c$ (TRANSITIVA)

DEF: SE $\sim$ É UMA RELAÇÃO DE EQUIVALÊNCIA SOBRE UM CONJUNTO S, ENTÃO A **CLASSE DE EQUIVALÊNCIA** DE $a \in S$, DENOTADA POR $[a] = \{b \in S \mid b \sim a\}$

TEOREMA: SE $\sim$ É UMA RELAÇÃO DE EQUIVALÊNCIA SOBRE S ENTÃO $S = \bigcup [a]$, ONDE A UNIÃO VARRE UM ELEMENTO DE CADA CLASSE, E ONDE $[a] \neq [b]$ IMPLICA QUE $[a] \cap [b] = \phi$. ISTO É, $\sim$ PARTICIONA S EM CLASSES DE EQUIVALÊNCIA.

DEM: COMO $a \in [a]$, TEMOS $\bigcup_{a \in S} [a] = S$. A DEMONSTRAÇÃO É SIMPLES.

(**DE FATO:** $[a] \subseteq S \Rightarrow \bigcup_{a \in S} [a] \subseteq S$ $\therefore$ $a \in S \Rightarrow a \in [a] \Rightarrow a \in \bigcup_{a \in S} [a]$)

$\therefore$ MOSTREMOS QUE $[a] \neq [b] \Rightarrow [a] \cap [b] = \phi$.

SUPONHA $[a] \cap [b] \neq \phi$. SEJA $c \in [a] \cap [b]$ $\therefore$

$c \in [a] \rightarrow c \sim a \xrightarrow{\text{SIMÉTRICA}} a \sim c$
$c \in [b] \rightarrow c \sim b$
$\Big\} \xrightarrow{\text{TRANSITIVA}} a \sim b \rightarrow a \in [b]$.

SEJA $x \in [a]$. ENTÃO $x \sim a$, $a \sim b \rightarrow x \sim b$ $\therefore [a] \subset [b]$.

COM ARGUMENTO ANÁLOGO, MOSTRAMOS QUE $[b] \subset [a]$

$\therefore$ MOSTRAMOS QUE $[a] \cap [b] \neq \phi \Rightarrow [a] = [b]$.

Ex: SEJA G GRUPO, $H \leq G$.

DEF: A RELAÇÃO SOBRE G.

$$a \sim b \overset{\text{def}}{\iff} ab^{-1} \in H. \qquad (a, b \in G).$$

AFS: $\sim$ É RELAÇÃO DE EQUIVALÊNCIA SOBRE G.

(i) $a \sim a$ ∴ (pois $aa^{-1} = e \in H$).

(ii) $a \sim b \Rightarrow (b \sim a)$ (pois $a \sim b \Rightarrow ab^{-1} \in H \overset{H \leq G}{\Longrightarrow} (ab^{-1})^{-1} = ba^{-1} \in H. \rightarrow b \sim a.$

(iii) $a \sim b$ e $b \sim c \Rightarrow a \sim c.$

$$\left.\begin{array}{l} a \sim b \rightarrow ab^{-1} \in H \\ b \sim c \rightarrow bc^{-1} \in H \end{array}\right\} \rightarrow \underbrace{(ab^{-1})}_{\in H} \cdot \underbrace{(bc^{-1})}_{\in H} = ac^{-1} \in A \rightarrow a \sim c.$$

∴ $\sim$ É RELAÇÃO DE EQUIVALÊNCIA SOBRE G.

∴ $a \in G$, $[a] = \{x \in G \mid x \sim a\} = \{x \in G \mid x a^{-1} \in H\} = Ha = \{ha \mid h \in H\}$

∴ $[a] = Ha.$

Ex: SEJA G GRUPO, $H \leq G$.

A RELAÇÃO $\sim$

$$a \sim b \overset{\text{def}}{\iff} ab^{-1} \in H. \qquad (a, b \in G).$$

↳ RELAÇÃO DE EQUIVALÊNCIA SOBRE G.

A CLASSE DO ELEMENTO a É $[a] = Ha$.

ANALOGAMENTE: $H \leq G$.

DEF: $a \sim b \iff a^{-1}b \in H$, $\forall a, b \in G$.

ANALOGAMENTE, $\sim$ É UMA RELAÇÃO DE EQUIVALÊNCIA SOBRE G.

E PARA $a \in G$, $[a] = aH$.

DEF: PARA QUALQUER $N \leq G$ (GRUPO) E QUALQUER $g \in G$

SEJAM $gN = \{gn \mid n \in N\}$ E $Ng = \{ng \mid n \in N\}$, CHAMADOS RESPECTIVAMENTE

UMA CLASSE LATERAL À ESQUERDA DE N EM G E UMA CLASSE LATERAL À DIREITA DE N EM G.

DEF: SEJA G GRUPO, $H \leq G$.

DEFINIMOS O ÍNDICE DE H EM G, DENOTADO $i_G(H)$ (OU $[G:H]$) COMO O NÚMERO DE CLASSES LATERAIS À DIREITA (OU À ESQUERDA) DE H EM G.

TEOREMA DE LAGRANGE: SEJA G GRUPO FINITO, $H \leq G$.
ENTÃO: $|G| = i_G(H) \cdot |H|$; em particular, $|H|$ divide $|G|$.

DEM: VIMOS QUE $\sim$ def por $a \sim b \Leftrightarrow ab^{-1} \in H$, É RELAÇÃO DE EQUIVALÊNCIA SOBRE G.

- PARA $a \in G$, $[a] = Ha$.

$\therefore G = \bigcup_{a \in G} Ha$. SEJA k O Nº DE CLASSES DE EQUIVALÊNCIAS DISTINTAS

$\therefore G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$

Af: CADA CLASSE Ha_i possui $|H|$ ELEMENTOS., $i = 1, \dots, k$

DEFINA: $\varphi_i : H \to Ha_i$, $h \mapsto ha_i$; afirmamos que φ_i é bijetora.

pl cada

· φ_i É INJETORA:

SUPONHA $\varphi_i(h) = \varphi_i(\tilde{h}) \Rightarrow ha_i = \tilde{h}a_i \Rightarrow h = \tilde{h}$ (Multiplicando à direita por a_i^{-1})

$a_i \in G$ pois é inverso

·· φ_i é sobrejetora:

Tome $\tilde{h}a_i \in Ha_i$. Então $\tilde{h}a_i = \varphi_i(\tilde{h})$ e φ_i é sobrejetora. ∴ φ_i é bijetora.

∴ $|H| = |Ha_i|$ $i = 1, .., k$.

··· Como $\sim$ é RELAÇÃO DE EQUIVALÊNCIA, $Ha_i \cap Ha_j = \phi$, se $i \neq j$.

$G = Ha_1 \cup Ha_2 \cup .. \cup Ha_k \longrightarrow |G| = k \cdot |H|$ ∎

· φ_i É INJETORA:

SUPONHA $\varphi_i(h) = \varphi_i(\tilde{h}) \Rightarrow ha_i = \tilde{h}a_i \Rightarrow h = \tilde{h}$ (Multiplicando à direita por a_i^{-1})

$a_i \in G$ pois é inverso

·· φ_i é sobrejetora:

Tome $\tilde{h}a_i \in Ha_i$. Então $\tilde{h}a_i = \varphi_i(\tilde{h})$ e φ_i é sobrejetora. ∴ φ_i é bijetora.

$\therefore |H| = |Ha_i| \quad i = 1, \ldots, k.$

··· Como $\sim$ é RELAÇÃO DE EQUIVALÊNCIA, $Ha_i \cap Ha_j = \phi$, se $i \neq j$.

$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k \longrightarrow |G| = k \cdot |H| \rightarrow k = \frac{|G|}{|H|}$.

Obs: G grupo finito, $H \leq G$.

Com raciocínio análogo, com a rel. $a \sim b \Leftrightarrow \bar{a}^1 b \in H$; $[a] = aH$.

Temos $G = a_1H \cup a_2H \cup \ldots \cup a_tH$, onde t é o NÚMERO de CLASSES DE EQUIVALÊNCIA DISTINTAS.

· AINDA, $a_iH \cap a_jH = \phi$, se $i \neq j$.

PROVA-SE DO MESMO MODO QUE $|H| = |a_iH|$, $i = 1, \ldots, t$.

DONDE $|G| = t \cdot |H| \longrightarrow t = \frac{|G|}{|H|}$. ISSO MOSTRA QUE O NÚMERO DE CLASSES LATERAIS À DIREITA E À ESQUERDA DE H EM G É IGUAL.

Def. SE G É GRUPO FINITO, $H \leq G$, O NÚMERO DE CLASSES LATERAIS À DIREITA (OU À ESQUERDA) DE H EM G É DENOTADO ÍNDICE DE H EM G, DENOTADO $i_G(H)$ (OU $[G:H]$).

Obs: G GRUPO FINITO, $H \leq G$. ENTÃO $i_G(H) = \frac{|G|}{|H|}$.

Teorema: SEJA G GRUPO FINITO DE ORDEM PRIMA. ENTÃO G É CÍCLICO.

Demi: SEJA $H \leq G$. POR LAGRANGE, $|H| \mid |G| = p$. p PRIMO.

$\therefore |H| = 1$ OU $|H| = p$. SO $|H| \neq 1$. ENTÃO $H = G$.

SE $a \in G$, $a \neq e$, ENTÃO AS POTÊNCIAS DE a, FORMAM UM SUBGRUPO $\langle a \rangle \neq e$. LOGO, $\langle a \rangle = G$. TODO ELEMENTO DE G É DA FORMA $x = a^i$ P/ ALGUM i. $\therefore$ G É CÍCLICO.

SEJA G GRUPO FINITO; $a \in G$.

ENTÃO EXISTE $m \in \mathbb{Z}$ TAL QUE $a^m = e$.

$\neq$ $\langle a \rangle = \{e; a, a^2, \ldots, a^m, \ldots\} \subseteq G$.

LOGO EXISTEM t, n INTEIROS $t \neq$ $a^t = a^n \longrightarrow a^{t-n} = e$
$t > n$

↓ POIS G É FINITO

DEF: SEJA G GRUPO, $a \in G$, O MENOR INTEIRO POSITIVO n (CASO EXISTA) TAL QUE $a^n = 1$, É DENOMINADO A ORDEM DO ELEMENTO a; CASO NÃO EXISTA TAL INTEIRO, DIZEMOS QUE a POSSUI ORDEM INFINITA. DENOTA: $o(a)$ (ou $|a|$)

COR: SE G GRUPO FINITO, $a \in G$. ENTÃO $o(a) \mid |G|$.

COR: SE G GRUPO FINITO DE ORDEM n. ENTÃO $a^n = e$, $\forall a \in G$.