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

G grupo, $x, y \in G$.

Def: $x \sim y \iff y = g^{-1} x g, \ \exists g \in G$.

$\sim$ É RELAÇÃO DE EQUIVALÊNCIA:

- $x \sim x$ (pois $x = e^{-1} x e$)
- $x \sim y \Rightarrow y \sim x$ ($y = g^{-1} x g, \exists g \in G \longrightarrow x = g y g^{-1} = (g^{-1})^{-1} y g^{-1}$)
- $x \sim y$ e $y \sim z \Rightarrow x \sim z$ $\left(\begin{array}{l} y = g^{-1} x g \ \exists g \in G \\ z = h^{-1} y h \ \exists h \in G \end{array} \right| \Rightarrow z = h^{-1} g^{-1} x g h$
$= (g h)^{-1} x g h$

$\therefore \sim$ É REL. DE EQUIVALÊNCIA.

A CLASSE DE EQU. VALÊNCIA $\bar{x} = \{ y \in G \mid y \sim x \}$ SERÁ DENOMINADA CLASSE DE CONJUGAÇÃO (EM G) DETERMINADA PELO ELEMENTO x. NOT.: $\bar{x} = C_x$

SE G GRUPO FINITO, COM n CLASSES DE CONJUGAÇÃO

$$G = C_{x_1} \dot{\cup} C_{x_2} \dot{\cup} \cdots \dot{\cup} C_{x_n}$$

$$\therefore |G| = |C_{x_1}| + |C_{x_2}| + \cdots + |C_{x_n}|$$

OBSERVE QUE $x \in Z(G) \iff C_x = \{x\}$.

$$\therefore |G| = |Z(G)| + \sum_{x_i \notin Z(G)}' |C_{x_i}|. \longrightarrow \text{EQUAÇÃO DAS CLASSES}$$

PROP: G GRUPO FINITO, $x \in G$. ENTÃO $|C_x| = [G : C_G(x)]$.

EM PARTICULAR, $|C_x| \mid |G|$, $\forall x \in G$.

DEM: DEF: $\psi : G/C_G(x) \longrightarrow C_x$, $\quad G/C_G(x) = \{ C_G(x) g \mid g \in G \}$.

OBS: $x^g = g^{-1} x g$.

$$C_G(x) g \longmapsto x^g$$

. ψ ESTÁ BEM DEFINIDA:

$$C_G(x) g_1 = C_G(x) g_2 \longrightarrow g_1 g_2^{-1} \in C_G(x) \longrightarrow g_1 g_2^{-1} x = x g_1 g_2^{-1}$$

$$\longrightarrow g_2^{-1} x g_2 = g_1^{-1} x g_1 \longrightarrow x^{g_2} = x^{g_1}.$$

. ψ É INJETORA:

$$\psi(C_G(x) g_1) = \psi(C_G(x) g_2) \longrightarrow$$

$$x^{g_1} = x^{g_2} \longrightarrow g_1 g_2^{-1} \in C_G(x)$$

$$\longrightarrow C_G(x) g_1 = C_G(x) g_2$$

. ψ É SOBREJETORA (CLARO!!)

$\therefore |C_x| = [G : C_G(x)]$

$\square$

DEF Seja p primo. Dizemos que um grupo G é um <u>p-grupo</u> se $|G| = p^n$, para algum $n \in \mathbb{N}$.

<u>TEOREMA</u>: Seja p primo, G p-grupo, $|G| = p^n > 1$.

Então $|Z(G)| = p^m > 1$.

<u>DEM</u>: Pela equação de classes:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)}{}' |C_{x_i}| \Rightarrow |Z(G)| = |G| - \sum_{x_i \notin Z(G)}{}' |C_{x_i}|$$

$$\left.\begin{array}{l} \forall x_i \notin Z(G) \to |C_{x_i}| > 1 \\ |C_{x_i}| \mid |G| \end{array}\right\} \Rightarrow \left.\begin{array}{l} p \mid |C_{x_i}| \quad \forall x_i \notin Z(G) \\ e \\ p \mid |G| \end{array}\right\} \overset{\text{Lagrange}}{\Rightarrow} |Z(G)| = p^m > 1$$

PROP: SEJA G GRUPO FINITO, $|G| = p^2$, p PRIMO. ENTÃO G É ABELIANO.

DEM: VIMOS $|G| = p^2 \longrightarrow |Z(G)| = p^m > 1$.

· SE $|Z(G)| = p^2$. ENTÃO $G = Z(G)$ É ABELIANO.

SUPONHA $|Z(G)| \lneq |G|$ $\therefore (\exists a \in G \setminus Z(G))$

$\therefore H := C_G(a) \supsetneq Z(G)$, $a \in H$, $a \notin Z(G)$

$\therefore Z(G) \subsetneq H$, $|H| = p^r > |Z(G)| = p \Rightarrow |H| = p^2$ e $G = H$.

Abs. pois $C_G(a) = G \rightarrow a \in Z(G)$.

TEOREMA: SEJA G GRUPO ABELIANO FINITO, p DIVISOR PRIMO DE $|G|$. ENTÃO G ADMITE ELEMENTO DE ORDEM p.

DEM: CASO 1) G CÍCLICO.

SUP. $G = \langle x \rangle$, p primo, $p \mid |G|$.

SABEMOS QUE $o(x) = p^r \cdot m$, onde $r \geq 1$, E $a = x^{p^{r-1} \cdot m}$ É TAL QUE $a^p = e$, $a \neq e$

CASO 2: G ABELIANO NÃO CÍCLICO

SEJA $x \in G$, $x \neq e$, p primo, $p \mid |G|$.

SE $p \mid |\langle x \rangle|$, O RESULTADO SEGUE DO CASO 1)

Suponha $p \nmid |N|$, $N = \langle x \rangle$. Por Lagrange, $p \mid |L|$, $L = \frac{G}{N}$

(Obs: $N \triangleleft G$, pois G abeliano). Como $|L| < |G| \xrightarrow{HI} (\exists \bar{g} \in L)$, $\bar{g} \neq \bar{e}$, $\bar{g}^p = \bar{e}$

Ou seja $g \notin N$, $g^p \in N$. Agora se $|N| = n \longrightarrow (g^p)^n = g^{pn} = e$,

$\therefore p \mid |\langle g \rangle| \longrightarrow$ O RESULTADO SEGUE DO CASO 1.

TEOREMA: SEJA G GRUPO NÃO ABELIANO FINITO, p DIVISOR PRIMO DE $|G|$. ENTÃO G ADMITE ELEMENTO DE ORDEM p.

DEM: TEMOS $Z(G) \neq G$.

SE $p \mid |Z(G)|$. O RESULTADO SEGUE DO TEOREMA ANTERIOR

SUPONHA $p \nmid |Z(G)|$. PELA EQ. DE CLASSES:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)}' [G : C_G(x_i)].$$

Como $p \mid |G|$ e $p \nmid |Z(G)|$ $\longrightarrow \left(\exists x_i \notin Z(G)\right)$ $p \nmid [G : C_G(x_i)]$

$\therefore p \mid |H|$, onde $H = C_G(x_i) \neq G$. Como $|H| < |G|$

PELA HIPÓTESE DE INDUÇÃO, $\exists a \in H$ t.q. $o(a) = p$ $\square$

TEOREMA (CAUCHY) SEJA G GRUPO FINITO, p DIVISOR DE $|G|$.
PRIMO
ENTÃO G ADMITE UM ELEMENTO DE ORDEM p.

COROL: SEJA G GRUPO DE ORDEM 6. ENTÃO OU G É CÍCLICO OU $G \cong S_3$.

DEM: SEJA G GRUPO, $|G|=6$. PELO T. DE CAUCHY, $\exists x, y \in G$, $o(x)=2$ E $o(y)=3$.

SEJA $N = \langle y \rangle = \{e, y, y^2\}$ $\therefore [G:N]=2 \longrightarrow N \triangleleft G$.

EM PARTICULAR, $x^{-1}yx \in N = \{e, y, y^2\} \longrightarrow x^{-1}yx = y$ OU $x^{-1}yx = y^2 = y^{-1}$.

$xy = yx$

NESTE CASO

$a = xy$,
$o(a) = 6$ E $G = \langle a \rangle$
CÍCLICO

$G = \{e, x, y, y^2, xy, xy^2\}$
ONDE $yx = xy^{-1}$

É FÁCIL DE MOSTRAR UMA CORRESPONDÊNCIA ENTRE $D_3 \cong S_3$ E G.

easy office

PROP: SEJA G GRUPO DE ORDEM $p \cdot q$; p, q PRIMOS DISTINTOS, $p > q$. SE $a \in G$, TEM ORDEM p, $A = \langle a \rangle$. ENTÃO $A \triangleleft G$.

DEM: AF: A É O ÚNICO SUBGRUPO DE ORDEM p DE G.

SUPONHA B OUTRO SUBGRUPO DE ORDEM p DE G.

SEJA $AB = \{ xy \mid x \in A, y \in B \}$

AF: AB POSSUI p^2 ELEMENTOS DISTINTOS.

SUP. $xy = uv$; $x, u \in A$; $y, v \in B$.

$$\therefore \underbrace{u^{-1}x}_{\in A} = \underbrace{vy^{-1}}_{\in B} \in A \cap B$$

Como $B \neq A$ e $A \cap B \leq A$, $|A| = p$ primo $\Big\} \to A \cap B = e \longrightarrow u^{-1}x = e \to u = x$.

Analogamente, $v = y$. LOGO O NÚMERO DE ELEMENTOS DISTINTOS EM AB É p^2.

MAS ESSES ELEMENTOS ESTÃO EM G, QUE POSSUI $pq < p^2$ ELEMENTOS (pois $p > q$)

ESSA CONTRADIÇÃO IMPLICA QUE $A = B$. $\therefore$ A É O ÚNICO SUBGRUPO DE G DE ORDEM p

PROP: SEJA G GRUPO DE ORDEM $p \cdot q$, p, q PRIMOS DISTINTOS, $p > q$.
SE $a \in G$, TEM ORDEM p, $A = \langle a \rangle$. ENTÃO $A \triangleleft G$.

DEM: **AF:** A É O ÚNICO SUBGRUPO DE ORDEM p DE G. ULC.

AGORA, SE $x \in G$, $B = x^{-1} A x$ É SUBGRUPO DE G,

B POSSUI ORDEM p.

PELO QUE VIMOS $x^{-1} A x = A$, $\forall x \in G$. $\square$