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

TEOREMA FUNDAMENTAL DOS GRUPOS ABELIANOS FINITOS.

TODO GRUPO ABELIANO FINITO É UM PRODUTO DIRETO DE SUBGRUPOS CÍCLICOS DE ORDEM POTÊNCIA DE UM PRIMO.

ALÉM DISSO, O NÚMERO DE TERMOS NO PRODUTO E A ORDEM DOS GRUPOS CÍCLICOS SÃO UNICAMENTE DETERMINADAS PELO GRUPO

LEMA: SEJA G GRUPO ABELIANO FINITO, $|G| = p^n m$, p PRIMO, $p \nmid m$ ENTÃO $G \cong H \times K$, ONDE $H = \{x \in G \mid x^{p^n} = e\}$ E $K = \{x \in G \mid x^m = e\}$. ALÉM DISSO, $|H| = p^n$.

DEMI: É FÁCIL DE VER QUE H E K SÃO SUBGRUPOS DE G.

PARA MOSTRAR QUE $G = H \times K$, TEMOS DE MOSTRAR QUE $G = HK$, $H \cap K = \{e\}$ (G ABELIANO, $H \trianglelefteq G$, $K \trianglelefteq G$).

$mdc(p^n, m) = 1 \xrightarrow[\text{BEZOUT}]{} 1 = sm + tp^n$, p/ alguns $s, t \in \mathbb{Z}$.

$\forall x \in G \longrightarrow x = x^1 = x^{sm+tp^n} = x^{sm} \cdot x^{tp^n} \xrightarrow[(\text{pois } x^{|G|} = e)]{} x^{sm} \in H \text{ E } x^{tp^n} \in K$

$\therefore G = HK$

(II) $x \in H \cap K \longrightarrow x^{p^n} = e = x^m \longrightarrow \left.\begin{matrix} o(x) \mid p^n \text{ E } o(x) \mid m \\ mdc(p^n, m) = 1 \end{matrix}\right\} \Rightarrow o(x) = 1 \rightarrow x = e.$

LEMA: SEJA G GRUPO ABELIANO FINITO, $|G| = p^n m$, p PRIMO, $p \nmid m$ ENTÃO $G \cong H \times K$, ONDE $H = \{x \in G \mid x^{p^n} = e\}$ E $K = \{x \in G \mid x^m = e\}$. ALÉM DISSO, $|H| = p^n$.

DEM: PARA A PARTE RESTANTE:

$$p^n m = |G| = |HK| = \frac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K|$$

[Por Cauchy, $p \mid |K| \rightarrow (\exists\, y \in G)\, o(y) = p$.
Além disso, se $x^j = e \rightarrow o(x) \mid j$.]

$\rightarrow p \nmid |K| \rightarrow |H| = p^n$.

LEMA: SEJA G GRUPO ABELIANO FINITO, $|G| = p^n m$, p PRIMO, $p \nmid m$ ENTÃO $G \cong H \times K$, ONDE $H = \{x \in G \mid x^{p^n} = e\}$ E $K = \{x \in G \mid x^m = e\}$. ALÉM DISSO, $|H| = p^n$.

DEM: PARA A PARTE RESTANTE:

$$p^n m = |G| = |HK| = \frac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K|$$

[Por Cauchy, $p \mid |G| \to (\exists\, y \in G)\ o(y) = p$.
Além disso, se $x^j = e \to o(x) \mid j$.]

$\to p \nmid |K| \to |H| = p^n$.

SEJA G GRUPO ABELIANO COM $|G| = p_1^{n_1} \cdots p_k^{n_k}$, p_i's PRIMOS DISTINTOS
SEJA $G(p_i) = \{x \in G \mid x^{p_i^{n_i}} = e\}$. ENTÃO POR INDUÇÃO E O LEMA,
TEMOS $G \cong G(p_1) \times G(p_2) \times \cdots \times G(p_k)$

LEMA: SEJA G GRUPO ABELIANO DE ORDEM POTÊNCIA DE UM PRIMO E SEJA a UM ELEMENTO DE ORDEM MAXIMAL EM G. ENTÃO G PODE SER ESCRITO NA FORMA $\langle a \rangle \times K$.

DEM: SUPONHA $|G| = p^n$. A DEMONSTRAÇÃO SERÁ POR INDUÇÃO EM n.

SE $n=1$ ENTÃO $G = \langle a \rangle \times \langle e \rangle$.

ASSUMA QUE A AFIRMAÇÃO É VÁLIDA PARA TODO GRUPO ABELIANO DE ORDEM p^k, com $k<n$.

ESCOLHA ENTRE OS ELEMENTOS DE G, UM ELEMENTO DE ORDEM MAXIMAL p^m.

$\therefore x^{p^m} = e, \forall x \in G$. PODEMOS SUPOR QUE $G \neq \langle a \rangle$ (SE $G = \langle a \rangle$ NADA A PROVAR)

ESCOLHA UM ELEMENTO EM G DE MENOR ORDEM, b, DE MODO QUE $b \notin \langle a \rangle$.

AF: $\langle a \rangle \cap \langle b \rangle = \{e\}$.

LEMA: SEJA G GRUPO ABELIANO DE ORDEM POTÊNCIA DE UM PRIMO E SEJA a UM ELEMENTO DE ORDEM MAXIMAL EM G. ENTÃO G PODE SER ESCRITO NA FORMA $\langle a \rangle \times K$.

DEM: COMO $|b^p| = \frac{|b|}{p}$ → SABEMOS QUE $b^p \in \langle a \rangle$. (PELA MANEIRA COMO b FOI ESCOLHIDO)

SUPONHA $b^p = a^i$. TEMOS QUE $= e = b^{p^m} = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}} \therefore |a^i| \leq p^{m-1}$

$\therefore a^i$ NÃO É GERADOR DE $\langle a \rangle$ → $\text{mdc}(p^m, i) \neq 1$. → $p \mid i \therefore i = pj, (\exists j \in \mathbb{Z})$

$\therefore b^p = a^i = a^{pj}$. CONSIDERE $c = a^{-j} b$.

OBSERVE QUE $c \notin \langle a \rangle$, CASO CONTRÁRIO, $b \in \langle a \rangle$.

$c^p = a^{-jp} b^p = a^{-i} b^p = b^p \cdot b^p = e$, $\therefore$ c É ELEMENTO DE ORDEM p QUE NÃO PERTENCE A $\langle a \rangle$.

COMO b FOI ESCOLHIDO COM A MENOR ORDEM DE MODO QUE $b \notin \langle a \rangle$, TEMOS QUE b TAMBÉM POSSUI ORDEM p. SEGUE QUE $\langle a \rangle \cap \langle b \rangle = \{e\}$.

CONSIDERE $\bar{G} = \frac{G}{\langle b \rangle}$ $\left(\bar{x} = x\langle b \rangle . \right)$.

SE $|\bar{a}| < |a| = p^m$ ENTÃO $|\bar{a}|^{p^{m-1}} = \bar{e} \rightarrow \left(a\langle b \rangle \right)^{p^{m-1}} = a^{p^{m-1}}\langle b \rangle = \langle b \rangle$.

$\rightarrow a^{p^{m-1}} \in \langle b \rangle \cap \langle a \rangle = \{e\}$.

ABSURDO, COM $|a| = p^m$.

$\therefore |\bar{a}| = |a| = p^m \rightarrow |\bar{a}|$ É ELEMENTO DE ORDEM MÁXIMAL EM $\bar{G}$.

PELA H. INDUÇÃO, $|\bar{G}|$ PODE SER EXPRESSO COMO $|\bar{G}| = \langle \bar{a} \rangle \times \bar{K}$, $\exists K \leq G$.

SEJA $\pi : G \rightarrow \frac{G}{\langle b \rangle}$ PROJEÇÃO CANÔNICA, SEJA $K = \pi^{-1}(\bar{K}) = \{x \in G \mid \underbrace{\bar{x}}_{\pi(x)} \in \bar{K}\}$

AF: $\langle a \rangle \cap K = \{e\}$. $x \in \langle a \rangle \cap K \rightarrow \bar{x} \in \langle \bar{a} \rangle \cap \bar{K} = \{\bar{e}\}$

$\rightarrow x \in \langle a \rangle \cap \langle b \rangle = \{e\}$.

$\therefore G = \langle a \rangle K$ $\therefore G = \langle a \rangle \times K$.

PELO LEMA ANTERIOR E INDUÇÃO NA ORDEM DO GRUPO OBTEMOS:

LEMA: UM GRUPO ABELIANO FINITO DE ORDEM POTÊNCIA DE PRIMO É UM PRODUTO DIRETO (INTERNO) DE GRUPOS CÍCLICOS.

LEMA: SEJA G GRUPO ABELIANO FINITO DE ORDEM POTÊNCIA DE PRIMO.
SE $G = H_1 \times H_2 \times \cdots \times H_m$ E $G = K_1 \times K_2 \times \cdots \times K_n$, ONDE OS H_i'S E K_j'S SÃO SUBGRUPOS CÍCLICOS NÃO TRIVIAIS COM $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ E $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$ ENTÃO $m = n$ E $|H_i| = |K_i|$.

PELO LEMA ANTERIOR E INDUÇÃO NA ORDEM DO GRUPO OBTEMOS:

LEMA: UM GRUPO ABELIANO FINITO DE ORDEM POTÊNCIA DE PRIMO É UM PRODUTO DIRETO (INTERNO) DE GRUPOS CÍCLICOS.

LEMA: SEJA G GRUPO ABELIANO FINITO DE ORDEM POTÊNCIA DE PRIMO.
SE $G = H_1 \times H_2 \times \cdots \times H_m$ E $G = K_1 \times K_2 \times \cdots \times K_n$, ONDE OS H_i'S E K_j'S SÃO SUBGRUPOS CÍCLICOS NÃO TRIVIAIS COM $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ E $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$ ENTÃO $m = n$ E $|H_i| = |K_i|$.

DEM: INDUÇÃO EM $|G|$.

SE $|G| = p$ PRIMO, O RESULTADO É VERDADEIRO.

SUPONHA QUE O RESULTADO É VERDADEIRO PARA GRUPOS ABELIANOS DE ORDEM MENOR QUE $|G|$.

PARA QUALQUER GRUPO ABELIANO L, O CONJUNTO $L^p = \{x^p \mid x \in L\}$ É SUBGRUPO DE L. SE p DIVIDE $|L|$, $L^p \lneq L$.

SEGUE QUE $G^p = H_1^p \times H_2^p \times \cdots \times H_{m'}^p$ E $G = K_1^p \times K_2^p \times \cdots \times K_{n'}^p$

ONDE m' É O MAIOR INTEIRO i TAL QUE $|H_i| > p$ E n' É O MAIOR INTEIRO j tq $|K_j| > p$.
(ISSO GARANTE QUE OS DOIS PRODUTOS DIRETOS PARA G^p SÃO NÃO TRIVIAIS)

COMO $|G^p| < |G| \underset{HI}{\Rightarrow} m' = n'$ E $|H_i^p| = |K_i^p|$; $i = 1, \cdots, m'$.

COMO $|H_i| = p \cdot |H_i^p| \rightarrow |H_i| = |K_i|$ PARA $i = 1, \cdots, m'$.

RESTA MOSTRAR QUE O NÚMERO DE SUBGRUPOS H_i DE ORDEM p. É IGUAL AO NÚMERO DE SUBGRUPOS K_i DE ORDEM p.

I.E. DEVEMOS MOSTRAR QUE $m - m' = n - n'$. (POIS $m' = n'$).

ISSO SEGUE DO FATO QUE:

$$|H_1| \cdot |H_2| \cdots |H_{m'}| \cdot p^{m-m'} = |G| = |K_1| \cdot |K_2| \cdots |K_{n'}| \cdot p^{n-n'}, \quad |H_i| = |K_i| \Rightarrow m' = n'.$$

ONDE m' É O MAIOR INTEIRO i TAL QUE $|H_i| > p$ E n' É O MAIOR INTEIRO j t.q. $|K_j| > p$.
(ISSO GARANTE QUE OS DOIS PRODUTOS DIRETOS PARA G^p SÃO NÃO TRIVIAIS)

Como $|G^p| < |G| \underset{HI}{\Rightarrow} m' = n'$. E $|H_i^p| = |K_i^p|$; $i = 1, \cdots, m'$.

Como $|H_i| = p \cdot |H_i^p| \rightarrow |H_i| = |K_i|$ para $i = 1, \cdots, m'$.

Ex: GRUPOS ABELIANOS DE ORDEM p^k, p primo, $k \in \mathbb{N}$.

$k = n_1 + n_2 + \dots + n_t \rightarrow$ PARTIÇÃO DE k., $n_j \in \mathbb{Z}$, $n_j \geq 0$.

$\mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \dots \oplus \mathbb{Z}_{p^{n_t}}$ É GRUPO ABELIANO DE ORDEM p^k.

ORDEM DE G	PARTIÇÕES DE K	POSSÍVEIS PRODUTOS DIRETOS
p^1	1	$\mathbb{Z}_p$
p^2	2	$\mathbb{Z}_{p^2}$
	1+1	$\mathbb{Z}_p \oplus \mathbb{Z}_p$
p^3	3	$\mathbb{Z}_{p^3}$
	2+1	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$
	1+1+1	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
p^4	4	$\mathbb{Z}_{p^4}$; $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$; $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$;
	3+1	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$; $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
	2+2	
	2+1+1	
	1+1+1+1	

Ex: $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$

SOB MULTIPLICAÇÃO módulo 65.

$|G| = 16 \longrightarrow$ G É ISOMORFO A UM DOS GRUPOS $\longrightarrow$

$\mathbb{Z}_{16}$
$\mathbb{Z}_8 \oplus \mathbb{Z}_2$
$\mathbb{Z}_4 \oplus \mathbb{Z}_4$
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

ELEMENTOS	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
ORDEM	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

POSSIBILIDADES: $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ E $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ $\longrightarrow$ TEM SUBGRUPO ISOMORFO A $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ TEM MAIS QUE 3 ELEMENTOS DE ORDEM 2.

$\therefore G \equiv \mathbb{Z}_4 \oplus \mathbb{Z}_4$

TOME UM ELEMENTO DE ORDEM MÁXIMA. Ex: B.

$\therefore \langle B \rangle$ É UM FATOR NO PRODUTO

. ESCOLHA UM ELEMENTO, a, COM ORDEM 4 $\left(\frac{|G|}{\langle B \rangle} = 4 \right)$ $|\langle B \rangle| = 4$

E a e a^2 NÃO ESTÃO EM $\langle B \rangle$.

$\langle B \rangle = \{1, B, 64, 57\}$, TOME $a = 12$

$\therefore G = \langle B \rangle \times \langle 12 \rangle$.

* ALGORITMO PARA GRUPOS ABELIANOS DE ORDEM p^n *

(1) - COMPUTE AS ORDENS DOS ELEMENTOS DO GRUPO G.

(2) - ESCOLHA UM ELEMENTO DE ORDEM MÁXIMA, a_i E DEFINA $G_i = \langle a_i \rangle$.

(3) - SE $|G| = |G_i|$ PARE O PROCESSO, CASO CONTRÁRIO, SUBSTITUA i POR $i+1$.

(4) - SELECIONE UM ELEMENTO a_i DE ORDEM MÁXIMA p^k T.Q. $p^k \leq \frac{|G|}{|G_{i-1}|}$ E NENHUM DOS ELEMENTOS $a_i, a_i^2, \ldots, a_i^{p^{k-1}}$ ESTÁ EM G_{i-1}, E DEFINA $G_i = G_{i-1} \times \langle a_i \rangle$.

(5) - RETORNE AO PASSO (3).