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

CONJUGAÇÃO EM S_n:

PROP. SEJAM $\sigma, \tau \in S_n$; SUPONHA QUE σ TENHA DECOMPOSIÇÃO EM CICLOS, $\sigma = (a_1, a_2 \dots a_{k_1})(b_1, b_2 \dots b_{k_2}) \dots$
ENTÃO $\tau\sigma\tau^{-1}$ POSSUI DECOMPOSIÇÃO EM CICLOS

$$(\tau(a_1)\ \tau(a_2) \cdots \tau(a_{k_1}))(\tau(b_1)\ \tau(b_2) \cdots \tau(b_{k_2})) \dots$$

DEM: SE $\sigma(i) = j$ ENTÃO $\tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$

SE O PAR ORDENADO i, j APARECE NA DECOMPOSIÇÃO EM CICLOS DE σ ENTÃO O PAR ORDENADO $\tau(i), \tau(j)$ APARECE NA DECOMPOSIÇÃO EM CICLOS DE $\tau\sigma\tau^{-1}$.

EX: $\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)$ $\quad \tau = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$

ENTÃO $\tau\sigma\tau^{-1} = (3\ 4)(5\ 6\ 7)(8\ 1\ 2\ 9)$

easy office

DEF. i) SE $\sigma \in S_n$ É O PRODUTO DE CÍCLOS DISJUNTOS DE COMPRIMENTOS $n_1, n_2, \ldots, n_r$ COM $n_1 \leq n_2 \leq \ldots \leq n_r$ (INCLUINDO OS 1-ciclos) ENTÃO OS INTEIROS $n_1, \ldots, n_r$ SÃO CHAMADOS OS TIPOS DO CICLO σ.

(2) SE $n \in \mathbb{Z}^+$, UMA PARTIÇÃO DE n É QUALQUER SEQUÊNCIA NÃO DECRESCENTE DE INTEIROS POSITIVOS CUJA SOMA SEJA n.

EX: UM m-ciclo EM S_n É DO TIPO $\underbrace{1, \ldots, 1}_{n-m}, m$

PROP: DOIS ELEMENTOS EM S_n SÃO CONJUGADOS EM S_n

⇕

ELES POSSUEM A MESMA DECOMPOSIÇÃO EM CÍCLOS DO MESMO TIPO.

($\Rightarrow$) SEGUE DA PROP. ANTERIOR

($\Leftarrow$) SUPONHA QUE σ_1 E σ_2 TENHAM A MESMA DECOMPOSIÇÃO EM CICLOS DO MESMO TIPO.

ORDENAMOS OS CICLOS PELOS COMPRIMENTOS DE MANEIRA CRESCENTE INCLUINDO OS 1-CICLOS.

IGNORANDO OS PARÊNTESIS, CADA DECOMPOSIÇÃO EM CICLOS É UMA LISTA NO QUAL OS ELEMENTOS DE 1 a n. APARECE UMA ÚNICA VEZ.

DEF: τ: FUNÇÃO QUE LEVA O i-ÉSIMO INTEIRO NA LISTA PARA σ_1 PARA O i-ÉSIMO INTEIRO NA LISTA PARA σ_2.

$\therefore$ τ É UMA PERMUTAÇÃO E COMO OS PARÊNTESIS QUE DELIMITAM A DECOMPOSIÇÃO EM CICLO APARECEM NA MESMA POSIÇÃO EM CADA LISTA, A PROPOSIÇÃO ANTERIOR GARANTE QUE $\tau\sigma_1\tau^{-1} = \sigma_2$ $\therefore$ σ_1 E σ_2 SÃO CONJUGADOS

EX: $\sigma_1 = (1)(3\,5)(8\,9)(2\,4\,7\,6)$ $\sigma_2 = (3)(4\,7)(8\,1)(5\,2\,6\,9)$

DEF. τ POR $\tau(1)=3$, $\tau(3)=4$, $\tau(5)=7$, $\tau(8)=8$, $\tau(9)=1$, $\tau(2)=5$, $\tau(4)=2$, $\tau(7)=6$, $\tau(6)=9$ $\therefore$ $\tau = (1\,3\,4\,2\,5\,7\,6\,9)(8)$

EX: SE TIVÉSSEMOS $\sigma_2 = (3)(8\,1)(4\,7)(5\,2\,6\,9)$ NO EXEMPLO ANTERIOR:

DEF $\tau(1)=3$, $\tau(3)=8$, $\tau(8)=1$, $\tau(8)=4$, $\tau(9)=7$, $\tau(2)=5$, $\tau(4)=2$, $\tau(7)=6$, $\tau(6)=9$

$\tau = (1\,3\,8\,4\,2\,5)(6\,9\,7)$

easy office

S, T subconjuntos do grupo G:

S e T são conjugados em G, se existe $g \in G$ t.q.

$$T = gSg^{-1}.$$

(i.e. $\Leftrightarrow$ eles estão na mesma órbita de G agindo sob seus subconjuntos por conjugação).

$\therefore$ SCG, o número de conjugados de S em G é igual ao índice $[G : G_S]$

Para a ação por conjugação: $G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S)$

easy office

$H \leq G$, G GRUPO.

QUANTOS SUBGRUPOS CONJUGADOS gHg^{-1} EXISTEM (QUANDO g VARIA? $g \in G$).

$g_1, g_2 \in G$ $\quad g_1 H g_1^{-1} = g_2 H g_2^{-1} \iff g_2^{-1} g_1 H g_1^{-1} g_2 = H$

$\iff g_2^{-1} g_1 \in N_G(H)$

$\iff g_1 \in g_2 N_G(H)$

$\iff g_1 N_G(H) = g_2 N_G(H)$

$\therefore$ há $[G : N_G(H)]$.

TEOREMAS DE SYLOW:

DEF: SEJA G GRUPO, p INTEIRO PRIMO.

(i) UM GRUPO DE ORDEM p^α PARA ALGUM $\alpha \geq 0$. É CHAMADO UM p-GRUPO

. SUBGRUPOS DE G QUE SÃO p-GRUPOS SÃO CHAMADOS p-SUBGRUPOS.

(ii) SE G É UM GRUPO DE ORDEM $p^\alpha m$, $p \nmid m$. ENTÃO UM SUBGRUPO DE ORDEM p^α É CHAMADO UM p-SUBGRUPO DE SYLOW DE G.

(iii) O CONJUNTO DOS p-SUBGRUPOS DE SYLOW DE G DENOTADO $Syl_p(G)$, E O NÚMERO DE p-SUBGRUPOS DE SYLOW DE G SERÁ DENOTADO $n_p(G)$.

easy office

TEOREMA (Sylow):

SEJA G GRUPO DE ORDEM $p^\alpha m$, p PRIMO, $p \nmid m$.

(I) p-SUBGRUPOS DE Sylow DE G EXISTEM, i.e, $Syl_p(G) \neq \emptyset$.

(II) SE P É UM p-SUBGRUPO DE Sylow DE G E Q É QUALQUER p-SUBGRUPO DE G ENTÃO EXISTE $g \in G$ TAL QUE $Q \leq gPg^{-1}$, I.E. Q ESTÁ CONTIDO EM ALGUM CONJUGADO DE P.

EM PARTICULAR, QUAISQUER DOIS p-SUBGRUPOS DE Sylow DE G SÃO CONJUGADOS EM G.

(III) O NÚMERO DE p-SUBGRUPOS DE Sylow DE G É DA FORMA $1+kp$, i.e, $n_p \equiv 1 \bmod p$.

ADICIONALMENTE, n_p É O ÍNDICE EM G DO NORMALIZADOR $N_G(P)$ PARA QUALQUER p-SUBGRUPO DE Sylow P, PORTANTO n_p DIVIDE m.

easy office

LEMA: SEJA $P \in Syl_p(G)$. SE Q É QUALQUER p-SUBGRUPO DE G. ENTÃO $Q \cap N_G(P) = Q \cap P$.

DEM: SEJA $H = N_G(P) \cap Q$.

COMO $P \subseteq N_G(P)$ ENTÃO CLARAMENTE $P \cap Q \subseteq N_G(P) \cap Q = H$.

BASTA MOSTRAR A INCLUSÃO CONTRÁRIA:

POR DEFINIÇÃO, $H \leq Q$. LOGO TEMOS QUE MOSTRAR $H \subseteq P$.

COMO $H \subseteq N_G(P) \longrightarrow PH$ É SUBGRUPO E $|PH| = \frac{|P| \cdot |H|}{|P \cap H|}$.

$\therefore PH$ É p-GRUPO

ALÉM DISSO, $P \leq PH \longrightarrow |PH|$ É DIVISÍVEL POR p^α.

E p^α É A MAIOR POTÊNCIA DE p QUE DIVIDE $|G|$.

$\therefore |PH| = p^\alpha = |P| \quad \therefore PH = P \longrightarrow H \leq P$.

□

easy office

DEM: (I) TEOREMA DE Sylow.

INDUÇÃO EM $|G|$.

SE $|G|=1$, NADA HÁ A PROVAR.

HI: SUPONHA QUE EXISTAM p-SUBGRUPOS DE SYLOW PARA TODOS OS GRUPOS DE ORDEM MENOR QUE $|G|$.

- SE $p \mid |Z(G)|$ ENTÃO POR CAUCHY, $Z(G)$ POSSUI SUBGRUPO N DE ORDEM p. $(N \subset Z(G) \to N \lhd G)$.

SEJA $\overline{G} = \frac{G}{N}$, $|\overline{G}| = \frac{p^d m}{p} = p^{d-1} \cdot m$

PELA HIPÓTESE DE INDUÇÃO, $\overline{G}$ POSSUI UM SUBGRUPO $\overline{P}$ DE ORDEM p^{d-1}.

TOME P SUBGRUPO DE G CONTENDO N TAL QUE $\frac{P}{N} \cong \overline{P}$.

ENTÃO $|P| = \left|\frac{P}{N}\right| \cdot |N| = p^d$

$\therefore$ P É UM p-SUBGRUPO DE SYLOW DE G.

DEM: (I) TEOREMA DE Sylow.

.. SUPONHA $p \nmid |Z(G)|$.

SEJAM $g_1, g_2, \dots, g_r$ REPRESENTANTES DAS CLASSES DE CONJUGAÇÃO NÃO CENTRAIS DISTINTAS DE G.

PELA EQUAÇÃO DE CLASSES:

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$$

SE $p \mid [G : C_G(g_i)]$ PARA TODO i ENTÃO COMO $p \mid |G|$ TERÍAMOS $p \mid |Z(G)|$ Abs.

LOGO EXISTE i_0 TAL QUE $p \nmid [G : C_G(g_{i_0})]$. SEJA $H = C_G(g_{i_0})$

ie $|H| = p^k$, $p \nmid k$.

COMO $g_{i_0} \notin Z(G)$, $|H| < |G|$.

PELA HIPÓTESE DE INDUÇÃO, H POSSUI UM p-SUBGRUPO DE Sylow P

COMO $|P| = p^k$, P É UM SUBGRUPO DE Sylow DE G.

DEM: Obs: Por (I), existe um p-subgrupo de Sylow P de G.

Sejam $\{P_1, P_2, \ldots, P_r\} = S$, o conjunto de todos os conjugados de P em G. (i.e. $S = \{gPg^{-1} \mid g \in G\}$)

e seja Q qualquer p-subgrupo de G.

Pela definição de S; G e portanto também Q, age por conjugação sobre S

Escreva S como união disjunta de órbitas sob esta ação por Q:

$$S = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \ldots \cup \mathcal{O}_s, \text{ onde } r = |\mathcal{O}_1| + |\mathcal{O}_2| + \ldots + |\mathcal{O}_s|$$

(r não depende de Q, mas o número de Q-órbitas depende).

Observe que G possui uma única órbita sobre S, mas um subgrupo Q de G pode ter mais do que uma órbita.

RENUMERE OS ELEMENTOS DE S SE NECESSÁRIO DE MODO QUE OS PRIMEIROS s ELEMENTOS DE S SÃO REPRESENTANTES DAS Q-ÓRBITAS, $P_i \in \Theta_i$, $1 \leq i \leq s$.

SEGUE DAÍ QUE $|\Theta_i| = [Q : N_Q(P_i)]$

POR DEFINIÇÃO, $N_Q(P_i) = N_G(P_i) \cap Q = P_i \cap Q$. (LEMA)

$\therefore |\Theta_i| = [Q : P_i \cap Q]$, $1 \leq i \leq s$

MOSTREMOS QUE $r \equiv 1 \bmod p$.

COMO Q FOI ARBITRÁRIO, TOME $Q = P_1$ E TEMOS $|\Theta_1| = 1$

AGORA PARA TODO $i > 1$, $P_1 \neq P_i$. $P_1 \cap P_i < P_1$ E

$|\Theta_i| = [P_1 : P_1 \cap P_i] > 1$, $2 \leq i \leq s$.

COMO P_1 É p-GRUPO $\longrightarrow$ $[P_1 : P_1 \cap P_i]$ É POTÊNCIA DE $p \rightarrow p \mid |\Theta_i|$, $2 \leq i \leq s$

$\therefore r = |\Theta_1| + |\Theta_2| + \dots + |\Theta_s| \equiv 1 \bmod p$.

easy office

- DEM (2) E (3):

SEJA Q p-SUBGRUPO QUALQUER DE G.

SUPONHA QUE Q NÃO ESTÁ CONTIDO EM P_i, $\forall i \in \{1, 2, \ldots, r\}$

$\therefore Q \cap P_i < Q$, $\forall i \in$ (i.e. $Q \nsubseteq gP_ig^{-1}$, $\forall g \in G$).

$|\Theta_i| = |Q : Q \cap P_i| > 1$, $1 \leq i \leq r$

$\therefore p \mid |\Theta_i|$, $\forall i \longrightarrow p \mid (|\Theta_1| + |\Theta_2| + \ldots + |\Theta_s| = r$. Abs, pois $r \equiv 1 \bmod p$.

$\therefore Q \leq gP_ig^{-1}$, PARA ALGUM $g \in G$.

easy office

DEM (2) E (3):

. TODOS OS p-SUBGRUPOS DE SYLOW SÃO CONJUGADOS

SEJA Q p-SUBGRUPO DE SYLOW DE G.

PELO QUE VIMOS, $Q \leq gPg^{-1}$, PARA ALGUM $g \in G$.

COMO $|Q| = |gPg^{-1}| = p^\alpha \longrightarrow Q = gPg^{-1}$

EM PARTICULAR, $S = Syl_p(G)$, POIS TODO p-SUBGRUPO DE SYLOW DE G É CONJUGADO A P. LOGO $n_p = r \equiv 1 \bmod p$.

FINALMENTE, COMO TODOS OS p-SUBGRUPOS DE SYLOW SÃO CONJUGADOS, TEMOS QUE $n_p = [G : N_G(P)]$ PARA QUALQUER $P \in Syl_p(G)$

$\therefore n_p \mid m$.

easy office

TEOREMA: SEJA G GRUPO FINITO, $|G| = p^\alpha m$, p primo, $p \nmid m$.

ENTÃO: (I) G CONTÉM UM SUBGRUPO DE ORDEM p^i, $\alpha \geq 1$, PARA CADA i, $1 \leq i \leq \alpha$.

(II) TODO SUBGRUPO H DE G DE ORDEM p^i É UM SUBGRUPO NORMAL DE UM SUBGRUPO DE ORDEM p^{i+1}, PARA $1 \leq i < n$.

LEMA. SEJA H p-SUBGRUPO DE UM GRUPO FINITO G. (p primo)

ENTÃO $[N_G(H) : H] \equiv [G : H) \bmod p$.

DEM: SEJA $\mathcal{L} = \{xH : x \in G\}$, $H \leq G$, $|\mathcal{L}| = [G : H]$.

E H AGE SOBRE $\mathcal{L}$ POR TRANSLAÇÃO À ESQUERDA, i.e.

$$H \times \mathcal{L} \to \mathcal{L}$$
$$(h, xH) \mapsto h \cdot xH := (hx)H.$$

SEJA $\mathcal{L}_H$ CLASSES LATERAIS À ESQUERDA DE H EM G QUE SÃO FIXADAS SOB A AÇÃO POR TODOS OS ELEMENTOS DE H.

$xH = hxH \ \forall h \in H \iff x^{-1}hxH = H, \ \forall h \in H \iff x^{-1}hx \in H, \ \forall x \in H$

$\Downarrow$

$x \in N_G(H)$.

$\therefore |\mathcal{L}_H| = [N_G(H) : H]$. PELO TEOREMA DA CONGRUÊNCIA DO PONTO FIXO,

$|\mathcal{L}| \equiv |\mathcal{L}_H| \bmod p \quad \therefore [G : H] \equiv [N_G(H) : H] \bmod p$.

easy office

TEOREMA: SEJA G GRUPO FINITO, $|G| = p^\alpha m$, p primo, $p \nmid m$.

ENTÃO: (I) G CONTÉM UM SUBGRUPO DE ORDEM p^i, $\alpha \geq 1$, PARA CADA i, $1 \leq i \leq \alpha$.

(II) TODO SUBGRUPO H DE G DE ORDEM p^i É UM SUBGRUPO NORMAL DE UM SUBGRUPO DE ORDEM p^{i+1}, PARA $1 \leq i < n$.

DEM: Por Cauchy, G possui um subgrupo de ordem p.

Suponha que existe um subgrupo de ordem $p^i < n$. Mostremos que existe um subgrupo de ordem p^{i+1}

Seja $H \leq G$. $|H| = p^i$. Como $i < n \longrightarrow p \mid [G:H]$

Pelo lema anterior, $p \mid [N_G(H) : H]$. Observe que: $H \trianglelefteq N_G(H)$.

Por Cauchy, $\frac{N_G(H)}{H}$ possui subgrupo K de ordem p.

Seja $\gamma : N_G(H) \twoheadrightarrow \frac{N_G(H)}{H}$ homomorfismo canônico.

$K \trianglelefteq \frac{N_G(H)}{H} \longrightarrow \gamma^{-1}(K) \trianglelefteq N_G(H)$, em particular, $\gamma^{-1}(K)$ subgrupo de G (Teorema da correspondência) contendo H

$\{x \in N_G(H) \mid \gamma(x) \in K\}$ (i.e. $\frac{\gamma^{-1}(K)}{H} \cong K \rightarrow |\gamma^{-1}(K)| = |H| \cdot |K| = p^{i+1}$)

easy office

TEOREMA: SEJA G GRUPO FINITO, $|G| = p^\alpha m$, p primo, $p \nmid m$.

ENTÃO: (i) G CONTÉM UM SUBGRUPO DE ORDEM p^i, $\alpha \geq 1$, PARA CADA i, $1 \leq i \leq \alpha$.

(ii) TODO SUBGRUPO H DE G DE ORDEM p^i É UM SUBGRUPO NORMAL DE UM SUBGRUPO DE ORDEM p^{i+1}, PARA $1 \leq i < n$.

DEM: (ii) REPETIMOS A CONSTRUÇÃO DE (i)

NOTE QUE $H \lhd f^{-1}(K) \leq N_G(H)$

$$|f^{-1}(K)| = p^{i+1}$$

COMO $H \lhd N_G(H) \longrightarrow H \lhd f^{-1}(K)$

easy office

Errata: no slide 17,

1)Enunciado do Teorema (ii) todo subgrupo H de G de ordem p^i é um subgrupo normal de um subgrupo de ordem p^{i+1}, para 1<= i < **\alpha.**

2)Na demonstração do Teorema: (segunda linha) “... Suponha que existe um subgrupo de ordem p^i < **\alpha.**

3)Na demonstração do Teorema (penúltima linha): K < (N_G(H))/H -→{\gamma}^{-1}(K) < N_G(H)