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

$\alpha \in S_n$, $r \geq 2$, α é um r-ciclo, se existem elementos DISTINTOS $a_1, a_2, \dots, a_r \in \{1, 2, \dots, n\}$ t.q.

$\alpha(a_1) = a_2$, $\alpha(a_2) = a_3$; $\dots$, $\alpha(a_{r-1}) = a_r$, $\alpha(a_r) = a_1$. E

$\alpha(j) = j$, $\forall j \in \{1, 2, \dots, n\} \setminus \{a_1, \dots, a_r\}$

O r-ciclo SERÁ DENOTADO $(a_1\ a_2\ \dots\ a_r)$. $r \to$ COMPRIMENTO DO r-ciclo

2-CICLO $\to$ TRANSPOSIÇÕES:

Ex: Em S_5, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$ É UM 3-CICLO $(1\ 4\ 3)$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ NÃO É UM r-CICLO, $\forall r$.

$=$

$(1\ 3\ 5)(2\ 4)$

DEF: SEJAM $\alpha \in S_n$ UM r-CICLO E $\beta \in S_n$, β UM s-CICLO.

α E β SÃO **DISJUNTOS** SE NENHUM ELEMENTO DE $\{1, 2, \dots, n\}$ É MOVIDO POR AMBOS, i.e. $\forall a \in \{1, \dots, n\}$, $\alpha(a) = a$ OU $\beta(a) = a$.

EX: EM S_5, $\alpha = (1\ 4\ 3)$ E $\beta = (2\ 5)$ SÃO DISJUNTOS

OBS: $\alpha = (a_1\ a_2 \cdots a_r)$ $\qquad \beta = (b_1\ b_2 \cdots b_s)$

α E β DISJUNTOS $\Longleftrightarrow \{a_1, a_2, \dots, a_r\} \cap \{b_1, \dots, b_s\} = \emptyset$.

EXERCÍCIO: (i) SEJAM $\alpha, \beta \in S_n$, CICLOS DISJUNTOS. ENTÃO $\alpha\beta = \beta\alpha$.

(ii) SEJA $\alpha \in S_n$ UM r-CICLO. MOSTRE QUE A ORDEM DE α É r.

(iii) SEJAM $\alpha_1, \dots, \alpha_t \in S_n$, CICLOS DISJUNTOS DE COMPRIMENTOS $r_1, \dots, r_t$, RESPECTIVAMENTE. MOSTRE QUE O PRODUTO $\alpha_1 \cdot \alpha_2 \cdots \alpha_t$ TEM ORDEM $\mathrm{mmc}\{r_1, r_2, \dots, r_t\}$

Ex: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1\ 3\ 5)(2\ 4)$

PROP: SEJA $\alpha \in S_n$, $\alpha \neq id$. ENTÃO α É UM PRODUTO DE CICLOS DISJUNTOS DE COMPRIMENTOS ≥ 2. E ESSA DECOMPOSIÇÃO É ÚNICA A MENOS DE ORDEM DOS FATORES.

DEM: COMO $\alpha \neq id$, $(\exists i_1)$ $\alpha(i_1) \neq i_1$

CONSIDERE A SEQUÊNCIA $i_1, \alpha(i_1), \alpha^2(i_1), \dots$

CLARAMENTE, $\exists r_1$ T.Q. $i_1, \alpha(i_1), \dots, \alpha^{r_1-1}(i_1)$ SÃO TODOS DISTINTOS

E $\alpha^{r_1}(i_1) \in \{i_1, \alpha(i_1), \dots, \alpha^{r_1-1}(i_1)\}$. É IMEDIATO VERIFICAR QUE $\alpha^{r_1}(i_1) = i_1$.

$$\therefore \alpha\big|_{\{i_1, \alpha(i_1), \dots, \alpha^{r_1-1}(i_1)\}} = (i_1\ \alpha(i_1)\ \dots\ \alpha^{r_1-1}(i_1))$$

DENOTE O r_1-CICLO $(i_1\ \alpha(i_1)\ \dots\ \alpha^{r_1-1}(i_1)) = \sigma_1$.

SE α RESTRITA AO COMPLEMENTAR DE $\{i_1\ \alpha(i_1)\ \dots\ \alpha^{r_1-1}(i_1)\}$ FOR A IDENTIDADE ENTÃO $\alpha = \sigma_1$.

CASO CONTRÁRIO, TOME $i_2 \in \{1, \dots, n\} \setminus \{i_1, \alpha(i_1), \dots, \alpha^{r_1-1}(i_1)\}$

T.Q $\alpha(i_2) \neq i_2$.

ANALOGAMENTE AO QUE VIMOS ANTERIORMENTE:

$$(\exists r_2 \geq 2) \quad \alpha\Big|_{\{i_2, \alpha(i_2), \dots, \alpha^{r_2-1}(i_2)\}} = \left(i_2 \ \ \alpha(i_2) \ \cdots \ \alpha^{r_2-1}(i_2)\right)$$

DENOTE ESSE r_2-CICLO $\left(i_2 \ \ \alpha(i_2) \ \cdots \ \alpha^{r_2-1}(i_2)\right)$ POR σ_2.

OBSERVE QUE σ_1 E σ_2 SÃO DISJUNTOS.

SE A RESTRIÇÃO DE α AO COMPLEMENTAR DO CONJUNTO $\{i_1, \alpha(i_1), \dots, \alpha^{r_1-1}(i_1), i_2, \alpha(i_2), \dots, \alpha^{r_2-1}(i_2)\}$ FOR A IDENTIDADE

ACABOU: $\alpha = \sigma_1\sigma_2 = \sigma_2\sigma_1$.

CASO CONTRÁRIO, TOME $i_3 \in \{1, 2, \dots, n\} \setminus \{i_1, \alpha(i_1), \dots, \alpha^{r_1-1}(i_1), i_2, \alpha(i_2), \dots, \alpha^{r_2-1}(i_2)\}$

T.Q. $\alpha(i_3) \neq i_3$. E CONTINUE O PROCESSO. O PROCESSO TEM DE PARAR APÓS UM NÚMERO FINITO DE PASSOS.

OBTEMOS $\alpha = \sigma_1\sigma_2 \dots \sigma_t$, $\sigma_1, \dots, \sigma_t$ CICLOS DISJUNTOS DE COMPRIMENTO ≥ 2

UNICIDADE:

SUPONHA $\alpha = \sigma_1 \sigma_2 \cdots \sigma_t = \tau_1 \tau_2 \cdots \tau_u$, σ_i, τ_j CICLOS DISJUNTOS

$\tau_1, \ldots, \tau_u$ DISJUNTOS DE COMPRIMENTO ≥ 2.

COMO $\tau_1 \tau_2 \cdots \tau_u (i_1) = \alpha(i_1) \neq i_1$.

E $\tau_1, \ldots, \tau_u$ CICLOS DISJUNTOS,

$\Rightarrow$ EXISTE UM ÚNICO τ_j COM $\tau_j(i_1) = \alpha(i_1)$. COMO OS τ_j's COMUTAM ENTRE SI,

PODEMOS SUPOR $j=1$, i.e. $\tau_1(i_1) = \alpha(i_1)$.

AF: $\tau_1 = \sigma_1$.

(τ_1 MAS FIXA $\alpha(i_1)$, i.e. $\tau_1(\alpha(i_1)) \neq \alpha(i_1)$, POIS τ_1 LEVA i_1 EM $\alpha(i_1)$).

COMO OS τ_i's SÃO DISJUNTOS $\longrightarrow \forall j \geq 2$, τ_j DEIXA $\alpha(i_1)$ FIXO.

$\longrightarrow \alpha(\alpha(i_1)) = \tau_1(\alpha(i_1))$

$\longrightarrow \tau_1(\alpha(i_1)) = \alpha^2(i_1)$

$\longrightarrow$ ANALOGAMENTE, $\tau_1(\alpha^{k-1}(i_1)) = \alpha^k(i_1)$, $\forall k \geq 0$

$\therefore \tau_1 = \sigma_1$.

ANALOGAMENTE, TOMANDO i_2 NO LUGAR DE i_1, OBTEMOS $\tau_2 = \sigma_2$.

$\vdots$

$\therefore u = t$ E A MENOS DE ORDEM $\tau_j = \sigma_j$ PARA CADA $j = 1, \ldots, t$

EXERCÍCIO: SEJA $\alpha \in S_n$.

(a) TODO ELEMENTO DE S_n É UM PRODUTO DE TRANSPOSIÇÕES, i.e.

$$S_n = \langle \{\text{TRANSPOSIÇÕES}\} \rangle.$$

(b) $S_n = \langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle$

(c) $S_n = \langle (1\ 2), (2\ 3), \ldots, (n-1\ n) \rangle$

EXERCÍCIO: SEJA $\alpha \in S_n$.

(a) TODO ELEMENTO DE S_n É UM PRODUTO DE TRANSPOSIÇÕES, i.e.

$$S_n = \langle \{\text{TRANSPOSIÇÕES}\} \rangle.$$

(b) $S_n = \langle (1\ 2), (1\ 3), \dots, (1\ n) \rangle$

(c) $S_n = \langle (1\ 2), (2\ 3), \dots, (n-1\ n) \rangle$

OBS: A DECOMPOSIÇÃO DE UM ELEMENTO $\alpha \in S_n$ COMO PRODUTO DE TRANSPOSIÇÕES NÃO É ÚNICA

Ex: EM S_3, $(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 3)(1\ 3)$

NO ENTANTO, A PARIDADE É ÚNICA.

PROP: SEJA $\alpha \in S_n$ E SEJA $\alpha = \tau_t \circ \cdots \circ \tau_1$ FATORAÇÃO QUALQUER DE α COMO PRODUTO DE TRANSPOSIÇÕES.

SE $x_1, x_2, \ldots, x_n$ SÃO INDETERMINADAS SOBRE $\mathbb{Z}$ ENTÃO

$$\prod_{1 \le i < j \le n} (x_{\alpha(j)} - x_{\alpha(i)}) = (-1)^t \prod_{1 \le i < j \le n} (x_j - x_i)$$

EM PARTICULAR, SE $\alpha = \tau_t \circ \cdots \circ \tau_1 = \mu_u \circ \cdots \circ \mu_1$ SÃO DUAS FATORAÇÕES DE α COMO PRODUTO DE TRANSPOSIÇÕES ENTÃO $t \equiv u \pmod 2$.

Suponha: $\Delta = \prod_{1 \le i < j < n} (x_j - x_i) = (x_2 - x_1)(x_3 - x_1)(x_4 - x_1)(x_3 - x_2)(x_4 - x_2)(x_4 - x_3)$

$n = 4$, $\sigma = (1\ 2\ 3\ 4)$

$$\sigma(\Delta) = \prod_{1 \le i < j \le 4} (x_{\sigma(j)} - x_{\sigma(i)}) = (x_3 - x_2)(x_4 - x_2)\underbrace{(x_1 - x_2)}_{= -(x_2 - x_1)}(x_4 - x_3)\underbrace{(x_1 - x_3)}_{= -(x_3 - x_1)}\underbrace{(x_1 - x_4)}_{= -(x_4 - x_1)}$$

DEF: UM ELEMENTO $\alpha \in S_n$ É UMA PERMUTAÇÃO PAR QUANDO α SE ESCREVE COMO UM PRODUTO DE UM NÚMERO PAR DE TRANSPOSIÇÕES, OU EQUIVALENTEMENTE

$$\prod_{1 \leq i < j \leq n} \left(x_{\alpha(j)} - x_{\alpha(i)}\right) = \prod_{1 \leq i < j \leq n} \left(x_j - x_i\right)$$

DEF: UM ELEMENTO $\alpha \in S_n$ É UMA PERMUTAÇÃO ÍMPAR QUANDO α SE ESCREVE COMO UM PRODUTO DE UM NÚMERO ÍMPAR DE TRANSPOSIÇÕES, OU EQUIVALENTEMENTE

$$\prod_{1 \leq i < j \leq n} (x_{\alpha(j)} - x_{\alpha(i)}) = -\prod_{1 \leq i < j \leq n} (x_j - x_i)$$

LEMA: $\tilde{\alpha}: \mathbb{Z}[x_1, \dots, x_n] \longrightarrow \mathbb{Z}[x_1, \dots, x_n]$, $\alpha \in S_n$

$f(x_1, \dots, x_n) \longmapsto f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)})$ (EXERCÍCIO)

$\tilde{\alpha}$ É ISOMORFISMO DE ANÉIS.

DEM: SEJA $g(x_1, x_2, \dots, x_n) = \prod\limits_{1 \leq i < j \leq n} (x_j - x_i)$

PARA CADA $j \in \{1, 2, \dots, n\}$, OS FATORES DE $g(x_1, \dots, x_n)$ QUE ENVOLVEM A VARIÁVEL x_j SÃO EXATAMENTE:

$$(x_n - x_j); (x_{n-1} - x_j), \dots, (x_{j+1} - x_j),$$
$$(x_j - x_{j-1}), \dots, (x_j - x_2), (x_j - x_1)$$

ENTÃO PARA UMA PERMUTAÇÃO $\beta \in S_n$ TEMOS:

$$(x_{\beta(n)} - x_{\beta(j)}); (x_{\beta(n-1)} - x_{\beta(j)}), \dots, (x_{\beta(j+1)} - x_{\beta(j)}),$$
$$(x_{\beta(j)} - x_{\beta(j-1)}), \dots, (x_{\beta(j)} - x_{\beta(2)}), (x_{\beta(j)} - x_{\beta(1)}),$$ SÃO

EXATAMENTE, A MENOS DE SINAL, OS FATORES DE $g(x_1, \dots, x_n)$ QUE ENVOLVEM A VARIÁVEL $x_{\beta(j)}$.

OBTEMOS:

$$\prod_{1\le i<j\le n}(x_{\beta(j)}-x_{\beta(i)})=\pm\prod_{1\le i<j\le n}(x_j-x_i)$$

VAMOS DETERMINAR O SINAL:

DEF: $\psi: S_n \longrightarrow \{\pm 1\}$

$$\psi(\beta)=1 \text{ se } \prod_{1\le i<j\le n}(x_{\beta(j)}-x_{\beta(i)})=\prod_{1\le i<j\le n}(x_j-x_i)$$

e

$$\psi(\beta)=-1 \text{ se } \prod_{1\le i<j\le n}(x_{\beta(j)}-x_{\beta(i)})=-\prod_{1\le i<j\le n}(x_j-x_i)$$

$\therefore$ ψ é HOMOMORFISMO DE GRUPOS, COM $\{\pm 1\}$ MUNIDO DE MULTIPLICAÇÃO

SEJAM $\beta, \gamma \in S_n$.

POR DEFINIÇÃO, $\prod_{1\le i<j\le n}(x_{\beta(j)}-x_{\beta(i)})=\psi(\beta)\prod_{1\le i<j\le n}(x_j-x_i)$

APLIQUE O ISOMORFISMO $\hat{\gamma}$:

$$\prod_{1\le i<j\le n}\left(x_{\gamma(\beta(j))}-x_{\gamma(\beta(i))}\right)=\psi(\beta)\prod_{1\le i<j\le n}\left(x_{\gamma(j)}-x_{\gamma(i)}\right)$$

$$=\psi(\beta)\psi(\gamma)\prod_{1\le i<j\le n}\left(x_j-x_i\right)$$

$$\therefore\ \psi(\gamma\beta)=\psi(\beta)\psi(\gamma)=\psi(\gamma)\psi(\beta).$$

SE τ É UMA TRANSPOSIÇÃO $(K \;\; K+1)$ ENTÃO $\chi(\tau) = -1$.

(DE FATO, . O FATOR $(X_{K+1} - X_K)$ É TRANSFORMADO EM $(X_K - X_{K+1})$ PELO ISOMORFISMO $\hat{\tau}$ E PORTANTO INDUZ UMA MUDANÇA DE SINAL.

.. OS FATORES $(x_j - x_i)$ COM $\{i,j\} \cap \{K, K+1\} = \phi$ PERMANECEM INALTERADOS POR $\hat{\tau}$ $\therefore$ NÃO INDUZEM UMA MUDANÇA DE SINAL

.. OS FATORES QUE SOBRAM SÃO $(x_j - x_K)$, $(x_j - x_{K+1})$ COM ÍNDICES $j \geq K+2$ e $(x_K - x_i)$, $(x_{K+1} - x_i)$ COM $i \leq K-1$.

OS PRODUTOS $(x_j - x_K)(x_j - x_{K+1})$ SÃO TRANSFORMADOS POR $\hat{\tau}$ NOS PRODUTOS $(x_j - x_{K+1})(x_j - x_K)$ i.e. PERMANECEM INALTERADOS POR $\hat{\tau}$.

$\therefore$ NÃO IMPLICAM UMA MUDANÇA DE SINAL.

ANALOGAMENTE, OS PRODUTOS $(x_K - x_i)(x_{K+1} - x_i)$ NÃO TRAZEM MUDANÇA DE SINAL.

Assim, $\tau(g(x_1,\dots,x_n)) = -g(x_1,\dots,x_n)$ $\therefore \psi(\tau) = -1$.

SE τ É UMA TRANSPOSIÇÃO QUALQUER $(k\ l)$ TEMOS:

$$(k\ l) = (l\ \ k+1)(k\ \ k+1)(l\ \ k+1)$$

LOGO

$$\psi(k\ l) = \psi((l\ \ k+1))\,\psi((k\ \ k+1))\,\psi((l\ \ k+1)) = \psi((k\ \ k+1)) = -1$$

FINALMENTE, SE $\alpha = \tau_t \circ \dots \circ \tau_1$ É UM PRODUTO DE TRANSPOSIÇÕES

ENTÃO $\psi(\alpha) = \psi(\tau_t)\cdots\psi(\tau_1) = (-1)^t$

PROP: SEJA $A_n = \{\alpha \in S_n \mid \alpha$ É PERMUTAÇÃO PAR$\}$. ENTÃO A_n É UM SUBGRUPO DE S_n DE ÍNDICE 2. (DENOMINADO GRUPO ALTERNADO OU GRUPO DAS PERMUTAÇÕES PARES)

DEM: $\psi : S_n \longrightarrow \{\pm 1\}$ DEF. ANTERIORMENTE

ψ HOMOMORFISMO (SINAL) DE GRUPOS, ψ É SOBREJETORA e $\ker\psi = A_n$.

PELO T. DO ISOMORFISMO, $\{\pm 1\} \cong \dfrac{S_n}{\ker\psi}$,

$\square$