grupo simétrico

Definição. Seja A um conjunto. Uma *permutação* de A é uma aplicação bijetiva de A em A.

Observação. Se A é um conjunto finito com n elementos ($n \in \mathbb{N}$), podemos estabelecer uma bijeção entre A e o conjunto $\{1, 2, ..., n\}$, pelo que aqui iremos adoptar esta última notação para qualquer conjunto com n elementos. Assim, dizemos, por exemplo, que

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

é uma permutação de um conjunto com 4 elementos.

Observação. Se A é um conjunto finito com n elementos ($n \in \mathbb{N}$), sabemos que podemos definir $n!$ permutações de A distintas. Mais ainda, se algebrizarmos este conjunto de $n!$ elementos com a composição de aplicações obtemos, obviamente, um grupo.

(i) A composta de duas permutações é uma permutação;

(ii) A composição de aplicações, em particular de permutações, é associativa;

(iii) A função identidade é uma permutação e é o elemento neutro para a composição de aplicações;

(iv) A aplicação inversa de uma permutação é uma permutação.

Definição. Chama-se *grupo simétrico* de um conjunto com n elementos, e representa-se por S_n, ao grupo das permutações desse conjunto.

Exemplo 43. Se considerarmos um conjunto com dois elementos,

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\};$$

Exemplo 44. Se considerarmos um conjunto com 3 elementos,

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Exemplo 45. Se considerarmos um conjunto com 4 elementos, temos que

$$\begin{aligned} S_4 = \Bigg\{ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \Bigg\}. \end{aligned}$$

Proposição. O grupo simétrico S_n é não comutativo, para todo $n \geq 3$.

Demonstração. Se f e g são as permutações de S_n definidas por

$$f(1) = 2,\ f(2) = 3,\ f(3) = 1,\ f(k) = k, \forall 4 \leq k \leq n,$$
$$g(1) = 2,\ g(2) = 1,\ g(k) = k, \forall 3 \leq k \leq n,$$

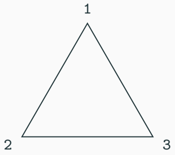
temos que

$$(f \circ g)(1) = 3 \neq 1 = (g \circ f)(1). \qquad \square$$

Definição. Chama-se *grupo diedral* ao grupo das simetrias e rotações de uma linha poligonal.

Representamos por D_n o grupo diedral de um polígono regular com n lados.

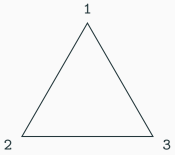
Exemplo 46. $D_3 = S_3$



Temos:

Rotações: 0^o; 120^o e 240^0;

Simetrias: 3 simetrias axiais.



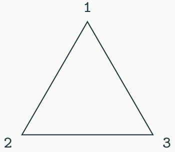
Representando as simetrias e rotações pelas permutações em $\{1, 2, 3\}$, temos:

Rotações de 0^o, 120^o e 240^o:

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};$$

simetrias em relação às bissetrizes dos ângulos 1, 2 e 3:

$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \theta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ e } \theta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$



Considerando a composição de funções, obtemos a tabela:

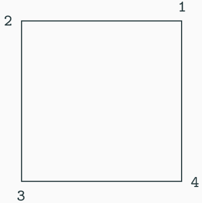
$\circ$	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_1	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_2	ρ_2	ρ_3	ρ_1	θ_3	θ_1	θ_2
ρ_3	ρ_3	ρ_1	ρ_2	θ_2	θ_3	θ_1
θ_1	θ_1	θ_2	θ_3	ρ_1	ρ_2	ρ_3
θ_2	θ_2	θ_3	θ_1	ρ_3	ρ_1	ρ_2
θ_3	θ_3	θ_1	θ_2	ρ_2	ρ_3	ρ_1

O grupo D_3 é (o menor grupo) não abeliano, $1_{D_3} = \rho_1$ e os seus subgrupos são:

$$\{\rho_1\}, \{\rho_1, \theta_1\}, \{\rho_1, \theta_2\}, \{\rho_1, \theta_3\}, \{\rho_1, \rho_2, \rho_3\} \text{ e } D_3.$$

Destes, quais são normais?

Exemplo 47. D_4 é um subgrupo próprio de S_4



Rotações de 0^o, 90^o, 180^o e 270^o:

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix},\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ e } \rho_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix};$$

Simetrias em relação às bissectrizes $[1,3]$ e $[2,4]$:

$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix};$$

Simetrias em relação às mediatrizes do lado $[1,2]$ e do lado $[2,3]$:

$$\theta_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \text{ e } \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Assim, D_4 tem 8 elementos enquanto que S_4 tem 24 elementos.

Considerando a composição de funções, obtemos a tabela

ρ_1	ρ_1	ρ_2	ρ_3	ρ_4	θ_1	θ_2	θ_3	θ_4
ρ_1	ρ_1	ρ_2	ρ_3	ρ_4	θ_1	θ_2	θ_3	θ_4
ρ_2	ρ_2	ρ_3	ρ_4	ρ_1	θ_2	θ_3	θ_4	θ_1
ρ_3	ρ_3	ρ_4	ρ_1	ρ_2	θ_3	θ_4	θ_1	θ_2
ρ_4	ρ_4	ρ_1	ρ_2	ρ_3	θ_4	θ_1	θ_2	θ_3
θ_1	θ_1	θ_4	θ_3	θ_2	ρ_1	ρ_4	ρ_3	ρ_2
θ_2	θ_2	θ_1	θ_4	θ_3	ρ_2	ρ_1	ρ_4	ρ_3
θ_3	θ_3	θ_2	θ_1	θ_4	ρ_3	ρ_2	ρ_1	ρ_4
θ_4	θ_4	θ_3	θ_2	θ_1	ρ_4	ρ_3	ρ_2	ρ_1

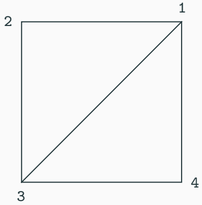
Os subgrupos de D_4 são

$$\{\rho_1\}, \{\rho_1, \theta_1\}, \{\rho_1, \theta_2\}, \{\rho_1, \theta_3\}, \{\rho_1, \theta_4\}, \{\rho_1, \rho_3\},$$

$$\{\rho_1, \rho_2, \rho_3, \rho_4\}, \{\rho_1, \rho_3, \theta_1, \theta_3\}, \{\rho_1, \rho_3, \theta_2, \theta_4\}, D_4\}.$$

Destes, quais são normais?

Exemplo 48. Relativamente à figura



o grupo diedral é composto pelas aplicações

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\phi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } \phi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Definição. Diz-se que uma permutação σ de um conjunto finito A é um ciclo de comprimento n se existirem $a_1, a_2, \ldots, a_n \in A$ tais que

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \ldots, \quad \sigma(a_{n-1}) = a_n, \quad \sigma(a_n) = a_1$$

e se

$$\sigma(x) = x, \qquad \forall x \in A \setminus \{a_1, a_2, ..., a_n\}.$$

Neste caso, representa-se este facto por

$$\sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n-1} & a_n \end{pmatrix}.$$

Exemplo 49. Se $A = \{1, 2, 3, 4, 5\}$, temos que

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 4 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 5 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 & 5 \end{pmatrix}. \end{aligned}$$

Observação. Em S_n, o produto (composição) de dois ciclos pode ou não ser um ciclo, como o prova o seguinte exemplo: em S_6,

$$\begin{pmatrix} 1 & 4 & 5 & 6 \end{pmatrix}\begin{pmatrix} 2 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

não é um ciclo. De facto, se representarmos este produto por σ, temos que $\sigma(2) = 4,\ \sigma(4) = 5,\ \sigma(5) = 2$ e $\sigma(1) \neq 1$.

Por outro lado,

$$\begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 6 & 4 \end{pmatrix}$$

Definição. Dado um conjunto A finito, dizemos que dois ciclos são *disjuntos* se não existir nenhum elemento de A que apareça simultaneamente na notação desses ciclos, i.e., se nenhum elemento de A for transformado simultaneamente pelos dois ciclos.

Exemplo 50. Em S_6,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1 \quad 6)\,(2 \quad 5 \quad 3)\,,$$

i.e., a permutação σ é o produto de dois ciclos disjuntos.

Teorema. Toda a permutação σ de um conjunto finito é um produto (composição) de ciclos disjuntos.

Demonstração. Suponhamos, sem perdas de generalidade, que $A = \{1, 2, 3, \ldots, n\}$. Consideremos então o primeiro elemento (1) e, para a permutação σ em A, consideremos a lista

$$1 \quad \sigma(1) \quad \sigma^2(1) \quad \sigma^4(1) \quad \ldots\ldots \tag{*}$$

Como A é finito, sabemos que os elementos de (*) não podem ser todos distintos. Seja $\sigma^r(1)$ o primeiro elemento que aparece repetido. Então, $\sigma^r(1) = 1$.

De facto, se

$$\sigma^r(1) = \sigma^s(1), \qquad \text{para algum } s \in \{1, 2, \ldots, r-1\},$$

concluíamos que

$$\sigma^{r-s}(1) = \mathrm{id}(1) = 1 \qquad \text{e} \quad 0 < r - s < r,$$

pelo que $\sigma^r(1)$ não seria o primeiro elemento a aparecer repetido.

Formamos então o ciclo

$$\rho_1 = \begin{pmatrix} 1 & \sigma(1) & \sigma^2(1) & \cdots & \sigma^{r-1}(1) \end{pmatrix}.$$

Seja, então, i o primeiro elemento de A que não aparece em ρ_1. Aplicamos a i o raciocínio aplicado a 1 e formamos o ciclo

$$\rho_2 = \begin{pmatrix} i & \sigma(i) & \sigma^2(i) & \cdots & \sigma^{t-1}(i) \end{pmatrix}.$$

Por raciocínios análogos, "percorremos" todos os elementos de A. Suponhamos que são k os ciclos que formamos. Então, $\sigma = \rho_1 \cdots \rho_k$.

Vejamos agora que os ciclos são disjuntos dois a dois.

Consideremos os ciclos ρ_1 e ρ_2. Suponhamos que existe $j \in A$ tal que j aparece no ciclo ρ_1 e no ciclo ρ_2. Suponhamos, sem perdas de generalidade, que $j = \sigma^2(1)$ e que $j = \sigma^3(i)$. Então,

$$\begin{aligned} \rho_1 &= \begin{pmatrix} \sigma^2(1) & \sigma^3(1) & \cdots & \sigma^{r-1}(1) & 1 \end{pmatrix} \\ &= \begin{pmatrix} j & \sigma(j) & \sigma^2(j) & \cdots \end{pmatrix} \\ &= \begin{pmatrix} \sigma^3(i) & \sigma^4(i) & \sigma^5(i) & \cdots \end{pmatrix} = \rho_2, \end{aligned}$$

o que não acontece pois i não aparece em ρ_1.

Generalizando esta demonstração, provamos que todos os ciclos são disjuntos dois a dois. $\square$

Questão: Porque é que é importante escrever uma permutação como produto de ciclos disjuntos?

Resposta: Porque ciclos disjuntos comutam!

$$\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}4 & 5\end{pmatrix} = \begin{pmatrix}4 & 5\end{pmatrix}\begin{pmatrix}1 & 2 & 3\end{pmatrix}$$

$$\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix} = \begin{pmatrix}1 & 3\end{pmatrix} \neq \begin{pmatrix}2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\end{pmatrix}$$

Observação. Relembrar que num grupo G, para $a, b \in G$,

$$ab = ba \Leftrightarrow \forall n \in \mathbb{Z},\ (ab)^n = a^n b^n.$$

Questão: Dada uma permutação σ num conjunto com n elementos, i.e., dado o elemento $\sigma \in S_n$, qual será a sua ordem?

Resposta:

1. se σ é um ciclo, então $o(\sigma)$ é o comprimento do ciclo.
2. se σ é um produto de pelo menos dois ciclos disjuntos, então $o(\sigma)$ é o m.m.c. entre os comprimentos dos ciclos em questão.

Exemplo 51. Em S_8, como
$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 7 & 8 & 5 & 6 \end{pmatrix} = (1 \quad 3 \quad 4)(5 \quad 7)(6 \quad 8)$, temos que $o(\phi) = 6$ pois o mínimo múltiplo comum entre as ordens dos três ciclos disjuntos é 6.

Definição. Uma *transposição* é um ciclo de comprimento 2.

Proposição. Qualquer ciclo é produto de transposições.

Demonstração. Imediata, tendo em conta que

$$(a_1 \quad a_2 \quad a_3 \quad \cdots \quad a_n) = (a_1 \quad a_n)\,(a_1 \quad a_{n-1}) \cdots (a_1 \quad a_3)\,(a_1 \quad a_2)\,.$$

$\square$

Observação. Considerando o teorema e a proposição anteriores, temos que qualquer permutação se escreve como produto de transposições.

Exemplo 52. Em S_7,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 1 & 7 & 5 & 6 \end{pmatrix} = (1 \quad 3 \quad 4)\,(5 \quad 7 \quad 6) = (1 \quad 4)\,(1 \quad 3)\,(5 \quad 6)\,(5 \quad 7)\,.$$

Teorema. Nenhuma permutação de um conjunto finito pode ser expressa simultaneamente como produto de um número par de transposições e como produto de um número ímpar de transposições. $\square$

Definição. Uma permutação diz-se *par* se se escreve como o produto de um número par de transposições. Uma permutação diz-se *ímpar* se se escreve como produto de um número ímpar de transposições.

Exemplo 53.

- Em S_n, a identidade é uma permutação par. De facto, se A tem n elementos
$$\mathrm{id} = (a_i \quad a_j)\,(a_i \quad a_j)\,,$$
para quaisquer $a_i, a_j \in A$.
- Em S_n, um ciclo de comprimento ímpar é uma permutação par e um ciclo de comprimento par é uma permutação ímpar
$$(1 \quad 2 \quad 3) = (1 \quad 3)\,(1 \quad 2) \qquad\qquad (1 \quad 2 \quad 3 \quad 4) = (1 \quad 4)\,(1 \quad 3)\,(1 \quad 2)\,.$$

Teorema. Seja A um conjunto com n elementos. Então, o conjunto das permutações pares em A é um subgrupo de S_n de ordem $\frac{n!}{2}$.

Demonstração. Seja

$$A_n = \{\sigma : \sigma \text{ é uma permutação par}\}.$$

Sabemos que $\mathrm{id} \in A_n$, que a composição de duas permutações pares é ainda uma permutação par e que a inversa de uma permutação par é ainda uma permutação par. Logo, temos que A_n é um subgrupo do grupo S_n.

Para demonstrar que $|A_n| = \frac{n!}{2}$, basta considerar uma transposição $\tau \in S_n$ e a aplicação

$$\begin{aligned} \phi_\tau : A_n &\longrightarrow B_n \\ \sigma &\longmapsto \tau\sigma, \end{aligned}$$

onde B_n é o conjunto das permutações ímpares.

Provando que ϕ_τ é bijetiva, temos que $\#(A_n) = \#(B_n)$ e, como

$\#(A_n) + \#(B_n) = \#(S_n) = n!$, o resultado é imediato. $\square$

Definição. Seja A um conjunto com n elementos. Chama-se *grupo alterno de A*, e representa-se por A_n, ao subgrupo de S_n das permutações pares.

Exemplo 54. $A_2 = \{id\}$

$A_3 = \{id, (1\,2\,3)\,, (1\,3\,2)\}$

$$A_4 = \{id, (1\,2\,3)\,, (1\,3\,2)\,, (1\,2\,4)\,, (1\,4\,2)\,, (1\,3\,4)\,, (1\,3\,4)\,,$$
$$(2\,3\,4)\,, (2\,4\,3)\,, (1\,2)\,(3\,4)\,, (1\,3)\,(2\,4)\,, (1\,4)\,(2\,3)\}$$

o teorema de representação de Cayley

Para finalizarmos este capítulo sobre grupos, vamos mostrar a importância do estudo do grupo simétrico na Teoria de Grupos. De facto, como se prova no próximo teorema, qualquer grupo é isomorfo a um subgrupo de um dado grupo simétrico.

Teorema. **(Teorema de representação de Cayley)**Todo o grupo é isomorfo a um grupo de permutações.

Demonstração. Para cada $x \in G$, a aplicação

$$\begin{array}{rcl} \lambda_x : G & \longrightarrow & G \\ a & \longmapsto & \lambda_x(a) = xa, \end{array}$$

é uma permutação em G.

Assim, se S é o grupo das permutações de G, consideramos a função

$$\begin{aligned} \theta : G &\longrightarrow S \\ x &\longmapsto \lambda_x . \end{aligned}$$

Então, para $x, y, g \in G$,

$$(\lambda_x \circ \lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg) = (xy)g = \lambda_{xy}(g),$$

pelo que

$$\theta(x)\theta(y) = \theta(xy),$$

i.e., θ é um morfismo.

Mais ainda,

$$x \in \mathrm{Nuc}\theta \Leftrightarrow \theta(\mathrm{x}) = \mathrm{id_G} \Leftrightarrow \lambda_\mathrm{x} = \mathrm{id_G} \Rightarrow \mathrm{x} = \lambda_\mathrm{x}(1_\mathrm{G}) = \mathrm{id_G}(1_\mathrm{G}) = 1_\mathrm{G},$$

e, portanto,

$$\mathrm{Nuc}\theta = \{1_\mathrm{G}\}.$$

Logo, θ é um monomorfismo, pelo que $G \cong \mathrm{Im}\theta < S$. $\square$

Exemplo 55. Seja $G = \mathbb{Z}_4$. Então, como para todos $a, x \in \mathbb{Z}_4$, $\lambda_a(x) = a + x$, temos que

$$\begin{aligned}
\lambda_{\bar{0}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{1} & \bar{2} & \bar{3} \end{pmatrix} = \mathrm{id} \\
\lambda_{\bar{1}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{1} & \bar{2} & \bar{3} & \bar{0} \end{pmatrix} = (\bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{3}) \\
\lambda_{\bar{2}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{2} & \bar{3} & \bar{0} & \bar{1} \end{pmatrix} = (\bar{0} \quad \bar{2})\,(\bar{1} \quad \bar{3}) \\
\lambda_{\bar{3}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{3} & \bar{0} & \bar{1} & \bar{2} \end{pmatrix} = (\bar{0} \quad \bar{3} \quad \bar{2} \quad \bar{1})\,.
\end{aligned}$$

Assim, $\mathbb{Z}_4 \cong \{\lambda_{\bar{0}}, \lambda_{\bar{1}}, \lambda_{\bar{2}}, \lambda_{\bar{3}}\}$.