1.7 Grupos cíclicos

Definição 1.7.1. Um grupo gerado por um elemento diz-se *cíclico*.

Nota 1.7.2. Os elementos de um grupo cíclico $G = \langle g \rangle$ são as potências g^k, $k \in \mathbb{Z}$. Um grupo cíclico é comutativo.

Exemplos 1.7.3. (i) O grupo aditivo $\mathbb{Z}$ é cíclico. Tem-se $\mathbb{Z} = \langle 1 \rangle$.
(ii) Para cada numero natural $n > 0$, $\mathbb{Z}_n$ é cíclico, gerado por $[1]_n = 1 + n\mathbb{Z}$.
(iii) Por 1.5.9, qualquer grupo de ordem prima é cíclico.
(iv) O grupo simétrico S_3 não é cíclico.

Proposição 1.7.4. *Sejam $G = \langle g \rangle$ um grupo cíclico e $\{e\} \neq H \subseteq G$ um subgrupo. Seja m o menor número natural positivo tal que $g^m \in H \setminus \{e\}$. Então $H = \langle g^m \rangle$.*

Demonstração: É claro que $\langle g^m \rangle \subseteq H$. Seja $n \in \mathbb{Z}$ tal que $g^n \in H$. Então existem $k \in \mathbb{Z}$ e $0 \leq r < m$ tais que $n = km + r$. Portanto $g^n = g^{km} g^r$. Como $g^{km} \in \langle g^m \rangle \subseteq H$, temos $g^r = g^n g^{-km} \in H$. Então $g^r = e$ e portanto $g^n = g^{km} \in \langle g^m \rangle$. □

Corolário 1.7.5. *Qualquer subgrupo de um grupo cíclico é cíclico.*

Corolário 1.7.6. *Os subgrupos de $\mathbb{Z}$ são os conjuntos $m\mathbb{Z}$, $m \in \mathbb{N}$.*

Corolário 1.7.7. *(Lema de Bézout) Sejam $a, b \in \mathbb{Z}$, não ambos iguais a 0, e $d = \mathrm{mdc}(a, b)$. Então existem $u, v \in \mathbb{Z}$ tais que $au + bv = d$.*

Demonstração: Como $d = \mathrm{mdc}(a, b)$, existem números primos entre si $a', b' \in \mathbb{Z}$ tais que $a = da'$ e $b = db'$. Por 1.7.6, o subgrupo $\langle a', b' \rangle$ de $\mathbb{Z}$ é gerado por um elemento $m \in \mathbb{N}$, que então é um divisor comum de a' e b'. Como a' e b' são primos entre si, $m = 1$. Segue-se que $\langle a', b' \rangle = \mathbb{Z}$ e então que existem $u, v \in \mathbb{Z}$ tais que $a'u + b'v = 1$. Multiplicando por d obtém-se $au + bv = d$. □

Teorema 1.7.8. *Seja $G = \langle g \rangle$ um grupo cíclico. Se G é infinito, então um isomorfismo $\mathbb{Z} \to G$ é dado por $k \mapsto g^k$. Se G é finito, então um isomorfismo $\mathbb{Z}_{|g|} \to G$ é dado por $k + |g|\mathbb{Z} \mapsto g^k$.*

Demonstração: Consideremos o epimorfismo $\phi \colon \mathbb{Z} \to G$ dado por $\phi(k) = g^k$. Por 1.7.6, existe $n \in \mathbb{N}$ tal que $\mathrm{Ker}(\phi) = n\mathbb{Z}$. Pelo Teorema do homomorfismo, um isomorfismo $f \colon \mathbb{Z}/n\mathbb{Z} \to G$ é dado por $k + n\mathbb{Z} \mapsto g^k$. Se G é finito, f é o isomorfismo procurado pois, neste caso, $n = |\mathbb{Z}/n\mathbb{Z}| = |g|$ e $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_{|g|}$. Se G é infinito, então $n = 0$ e $\mathrm{Ker}(\phi) = n\mathbb{Z} = \{0\}$, pelo que o epimorfismo ϕ é um isomorfismo. □

Corolário 1.7.9. *Seja $G = \langle g \rangle$ um grupo cíclico finito. Então*

(i) $G = \{e, g, \ldots, g^{|g|-1}\}$;

(ii) para todo o $m \in \mathbb{Z}$, $g^m = e$ *se e só se* $m \in |g|\mathbb{Z}$;

(iii) a ordem de G *é o menor inteiro positivo* m *tal que* $g^m = e$.

Demonstração: Seja $f\colon \mathbb{Z}_{|g|} \to G$ o isomorfismo dado por $f(k + |g|\mathbb{Z}) = g^k$.
(i) Tem-se $G = Im(f) = \{f(\bar{0}), \ldots, f(\overline{|g|-1})\} = \{e, g, \ldots, g^{|g|-1}\}$.
(ii) Para todo o $m \in \mathbb{Z}$,

$$g^m = e \Leftrightarrow f(m + |g|\mathbb{Z}) = f(|g|\mathbb{Z}) \Leftrightarrow m + |g|\mathbb{Z} = |g|\mathbb{Z} \Leftrightarrow m \in |g|\mathbb{Z}.$$

(iii) segue imediatamente de (ii). □

Proposição 1.7.10. *Sejam $G = \langle g \rangle$ um grupo cíclico finito.*

(a) Para todo o $k \in \mathbb{Z} \setminus \{0\}$, $|g^k| = \dfrac{|g|}{\mathrm{mdc}(|g|, k)}$. *Em particular,* $G = \langle g^k \rangle$ *se e só se a ordem de* G *e* k *são primos entre si.*

(b) Para cada divisor $d \geq 1$ *da ordem de* G *existe exactamente um subgrupo de* G *de ordem* d. *Este subgrupo é* $\langle g^{\frac{|g|}{d}} \rangle$.

Demonstração: Seja $n = |g| = |G|$.

(a) Seja $d = \mathrm{mdc}(k, n)$. Escrevemos $n = n'd$ e $k = k'd$ onde $\mathrm{mdc}(n', k') = 1$. Por 1.7.9 (iii), $|g^k|$ é o menor inteiro positivo m tal que $g^{km} = e$. Por 1.7.9 (ii), isto implica que $|g^k|$ é o menor inteiro positivo m tal que $km \in n\mathbb{Z}$. Como $n' \geq 1$ e $g^{kn'} = g^{k'n} = e$ temos $|g^k| \leq n'$. Como $n = n'd$ divide $|g^k|k = |g^k|k'd$ obtemos que n' divide $|g^k|k'$. Como $\mathrm{mdc}(n', k') = 1$ podemos concluir que n' divide $|g^k|$ e portanto que $|g^k| = n' = \dfrac{n}{\mathrm{mdc}(n, k)}$.

(b) O único subgrupo de G de ordem 1 é o subgrupo trivial $\{e\} = \langle g^{|g|} \rangle$. Seja $d > 1$ um divisor de $|g|$. Seja $k = \dfrac{|g|}{d}$. Então $\langle g^k \rangle$ é um subgrupo de G e tem-se $|g^k| = \dfrac{|g|}{\mathrm{mdc}(|g|, k)} = \dfrac{|g|}{k} = d$. Seja $H \leq G$ com $|H| = d$. Seja m o menor número natural positivo tal que $g^m \in H \setminus \{e\}$. Por 1.7.4, $H = \langle g^m \rangle$. Por 1.7.9(i), $0 < m < |g|$. Tem-se $d = |g^m| = \dfrac{|g|}{\mathrm{mdc}(|g|, m)} = \dfrac{|g|}{m}$ e portanto $m = \dfrac{|g|}{d} = k$. Segue-se que $H = \langle g^k \rangle$. Logo existe exactamente um subgrupo de G de ordem d e este é $\langle g^k \rangle$. □

Corolário 1.7.11. *Os subgrupos de um grupo cíclico finito $G = \langle g \rangle$ são os grupos da forma $\langle g^{\frac{|g|}{d}} \rangle$, onde $d \geq 1$ é um divisor de $|g|$.*

Definição 1.7.12. O *produto directo* dos grupos $G_1, \ldots, G_n$ é o grupo cujo conjunto subjacente é o produto cartesiano $G_1 \times \cdots \times G_n$ e cuja operação é dada por

$$(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n).$$

Verifica-se facilmente que o produto directo dos grupos $G_1, \ldots, G_n$ é de facto um grupo. Este grupo é denotado por $\prod_{i=1}^{n} G_i$ ou por $G_1 \times \cdots \times G_n$.

Exemplo 1.7.13. O exemplo $\mathbb{Z}_2 \times \mathbb{Z}_2$ mostra que o produto directo de dois grupos cíclicos não é, em geral, um gupo cíclico. Com efeito, $\mathbb{Z}_2 \times \mathbb{Z}_2$ tem dois subgrupos diferentes de ordem 2, nomeadamente $\mathbb{Z}_2 \times \{[0]_2\}$ e $\{[0]_2\} \times \mathbb{Z}_2$, e um grupo cíclico não pode ter mais do que um subgrupo de uma dada ordem.

Proposição 1.7.14. *Sejam $n_1, \ldots n_k \geq 1$ inteiros. Então o produto directo $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$ é cíclico se e só os inteiros $n_1, \ldots n_k$ são dois a dois primos entre si. Neste caso um isomorfismo $\mathbb{Z}_{n_1 \cdots n_k} \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$ é dado por $m + n_1 \cdots n_k \mathbb{Z} \mapsto (m + n_1\mathbb{Z}, \ldots, m + n_k\mathbb{Z})$.*

Demonstração: Suponhamos primeiramente os inteiros $n_1, \ldots n_k$ são dois a dois primos entre si. Consideremos o homomorfismo $f \colon \mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$ definido por

$$f(m) = (m + n_1\mathbb{Z}, \ldots, m + n_k\mathbb{Z}).$$

É claro que $n_1 \cdots n_k \mathbb{Z} \subseteq \mathrm{Ker}(f)$. Por outro lado, seja $m \in \mathrm{Ker}(f)$. Então existem $u_1, \ldots, u_k \in \mathbb{Z}$ tais que $m = n_1 u_1 = \cdots = n_k u_k$, ou seja, cada n_i divide m. Como os n_i são dois a dois primos entre si, o produto $n_1 \cdots n_k$ divide m. Logo $m \in n_1 \cdots n_k \mathbb{Z}$ e $\mathrm{Ker}(f) = n_1 \cdots n_k \mathbb{Z}$. Pelo teorema 1.6.13, $\bar{f} \colon \mathbb{Z}_{n_1 \cdots n_k} \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$, $\bar{f}(m + n_1 \cdots n_k \mathbb{Z}) = (m + n_1\mathbb{Z}, \ldots, m + n_k\mathbb{Z})$ é um monomorfismo. Como $|\mathbb{Z}_{n_1 \cdots n_k}| = n_1 \cdots n_k = |\prod_{i=1}^{k} \mathbb{Z}_{n_i}|$, $\bar{f}$ é de facto um isomorfismo e $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$ é cíclico.

Suponhamos agora que os inteiros $n_1, \ldots n_k$ não são dois a dois primos entre si. Então existem $i \neq j \in \{1, \ldots, k\}$ tais que n_i e n_j têm um divisor comum $d > 1$. Como $\mathbb{Z}_{n_i}$ e $\mathbb{Z}_{n_j}$ são cíclicos, existem subgrupos $U_i \leq \mathbb{Z}_{n_i}$ e $V_j \leq \mathbb{Z}_{n_j}$ de ordem d. Pomos $U_l = \{n_l\mathbb{Z}\}$ para $l \neq i$ e $V_l = \{n_l\mathbb{Z}\}$ para $l \neq j$. Então $\prod_{l=1}^{n} U_l$ e $\prod_{l=1}^{n} V_l$ são dois subgrupos diferentes de ordem d de $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$. Logo $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$ não é cíclico. □

1.8 Grupos simétricos

Recorde que para um conjunto $X \neq \emptyset$, $S(X) = \{f : X \to X \ : \ f \text{ bijeção}\}$ é um grupo relativamente à composição, chamado grupo simétrico. Recorde ainda que S_n designa o grupo simétrico $S(\{1, 2, \ldots, n\})$.

Teorema 1.8.1. *(Teorema de Cayley) Cada grupo G é isomorfo a um subgrupo do grupo simétrico $S(G)$.*

Demonstração: Para $g \in G$ seja $\lambda_g \colon G \to G$ a função definida por $\lambda_g(x) = gx$. Para quaisquer $g, h, x \in G$, $\lambda_{gh}(x) = ghx = g\lambda_h(x) = \lambda_g(\lambda_h(x)) = \lambda_g \circ \lambda_h(x)$. Segue-se que cada λ_g é bijectiva com função inversa $\lambda_{g^{-1}}$ e que a função $f \colon G \to S(G)$, $f(g) = \lambda_g$ é um homomorfismo. Seja $g \in Ker(f)$. Então $f(g) = \lambda_g = id_G$. Logo $g^2 = \lambda_g(g) = g = eg$. Pelas leis do corte, $g = e$ e temos $\mathrm{Ker}(f) = \{e\}$. Segue-se que f é um monomorfismo e portanto que $G \cong \mathrm{Im}(f)$. □

Corolário 1.8.2. *Cada grupo finito G de ordem n é isomorfo a um subgrupo de S_n.*

Demonstração: Seja $\alpha : G \to \{1, 2, \ldots n\}$ uma bijeção. Verifica-se que $\Psi : S(G) \to S_n$ dada por $\Psi(f) = \alpha \circ f \circ \alpha^{-1}$ é um isomorfismo de grupos (nota: isto não utiliza a estrutura de grupo de G, tal isomorfismo existe para qualquer conjunto com n elementos). Como, pelo Teorema de Cayley, G é subgrupo de $S(G)$ e como Ψ é um isomorfismo de grupos, podemos concluir que G é isomormorfo a um subgrupo de S_n. □

Notação 1.8.3. Uma permutação $\sigma \in S_n$ é muitas vezes representada sob a forma

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Observação 1.8.4. Um monomorfismo $S_n \to S_{n+1}$ é dado por

$$\sigma \mapsto \begin{pmatrix} 1 & \cdots & n & n+1 \\ \sigma(1) & \cdots & \sigma(n) & n+1 \end{pmatrix}.$$

Por conseguinte, S_n é isomorfo ao subgrupo de S_{n+1} das permutações α com $\alpha(n+1) = n+1$.

Proposição 1.8.5. $|S_n| = n!$

Definição 1.8.6. Uma permutação $\sigma \in S_n$ diz-se um *cíclo* se existem $k, i_1, \ldots, i_k \in \{1, \ldots, n\}$ tais que $\sigma(i_j) = i_{j+1}$ para $1 \leq j < k$, $\sigma(i_k) = i_1$ e $\sigma(i) = i$ para $i \notin \{i_1, \ldots, i_k\}$. O cíclo assim definido é denotado por $(i_1, \ldots, i_k)$. Aos cíclos da forma (i, j) com $i \neq j \in \{1, \ldots, n\}$ chama-se também *transposições*. Dois cíclos $(i_1, \ldots, i_k)$ e $(j_1, \ldots, j_l)$ dizem-se *disjuntos* se $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$.

Observações 1.8.7. (i) A identidade de $\{1,\ldots,n\}$ é um cíclo. Para cada $i \in \{1,\ldots,n\}$, $id_{\{1,\ldots,n\}} = (i)$.

(ii) Para quaisquer k números distintos $i_1,\ldots i_k \in \{1,\ldots,n\}$, $|(i_1,\ldots,i_k)| = k$.

(iii) Se $\alpha,\beta \in S_n$ são cíclos disjuntos, então $\alpha\beta = \beta\alpha$. Logo se $\alpha_1,\ldots\alpha_l \in S_n$ são cíclos dois a dois disjuntos, então $|\alpha_1\cdots\alpha_l| = \text{mmc}(|\alpha_1|,\ldots,|\alpha_l|)$.

(iv) Para cada transposição $\tau \in S_n$, $\tau^2 = id$.

Proposição 1.8.8. *Cada permutação $\sigma \in S_n \setminus \{id\}$ pode ser factorizada em cíclos dois a dois disjuntos de $S_n \setminus \{id\}$.*

Demonstração: Seja $\sigma \in S_n \setminus \{id\}$. Para $i \in \{1,\ldots,n\}$, seja

$$k_i = \min\{k \in \{1,\ldots,n!\} \mid \sigma^k(i) = i\}.$$

Note-se que este mínimo existe pois $\sigma^{n!} = id$ pelo Exercício 2 da Folha 5. Definimos os números $j_1,\ldots,j_m \in \{1,\ldots,n\}$ recursivamente como se segue: Enquanto tal i existe, j_l é o menor

$$i \in \{1,\ldots,n\} \setminus \{j_1,\sigma(j_1),\ldots,\sigma^{k_{j_1}-1}(j_1),\ldots,j_{l-1},\sigma(j_{l-1}),\ldots,\sigma^{k_{j_{l-1}}-1}(j_{l-1})\}$$

tal que $\sigma(i) \neq i$. Como $\sigma \neq id$, j_1 existe. Como $\{1,\ldots,n\}$ é finito, o processo pára depois de um número finito, m, de iterações. Para cada $l \in \{1,\ldots,m\}$, $(j_l,\sigma(j_l),\ldots,\sigma^{k_{j_l}-1}(j_l))$ é um cíclo em $S_n \setminus \{id\}$. Sejam $l,r \in \{1,\ldots,m\}$, $0 \leq k < k_{j_l}$ e $0 \leq s < k_{j_r}$ tais que $\sigma^k(j_l) = \sigma^s(j_r)$. Então $j_r = \sigma^{k_{j_r}}(j_r) \in \{j_l,\sigma(j_l),\ldots,\sigma^{k_{j_l}-1}(j_l)\}$, pelo que $r \leq l$. Do mesmo modo temos $l \leq r$ e então $r = l$. Segue-se que os cíclos $(j_l,\sigma(j_l),\ldots,\sigma^{k_{j_l}-1}(j_l))$ são dois a dois disjuntos. Seja

$$\psi = (j_1,\sigma(j_1),\ldots,\sigma^{k_{j_1}-1}(j_1))\cdots(j_m,\sigma(j_m),\ldots,\sigma^{k_{j_m}-1}(j_m)).$$

Temos $\psi(\sigma^k(j_l)) = \sigma^{k+1}(j_l)$ e $\sigma(i) = i = \psi(i)$ para

$$i \notin \{j_1,\sigma(j_1),\ldots,\sigma^{k_{j_1}-1}(j_1),\ldots,j_m,\sigma(j_m),\ldots,\sigma^{k_{j_m}-1}(j_m)\}.$$

Logo $\sigma = \psi$. □

Corolário 1.8.9. *S_n é gerado pelos cíclos.*

Exemplo 1.8.10. Consideremos a permutação $\sigma \in S_6$ dada por

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

Tem-se $\sigma = (2,5,3)(4,6)$.

Nota 1.8.11. É possível mostrar que a factorização de uma permutação $\sigma \in S_n \setminus \{id\}$ em cíclos dois a dois disjuntos de $S_n \setminus \{id\}$ é única a menos da ordem dos factores (exercício).

Proposição 1.8.12. *Sejam $i_1, \ldots, i_k \in \{1, \ldots, n\}$ número distintos com $k \geq 3$. Então $(i_1, \ldots, i_k) = (i_1, i_k) \cdots (i_1, i_2)$.*

Demonstração: Tem-se

$$(i_1, i_k) \cdots (i_1, i_2)(i_1) = (i_1, i_k) \cdots (i_1, i_3)(i_2) = i_2,$$

$$(i_1, i_k) \cdots (i_1, i_2)(i_k) = (i_1, i_k)(i_k) = i_1,$$

$$\begin{aligned} (i_1, i_k) \cdots (i_1, i_2)(i_l) &= (i_1, i_k) \cdots (i_1, i_l)(i_l) \\ &= (i_1, i_k) \cdots (i_1, i_{l+1})(i_1) \\ &= (i_1, i_k) \cdots (i_1, i_{l+2})(i_{l+1}) \\ &= i_{l+1} \end{aligned}$$

para $1 < l < k$ e $(i_1, i_k) \cdots (i_1, i_2)(i) = i$ para $i \notin \{i_1, \ldots, i_k\}$. □

Corolário 1.8.13. *S_n é gerado pelas transposições.*

Definição 1.8.14. Seja $\sigma \in S_n$ uma permutação. Uma *inversão* em σ é um par $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ tal que $i < j$ e $\sigma(i) > \sigma(j)$. O *sinal* de σ, $\operatorname{sgn}(\sigma)$, é 1 se existe um número par de inversões em σ e -1 caso contrário. Uma permutação diz-se *par (ímpar)* se tem sinal 1 (-1).

Observações 1.8.15. (i) Se m é o numéro de inversões em $\sigma \in S_n$, então $\operatorname{sgn}(\sigma) = (-1)^m$.
(ii) O sinal de qualquer transposição é -1.

Proposição 1.8.16. *O sinal é um homomorfismo de S_n para o grupo multiplicativo $\{1, -1\}$.*

Demonstração: Sejam $\alpha, \beta \in S_n$, k o número de inversões em α e l o número de inversões em β. Um par $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ com $i < j$ é uma inversão em $\alpha\beta$ se e só se satisfaz uma das condições seguintes:

(a) (i, j) é uma inversão em β mas $(\beta(j), \beta(i))$ não é uma inversão em α;

(b) (i, j) não é uma inversão em β mas $(\beta(i), \beta(j))$ é uma inversão em α.

Seja r o número de pares (i,j) com $i<j$ que satisfazem a condição (a) e seja s o número de pares (i,j) com $i<j$ que satisfazem a condição (b). Então $\text{sgn}(\alpha\beta)=(-1)^{r+s}$. Seja m o número de inversões (i,j) em β tais que $(\beta(j),\beta(i))$ é uma inversão em α. Então $l=r+m$. Também temos $k=s+m$. Com efeito, os pares (i,j) com $i<j$ que satisfazem a condição (b) estão em correspondência bijectiva com as inversões (x,y) em α com $\beta^{-1}(x)<\beta^{-1}(y)$, pelo que o número destas inversões em α é s. E as inversões (i,j) em β tais que $(\beta(j),\beta(i))$ é uma inversão em α estão em correspondência bijectiva com as inversões (x,y) em α com $\beta^{-1}(y)<\beta^{-1}(x)$, pelo que o número destas inversões em α é m. Segue-se que $\text{sgn}(\alpha\beta)=(-1)^{r+s}=(-1)^{l+k-2m}=(-1)^l(-1)^k(-1)^{-2m}=(-1)^l(-1)^k=(-1)^k(-1)^l=\text{sgn}(\alpha)\text{sgn}(\beta)$. □

Observação 1.8.17. Pela proposição precedente, um produto de um número par de transposições tem sinal 1 e um produto de um número ímpar de transposições tem sinal -1. Segue-se que uma permutação não pode ao mesmo tempo ser factorizada num número par e num número ímpar de transposições e que uma permutação é par se e só se ela pode ser factorizada num número par de transposições. Em particular, pela Proposição 1.8.12, um cíclo de ordem par é ímpar e um cíclo de ordem ímpar é par.

Proposição 1.8.18. *Sejam $i_1,\ldots,i_k\in\{1,\ldots,n\}$ k números distintos e seja σ o cíclo $(i_1,\ldots,i_k)$. Tem-se* $\text{sgn}(\sigma)=(-1)^{k-1}$.

Observação 1.8.19. Em geral, para uma permutação qualquer $\sigma\in S_n$, não temos $\text{sgn}(\sigma)=(-1)^{|\sigma|-1}$. Por exemplo, a permutação $\sigma=(1,2)(3,4,5,6,7,8)$ de S_8 têm ordem 6 mas $\text{sgn}(\sigma)=1\neq(-1)^5$.