Grupos e Corpos

Prof. Lucas Calixto

Aula 2 - Grupos cíclicos e de permutações

Grupos cíclicos

Ideia: Estudar grupos gerados por um único elemento

Exemplos:

• $3\mathbb{Z} = \{3n \mid n \in \mathbb{Z}\}$ é um subgrupo de $(\mathbb{Z}, +)$ completamente determinado pelo número 3

• $H = \{2^n \mid n \in \mathbb{Z}\}$ é um subgrupo de $(\mathbb{Q}^*, +)$ completamente determinado pelo número 2

Em geral, temos

Proposição Se G é um grupo, então

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \quad a^0 = e \text{ por definição}$$

é o menor subgrupo de G que contem a.

Prova: $\langle a \rangle \neq \emptyset$ pois $e = a^0 \in \langle a \rangle$. Por outro lado,

$$g, h \in \langle a \rangle \Rightarrow g = a^m,\ h = a^n \Rightarrow h^{-1} = a^{-n} \Rightarrow gh^{-1} = a^m a^{-n} = a^{m-n} \in \langle a \rangle$$

Logo $\langle a \rangle$ é subgrupo de G.

Se $H \subset G$ é subgrupo e $a \in H$, então $a^m \in H$, $\forall m \in \mathbb{Z}$ e portanto $\langle a \rangle \subset H$ $\blacksquare$

O grupo $\langle a \rangle$ é chamado grupo cíclico gerado por a

Note: Se estivermos usando $+$ em vez de $\cdot$, então

$$\langle a \rangle = \{na \mid n \in \mathbb{Z}\} \quad 0a = 0 \text{ por definição}$$

G é um grupo cíclico, se existe $a \in G$ tal que $G = \langle a \rangle$

Note: Todo grupo cíclico é abeliano

A ordem de um elemento $a \in G$ é o menor $n \in \mathbb{Z}_{\geq 0}$ tal que $a^n = e$. Nesse caso, escrevemos $|a| = n$. O elemento a tem ordem infinita se tal n não existe, e escrevemos $|a| = \infty$. Note: se $0 \leq k, \ell < |a|$ e $k \neq \ell$, então $a^k \neq a^\ell$

Logo, $G = \langle a \rangle \Rightarrow |G| = |a|$

Exemplos

- $\mathbb{Z} = \langle 1 \rangle$

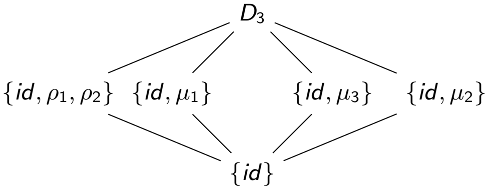
- $\mathbb{Z}_n = \langle 1 \rangle$

- Um grupo cíclico pode ter mais de um gerador:

$$\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle, \quad \mathbb{Z}_6 \neq \langle 2 \rangle = \{0, 2, 4\}$$

- O grupo D_3 (simetrias do Δ) não é cíclico. Contudo, todo subgrupo próprio de D_3 é cíclico (lembrem: $\rho_1 = 120^\circ$, $\rho_2 = 240^\circ$ e μ_i são reflexões)

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id



Subgrupos de grupos cíclicos

Proposição Se G é grupo cíclico $(G = \langle a \rangle)$ e $H \leq G$ então H é cíclico

Prova: Se $H = \{e\}$, OK.

Suponha $\exists\ g \in H$, $g \neq e$. Como $g = a^n$ para algum $n \in \mathbb{Z}$ e $a^{-n} = g^{-1} \in H$, podemos assumir que $n > 0$

Afirmação: se $m \in \mathbb{Z}_{>0}$ é minimal tal que $a^m \in H$, então $H = \langle h = a^m \rangle$

Se $g \in H$, então $g = a^k$ e $k = mq + r$ para algum $q \in \mathbb{Z}$ e $0 \leq r < m$ (algoritmo da divisão). Assim,

$$a^k = a^{mq+r} = a^{mq} a^r = h^q a^r \Rightarrow a^r = a^k h^{-q} \in H$$

Como m é minimal em $\mathbb{Z}_{>0}$ tal que $a^m \in H \Rightarrow r = 0$

Logo $g = a^k = a^{mq} = h^q \in \langle h \rangle \Rightarrow H = \langle h \rangle$ $\blacksquare$

Corolário: Se $H \leq \mathbb{Z} = \langle 1 \rangle$, então $H = n\mathbb{Z}$ para algum $n \in \mathbb{Z}_{\geq 0}$

Proposição: Se $G = \langle a \rangle$ é grupo cíclico de ordem n, então $a^k = e$ se e só se $n|k$

Prova: Note que $G = \langle a \rangle \Rightarrow |G| = |a| \Rightarrow |a| = n \Rightarrow n$ é mínimo tal que $a^n = e$

$(\Rightarrow)$ Escreva $k = nq + r$ com $q \in \mathbb{Z}$ e $0 \leq r < n$. Assim

$$e = a^k = a^{nq+r} = a^{nq}a^r = a^r$$

Como n é mínimo tal que $a^n = e$, segue que $r = 0$ e $n|k$

$(\Rightarrow)$ Se $k = qn$, então $a^k = a^{nq} = (a^n)^q = e^q = e$ $\blacksquare$

Proposição: Seja $G = \langle a \rangle$ tal que $|G| = n$. Se $b = a^k$, então $|b| = n/d$, onde $d = mdc(n,k)$

Prova: Seja $|b| = m$. Dai, $m \in \mathbb{Z}_{>0}$ é minimal tal que

$$e = b^m = a^{km} \Leftrightarrow n|km \quad \text{(Proposição anterior)}$$

Logo, $m \in \mathbb{Z}_{>0}$ é minimal tal que $n|km$, ou equivalentemente, $m \in \mathbb{Z}_{>0}$ é minimal tal que $\frac{n}{d}|m(\frac{k}{d})$

Obviamente, $\frac{n}{d}|\frac{n}{d}(\frac{k}{d})$ e assim $m \leq \frac{n}{d}$

Por outro lado, $d = mdc(n,k) \Leftrightarrow mdc(\frac{n}{d}, \frac{k}{d}) = 1$, e

$$\frac{n}{d}|m(\frac{k}{d}) \Rightarrow \frac{n}{d}|m \Rightarrow \frac{n}{d} \leq m$$

Logo $m = \frac{n}{d}$ ■

Corolário: Os geradores de $\mathbb{Z}_n$ são exatamente elementos $b \in \mathbb{Z}_n$ tais que $mdc(b, n) = 1$

Prova: Sabemos que $\mathbb{Z}_n = \langle 1 \rangle$ e que $\mathbb{Z}_n = \langle b \rangle \Leftrightarrow n = |\mathbb{Z}_n| = |b|$

Como $b = b1 = 1^b$ (na notação usual), a Proposição anterior implica $|b| = n/d$, onde $d = mdc(n, b)$. Então,

$$n = |b| \Leftrightarrow n = n/d \Leftrightarrow d = 1$$

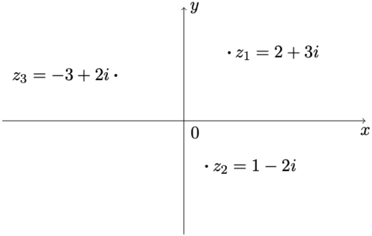
$\blacksquare$

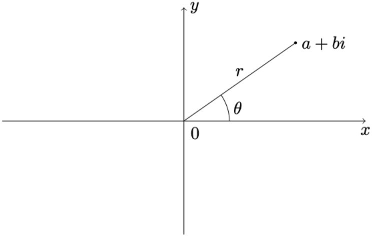
Exemplo: Os geradores de $\mathbb{Z}_{16}$ são $1, 3, 5, 7, 9, 11, 13, 15$

O grupo $\mathbb{C}^*$ e seus subgrupos

Diferentemente dos grupos $\mathbb{R}^*$ e $\mathbb{Q}^*$, o grupo $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ possui vários subgrupos interessantes

Podemos pensar nos elementos de $\mathbb{C}$ no plano xy em coordenadas cartesianas ou polares. (**Lembrem:** $e^{i\theta} = \cos(\theta) + i\sin(\theta)$)





$$z = a + bi = r(\cos(\theta) + i\sin(\theta)) = re^{i\theta}$$

$$r = \sqrt{a^2 + b^2}, \quad a = r\cos(\theta), \quad b = r\sin(\theta), \quad 0 \leq \theta < 2\pi$$

Proposição: Se $z = re^{i\theta}$ e $w = se^{i\phi}$, então

1. $zw = rse^{i(\theta+\phi)}$ (grande vantagem de coordenadas polares)
2. $z^{-1} = r^{-1}e^{(-\theta)}$
3. $z^n = r^n e^{(n\theta)}$

Proposição: O círculo de raio 1, $T = \{z \in \mathbb{C} \mid ||z|| = 1\}$ é um subgrupo de $(\mathbb{C}^*, \cdot)$

Um número $z \in \mathbb{C}$ tal que $z^n = 1$ é uma raiz n-ésima da unidade

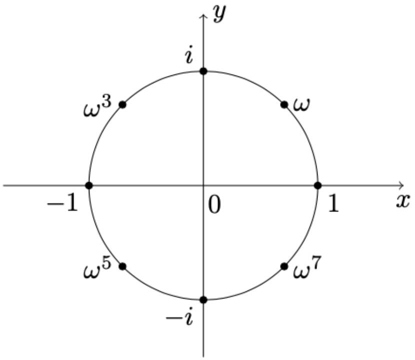
Proposição: As raízes n-ésimas da unidade são $e^{\frac{2k\pi}{n}}$, $k = 0, \ldots, n-1$. Além disso, o conjunto

$$\{e^{\frac{2k\pi}{n}} \mid k = 0, \ldots, n-1\}$$

é um subgrupo cíclico de $\mathbb{C}^*$ de T de ordem n

Os geradores de $\{e^{\frac{2k\pi}{n}} \mid k = 0, \ldots, n-1\}$ são chamados raízes n-ésimas primitivas da unidade

Exemplo: As raízes 8-ésimas primitivas da unidade são: $w = e^{\frac{\pi}{4}}$, $w^3 = e^{\frac{2\pi}{4}}$, $w^5 = e^{\frac{4\pi}{4}}$, $w^7 = e^{\frac{7\pi}{4}}$



Grupos de permutações

Definição: Uma permutação de um conjunto X é uma função bijetora $f : X \to X$

Note: o conjunto das permutações de X, $S_X = \{f : X \to X \mid f \text{ é permutação}\}$ é um grupo munido da composição de funções

- $S_X \times S_X \to S_X$, $(f, g) \mapsto f \circ g$ é bem definida e é associativa
- Elemento neutro: $id \in S_X$
- Elemento inverso: $f \in S_X \Rightarrow f^{-1} \in S_X$

Se $|X| = n$, podemos supor $X = \{1, \ldots, n\}$ e escrevemos S_n em vez de S_X

S_n é chamado de grupo simétrico de n elementos

Observe: $|S_n| = n!$ e portanto S_n tem ordem $n!$

Um subgrupo de S_n é chamado um grupo de permutações

Exemplo: O conjunto $G = \{id, \sigma, \tau, \mu\} \subset S_5$, onde

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}, \ \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

é um subgrupo de S_5:

$\circ$	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

Note: Nesse caso G é abeliano. Isso não é sempre o caso

Exemplo: Em S_4, se $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ e $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, então

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 1 \end{pmatrix} \neq \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

ciclos

Definição: Uma permutação $\sigma \in S_X$ é um ciclo de comprimento k, se existem $a_1, \dots, a_k \in X$ tais que

$$a_1 \overset{\sigma}{\mapsto} a_2 \quad a_2 \overset{\sigma}{\mapsto} a_3 \quad \cdots \quad a_k \overset{\sigma}{\mapsto} a_1$$

e $\sigma(x) = x$ para todos outros elementos de X. Nesse caso, escrevemos

$$\sigma = (a_1 a_2 \cdots a_k)$$

Fato: qualquer permutação pode ser escrita em termos de ciclos

- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (162354)$

- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1243)(56) \Rightarrow$ nem toda permutação é um ciclo

Obs: o processo termina quando todos elementos de X que não são fixados por σ aparecem em algum ciclo

Dois ciclos $\sigma = (a_1 \cdots a_k)$ e $\tau = (b_1 \cdots b_l)$ são disjuntos se $a_i \neq b_j$ para todos i, j

Exemplo • (135) e (347) não são disjuntos e

$$(135)(347) = (13475) \quad \text{(simplificado!)}$$

• (135) e (27) são disjuntos e o produto (135)(27) não pode ser simplificado

Proposição: Se $\sigma, \tau \in S_X$ são ciclos disjuntos, então $\sigma\tau = \tau\sigma$

Prova: Suponha $\sigma = (a_1 \cdots a_k)$ e $\tau = (b_1 \cdots b_l)$ e que $a_i \neq b_j$ para todos os índices

Se $x \in X \setminus \{a_1, \ldots, a_k, b_1, \ldots, b_l\}$, então $\sigma(x) = \tau(x) = x \Rightarrow \sigma\tau(x) = \tau\sigma(x) = x$

Se $x = a_i$, então $\tau(x) = x$ e $\tau\sigma(x) = \sigma(x) \Rightarrow \sigma\tau(x) = \sigma(x) = \tau\sigma(x)$

Se $x = b_i$, então $\sigma(x) = x$ e $\sigma\tau(x) = \tau(x) \Rightarrow \sigma\tau(x) = \tau(x) = \tau\sigma(x)$ ■

Proposição: Toda permutação $\sigma \in S_n$ é produto de ciclos disjuntos

Prova: Lembre $S_n = S_X$ onde $X = \{1, \dots, n\}$

Defina $X_1 = \{1, \sigma(1), \dots, \sigma^{n_1}(1)\} \subset X$ com n_1 minimal tal que $\sigma^{n_1+1}(1) = 1$

Se $X_1 \neq X$, tome $i_2 \in X \setminus X_1$ minimal e defina $X_2 = \{i_2, \sigma(i_2), \dots, \sigma^{n_2}(i_2)\}$

Se $X_1 \cup X_2 \neq X$, tome $i_3 \in X \setminus X_1 \cup X_2$ minimal, $X_3 = \{i_3, \sigma(i_3), \dots, \sigma^{n_3}(i_3)\}$

$\vdots$

$X = X_1 \cup \cdots \cup X_r$.

Se $x \in X_j \cap X_k$ para $j \neq k$ (assuma $j < k$), então

$$x = \sigma^{m_k}(i_k) = \sigma^{m_j}(i_j) \Rightarrow i_k = \sigma^{m_k+\ell}(i_k) = \sigma^{m_j+\ell}(i_j) \in X_j \quad \text{tal } \ell \text{ existe}$$

Contradição, pois $i_k \notin X_p$ para $1 \leq p < k$

Defina: $\sigma_j : X \to X$, $\sigma_j(x) = x$ se $x \notin X_j$ e $\sigma_j(x) = \sigma(x)$ se $x \in X_j$

- $\sigma_j = (i_j\sigma(i_j)\cdots\sigma^{n_j}(i_j)) \Rightarrow \sigma_j$ é ciclo

- σ_j, σ_k são disjuntos

- $\sigma = \sigma_1 \cdots \sigma_r$ $\blacksquare$

Exemplo: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1243)(56)$

Transposições

Uma transposição é um ciclo de comprimento 2

Note: Todo ciclo é produto de transposições

$$(a_1 a_2 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$$

Proposição: Toda permutação de S_n $(n > 1)$ é produto de transposições

Note: em geral existe mais de uma forma de fazer isso

- $(16)(253) = (16)(23)(25) = (16)(45)(23)(45)(25)$
- $(1) = (12)(12) = (23)(23)$

Vamos ver que a paridade do número de transposições é preservada

Lema: Se $id = \tau_1 \cdots \tau_r$ onde τ_i são transposições, então $r \in 2\mathbb{Z}$.

Prova: Indução em r. O menor valor possível para r é $r = 2$ ($r = 1 \Rightarrow id$ é transposição, o que não é verdade)

Se $r = 2$, ok

Assuma $r > 2$ e note que uma das possibilidades para o produto $\tau_{r-1}\tau_r$ vale:

$$\begin{aligned}(ab)(ab) &= id\\ (ac)(ab) &= (ab)(bc)\\ (bc)(ab) &= (ac)(bc)\\ (cd)(ab) &= (ab)(cd)\end{aligned}$$

com a, b, c, d distintos.

Denote o lado direito das ultimas 3 equações acima por $(a*)t_r$

Se $\tau_{r-1}\tau_r = id$, então $id = \tau_1 \cdots \tau_{r-2}$. Por indução $r - 2$ é par, e portanto r é par

Se algum dos 3 últimos casos ocorre, então

$$id = \tau_1 \cdots \tau_r = \tau_1 \cdots \tau_{r-2}(a*)t_r$$

e a última ocorrência de a em id é em $(a*)$

Repita o argumento para $\tau_{r-2}(a*)$: $\tau_{r-2}(a*) = id$ ou $\tau_{r-2}(a*) = (a*)t_{r-1}$. Se $\tau_{r-2}(a*) = id$ aplique indução. Caso contrário, substitua $\tau_{r-2}(a*)$ por $(a*)t_{r-1}$

$$id = \tau_1 \cdots \tau_{r-2}\tau_{r-1}\tau_r = \tau_1 \cdots (a*)t_{r-1}t_r$$

e note que última ocorrência de a em id é em $(a*)$

Se id nunca ocorre nesse processo, teremos $id = (a*)t_2 \cdots t_r$ e a só ocorre na primeira transposição $\Rightarrow id(a) = * \neq a$

Logo id deve aparecer em algum passo e podemos aplicar indução em $r-2$ ■

Teorema: Se $\sigma \in S_X$ e $\sigma = \tau_1 \cdots \tau_p = \gamma_1 \cdots \gamma_q$ onde τ_i e γ_i são transposições, então p e q tem a mesma paridade

Prova: Note que $\gamma_q \cdots \gamma_1 = \sigma^{-1}$, pois $\tau^2 = id$ para qualquer transposição

Daí

$$id = \tau_1 \cdots \tau_p \gamma_q \cdots \gamma_1 \Rightarrow p + q \in 2\mathbb{Z} \Rightarrow p + q \text{ tem a mesma paridade}$$

■

Teorema: $A_n = \{\tau_1 \cdots \tau_n \mid \tau_i \text{ é transposição e } n \in 2\mathbb{Z}_{>0}\}$ é um subgrupo de S_n

O grupo A_n é chamado grupo alternado de S_n

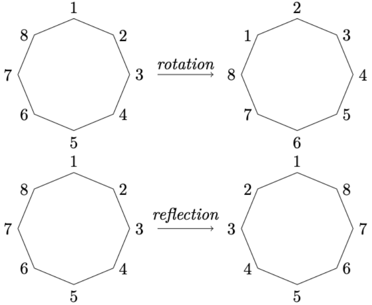
Proposição: Se $n > 1$, então $|A_n| = |B_n = \{\tau_1 \cdots \tau_n \mid \tau_i \text{ é transp. e } n \text{ é impar}\}|$

Prova: $\tau \in S_n$ transposição $\Rightarrow f_\tau : A_n \to B_n$, $\sigma \mapsto \tau\sigma$ é bijeção $(f_\tau^{-1} = f_\tau)$

Grupos diedrais

Lembrem: um movimento rígido de um objeto geométrico é uma combinação (composição) de rotações e reflexões que preservam tal objeto

Defina, para $n \geq 3$, o n-ésimo grupo diedral D_n como sendo o grupo dos movimentos rígidos de um polígono regular de n lados



Note: o vértice 1 de D_n pode ser enviado para n vértices de duas formas diferentes (movimento rígido $\Rightarrow$ escolha de onde enviar o par de vértices (1,2) determina tudo):

$$(n, 1, 2) \mapsto (k-1, k, k+1) \text{ ou } (n, 1, 2) \mapsto (k+1, k, k-1)$$

Se $k = n$, pense em $k + 1 = 1$, se $k = 1$, pense em $k - 1 = n$, ou seja, a conta nos vértices é feita em $\mathbb{Z}_n$

Logo: $|D_n| = 2n$

Teorema: O grupo D_n ($n \geq 3$) consiste de todos os produtos de elementos $r, s \in D_n$ tais que

$$r^n = 1, \quad s^2 = 1, \quad srs = r^{-1}$$

Prova: Existem n rotações

$$id, \frac{360^\circ}{n}, 2\frac{360^\circ}{n}, \ldots, (n-1)\frac{360^\circ}{n}$$

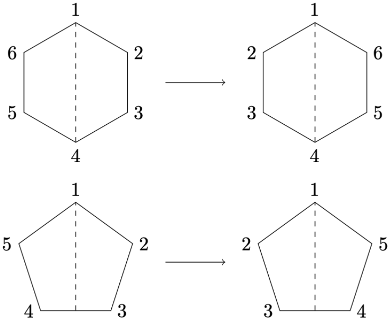
todas são composições de $r = \frac{360^\circ}{n}$, e $r^n = id$

Seja s_i a reflexão que deixa o vértice i fixo (referente a reta bissetriz ao vértice i)

n par $\Rightarrow$ o vértice i e seu antipodal $n/2 + i$ são fixados por $s_i \Rightarrow s_i = s_{n/2+i}$

n ímpar $\Rightarrow$ somente o vértice i é fixado por $s_i \Rightarrow s_i \neq s_j$ se $i \neq j$

Seja $s = s_1$ (óbvio que $s^2 = s$)



Se t é um movimento rígido do polígono, então

- $(n,1,2) \mapsto (k-1,k,k+1) \Rightarrow t = r^k$
- $(n,1,2) \mapsto (k+1,k,k-1) \Rightarrow t = r^k s$

Logo D_n é gerado por r, s, já que

$$D_n = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$$

Finalmente, $srs = r^{-1}$ pois (destacando a posição fixada por s)

$$(n-1, n, 1, 2, 3) \overset{s}{\mapsto} (3, 2, 1, n, n-1) \overset{r}{\mapsto} (4, 3, 2, 1, n) \overset{s}{\mapsto} (n, 1, 2, 3, 4)$$

e

$$(n-1, n, 1, 2, 3) \xmapsto{r^{-1}} (n, 1, 2, 3, 4)$$

$\blacksquare$

Exemplo: No quadrado com vértices $1, 2, 3, 4$, temos D_4 com rotações

$$r = (1234), \quad r^2 = (13)(24), \quad r^3 = (1432), \quad r^4 = id$$

e reflexões $s_1 = (24)$, $s_2 = (13)$. Temos ainda as composições $rs_1 = (12)(34)$ e $r^3 s_1 = (14)(23)$. Em particular, $|D_4| = 2.4 = 8$