GRUPOS

Maria Lúcia Torres Villela
Instituto de Matemática
Universidade Federal Fluminense
Revisto em novembro de 2009

Sumário

Introdução

O objetivo deste texto é ser um apoio às disciplinas Álgebra II e Álgebra III do Curso de Graduação em Matemática da Universidade Federal Fluminense, no conteúdo correspondente à estrutura algébrica de Grupos.

Na Parte 1 está o conteúdo básico da Teoria de Grupos, abordado em Álgebra II, disciplina obrigatória comum do Bacharelado e Licenciatura em Matemática. São apresentados o conceito de grupo, subgrupo, grupos finitos, grupos infinitos, grupos abelianos e grupos não-abelianos. Veremos a relação de equivalência módulo H, onde H é um subgrupo do grupo G, o belíssimo Teorema de Lagrange e suas conseqüências aos grupos finitos. Introduziremos os conceitos de ordem de um elemento e de grupo cíclico e veremos o Teorema de estrutura dos grupos cíclicos. Após o conceito de homomorfismo, isomorfismo e automorfismo de grupos, veremos o Teorema de Cayley, motivando o estudo do grupo S_n, grupo das bijeções de um conjunto com n elementos.

Na Parte 2 está o conteúdo mais sofisticado da Teoria de Grupos, abordado em Álgebra III, disciplina obrigatória do Bacharelado em Matemática Pura e optativa da Licenciatura em Matemática e de outras modalidades do Bacharelado em Matemática. O objetivo aqui é estudar o Teorema de Sylow e o conceito de produto direto, que permitem classificar alguns grupos. Começamos com os subgrupos normais, o grupo quociente e o Teorema Fundamental dos Homomorfismos. Apresentamos a equação de classe e aplicações. Após o Teorema de Sylow, são dadas condições necessárias e suficientes para um grupo ser isomorfo a um produto direto, fundamental para classificar grupos, a partir de grupos menos complexos. Concluímos com o estudo de p-grupos abelianos finitos e com o Teorema de estrutura dos grupos abelianos finitos.

Após cada Seção há uma Lista de Exercícios, que complementa a apresentação da teoria e é parte integrante do texto. A resolução dos Exercícios propostos ajuda o aluno a atingir os objetivos propostos nas duas disciplinas.

Bibliografia:

Recomendamos a consulta aos seguintes textos:

- *Elements of Abstract Algebra*, R.A. Dean, Wiley International, 1974.
- *A First Course in Abstract Algebra*, John B. Fraleigh, Addison-Wesley Publishing Company, 1967.

(Esse texto tem uma abordagem ressaltando a importância do conceito de Grupos a outras áreas da Matemática.)

- *Elementos de Álgebra*, Arnaldo Garcia e Yves Lequain, IMPA, 4ª edição, 2006.

- *Introdução à Álgebra*, Adilson Gonçalves, Projeto Euclides, IMPA, 2000.

- *Topics in Algebra*, I. N. Herstein, John Wiley & Sons, 2nd edition, 1975.

- *Algebra*, Thomas W. Hungerford, Springer Verlag, 1974.

Parte 1

Conceitos fundamentais

Introduziremos a estrutura algébrica de grupo, as suas propriedades elementares, grupos finitos, grupos infinitos, grupos abelianos e não-abelianos.

O conceito de subgrupo é muito importante. A congruência módulo H, onde H é um subgrupo do grupo G, permite visualizar G por meio das classes de congruência módulo H. Dessa maneira, quando $|G|$ é finita, obtemos o Teorema de Lagrange, que diz que $|H|$ divide $|G|$.

Introduzimos o conceito de subgrupo gerado por um elemento a, assim como, de ordem de a. Obteremos diversas conseqüências importantes do Teorema de Lagrange, tais como: a ordem de a divide $|G|$, quando $|G| < \infty$, e se $a^m = e$, com $m \neq 0$ e $m \in \mathbb{Z}$, então a ordem de a é finita e divide m.

Veremos o Teorema de estrutura dos grupos cíclicos.

Estudaremos o conceito de homomorfismo de grupos, suas propriedades elementares, assim como, isomorfismo e automorfismo de grupos.

Apresentaremos o Teorema de Cayley, que diz que todo grupo é isomorfo a um subgrupo do grupo de bijeções de um conjunto.

Como conseqüência do Teorema de Cayley, os grupos finitos são isomorfos a um subgrupo de S_n, para algum $n \geq 1$, motivando o estudo mais detalhado do grupo S_n, grupo das bijeções de um conjunto com n elementos. Definiremos r-ciclo, órbita de $\theta \in S_n$, permutação par e permutação ímpar. Mostraremos que todo $\theta \in S_n$ é produto de 2-ciclos.

Vamos apresentar o grupo diedral n, denotado por D_n, com $2n$ elementos, subgrupo importante de S_n, definido como grupo das simetrias do polígono regular de n lados, exemplo de grupo gerado por dois elementos.

Apresentamos muitos exemplos, não esquecendo de classificar alguns tipos especiais de grupos, usando os teoremas elementares abordados.

Os Exercícios ao final de cada Seção complementam a teoria apresentada e são muito importantes para vocês adquirirem habilidade no conteúdo abordado.

O conceito de grupo

Um conjunto não-vazio G está *munido com uma operação* $\star$ se, e somente se, para cada par de elementos de G sabemos associar um único $c \in G$, denotado por $c = a \star b$. Equivalentemente, existe uma função

$$\begin{array}{rcl} \star : G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & a \star b \end{array}$$

Definição 1 (Grupo)
Um conjunto não-vazio G munido de uma operação $\star$ é chamado de *grupo* se, e somente, $\star$ tem as seguintes propriedades:

(i) (Associativa) $a \star (b \star c) = (a \star b) \star c$, para quaisquer $a, b, c \in G$.

(ii) (Existência de elemento neutro) Existe $e \in G$, tal que $a \star e = e \star a = a$, para qualquer $a \in G$.

(iii) (Existência de inverso) Para cada $a \in G$, existe $b \in G$, tal que $a \star b = b \star a = e$.

Denotamos um grupo G com a operação $\star$ por $(G, \star)$.

Exemplo 1
Todo anel é um grupo com a operação de adição do anel. Em particular, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ e $(\mathbb{Z}_n, +_{\mod n})$, para $n \geq 1$, são exemplos de grupos aditivos.

Exemplo 2
Seja A um anel com unidade 1_A. Como a multiplicação de A é associativa, temos que $A^\star = \{a \in A \ ; \ a \text{ é invertível}\}$ é um grupo com a multiplicação de A.

Em particular, $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}\backslash\{0\}, \cdot)$, $(\mathbb{Z}^\star, \cdot) = (\{-1, 1\}, \cdot)$ e $(\mathbb{Z}_n^*, \cdot_{\mod n})$ são exemplos de grupos multiplicativos.

Exemplo 3
Seja $G = \{A \in M_{n\times n}(\mathbb{R}) \ ; \ \det(A) \neq 0\}$ munido com a operação usual de multiplicação de matrizes. Então, $(G, \cdot)$ é um grupo.

Verifique.

Definição 2 (Ordem de um grupo)
A *ordem de um grupo* $(G, \star)$ é denotada por $|G|$ e é o número de elementos do conjunto G. Dizemos que G é um *grupo finito* se, e somente se, o conjunto G é um conjunto finito. Caso contrário, dizemos que G tem *ordem infinita*, escrevemos $|G| = \infty$ e G é dito *grupo infinito*.

Definição 3 (Grupo abeliano)
Dizemos que um $(G, \star)$ é *grupo abeliano* se, e somente se, $a \star b = b \star a$, para quaisquer $a, b \in G$. Caso contrário, dizemos que G é um *grupo não-abeliano*.

Exemplo 4
Para todo $n \geq 1$ o grupo $(\mathbb{Z}_n, +_{\mod n})$ é exemplo de um grupo abeliano com n elementos.

Exemplo 5
Para todo $n \geq 2$ o grupo $(\mathbb{Z}_n^*, \cdot_{\mod n})$ é exemplo de um grupo abeliano com $\phi(n)$ elementos, onde ϕ é a função de Euler definida por

$$\phi(n) = \sharp\{\, j \,;\, 1 \leq j < n \text{ e } \mathrm{mdc}(j, n) = 1\}.$$

Exemplo 6
Seja $n \in \mathbb{N}$, $n \geq 1$. Consideremos $U_n(\mathbb{C}) = \{x \in \mathbb{C} \,;\, x^n - 1 = 0\}$ com a operação de multiplicação de números complexos. $U_n(\mathbb{C})$ é o conjunto das raízes complexas n-ésimas da unidade.

Temos que $U_n(\mathbb{C}) = \{\alpha \in \mathbb{C} \,;\, \alpha^n = 1\}$. Se $\alpha, \beta \in U_n(\mathbb{C})$, então $(\alpha \cdot \beta)^n = \alpha^n \cdot \beta^n = 1 \cdot 1 = 1$, logo $\alpha \cdot \beta \in U_n(\mathbb{C})$ e a multiplicação de $\mathbb{C}$ está fechada em $U_n(\mathbb{C})$. É claro que $1^n = 1$, logo $1 \in U_n(\mathbb{C})$. A igualdade $1 = \alpha^n = \alpha^{n-1} \cdot \alpha$ diz que α^{n-1} é o inverso de α. Como $(\alpha^{n-1})^n = \alpha^{(n-1)\cdot n} = (\alpha^n)^{n-1} = 1^{n-1} = 1$, então $\alpha^{n-1} \in U_n(\mathbb{C})$. A multiplicação sendo associativa e comutativa em $\mathbb{C}$ é associativa e comutativa em qualquer subconjunto de $\mathbb{C}$, em particular, é associativa e comutativa em $U_n(\mathbb{C})$. Logo, $U_n(\mathbb{C})$ é um grupo abeliano com a multiplicação de $\mathbb{C}$.

Tomando $\omega = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$, sabemos que

$$U_n(\mathbb{C}) = \{\omega^j \,;\, j = 0, \ldots, n-1\}.$$

Então, $|U_n(\mathbb{C})| = n$ e $(U_n(\mathbb{C}), \cdot)$ é um grupo abeliano de ordem n.

Exemplo 7
O grupo do Exemplo 3 é um grupo não-abeliano de ordem infinita.

Exemplo 8
Seja C um conjunto não-vazio. Definimos

$$S_C = \{\sigma : C \longrightarrow C \,;\, \sigma \text{ é uma função bijetora }\},$$

com a operação usual de composição de funções. Vale que:
(i) a composição de bijeções é uma bijeção;

(ii) a composição de funções é associativa;

(iii) a função $I : C \longrightarrow C$ definida por $I(c) = c$, para cada $c \in C$, é o elemento neutro de S_C, pois $I \circ \sigma = \sigma \circ I = \sigma$, para todo $\sigma \in S_C$.

(iv) Se $\sigma \in S_C$, então a função $\tau : C \longrightarrow C$ definida por

$$\tau(c) = d \Longleftrightarrow \sigma(d) = c$$

tem a propriedade de $\tau \circ \sigma = I$ e $\sigma \circ \tau = I$. Logo, $\tau = \sigma^{-1}$.

Portanto, $(S_C, \circ)$ é um grupo.

Proposição 1 (Propriedades elementares)
Seja $(G, \star)$ um grupo. Valem as seguintes propriedades:

(i) O elemento neutro é único.

(ii) O inverso de cada elemento de G é único.

Demonstração:

(i) Sejam e, e' elementos neutros de G. Então,

$$e' \overset{(1)}{=} e \star e' \overset{(2)}{=} e.$$

Em (1) usamos que e é elemento neutro e, em (2), que e' é elemento neutro.

(ii) Sejam $b, c \in G$ inversos de $a \in G$.

Então, $e = c \star a = a \star c$ e $e = b \star a = a \star b$. Logo,

$$b = e \star b = (c \star a) \star b \overset{(3)}{=} c \star (a \star b) = c \star e = c. \quad \blacksquare$$

A igualdade (3) segue da associatividade da operação de G.

Na notação multiplicativa, denotamos o inverso de a por a^{-1} e, na notação aditiva, denotamos o inverso de a por $-a$. Nesse último caso, costumamos chamar $-a$ de *simétrico* de a.

Quando fazemos a teoria geral dos grupos, escrevemos na notação multiplicativa. Daqui por diante, por simplicidade, denotaremos na teoria um grupo por $(G, \cdot)$.

Proposição 2 (Propriedades adicionais)
Seja $(G, \cdot)$ um grupo. Sejam $a, b \in G$. Então,

(i) $\left(a^{-1}\right)^{-1} = a$.

(ii) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Demonstração:

(i) Da unicidade do inverso e da igualdade

$$a \cdot a^{-1} = a^{-1} \cdot a = e,$$

segue que a^{-1} é o inverso de a, assim como, a é o inverso de a^{-1}, isto é, $a = \left(a^{-1}\right)^{-1}$.

(ii) Temos que

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e.$$

Analogamente, obtemos $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$. Portanto, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

■

Exemplo 9

Seja $C = \{1, 2, \ldots, n\}$. O grupo S_C das bijeções de C é denotado por S_n e é chamado de *grupo simétrico de grau n* .

Seja $C = \{1, \ldots, n\}$ e $\sigma : C \longrightarrow C$ uma bijeção.

Como σ é sobrejetora, para cada $j_k \in C$, existe $k \in C$ tal que $j_k = \sigma(k)$ e k é único, pois σ é injetora. Assim,

$$\{\sigma(1) = j_1, \sigma(2) = j_2, \ldots, \sigma(n) = j_n\} = \{1, 2, \ldots, n\}.$$

Logo, de maneira natural, cada bijeção $\sigma : C \longrightarrow C$ induz uma permutação dos elementos de C.

$$\underline{1} \quad \underline{2} \quad \ldots \quad \underline{n} \quad \overset{\sigma}{\longmapsto} \quad \underline{j_1} \quad \underline{j_2} \quad \ldots \quad \underline{j_n}$$

onde $j_k = \sigma(k)$.

Exemplo 10

Seja $\sigma : \{1, 2, 3\} \longmapsto \{1, 2, 3\}$ definida por $\sigma(1) = 2$, $\sigma(2) = 3$ e $\sigma(3) = 1$. Então,

$$\underline{1} \quad \underline{2} \quad \underline{3} \quad \overset{\sigma}{\longmapsto} \quad \underline{2} \quad \underline{3} \quad \underline{1}$$

Cada permutação $\underline{j_1} \quad \underline{j_2} \quad \ldots \quad \underline{j_n}$ de $\underline{1} \quad \underline{2} \quad \ldots \quad \underline{n}$ define uma bijeção $\sigma : C \longrightarrow C$, onde $C = \{1, 2, \ldots, n\}$, por $\sigma(1) = j_1$, $\sigma(2) = j_2$, $\ldots$, $\sigma(n) = j_n$.

Exemplo 11

$\underline{2} \quad \underline{3} \quad \underline{4} \quad \underline{1}$ é uma permutação de $\underline{1} \quad \underline{2} \quad \underline{3} \quad \underline{4}$. Seja $C = \{1, 2, 3, 4\}$.

Definimos a bijeção $\sigma : C \longrightarrow C$, por $\sigma(1) = 2 = j_1$, $\sigma(2) = 3 = j_2$, $\sigma(3) = 4 = j_3$ e $\sigma(4) = 1 = j_4$.

Portanto, o conjunto das bijeções de $C = \{1, 2, \ldots, n\}$ está em bijeção com o conjunto das permutações de $\underline{1} \quad \underline{2} \quad \ldots \quad \underline{n}$, justificando a seguinte definição.

Definição 4 (Permutação)
Seja $C = \{1, \ldots, n\}$. Toda bijeção $\sigma : C \longrightarrow C$ é chamada uma *permutação* de C. O grupo $S_n = \{\sigma : C \longrightarrow C \; ; \; \sigma \text{ é uma bijeção } \}$ também é chamado de *grupo das permutações de* n elementos.

Como há $n!$ permutações de n elementos e o conjunto das permutações de n elementos está em bijeção com S_n, portanto a ordem de S_n é $|S_n| = n!$.
A bijeção $\sigma \in S_n$ definida por

$$\begin{array}{rcl} 1 & \mapsto & \sigma(1) \\ 2 & \mapsto & \sigma(2) \\ & \vdots & \\ n & \mapsto & \sigma(n) \end{array} \quad \text{é representada por } \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

O elemento neutro de S_n é a bijeção $I = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$.

Se $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ e $\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}$, então

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

Por exemplo, sejam

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

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

Observamos que dado $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$, trocando a primeira linha (domínio de σ) com a segunda (as correspondentes imagens por σ), temos que $\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$. Depois, caso necessário, permutamos as colunas, reenumerando a primeira linha como $1, 2, \ldots, n$. Por exemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \Longrightarrow \sigma^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Exemplo 12
S_2 tem 2 elementos, a saber, $I = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ e $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.
Observamos que $\sigma^2 = \sigma \circ \sigma = I$.

Exemplo 13
O grupo S_3 tem 6 elementos, as bijecões:

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Verifique as relações ao lado.

Observamos que S_3 pode ser descrito usando apenas as bijeções σ e τ, pois $f_4 = \tau^2$, $f_6 = \sigma \circ \tau$ e $f_5 = \sigma \circ \tau^2$. Temos que $\sigma^2 = I$, $\tau^3 = I$. Também, $(\sigma \circ \tau)^2 = I$ e $(\sigma \circ \tau^2)^2 = I$. Como $\tau \circ \sigma = \sigma \circ \tau^2$, vemos que S_3 é um grupo não-abeliano.

Assim,
$S_3 = \{\sigma^i \circ \tau^j \ ; \ \sigma^2 = I, \tau^3 = I, \tau \circ \sigma = \sigma \circ \tau^2;$ com $i = 0, 1$ e $j = 0, 1, 2\}$.

Proposição 3
Para todo $n \geq 3$, S_n é um grupo não-abeliano.

Demonstração: Seja $n \geq 3$ e seja $S = \{1, 2, \ldots, n\}$. Basta exibir duas bijeções do conjunto S, tais que $\sigma \circ \tau \neq \tau \circ \sigma$. Sejam σ e τ definidas por:

$\sigma(1) = 2$, $\sigma(2) = 1$ e $\sigma(x) = x$, para todo $x \geq 3$;

$\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 2$ e $\tau(x) = x$, para todo $x \geq 4$.

Então, $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(1) = 2$ e $(\tau \circ \sigma)(1) = \tau(\sigma(1)) = \tau(2) = 3$, mostrando que $\sigma \circ \tau \neq \tau \circ \sigma$. ■

Definição 5 (Subgrupo)
Um subconjunto não-vazio H de um grupo $(G, \cdot)$ é chamado de *subgrupo* de G se, e somente se, H é um grupo com a operação de G.

Quais propriedades H deve ter para ser um subgrupo do grupo G? A resposta está na seguinte Proposição.

Proposição 4
Um subconjunto não-vazio H de um grupo $(G, \cdot)$ é um *subgrupo* se, e somente se,

(i) $e_G \in H$;

(ii) se $a, b \in H$, então $a \cdot b \in H$;

(iii) se $a \in H$, então $a^{-1} \in H$.

Demonstração: Suponhamos que $H \subset G$ seja um subgrupo de G. Então, por definição de subgrupo, a operação de G está fechada em H, valendo (ii) e (iii). Como $H \neq \emptyset$, existe $c \in H$. Então, de (iii) $c^{-1} \in H$ e de (ii) $e_G = c \cdot c^{-1} \in H$, valendo (i). Reciprocamente, suponhamos que $H \subset G$ seja um subconjunto que tenha as propriedades (i), (ii) e (iii) do enunciado. De (i) segue que $H \neq \emptyset$. De (ii) segue que H está munido com a operação de G e de (iii) a existência de inverso em H de cada elemento de H. Para mostrar que H é um grupo, basta observar que a operação sendo associativa em G é associativa em qualquer subconjunto, em particular, é associativa em H. ■

Exemplo 14

Seja $(G, \cdot)$ um grupo.

Então, $\{e\}$ e G são subgrupos de G, chamados de subgrupos triviais.

Exemplo 15

$(\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Q}, +)$.

$(\mathbb{Q}, +)$ é subgrupo de $(\mathbb{R}, +)$.

$(\mathbb{R}, +)$ é subgrupo de $(\mathbb{C}, +)$.

$(\{-1, 1\}, \cdot)$ é subgrupo de $(\mathbb{Q}^\star, \cdot)$.

$(\mathbb{Q}^\star, \cdot)$ é subgrupo de $(\mathbb{R}^\star, \cdot)$.

$(\mathbb{R}^\star, \cdot)$ é subgrupo de $(\mathbb{C}^\star, \cdot)$.

Exemplo 16

Consideremos o grupo multiplicativo $(\mathbb{C}^\star, \cdot)$.

Seja $S^1 = \{z = a + bi \in \mathbb{C} \,;\, a^2 + b^2 = 1\}$.

Então, S^1 é um subgrupo de $\mathbb{C}^\star$. De fato,

(i) Tomando $a = 1$ e $b = 0$, temos $1 \in S^1$.

(ii) Se $z = a + bi \in S^1$ e $w = c + di \in S^1$, então $a^2 + b^2 = 1$, $c^2 + d^2 = 1$ e

$$z \cdot w = (a + bi) \cdot (c + di) = ac - bd + (ad + bc)i, \text{ com}$$

$$\begin{aligned}(ac-bd)^2+(ad+bc)^2 &= a^2c^2-2acbd+b^2d^2+a^2d^2+2adbc+b^2c^2\\ &= a^2c^2+b^2d^2+a^2d^2+b^2c^2\\ &= a^2(c^2+d^2)+b^2(d^2+c^2)\\ &= (a^2+b^2)\cdot(c^2+d^2)\\ &= 1\cdot 1\\ &= 1\end{aligned}$$

$c^2+d^2=1$ e $a^2+b^2=1$.

Logo, $z\cdot w\in S^1$.

(iii) Se $z=a+bi\in S^1$, então

$$z^{-1}\overset{(1)}{=}\frac{1}{a+bi}=\frac{a-bi}{a^2+b^2}=a-bi \text{ e } a^2+(-b)^2=a^2+b^2=1,$$

Como $z\neq 0$, em (1) calculamos o seu inverso em $\mathbb{C}$.

mostrando que $z^{-1}\in S^1$.

Exemplo 17

O conjunto $G=\{A\in M_{2\times 2}(\mathbb{R})\ ;\ \det(A)\neq 0\}$, com a operação de multiplicação usual de matrizes, é um grupo.

Seja $H=\{A\in M_{2\times 2}(\mathbb{Z})\ ;\ \det(A)\in\{-1,1\}\}$. Então, H é um subgrupo de G.

De fato, $\begin{pmatrix}1&0\\0&1\end{pmatrix}\in H$. Se $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ e $B=\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}$ estão em H, então $A\cdot B=\begin{pmatrix}aa'+bc'&ab'+bd'\\ca'+dc'&cb'+dd'\end{pmatrix}\in H$, pois a soma de produtos de números inteiros é um número inteiro e $\det(A\cdot B)=\det(A)\cdot\det(B)\in\{1,-1\}$.

Se $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in H$, então em G temos

$$A^{-1}=\frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$$

Agora, $A^{-1}\in H$, pois $ad-bc=\det(A)\in\{-1,1\}$ nos dá que $\dfrac{d}{ad-bc}$, $\dfrac{-b}{ad-bc}$, $\dfrac{-c}{ad-bc}$ e $\dfrac{a}{ad-bc}$ estão em $\mathbb{Z}$.

Definição 6

Seja $(G,\cdot)$ um grupo. Sejam $a\in G$ e $n\in\mathbb{Z}$. Definimos

$$a^n=\begin{cases}\underbrace{a\cdot a\cdot\ldots\cdot a}_{n\text{ fatores}}, & \text{se } n\geq 1\\ e_G, & \text{se } n=0\\ \underbrace{a^{-1}\cdot a^{-1}\cdot\ldots\cdot a^{-1}}_{-n\text{ fatores}}, & \text{se } n\leq -1\end{cases}$$

Na notação aditiva, definimos

$$na = \begin{cases} \underbrace{a + a + \ldots + a}_{n \text{ parcelas}}, \text{ se } n \geq 1 \\ 0, \text{ se } n = 0 \\ \underbrace{(-a) + (-a) + \ldots + (-a)}_{-n \text{ parcelas}}, \text{ se } n \leq -1 \end{cases}$$

Proposição 5

Sejam $(G, \cdot)$ um grupo e $a \in G$. Valem as seguintes propriedades:

(i) $a^n \cdot a^m = a^{n+m}$, para quaisquer $n, m \in \mathbb{Z}$.

(ii) $(a^n)^m = a^{nm}$, para quaisquer $n, m \in \mathbb{Z}$;

Demonstração:

(i) Seja $n \in \mathbb{Z}$. Faremos indução sobre $m \geq 0$. Temos que $a^{n+0} = a^n = a^n \cdot e = a^n \cdot a^0$.

Seja $m \geq 0$ e suponhamos que $a^n \cdot a^m = a^{n+m}$. Então,

$$a^n \cdot a^{m+1} \overset{(1)}{=} a^n \cdot (a^m \cdot a) \overset{(2)}{=} (a^n \cdot a^m) \cdot a \overset{(3)}{=} a^{n+m} \cdot a \overset{(4)}{=} a^{(n+m)+1} \overset{(5)}{=} a^{n+(m+1)}.$$

Em (1) usamos a definição da potência $m+1$; em (2), a associatividade da operação de G; em (3), a hipótese de indução; em (4), a definição da potência $(n+m)+1$ e em (5), a associatividade da adição de inteiros.

Para concluir a demonstração, observamos, primeiramente, que, para todo $n \in \mathbb{Z}$, segue da definição de potência que $(a^{-1})^n = a^{-n}$. Seja agora $m < 0$. Então, $-m > 0$

$$a^{n+m} \overset{(6)}{=} (a^{-1})^{-(n+m)} \overset{(7)}{=} (a^{-1})^{-n+(-m)} \overset{(8)}{=} (a^{-1})^{-n} \cdot (a^{-1})^{-m} \overset{(9)}{=} a^n \cdot a^m.$$

Em (6) e (9) usamos a observação acima; em (7) propriedade dos inteiros e em (8), o caso já demonstrado.

(ii) Seja $n \in \mathbb{Z}$. A demonstração será por indução sobre $m \geq 0$. Se $m = 0$, então $(a^n)^0 = e = a^{n \cdot 0}$. Seja $m \geq 0$ tal que $(a^n)^m = a^{nm}$. Então,

$$(a^n)^{m+1} \overset{(10)}{=} (a^n)^m \cdot a^n \overset{(11)}{=} a^{nm} \cdot a^n \overset{(12)}{=} a^{nm+n} \overset{(13)}{=} a^{n(m+1)}.$$

Em (10) usamos a definição de potência $m+1$; em (11), a hipótese de indução; em (12), o item (i) e em (13), a distributividade em $\mathbb{Z}$.

Se $m < 0$, então $-m > 0$ e

$$(a^n)^m \overset{(14)}{=} ((a^n)^{-1})^{-m} \overset{(15)}{=} (a^{-n})^{-m} \overset{(16)}{=} a^{(-n)(-m)} \overset{(17)}{=} a^{nm}. \qquad \blacksquare$$

Em (14) usamos que $b^m = (b^{-1})^{-m}$; em (15), o item (i); em (16), o caso já demonstrado do item (ii) e em (17), propriedade de números inteiros.

Definição 7 (Subgrupo gerado por um elemento)

Sejam $(G, \cdot)$ um grupo e $a \in G$. O conjunto

$$\langle a \rangle = \{a^n \,;\, n \in \mathbb{Z}\}$$

é um subgrupo de G, chamado de *subgrupo gerado por* a.

De fato, $e = a^0 \in \langle a \rangle$, o inverso de a^n é $a^{-n} \in \langle a \rangle$ e, além disso, temos $a^n \cdot a^m = a^{n+m} \in \langle a \rangle$.

Definição 8 (Ordem de um elemento)
Seja $(G, \cdot)$ um grupo. Quando $\langle a \rangle$ é um grupo finito, chamamos $|\langle a \rangle|$ de *ordem* de a e escrevemos $\circ(a) = |\langle a \rangle|$. Quando $\langle a \rangle$ é um grupo infinito, dizemos que a *ordem de* a é *infinita* e escrevemos $\circ(a) = \infty$.

Observação: Na notação aditiva o subgrupo gerado por a é

$$\langle a \rangle = \{na \ ; \ n \in \mathbb{Z}\}.$$

Exemplo 18
O subgrupo de S_3 gerado por τ é

$$\langle \tau \rangle = \{\tau^n \ ; \ n \in \mathbb{Z}\} = \{I, \tau, \tau^2\}.$$

De fato, $\tau^3 = I$ e, para cada $n \in \mathbb{Z}$, pela divisão euclidiana de n por 3, existem $q, r \in \mathbb{Z}$ unicamente determinados tais que $n = 3q+r$, com $0 \leq r \leq 2$. Então, $\tau^n = \tau^{3q+r} = \tau^{3q} \circ \tau^r = (\tau^3)^q \circ \tau^r = I^q \circ \tau^r = I \circ \tau^r = \tau^r$, onde $r = 0, 1, 2$.

Nesse caso, $\circ(\tau) = 3$.

Exemplo 19
O subgrupo de $\mathbb{Q}^\star$ gerado por 2 é

$$\langle 2 \rangle = \{2^n \ ; \ n \in \mathbb{Z}\} = \{\ldots, \tfrac{1}{8}, \tfrac{1}{4}, \tfrac{1}{2}, 1, 2, 4, 8, \ldots\}.$$

Nesse caso, $\circ(2) = \infty$.

Exemplo 20
O subgrupo de $\mathbb{Z}$ gerado por 2 é

$$\langle 2 \rangle = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}.$$

Nesse caso, $\circ(2) = \infty$.

Proposição 6
Seja H um subgrupo de $(\mathbb{Z}, +)$. Então, existe $n \geq 0$, tal que $H = n\mathbb{Z} = \langle n \rangle$.

Demonstração: Se $H = \{0\}$, então $H = \langle 0 \rangle$. Seja $H \neq \{0\}$ um subgrupo de $\mathbb{Z}$. Consideremos $S = \{x \in H \ ; \ x > 0\}$. Como $H \neq \{0\}$, existe $a \neq 0$, tal que $a \in H$. Então, $-a \in H$ e a ou $-a$ é positivo. Logo, $S \neq \emptyset$.

Como S é um subconjunto dos inteiros limitado inferiormente, pelo Princípio da Boa Ordenação, tem menor elemento, digamos $n > 0$. Afirmamos que $H = \langle n \rangle$. De fato, como $n \in S \subset H$, então $\langle n \rangle \subset H$. Seja $m \in H$. Pela divisão euclidiana de m por n, existem $q, r \in \mathbb{Z}$ tais que $m = qn + r$, com $0 \leq r < n$. Como $r = m - qn \in H$, se $r > 0$, então $r \in S$, com $r < n$, contradizendo a escolha de n. Portanto, $r = 0$, concluímos que $m = qn \in n\mathbb{Z}$ e $H \subset n\mathbb{Z} = \langle n \rangle$. ■

Exercícios

1. Mostre que se a, b, c são elementos de um grupo $(G, \cdot)$, então valem as seguintes propriedades:

   (a) cancelamento à direita: $a \cdot c = b \cdot c \Longrightarrow a = b$.

   (b) cancelamento à esquerda: $c \cdot a = c \cdot b \Longrightarrow a = b$.

   (c) a equação $x \cdot a = b$ tem uma única solução em G.

   (d) a equação $a \cdot x = b$ tem uma única solução em G.

2. Sejam $(G, \star_1)$ e $(G', \star_2)$ grupos.

   (a) Mostre que $G \times G' = \{(x, x') \ ; \ x \in G, x' \in G'\}$ é um grupo com a operação $\star$ definida por

   $$(x, x') \star (y, y') := (x \star_1 y, x' \star_2 y'),$$

   para quaisquer $x, y \in G$ e $x', y' \in G'$.

   (b) Mostre que se H é um subgrupo de G e H' é um subgrupo de G', então $H \times H'$ é um subgrupo de $G \times G'$.

   (c) Dê exemplos de grupos G, G' tais que $G \times G'$ seja abeliano.

   (d) Dê exemplos de grupos G, G' tais que $G \times G'$ seja não-abeliano.

3. Sejam $\sigma, \tau \in S_4$ dadas por $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ e $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

   Determine: $\sigma \circ \tau$, $\tau \circ \sigma$, $\sigma^3 \circ \tau^2$, σ^{-1}, τ^{-3}, $\sigma \circ \tau \circ \sigma^{-1}$, σ^{527}, τ^{1001}.

4. Sejam $(G, \cdot)$ um grupo e H, K subgrupos de G. Mostre que:

   (a) $H \cap K$ é um subgrupo de G.

(b) $H \cup K$ é um subgrupo de G se, e somente se, $H \subset K$ ou $K \subset H$.

5. Sejam $a, b \in \mathbb{R}$, com $a \neq 0$. Definimos

$$\begin{aligned} \sigma_{a,b} : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto ax + b \end{aligned}$$

Seja $G = \{\sigma_{a,b} \; ; \; a, b \in \mathbb{R}, a \neq 0\}$.

(a) Mostre que $(G, \circ)$ é um grupo, onde $\circ$ é a composição de funções.

(b) Seja $N = \{\sigma_{1,b} \; ; \; b \in \mathbb{R}\}$.
Mostre que N é um subgrupo de G.

(c) Mostre que para todo $\tau = \sigma_{a,b} \in G$, $\tau \circ N \circ \tau^{-1} \subset N$.

6. Sejam $(G, \cdot)$ um grupo e H um subgrupo de G.

(a) Fixe $a \in G$.
Mostre que $aHa^{-1} = \{ \, a \cdot h \cdot a^{-1} \; ; \; h \in H \, \}$ é um subgrupo de G.

$N(H)$ é chamado de *normalizador de* H.

(b) Seja $N(H) = \{ \, x \in G \; ; \; xHx^{-1} = H \, \}$.
Mostre $N(H)$ é um subgrupo de G e $H \subset N(H)$.

7. Seja $(G, \cdot)$ um grupo e fixe $a \in G$.

Seja $N(a) = \{x \in G \; ; \; a \cdot x = x \cdot a \, \}$.

$N(a)$ é chamado de *normalizador de* a.

Mostre que $N(a)$ é um subgrupo de G.

8. Seja $(G, \cdot)$ um grupo.

$Z(G)$ é chamado de *centro de* G.

(a) Seja $Z(G) = \{ \, x \in G \; ; \; g \cdot x = x \cdot g \;$ para todo $\; g \in G \, \}$.
Mostre que $Z(G)$ é um subgrupo de G.

(b) Mostre que para todo $a \in G$, $Z(G)$ é um subgrupo de $N(a)$.

(c) Mostre que G é abeliano se, e somente se, $Z(G) = G$.

(d) Mostre que $a \in Z(G)$ se, e somente se, $N(a) = G$.

9. Seja $G = S_3$ o grupo das bijeções do conjunto com três elementos.

Sejam $\sigma, \tau \in S_3$ dadas por $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ e $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

(a) Mostre que

$$\begin{aligned} S_3 &= \{I, \sigma, \tau, \tau^2, \sigma\circ\tau, \sigma\circ\tau^2\} \\ &= \{\sigma^r\circ\tau^s \ ; \ r = 0,1; s = 0,1,2; \sigma^2 = I, \tau^3 = I, \tau\circ\sigma = \sigma\circ\tau^2\}. \end{aligned}$$

(b) Mostre que os subgrupos não-triviais de S_3 são $\{I, \sigma\}$, $\{I, \sigma\circ\tau\}$, $\{I, \sigma\circ\tau^2\}$ e $\{I, \tau, \tau^2\}$.

(c) Determine os normalizadores $N(\tau)$ e $N(\sigma)$.

(d) Determine o centro $Z(S_3)$.

10. Mostre que $\{I, \sigma, \tau, \xi\}$ é um subgrupo de S_4, onde $I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ e $\xi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

11. Determine o subgrupo de S_4 gerado por $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

12. Liste todos os elementos de S_4.

13. Seja $G = \{ A \in M_{2\times 2}(\mathbb{R}) \ ; \ \det(A) \neq 0 \}$.

(a) Mostre que G é um grupo com a multiplicação usual de matrizes.

(b) Seja $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ ; \ a, b, c, d \in \mathbb{Q} \text{ e } ad - bc \neq 0 \right\}$.
Mostre que H é um subgrupo de G.

(c) Seja $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \ ; \ a^2 + b^2 \neq 0, \ a, b \in \mathbb{R} \right\}$.
Mostre que K é um subgrupo de G.

14. Seja $(G, \cdot)$ um grupo e H um subconjunto finito de G. Mostre que se H é fechado para a operação de G, então H é um subgrupo de G.

15. Seja $(G, \cdot)$ um grupo tal que para todo $x \in G$ temos $x^2 = e_G$. Mostre que G é abeliano.

16. Seja $G' = \{(a, b) \ ; \ a, b \in \mathbb{R} \text{ e } a \neq 0\}$.

Definimos $(a, b)\cdot(c, d) = (ac, ad+b)$, para quaisquer $(a, b), (c, d) \in G'$.

(a) Mostre que $(G', \cdot)$ é um grupo.

(b) Mostre que $N' = \{(1, b) \ ; \ b \in \mathbb{R}\}$ é um subgrupo de G'.

17. Seja $\mathbb{R}^+ = \{x \in \mathbb{R} \,;\, x > 0\}$.

    (a) Mostre que $(\mathbb{R}^+, \cdot)$ é um grupo.

    (b) Mostre que $H = \{3^x \,;\, x \in \mathbb{R}\}$ é um subgrupo de $(\mathbb{R}^+, \cdot)$.

    (c) Mostre que $K = \{\log x \,;\, x \in \mathbb{R}^+\}$ é um subgrupo de $(\mathbb{R}, +)$.

D_4 é o grupo das simetrias do quadrado e é chamado de grupo diedral 4. Esse é um dos dois grupos não-abelianos com 8 elementos.

18. Seja $D_4 = \{I, R, R^2, R^3, S, SR, SR^2, SR^3\} \subset S_4$, onde

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

    (a) Mostre que $S^2 = I$, $R^4 = I$ e $RS = SR^3$.

    (b) Mostre que D_4 é um subgrupo de S_4.

Teorema de Lagrange e aplicações

Seja $(G, \cdot)$ um grupo e H um subgrupo de G. Quando a ordem de G é finita, então a ordem de H é finita e Lagrange mostrou que $|H|$ divide $|G|$. Para isto, é necessário um novo conceito. Vamos definir uma relação de equivalência em G de modo a visualizar o grupo por meio de suas classes de equivalência.

Definição 9 (Congruência módulo H)
Sejam $(G, \cdot)$ um grupo e H um subgrupo de G. Dados $a, b \in H$ dizemos que a é *congruente a* b *módulo* H se, e somente se, $a \cdot b^{-1} \in H$. Nesse caso, escrevemos $a \equiv b \mod H$. Caso contrário, dizemos que a *não é congruente a* $b \mod H$ e escrevemos $a \not\equiv b \mod H$. Chamamos esta relação binária em G de *congruência módulo* H.

Exemplo 21
Consideremos o grupo $(\mathbb{Z}, +)$ e o subgrupo $H = n\mathbb{Z}$, onde $n \geq 1$. Sejam $a, b \in \mathbb{Z}$. Então,

$$a \equiv b \mod n\mathbb{Z} \iff a - b \in n\mathbb{Z} \iff n \mid (a - b) \iff a \equiv b \mod n.$$

Portanto, a congruência $\mod n\mathbb{Z}$ é a congruência módulo n.

Proposição 7
Sejam $(G, \cdot)$ um grupo e H um subgrupo de G. A congruência módulo H é uma relação de equivalência em G.

Demonstração: Para todo $a \in G$, $a \cdot a^{-1} = e \in H$, logo $a \equiv a \mod H$ e a relação é reflexiva. Dados $a, b \in G$, tais que $a \equiv b \mod H$, então $a \cdot b^{-1} \in H$, logo $b \cdot a^{-1} = (a \cdot b^{-1})^{-1} \in H$, que é equivalente a $b \equiv a \mod H$ e a congruência módulo H é simétrica. Finalmente, sejam $a, b, c \in G$, tais que $a \equiv b \mod H$ e $b \equiv c \mod H$. Então, $a \cdot b^{-1} \in H$ e $b \cdot c^{-1} \in H$, logo $a \cdot c^{-1} = a \cdot (b^{-1} \cdot b) \cdot c^{-1} = (a \cdot b^{-1}) \cdot (b \cdot c^{-1}) \in H$, assim $a \equiv c \mod H$, mostrando que a congruência módulo H é transitiva. ■

Sejam $(G, \cdot)$ um grupo e H um subgrupo de G. Para visualizar G por meio das suas classes de equivalência precisamos entender quem é a classe de congruência módulo H de cada elemento $a \in G$.

Para cada $a \in G$ a *classe de congruência módulo* H de a é

$$\begin{aligned}\overline{a} &= \{x \in G\ ;\ x \equiv a \mod H\}\\ &= \{x \in G\ ;\ x \cdot a^{-1} \in H\}\\ &= \{x \in G\ ;\ x \cdot a^{-1} = h \in H\}\\ &= \{x \in G\ ;\ x = h \cdot a, \text{ para algum } h \in H\}\\ &= \{h \cdot a\ ;\ h \in H\}\\ &= H \cdot a.\end{aligned}$$

$H \cdot a$ é chamada de *classe à direita* de H em G.

Das propriedades de uma relação de equivalência em um conjunto, temos:

$a \equiv b \mod H$ se, e somente se, $a \cdot b^{-1} \in H$.

(i) $H \cdot a = H \cdot b$ se, e somente se, $a \cdot b^{-1} \in H$.

(ii) Se $(H \cdot a) \cap (H \cdot b) \neq \emptyset$, então $H \cdot a = H \cdot b$.

(iii) $G = \bigcup_{x \in G} H \cdot x$.

Segue da propriedade (ii) que se $H \cdot a \neq H \cdot b$, então $(H \cdot a) \cap (H \cdot b) = \emptyset$. Portanto, a união em (iii) é disjunta, se tomamos um único representante em cada classe de congruência.

Exemplo 22

As classes de congruência módulo $n\mathbb{Z}$ em $\mathbb{Z}$ são as classes residuais módulo n, para $n \geq 1$.

De fato, dado $a \in \mathbb{Z}$, pela divisão euclidiana de a por n, existem $q, r \in \mathbb{Z}$, unicamente determinados tais que $a = q \cdot n + r$, com $0 \leq r \leq n - 1$. Então,

$$\begin{aligned}\overline{a} &= \{x \in \mathbb{Z}\ ;\ x \equiv a \mod n\mathbb{Z}\}\\ &= \{x \in \mathbb{Z}\ ;\ x - a \in n\mathbb{Z}\}\\ &= \{x \in \mathbb{Z}\ ;\ x - a = ny, \text{ para algum } y \in \mathbb{Z}\}\\ &= \{x \in \mathbb{Z}\ ;\ x = ny + a, \text{ para algum } y \in \mathbb{Z}\}\\ &= n\mathbb{Z} + a\\ &= n\mathbb{Z} + nq + r\\ &= n\mathbb{Z} + r\end{aligned}$$

Há n classes de congruência módulo $n\mathbb{Z}$ distintas, a saber,

$$n\mathbb{Z},\ n\mathbb{Z} + 1,\ \ldots,\ n\mathbb{Z} + (n-1).$$

Definição 10

Sejam $(G, \cdot)$ um grupo e H um subgrupo de G. O número de classes à direita de H em G é chamada de *índice de* H em G e é denotado por $(G : H)$.

Exemplo 23
Consideremos o grupo $(\mathbb{Z}, +)$ e o subgrupo $H = n\mathbb{Z}$, onde $n \geq 1$. Então, $(\mathbb{Z} : n\mathbb{Z}) = n$.

Teorema 1 (Lagrange)
Se $(G, \cdot)$ é um grupo finito e H é um subgrupo de G, então $|H|$ divide $|G|$. Nesse caso, $(G : H) = \frac{|G|}{|H|}$.

Demonstração: É claro que $|H| \leq |G|$. Primeiramente, vamos mostrar que todas as classes de congruência módulo H têm o mesmo número de elementos que H. Para isso, para cada $a \in G$ consideremos a função

$$\begin{array}{rcl} \varphi : H & \longrightarrow & H \cdot a \\ h & \longmapsto & h \cdot a \end{array}$$

φ é injetora, pois

$$\varphi(h) = \varphi(h') \Longleftrightarrow h \cdot a = h' \cdot a \Longleftrightarrow h = h'.$$

Multiplicamos à direita da penúltima igualdade por a^{-1}.

φ é sobrejetora, pois todo elemento de Ha é da forma $ha = \varphi(h)$, para algum $h \in H$. Portanto, $|H| = |H \cdot a|$. É claro que só há um número finito de classes de congruência de H em G, isto é, $(G : H) < \infty$.

Como $G = \bigcup_{x \in G} H \cdot x$ e esta união é disjunta nas classes distintas, obtemos:

$$|G| = \sum |H \cdot x|,$$

onde a soma é feita tomando apenas um representante em cada classe.

Como $|H \cdot x| = |H|$, para cada $x \in G$, se $\ell = (G : H)$ é o número de classes distintas então,

$$|G| = \ell \cdot |H|.$$

Nesse caso, $|G| = (G : H)|H|$, seguindo que $(G : H) = \frac{|G|}{|H|}$. ■

Exemplo 24
O grupo S_3 tem 6 elementos. Um subgrupo H de S_3, pelo Teorema de Lagrange, só pode ter $|H| \in \{1, 2, 3\}$, que são os divisores de 6.

O único subgrupo de ordem 1 é $\{I\}$.

Os subgrupos de ordem 2 são: $\langle \sigma \rangle = \{I, \sigma\}$, $\langle \sigma \circ \tau \rangle = \{I, \sigma \circ \tau\}$ e $\langle \sigma \circ \tau^2 \rangle = \{I, \sigma \circ \tau^2\}$.

O único subgrupo de ordem 3 é $\langle \tau \rangle = \{I, \tau, \tau^2\} = \langle \tau^2 \rangle$.

Observação: Dados um grupo $(G, \cdot)$ e um subgrupo H de G, podemos definir em G uma outra relação de equivalência, a saber, se $a, b \in G$ dizemos que a é *congruente (à esquerda) a* b *módulo* H se, e somente se, $a^{-1} \cdot b \in H$. Nesse caso, a classe de $a \in G$ é $a \cdot H$ e é chamada uma *classe à esquerda de* H em G. Quando G é finito, $|a \cdot H| = |H|$ e o número de classes à esquerda de H em G coincide com o número de classes à direita de H em G.

Um subgrupo H de G tal que $a \cdot H = H \cdot a$, para cada $a \in G$, é chamado de *subgrupo normal*. O subgrupo normal é importante para a construção do *grupo quociente* G/H (veja na Parte 2).

Quando o grupo é abeliano, toda classe à direita é uma classe à esquerda. Nesse texto só usaremos classes à direita.

Proposição 8
Seja $(G, \cdot)$ um grupo e seja $a \in G$.

(i) $\langle a \rangle$ é finito se, e somente se, existe $m \geq 1$, tal que $a^m = e$.

(ii) Nesse caso, $\circ(a) = \min\{\, n \geq 1 \,;\, a^n = e \,\}$ e

$$\langle a \rangle = \{\, e, a, \ldots, a^{\circ(a)-1} \,;\, a^{\circ(a)} = e\},$$

com $a^i \neq a^j$, para $1 \leq i < j \leq \circ(a) - 1$.

Demonstração:

(i) ($\Longrightarrow$:) Suponhamos que o subgrupo gerado por a seja finito. Então, na lista a, a^2, a^3, ... de elementos de $\langle a \rangle$ há repetições. Logo, existem $r, s \geq 1$, com $s < r$, tais que $a^s = a^r$. Portanto,

$$a^{r-s} = a^r \cdot a^{-s} = a^r \cdot (a^s)^{-1} = a^s \cdot (a^s)^{-1} = e, \text{ com } r - s > 0.$$

Tomamos $m = r - s$.

Pode haver repetições de elementos.

(i) ($\Longleftarrow$:) Suponhamos que exista $m \geq 1$ tal que $a^m = e$. Afirmamos que $\langle a \rangle = \{e, a, \ldots, a^{m-1}\}$.

De fato, é claro que $\{e, a, \ldots, a^{m-1}\} \subset \langle a \rangle$. Seja agora $b \in \langle a \rangle$. Então, existe $s \in \mathbb{Z}$ tal que $b = a^s$. Pela divisão euclidiana de s por m, existem $q, r \in \mathbb{Z}$, unicamente determinados, tais que $s = m \cdot q + r$ com $0 \leq r \leq m-1$. Assim,

$$b = a^s = a^{m \cdot q + r} = a^{m \cdot q} \cdot a^r = (a^m)^q \cdot a^r = e^q \cdot a^r = a^r \in \{e, a, \ldots, a^{m-1}\},$$

mostrando que $\langle a \rangle \subset \{e, a, \ldots, a^{m-1}\}$.

(ii) Suponhamos que $\circ(a)$ seja finito. Pelo item (i), existe $m \geq 1$, tal que $a^m = e$. Seja $S = \{n \geq 1 \,;\, n \in \mathbb{Z} \text{ e } a^n = e\}$. Então, S é um conjunto não-vazio de inteiros positivos, pelo Princípio da Boa Ordenação, S tem menor elemento, digamos n_0. Vamos mostrar que $n_0 = \circ(a)$.

Como $n_0 \in S$, então $n_0 \geq 1$ e $a^{n_0} = e$. Da demonstração do item (i), temos que

$$\langle a \rangle = \{e, a, \ldots, a^{n_0-1}\}.$$

Vamos mostrar que não há repetições de potências de a na lista acima, concluindo que $|\{e, a, \ldots, a^{n_0-1}\}| = n_0 = |\langle a \rangle| = \circ(a)$.

Sejam $i, j \in \mathbb{Z}$ tais que $0 \leq i < j \leq n_0 - 1$ e suponhamos $a^i = a^j$. Então, $a^{j-i} = a^j \cdot (a^i)^{-1} = a^i \cdot (a^i)^{-1} = e$, com $0 < j - i \leq n_0 - 1$, contradizendo a escolha de n_0. ■

Observação: Seja $a \in G$ tal que $\circ(a) = \infty$. Segue do item (i) da Proposição anterior que $a^m \neq e$, para todo $m \geq 1$, e a, a^2, a^3, ...são distintos. Se $m \leq -1$, então $a^m = (a^{-1})^{-m} \neq e$. Nesse caso, $a^n = e$, com $n \in \mathbb{Z}$ se, e somente se, $n = 0$.

Proposição 9
Sejam $(G, \cdot)$ um grupo, $a \in G$, tal que $\circ(a)$ é finito e $m \in \mathbb{Z}$. Então, $a^m = e$ se, e somente se, $\circ(a)$ divide m.

Demonstração: Seja $I = \{n \in \mathbb{Z} \,;\, a^n = e\} \subset \mathbb{Z}$.

Afirmamos que I é um ideal de $\mathbb{Z}$.

De fato,

(i) $0 \in I$, pois por definição $a^0 = e$;

(ii) Se $r, s \in I$, então $a^r = e$, $a^s = e$ e $a^{r+s} = a^r \cdot a^s = e \cdot e = e$, logo $r + s \in I$;

(iii) Se $r \in \mathbb{Z}$ e $s \in I$, então $a^s = e$ e $a^{s \cdot r} = (a^s)^r = e^r = e$, logo $s \cdot r \in I$.

Como $\circ(a) \in I$, então $I \neq \{0\}$. Então, $I = I(n_0)$, para algum $n_0 \geq 1$. Sabemos que n_0 é o menor elemento positivo de I. Portanto, $a^{n_0} = e$ e n_0 é o menor inteiro positivo com essa propriedade logo, pela Proposição anterior, $n_0 = \circ(a)$. Portanto,
$a^m = e \iff m \in I = I(\circ(a)) \iff m$ é múltiplo de $\circ(a) \iff \circ(a)$ divide m.

■

Corolário 1
Seja $(G, \cdot)$ um grupo finito. Então, para todo $a \in G$, $a^{|G|} = e$.

Demonstração: Como $\langle a \rangle$ é um subgrupo de G, pelo Teorema de Lagrange, $|\langle a \rangle| = \circ(a)$ divide $|G|$ e, pela Proposição anterior, $a^{|G|} = e$. ■

Definição 11 (Grupo cíclico)
Um grupo $(G, \cdot)$ é chamado *cíclico* se, e somente se, existe $a \in G$, tal que $G = \langle a \rangle = \{a^n \,;\, n \in \mathbb{Z}\}$. Nesse caso, dizemos que a é um *gerador* de G.

Exemplo 25
Existem grupos cíclicos infinitos.

$(\mathbb{Z}, +)$ é grupo cíclico infinito, gerado por 1 ou por -1.

No Exemplo 19 temos um grupo cíclico multiplicativo infinito, contido em $(\mathbb{Q}^*, \cdot)$.

Exemplo 26

Para cada natural $n \geq 1$, existe um grupo cíclico com n elementos.

Modelo multiplicativo:

Seja $\omega = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n} \in \mathbb{C}^*$, então o subgrupo de $\mathbb{C}^*$ gerado por ω é

$$\langle\omega\rangle = \{\omega^j\ ;\ j \in \mathbb{Z}\} = \{1, \omega, \ldots, \omega^{n-1}\} = U_n(\mathbb{C}).$$

Logo, o grupo das raízes complexas n-ésimas da unidade é cíclico e $|U_n(\mathbb{C})| = n$.

Toda raiz primitiva n-ésima da unidade é outro gerador de $U_n(\mathbb{C})$, a saber ω^j é gerador de $U_n(\mathbb{C})$ se, e somente se, $\mathrm{mdc}(n, j) = 1$.

Modelo aditivo

O grupo das classes residuais módulo n, $(\mathbb{Z}_n, +\mod n)$ é um grupo cíclico com n elementos, gerado por $\overline{1}$.

Proposição 10 (Classificação dos grupos de ordem prima)

Seja $(G, \cdot)$ um grupo com $|G| = p$, onde p é primo. Então, G é cíclico e qualquer $a \in G$, $a \neq e$, é gerador de G.

Demonstração: Seja $a \in G$, $a \neq e$. Temos que $\circ(a)$ divide $|G| = p$ e $\circ(a) \neq 1$, então $\circ(a) = p$. Portanto, $\langle a\rangle = \{e, a, \ldots, a^{p-1};\ a^p = e\} \subset G$. Como ambos os conjuntos têm p elementos, $\langle a\rangle = G$. ■

Tal elemento existe, pois $p = |G| \geq 2$. Se $\circ(a) = 1$, então $a = a^1 = e$.

Exemplo 27

Vamos classificar os grupos de ordem 4.

Quem são os grupos com 4 elementos?

Sabemos que para todo $n \geq 1$ existe grupo cíclico com n elementos, a saber, $\mathbb{Z}_n$ ou $U_n(\mathbb{C})$, em particular, existe grupo cíclico com 4 elementos.

Verifique! Fez o Exercício 2 da Seção 1?

$\mathbb{Z}_2 \times \mathbb{Z}_2$ é um exemplo de grupo com 4 elementos não-cíclico.

Seja $(G, \cdot)$ um grupo não-cíclico com 4 elementos. É claro que o elemento de ordem 1 é e_G. Os elementos de G diferentes de e_G têm ordem 2, pois devem ter como ordem um divisor de 4 diferente de 1 e de 4.

Pela divisão euclidiana de n por 2, existem $q, r \in \mathbb{Z}$ tais que $n = 2q + r$, com $r = 0, 1$. Logo, $a^n = a^{2q+r} = (a^2)^q \cdot a^r = a^r$. Então, $a^n \in \{e_g, a\}$.

Assim, existe $a \in G$ tal que $\circ(a) = 2$. Temos, $e_G \neq a$ e, como $e = a^2 = a \cdot a$, então $a^{-1} = a$ e $a^n \in \{e_G, a\}$, para todo $n \in \mathbb{Z}$. Logo, existe $b \in G$ tal que $b \neq e_G$, $b \neq a$ e $b^2 = e_G$. O elemento $a \cdot b \in G$ e :

se $a \cdot b = e_G$, então $a = b^{-1} = b$, é uma contradição;

se $a \cdot b = a$, então $b = e_G$, também é uma contradição;

se $a \cdot b = b$, então $a = e_G$, novamente, é uma contradição.

Portanto, $\{e_G, a, b, a \cdot b\} \subset G$ tem 4 elementos. Logo, $G = \{e_G, a, b, a \cdot b\}$.

Também, $b \cdot a \in G$ e, analogamente, $b \cdot a \neq e_G$, $b \cdot a \neq a$ e $b \cdot a \neq b$. A única possibilidade é $b \cdot a = a \cdot b$. Logo,

$$G = \{e_G, a, b, a \cdot b;\ b \cdot a = a \cdot b, a^2 = e_G \text{ e } b^2 = e_G\}$$

Observação: O grupo não-abeliano finito de menor ordem tem ordem 6 e é o S_3. Veremos que há cinco grupos de ordem 8, três deles abelianos e dois não-abelianos, os grupos diedral 4 e dos quatérnios. Lembramos que

$$D_4 = \{I, R, R^2, R^3, S, SR, SR^2, SR^3\ ;\ S^2 = I, R^4 = I \text{ e } RS = SR^3\}.$$

Fez o Exercício 18 da Seção 1?

No próximo exemplo o grupo dos quatérnios, um dos dois grupos não-abelianos com 8 elementos.

Exemplo 28

Seja $\mathcal{Q} = \{1, i, j, k, -1, -i, -j, -k\}$, com a operação

$$\begin{array}{lll} i \cdot j = k, & j \cdot k = i, & k \cdot i = j, \\ j \cdot i = -k, & k \cdot j = -i, & i \cdot k = -j, \\ i^2 = -1, & j^2 = -1, & k^2 = -1, \\ (-1) \cdot i = -i, & (-1) \cdot j = -j, & (-1) \cdot k = -k, \quad (-1)^2 = 1 \end{array}$$

onde 1 é o elemento neutro.

Verifique que $\mathcal{Q}$ é um grupo, $\mathcal{Q}$ é chamado de *grupo de quatérnios.*

Proposição 11

Seja $(G, \cdot)$ um grupo e seja $a \in G$ com $\circ(a) < \infty$. Então, para todo $s \in \mathbb{Z}$,

$$\circ(a^s) = \frac{\circ(a)}{\text{mdc}(\circ(a), s)}.$$

Demonstração: O caso $s = 0$ é trivial. Seja $s > 0$. Sejam $n = \circ(a)$ e $m = \circ(a^s)$. Então, m é o menor inteiro positivo tal que $e = (a^s)^m = a^{s \cdot m}$. Pela Proposição 9, $n = \circ(a)$ divide $s \cdot m$. Como s divide $s \cdot m$, então $s \cdot m$ é o menor inteiro positivo que é múltiplo comum de n e s, isto é, $s \cdot m = \text{mmc}(n, s)$. Logo,

$$m = \frac{\text{mmc}(n, s)}{s} = \frac{s \cdot n}{\text{mdc}(n, s)} \cdot \frac{1}{s} = \frac{n}{\text{mdc}(n, s)}.$$

Se $a > 0$ e $b > 0$, então $\text{mdc}(a, b)\text{mmc}(a, b) = ab$.

No caso $s < 0$, substituímos $b = a^s$ por $b^{-1} = a^{-s}$ e usamos o Exercício 1 dessa Seção. ■

Lema 1

Seja $(G, \cdot)$ um grupo e seja $a \in G$ tal que $\circ(a) = n$. Então, $\langle a^s \rangle = \langle a^{\text{mdc}(s,n)} \rangle$.

Demonstração:

Se $b \in H$ e H é um subgrupo, então $\langle b\rangle \subset H$.

($\subset$:) Como $s = m \cdot \mathrm{mdc}(s,n)$, para algum $m \in \mathbb{Z}$, então

$$a^s = a^{m\cdot \mathrm{mdc}(s,n)} = (a^{\mathrm{mdc}(s,n)})^m \in \langle a^{\mathrm{mdc}(s,n)}\rangle.$$

Logo, $\langle a^s\rangle \subset \langle a^{\mathrm{mdc}(s,n)}\rangle$.

($\supset$:) Sejam $\alpha, \beta \in \mathbb{Z}$ tais que $\mathrm{mdc}(s,n) = \alpha n + \beta s$. Então.

$$a^{\mathrm{mdc}(s,n)} = a^{\alpha n+\beta s} = a^{\alpha n}\cdot a^{\beta s} = (a^n)^\alpha \cdot (a^s)^\beta = e\cdot (a^s)^\beta = (a^s)^\beta.$$

Logo, $a^{\mathrm{mdc}(s,n)} \in \langle a^s\rangle$. Portanto, $\langle a^{\mathrm{mdc}(s,n)}\rangle \subset \langle a^s\rangle$. ■

Agora estamos prontos para os Teoremas de estrutura dos grupos cíclicos, infinitos e finitos.

Teorema 2

Todo subgrupo de um grupo cíclico é cíclico.

Demonstração: Seja $(G,\cdot)$ grupo cíclico gerado por a. Se $H = \{e\}$, então $H = \langle e\rangle$, com $e = a^0$. Suponhamos que H seja um subgrupo de G, $H \neq \{e\}$. Então, existe $m \in \mathbb{Z}$, $m \neq 0$, tal que $a^m \in H$. Como $a^m, a^{-m} = (a^m)^{-1} \in H$, então existe um inteiro positivo n_0, tal que $a^{n_0} \in H$.

Seja $S = \{n > 0\,;\ a^n \in H\}$. S é não-vazio e $S \subset \mathbb{N}$ então, pelo Princípio da Boa Ordenação, S tem um menor elemento, digamos s. Como $s \in S$, temos que $a^s \in H$ e $s > 0$.

Lembre que ...
Se H é um subgrupo de G e $c \in H$, então $\langle c\rangle \subset H$.

Afirmamos que $\langle a^s\rangle = H$.

De fato, $\langle a^s\rangle \subset H$, pois $a^s \in H$.

Seja agora $b \in H \subset G = \langle a\rangle$. Logo, existe $n \in \mathbb{Z}$ tal que $b = a^n$. Pela divisão euclidiana de n por s, existem q, r em $\mathbb{Z}$, unicamente determinados, tais que $n = qs + r$, com $0 \leq r < s$. Assim,

$$b = a^n = a^{sq+r} = a^{sq}\cdot a^r = (a^s)^q \cdot a^r$$

Logo, $a^r = b\cdot (a^s)^{-q} \in H$, com $0 \leq r < s$. Pela escolha de s, temos $r = 0$. Portanto, $b = (a^s)^q \in \langle a^s\rangle$ e $H \subset \langle a^s\rangle$. ■

Teorema 3

Seja $(G,\cdot)$ um grupo cíclico infinito gerado por a, $G = \langle a\rangle$. Para cada $s \geq 0$, existe um único subgrupo de G gerado por a^s, $H_s = \langle a^s\rangle$. Quando $s > 0$, s é o menor inteiro positivo m, tal que $a^m \in H_s$.

Demonstração:

$$\begin{aligned} G = \langle a\rangle \text{ é infinito} &\iff a^i \neq a^j, \text{ se } i \neq j \\ &\iff G = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\},\ a^i \neq a^j, \text{ se } i \neq j \end{aligned}$$

$H = \{e\} = \langle a^0\rangle$ é o único subgrupo finito. Para cada $s > 0$, temos

$$H_s = \langle a^s\rangle = \{\ldots, a^{-3s}, a^{-2s}, a^{-s}, e, a^s, a^{2s}, a^{3s}, \ldots\} = \langle a^{-s}\rangle$$

é cíclico infinito. Para $0 < r < s$, observamos que $H_s \neq H_r$, pois $a^r \in H_r$ e $a^r \notin H_s$. ■

Teorema 4

Seja $(G, \cdot)$ um grupo cíclico com n elementos gerado por a. Para cada $d \geq 1$ divisor de n existe um único subgrupo de G com d elementos, a saber, $H_d = \langle a^{\frac{n}{d}} \rangle$.

Demonstração: Nesse caso, $G = \langle a \rangle = \{e, a, \ldots, a^{n-1} \; ; \; a^n = e\}$.

Para cada $d \geq 1$ tal que d divide n é clara a existência dos subgrupos $H_d = \langle a^{\frac{n}{d}} \rangle$, com $|H_d| = \circ(a^{\frac{n}{d}}) = d$.

Use a fórmula da Proposição 11.

Seja H um subgrupo de G com d elementos, onde d divide n. Pelo Teorema 2, existe $s \geq 0$ tal que $H = \langle a^s \rangle$. Pelo Lema anterior, $\langle a^s \rangle = \langle a^{\mathrm{mdc}(s,n)} \rangle$. Logo,

$$d = |H| = \circ(a^s) = \frac{n}{\mathrm{mdc}(s, n)},$$

seguindo a última igualdade da Proposição 11. Portanto, $\mathrm{mdc}(s, n) = \dfrac{n}{d}$ e $H = \langle a^{\frac{n}{d}} \rangle$. ■

Corolário 2

Seja $(G, \cdot)$ um grupo cíclico com n elementos gerado por a. O elemento a^s gera G se, e somente se, $\mathrm{mdc}(s, \circ(a)) = 1$. Em particular, G tem $\phi(n)$ geradores, onde ϕ é a função de Euler.

Demonstração:

$$\begin{aligned} a^s \text{ gera } G \quad & \text{se, e somente se,} \quad n = \circ(a^s) = \frac{n}{\mathrm{mdc}(s, n)} \\ & \text{se, e somente se,} \quad \mathrm{mdc}(s, n) = 1. \end{aligned}$$

A última afirmação é clara. ■

Exemplo 29

$(\mathbb{Z}_{19}^*, \cdot \mod 19)$ é um grupo com 18 elementos.

Verifique que $\mathbb{Z}_{19}^* = \langle \overline{2} \rangle$.

Os divisores de 18 são $1, 2, 3, 6, 9$ e 18. Portanto, $\mathbb{Z}_{19}^*$ tem 6 subgrupos.

Os subgrupos não-triviais de $\mathbb{Z}_{19}^*$ são $H_2 = \langle \overline{2}^9 \rangle = \{\overline{1}, \overline{-1}\}$, $H_3 = \langle \overline{2}^6 \rangle$, $H_6 = \langle \overline{2}^3 \rangle$ e $H_9 = \langle \overline{2}^2 \rangle$.

Exercícios

1. Seja $(G, \cdot)$ um grupo. Mostre que $\circ(a) = \circ(a^{-1})$, para todo $a \in G$.
2. Seja $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; ; \; a, b, c, d \in \mathbb{Z}_2 \text{ e } ad - bc \neq \overline{0} \right\}$.

(a) Mostre que G é um grupo com a operação usual de multiplicação de matrizes.

(b) Determine a ordem de G.

(c) Calcule a ordem de $\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}$.

(d) G é um grupo cíclico?

3. Seja $\theta \in \mathbb{R}$ e seja $H_\theta = \{(\cos\theta + i\,\mathrm{sen}\,\theta)^n\ ;\ n \in \mathbb{Z}\}$.

(a) Mostre que H_θ é um subgrupo de S^1.

(b) Mostre que H_θ é finito se, e somente se, $\frac{\theta}{\pi} \in \mathbb{Q}$.

(c) Determine a ordem (o número de elementos) de H_θ, quando $\frac{\theta}{\pi} = \frac{2}{3}$.

(d) Identifique H_θ, quando $\frac{\theta}{\pi} = \frac{3}{4}$.

4. Seja $(G, \cdot)$ um grupo. Mostre que se H e K são subgrupos finitos de G, tais que $\mathrm{mdc}(|H|, |K|) = 1$, então $H \cap K = \{e\}$.

5. Seja $(G, \cdot)$ um grupo de ordem prima. Mostre que os seus únicos subgrupos são os triviais, isto é, G e $\{e\}$.

6. Seja $(G, \cdot)$ um grupo, $G \neq \{e\}$, tal que seus únicos subgrupos são $\{e\}$ e G. Mostre que G é cíclico finito de ordem prima.

7. Mostre que $\mathbb{Z}_{10}^*$ é um grupo cíclico e $\mathbb{Z}_8^*$ não é um grupo cíclico.

8. Seja $G = \mathbb{Z}_{17}^*$ com a multiplicação $\cdot \mod 17$.

(a) Mostre que G é um grupo cíclico e dê todos os seus geradores.

(b) Dê todos os seus subgrupos.

9. Mostre que os seguintes grupos são cíclicos: $\mathbb{Z}_9^*$, $\mathbb{Z}_{18}^*$, $\mathbb{Z}_{25}^*$ e $\mathbb{Z}_{27}^*$.

10. Determine, para cada um dos grupos do exercício anterior, todos os seus geradores e todos os seus subgrupos.

11. Seja $(G, \cdot)$ um grupo. Sejam $a, b \in G$ tais que $a \cdot b = b \cdot a$.

(a) Mostre que $(a \cdot b)^n = a^n \cdot b^n$, para todo $n \in \mathbb{Z}$.

(b) Mostre que se $\circ(a) = r$, $\circ(b) = s$ e $\mathrm{mdc}(r, s) = 1$, então $\circ(a \cdot b) = r \cdot s$.

(c) Mostre que se $\circ(a) = r$ e $\circ(b) = s$, então existe $c \in G$, tal que $\circ(c) = \mathrm{mmc}(r, s)$.

Grupos Diedrais

Mostraremos agora que para cada $n \geq 3$ existe um grupo não-abeliano com $2n$ elementos, chamado de *grupo diedral* n e denotado por D_n.

D_n é subgrupo do S_n e é o grupo das simetrias do polígono regular de n lados.

Fixemos $\mathcal{P}$ um polígono regular de n lados. Consideremos D_n o conjunto das bijeções do plano que deixam $\mathcal{P}$ invariante.

Denotando por Π o plano. Temos

$$D_n = \{\sigma : \Pi \longrightarrow \Pi \,;\ \sigma \text{ é uma bijeção e } \sigma(\mathcal{P}) = \mathcal{P}\}.$$

D_n é subgrupo do grupo das bijeções do plano. De fato,

(i) Como $I : \Pi \longrightarrow \Pi$ é uma bijeção tal que $I(\mathcal{P}) = \mathcal{P}$, então $I \in D_n$.

(ii) $\sigma, \tau \in D_n$, se, e somente se, $\sigma : \Pi \longrightarrow \Pi$ e $\tau : \Pi \longrightarrow \Pi$ são bijeções, tais que $\sigma(\mathcal{P}) = \mathcal{P}$ e $\tau(\mathcal{P}) = \mathcal{P}$, então $\sigma \circ \tau : \Pi \longrightarrow \Pi$ é uma bijeção e $(\sigma \circ \tau)(\mathcal{P}) = \sigma(\tau(\mathcal{P})) = \sigma(\mathcal{P}) = \mathcal{P}$. Logo, $\sigma \circ \tau \in D_n$.

(iii) Se $\sigma \in D_n$, então existe $\tau : \Pi \longrightarrow \Pi$, tal que $\sigma \circ \tau = \tau \circ \sigma = I$, pois σ é uma bijeção no plano Π. Como $\sigma(\mathcal{P}) = \mathcal{P}$, então

$$\mathcal{P} = I(\mathcal{P}) = (\tau \circ \sigma)(\mathcal{P}) = \tau(\sigma(\mathcal{P})) = \tau(P),$$

logo $\sigma^{-1} = \tau \in D_n$.

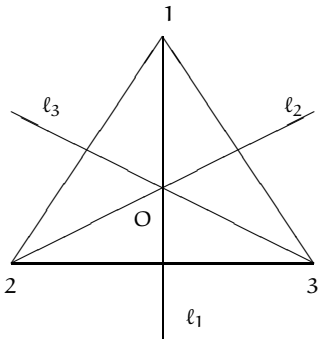
Portanto, D_n é um grupo. Quem é D_n?

Faremos as construções detalhadas de D_3, o grupo das simetrias do triângulo equilátero, e de D_4, o grupo das simetrias do quadrado. A construção de D_n para n ímpar é análoga ao caso $n = 3$ e, para n par, ao caso $n = 4$.

O grupo diedral 3, D_3

Fixemos um triângulo equilátero $\triangle$. O grupo das bijeções do plano que deixam $\triangle$ invariante é o grupo das simetrias de $\triangle$.

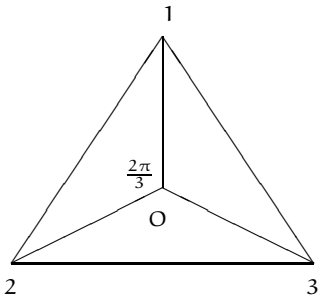
Para visualizarmos as bijeções e a imagem dos pontos de $\triangle$, consideremos os vértices do triângulo numerados por 1, 2 e 3. O triângulo $\triangle$ está inscrito num círculo de centro O, conforme a figura a seguir.



Temos 3 retas no plano, cujas simetrias do plano com respeito a elas, deixam $\triangle$ invariante. Para cada $j = 1, 2, 3$, seja ℓ_j a reta que passa pelo vértice j e pelo centro O de $\triangle$. A reta ℓ_j é perpendicular ao lado oposto ao vértice j e divide-o ao meio (é uma mediana).

Sejam S'_1, S'_2 e S'_3 as simetrias do plano com respeito, respectivamente, às retas ℓ_1, ℓ_2 e ℓ_3. Essa bijeções do plano têm a propriedade de $S'_j(\triangle) = \triangle$.

O ângulo interno $1\hat{O}2$ do triângulo equilátero, medido em radianos, é $\frac{2\pi}{3}$.



Temos três rotações do plano em torno do ponto O, no sentido anti-horário, que deixam $\triangle$ invariante, isto é, $R_j(\triangle) = \triangle$, para $j = 1, 2, 3$: R_1, a rotação de $\frac{2\pi}{3}$; R_2, a rotação de $\frac{2\cdot(2\pi)}{3} = \frac{4\pi}{3}$ e R_3, a rotação de $\frac{3\cdot(2\pi)}{3}$. É claro que $R_3 = I$, a função identidade no plano.

As 6 bijeções estão perfeitamente determinadas pelas imagens dos vértices do triângulo. Podemos representar as 6 bijeções do plano que deixam $\triangle$ invariante por bijeções do conjunto $\{1, 2, 3\}$, os vértices do triângulo, a saber,

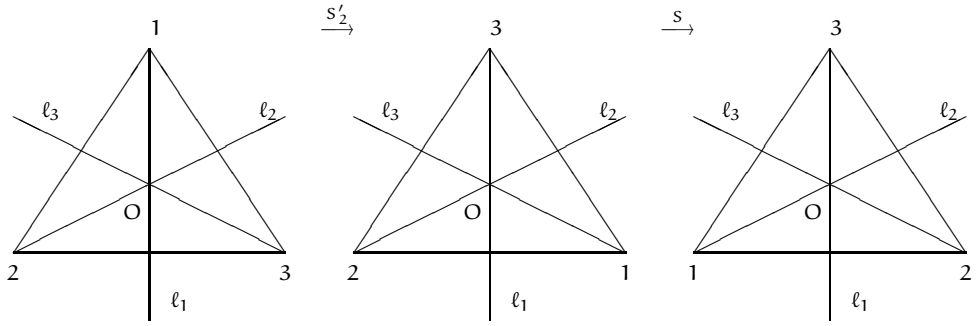
$$S'_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad S'_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad S'_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$R_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad R_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad R_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$$

Podemos descrever essas seis bijeções a partir de $S = S'_1$ e $R = R_1$. Primeiramente, observamos que $R_2 = R^2$, $R_3 = R^3 = I$ e $S^2 = I$. Temos que $S'_2 = SR$, $S'_3 = SR^2$ e $RS = SR^2$.

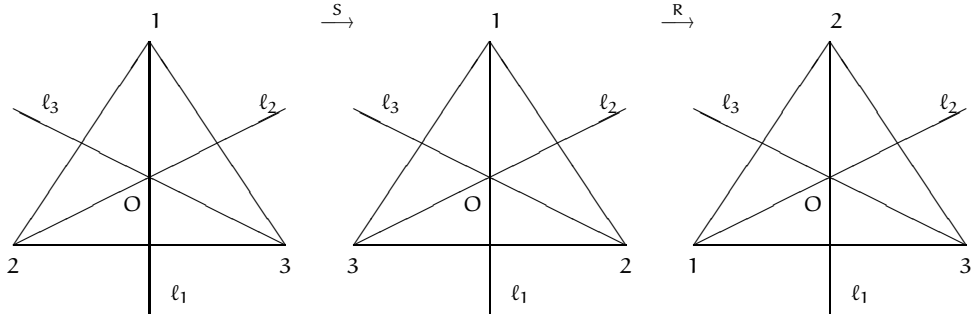
Verifique essas relações.

No desenho abaixo vamos visualizar a composição $S'_1S'_2 = SS'_2 = R$. Não esqueça que as retas estão fixas.



Comparando a configuração inicial com a final, observamos que $SS'_2 = R$. Como $S^2 = I$, compondo com S à esquerda, obtemos que $S'_2 = SR$. Faça, de modo análogo, a verificação de que $SS'_3 = R^2$ e conclua que $S'_3 = SR^2$.

No desenho abaixo vamos visualizar a composição $RS = SR^2 = S'_3$. Não esqueça que as retas estão fixas, assim como o ponto O. No processo, as retas ℓ_1, ℓ_2 e ℓ_3 determinam as simetrias.



Portanto,

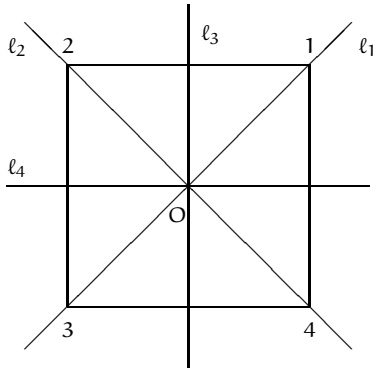
$$\begin{aligned} D_3 &= \{I, R, R^2, S, SR, SR^2 \,;\, R^3 = I, S^2 = I, RS = SR^2\} \\ &= \{S^iR^j \,;\, i = 0, 1,\, j = 0, 1, 2,\, S^2 = I, R^3 = I, RS = SR^2\} \end{aligned}$$

Nesse caso, $D_3 = S_3$.

O grupo diedral 4, D_4

Fixemos um quadrado $\square$. O grupo das bijeções do plano que deixam $\square$ invariante é o grupo das simetrias do quadrado.

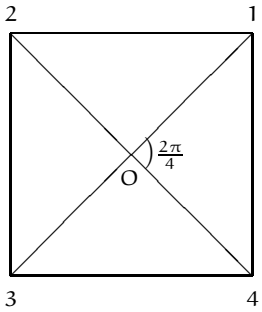
Para visualizarmos as bijeções do plano e a imagem dos pontos de $\square$, consideremos os vértices do quadrado numerados por 1, 2, 3 e 4. O quadrado está inscrito num círculo de centro O, conforme a figura a seguir.



Temos 4 retas no plano, cujas simetrias do plano com respeito a elas, deixam $\square$ invariante. Para $j = 1, 2$ seja ℓ_j a reta que passa pelo centro O e pelo vértice j (tem um vértice do quadrado oposto a j). Para $j = 1, 2$, seja ℓ_{2+j} a reta que passa pelo centro O e é perpendicular ao lado que contém os vértices j e $j+1$ (há dois lados do quadrado paralelos perpendiculares a ℓ_{2+j}, que divide-os ao meio).

Sejam S'_1, S'_2, S'_3 e S'_4 as simetrias do plano com respeito, respectivamente, às retas ℓ_1, ℓ_2, ℓ_3 e ℓ_4. Essa bijeções do plano têm a propriedade de $S'_j(\square) = \square$.

O ângulo interno $4\hat{O}1$ do quadrado é $\frac{2\pi}{4} = \frac{\pi}{2}$.



Temos quatro rotações do plano em torno do ponto O, no sentido anti-horário, que deixam $\square$ invariante, isto é, $R_j(\square) = \square$, para $j = 1, 2, 3, 4$: R_1, a rotação de $\frac{2\pi}{4} = \frac{\pi}{2}$; R_2, a rotação de $\frac{2\cdot(2\pi)}{4} = \pi$; R_3, a rotação de $\frac{3\cdot(2\pi)}{4} = \frac{3\pi}{2}$ e R_4, a rotação de $\frac{4\cdot(2\pi)}{4} = 2\pi$, com $R_4 = I$.

Podemos representar as 8 bijeções do plano que deixam $\square$ invariante por bijeções do conjunto $\{1, 2, 3, 4\}$, a saber,

$$S_1' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \qquad S_2' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$S_3' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad S_4' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

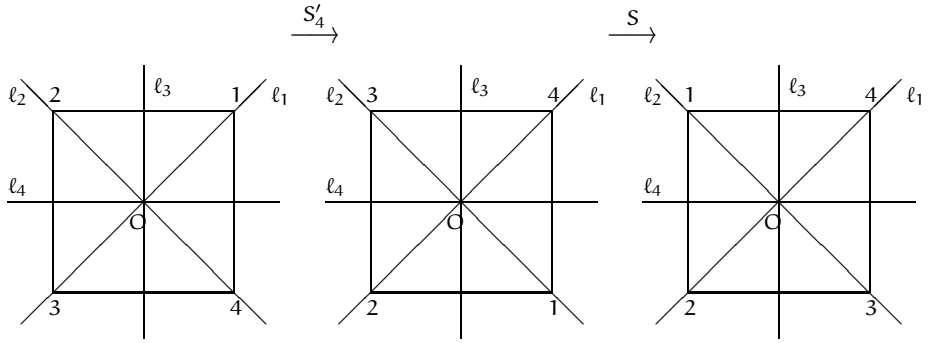
$$R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \qquad R_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I$$

Podemos descrever essas 8 bijeções a partir de $S = S_1'$ e $R = R_1$.

Verifique essas relações.

Observamos que $R_2 = R^2$, $R_3 = R^3$, $R_4 = R^4 = I$, $S^2 = I$ e $S_2' = SR^2$, $S_3' = SR^3$, $S_4' = SR$ e $RS = SR^3$.

Ilustramos com a composição $SS_4' = R$. Não esqueça que as retas estão fixas.



A configuração do último quadrado corresponde a $R(\square)$. Logo, $SS_4' = R$ e como $S^2 = I$, compondo à esquerda da igualdade com S, obtemos $S_4' = SR$.

Temos

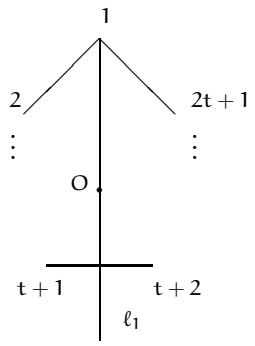
$$\begin{aligned} D_4 &= \{I, R, R^2, R^3, S, SR, SR^2, SR^3 \,;\, R^4 = I, S^2 = I, RS = SR^3\} \\ &= \{S^i R^j \,;\, i = 1, 0,\, j = 0, 1, 2, 3,\, S^2 = I, R^4 = I, RS = SR^3\} \end{aligned}$$

Nesse caso, $D_4 \subsetneq S_4$.

O grupo diedral n, D_n, com $n = 2t + 1$

Fixemos um polígono regular $\mathcal{P}$ com $n = 2t + 1$ lados. O grupo das bijeções do plano que deixam $\mathcal{P}$ invariante é o grupo das simetrias de $\mathcal{P}$.

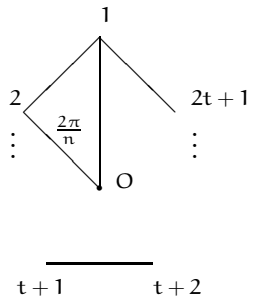
Para visualizarmos as bijeções e a imagem dos pontos de $\mathcal{P}$, consideremos os vértices do polígono numerados por $1, 2, \ldots, 2t + 1$. O polígono regular $\mathcal{P}$ está inscrito num círculo de centro O, conforme a figura a seguir.



Temos $n = 2t+1$ retas no plano, cujas simetrias do plano com respeito a elas, deixam $\mathcal{P}$ invariante. Para cada $j = 1, \ldots, 2t+1$, seja ℓ_j a reta que passa pelo vértice j e pelo centro O de $\mathcal{P}$. A reta ℓ_j é perpendicular ao lado oposto ao vértice j e divide-o ao meio.

Sejam S'_1, ..., S'_{2t+1} as simetrias do plano com respeito, respectivamente, às retas ℓ_1, ..., ℓ_{2t+1}. Essa bijeções do plano têm a propriedade de $S'_j(\mathcal{P}) = \mathcal{P}$.

O ângulo interno $1\hat{O}2$ de $\mathcal{P}$ é $\frac{2\pi}{n}$, onde $n = 2t+1$.



Temos $n = 2t+1$ rotações no plano em torno do ponto O, no sentido anti-horário, que deixam $\mathcal{P}$ invariante, isto é, $R_j(\mathcal{P}) = \mathcal{P}$, para $j = 1, \ldots, n$: R_1, a rotação de $\frac{2\pi}{n}$; R_2, a rotação de $\frac{2\cdot(2\pi)}{3} = \frac{4\pi}{3}$, ...; R_{n-1}, a rotação de $\frac{(n-1)\cdot(2\pi)}{n}$; e R_n, a rotação de $\frac{n\cdot(2\pi)}{n} = 2\pi$. Assim, $R_n = I$.

Podemos representar as $2n$ bijeções de $\mathcal{P}$ por bijeções do conjunto $\{1, 2, \ldots, n\}$, usando apenas $S = S'_1$ e $R = R_1$:

$$S = S'_1 = \begin{pmatrix} 1 & 2 & \ldots & t+1 & t+2 & \ldots & 2t+1 \\ 1 & 2t+1 & \ldots & t+2 & t+1 & \ldots & 2 \end{pmatrix} \text{ e}$$

$$R = R_1 = \begin{pmatrix} 1 & 2 & \ldots & 2t & 2t+1 \\ 2 & 3 & \ldots & 2t+1 & 1 \end{pmatrix}$$

Observamos que $R_j = R^j$, para cada $j = 1, \ldots, n-1$ e $R^n = I$, $S^2 = I$, $RS = SR^{n-1}$. Além disso, SR^j é uma simetria para cada $j = 1, \ldots, n-1$. Portanto,

Verifique essas relações.

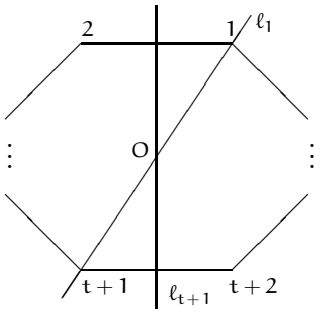
$$\begin{aligned} D_n &= \{I, R, \ldots, R^{n-1}, S, SR, \ldots, SR^{n-1}\ ;\ R^n = I, S^2 = I, RS = SR^{n-1}\} \\ &= \{S^iR^j\ ;\ i = 0, 1, j = 0, \ldots, n-1\ , R^n = I, S^2 = I, RS = SR^{n-1}\} \end{aligned}$$

Observamos que $D_n \subsetneq S_n$, para n ímpar e $n > 3$.

O grupo diedral n, D_n, com $n = 2t$

Fixemos um polígono regular $\mathcal{P}$ com $n = 2t$ lados. O grupo das bijeções do plano que deixam $\mathcal{P}$ invariante é o grupo das simetrias de $\mathcal{P}$.

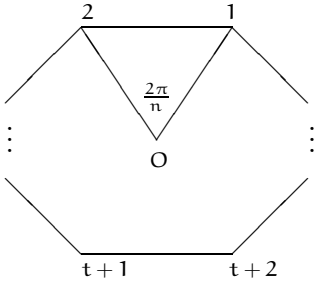
Para visualizarmos as bijeções e a imagem dos pontos de $\mathcal{P}$, consideremos os vértices do polígono numerados por 1, 2, ..., $2t$. O polígono regular $\mathcal{P}$ está inscrito num círculo de centro O, conforme a figura a seguir.



Temos $n = 2t$ retas no plano, cujas simetrias do plano com respeito a elas, deixam $\mathcal{P}$ invariante. Para cada $j = 1, \ldots, t$, seja ℓ_j a reta que passa pelo vértice j e pelo centro O de $\mathcal{P}$, o vértice $t+j$ é oposto ao vértice j e está na reta ℓ_j. Para cada $j = 1, \ldots, t$, seja ℓ_{t+j} a reta que passa pelo centro O e é perpendicular ao lado que contém os vértices j e $j+1$. Há t dessas retas, que são perpendiculares a dois lados paralelos de $\mathcal{P}$ e passam pelo ponto médio desses lados.

Sejam $S'_1, \ldots, S'_{2t}$ as simetrias do plano com respeito, respectivamente, às retas $\ell_1, \ldots, \ell_{2t}$. Essas bijeções do plano têm a propriedade de $S'_j(\mathcal{P}) = \mathcal{P}$.

O ângulo interno $1\hat{O}2$ de $\mathcal{P}$ é $\frac{2\pi}{n}$, onde $n = 2t$.



Temos $n = 2t$ rotações do plano em torno do ponto O, no sentido anti-horário, que deixam $\mathcal{P}$ invariante, isto é, $R_j(\mathcal{P}) = \mathcal{P}$, para $j = 1, \ldots, n$: R_1, a rotação de $\frac{2\pi}{n}$; R_2, a rotação de $\frac{2\cdot(2\pi)}{3} = \frac{4\pi}{3}$, $\ldots$; R_{n-1}, a rotação de $\frac{(n-1)\cdot(2\pi)}{n}$; e R_n, a rotação de $\frac{n\cdot(2\pi)}{n} = 2\pi$. Assim, $R_n = I$.

Podemos representar as $2n$ bijeções de $\mathcal{P}$ por bijeções do conjunto $\{1, 2, \ldots, n\}$, usando apenas $S = S'_1$ e $R = R_1$:

$$S = S'_1 = \begin{pmatrix} 1 & 2 & 3 & \ldots & t & t+1 & t+2 & \ldots & 2t-1 & 2t \\ 1 & 2t & 2t-1 & \ldots & t+2 & t+1 & t & \ldots & 3 & 2 \end{pmatrix} \text{ e}$$

$$R = R_1 = \begin{pmatrix} 1 & 2 & 3 & \ldots & 2t-1 & 2t \\ 2 & 3 & 4 & \ldots & 2t & 1 \end{pmatrix}$$

Verifique essas relações.

Observamos que $R_j = R^j$, para cada $j = 1, \ldots, n-1$ e $R^n = I$, $S^2 = I$, $RS = SR^{n-1}$. Além disso, SR^j é uma simetria para cada $j = 1, \ldots, n-1$. Portanto,

$$\begin{aligned} D_n &= \{I, R, \ldots, R^{n-1}, S, SR, \ldots, SR^{n-1} \,;\, R^n = I, S^2 = I, RS = SR^{n-1}\} \\ &= \{S^i R^j \,;\, i = 0, 1, j = 0, \ldots, n-1 \,, R^n = I, S^2 = I, RS = SR^{n-1}\} \end{aligned}$$

Observamos que $D_n \subsetneq S_n$, para n par e $n \geq 4$.

Homomorfismo e isomorfismo

Agora vamos apresentar as funções que interessam no estudo de grupos.

Definição 12 (Homomorfismo de grupos)
Sejam $(G,\cdot)$ e $(G',\star)$ grupos. A função $\varphi : G \longrightarrow G'$ é chamada de *homomorfismo de grupos,* se e somente se, $\varphi(a\cdot b) = \varphi(a)\star\varphi(b)$, para quaisquer $a, b \in G$.

Exemplo 30
Seja $\mathbb{R}^+ = \{x \in \mathbb{R} \ ; \ x > 0\}$. Como o produto de reais positivos é um real positivo, o inverso de um real positivo é um real positivo e 1 é um real positivo, então $\mathbb{R}^+$ é um subgrupo de $\mathbb{R}^*$. Logo, $(\mathbb{R}^+,\cdot)$ é um grupo.

Consideremos os grupos $(\mathbb{C}^*,\cdot)$ e $(\mathbb{R}^+,\cdot)$. A função

$$\begin{array}{rcl} \varphi : \mathbb{C}^* & \longrightarrow & \mathbb{R}^+ \\ z & \longmapsto & |\,z\,| \end{array}$$

é um homomorfismo de grupos, pois

$$\varphi(z\cdot w) = |\,z\cdot w\,| = |\,z\,|\cdot|\,w\,| = \varphi(z)\cdot\varphi(w),$$

para quaisquer $z, w \in \mathbb{C}^*$.

Exemplo 31
Sejam $(G,\cdot)$ e $(G',\star)$ grupos. A função $\varphi : G \longrightarrow G'$ definida por $\varphi(a) = e_{G'}$ é um homomorfismo de grupos, chamado de *homomorfismo trivial*.

Proposição 12 (Propriedades dos homomorfismos)
Sejam $(G,\cdot)$ e $(G',\star)$ grupos e $\varphi : G \longrightarrow G'$ um homomorfismo de grupos. Então:

(i) $\varphi(e_G) = e_{G'}$.

(ii) $\varphi(a^{-1}) = (\varphi(a))^{-1}$, para todo $a \in G$.

(iii) A imagem de φ é um subgrupo de G'.

Demonstração:

(i) Temos $\varphi(e_G) = \varphi(e_G\cdot e_G) = \varphi(e_G)\star\varphi(e_G)$. Operando em ambos os lados da igualdade com $(\varphi(e_G))^{-1}$, obtemos $e_{G'} = \varphi(e_G)$.

(ii) Temos que $e_{G'} = \varphi(e_G) = \varphi(a\cdot a^{-1}) \overset{(1)}{=} \varphi(a)\star\varphi(a^{-1})$. Analogamente, $e_{G'} = \varphi(a^{-1})\star\varphi(a)$. Dessas igualdades segue que $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Em (1) usamos que φ é um homomorfismo.

(iii) Veja o Exercício 1. ■

Proposição 13

Sejam $(G,\cdot)$, $(G',\star)$ e $(G'',\star')$ grupos. Se $\varphi : G \longrightarrow G'$ e $\psi : G' \longrightarrow G''$ são homomorfismos de grupos, então $\psi \circ \varphi : G \longrightarrow G''$ é um homomorfismo de grupos.

Demonstração: Seja $a, b \in G$. Então,

$$\begin{aligned}(\psi \circ \varphi)(a \cdot b) &\overset{(1)}{=} \psi\big(\varphi(a \cdot b)\big)\\ &\overset{(2)}{=} \psi\big(\varphi(a) \star \varphi(b)\big)\\ &\overset{(3)}{=} \psi(\varphi(a)) \star' \psi(\varphi(b))\\ &\overset{(4)}{=} (\psi \circ \varphi)(a) \star' (\psi \circ \varphi)(b). \ \blacksquare\end{aligned}$$

Em (1) e (4) usamos a definição de composição de funções; em (2), que φ é homomorfismo de grupos e em (3), que ψ é homomorfismo de grupos.

Definição 13 (Núcleo)

Sejam $(G,\cdot)$ e $(G',\star)$ grupos e $\varphi : G \longrightarrow G'$ um homomorfismo de grupos. O *núcleo* de φ é o conjunto

$$\text{Núcleo}(\varphi) = \{x \in G \ ; \ \varphi(x) = e_{G'}\}.$$

Exemplo 32

No Exemplo 30 temos $\text{Núcleo}(\varphi) = \{z \in \mathbb{C}^* \ ; \ |\, z \,| = 1\} = S^1$.

No Exemplo 31 temos $\text{Núcleo}(\varphi) = G$.

Proposição 14 (Propriedades do núcleo)

Sejam $(G,\cdot)$ e $(G',\star)$ grupos e $\varphi : G \longrightarrow G'$ um homomorfismo de grupos. Então,

(i) $\text{Núcleo}(\varphi)$ é um subgrupo de G.

(ii) φ é injetora se, e somente se, $\text{Núcleo}(\varphi) = \{e_G\}$.

Demonstração:

(i) Como $\varphi(e_G) = e_{G'}$, temos que $e_G \in \text{Núcleo}(\varphi)$. Além disso, se a, b estão no $\text{Núcleo}(\varphi)$, então $\varphi(a \cdot b) = \varphi(a) \star \varphi(b) = e_{G'} \star e_{G'} = e_{G'}$ e $\varphi(a^{-1}) \overset{(1)}{=} (\varphi(a))^{-1} = e_{G'}^{-1} = e_{G'}$, logo $a \cdot b \in \text{Núcleo}(\varphi)$ e $a^{-1} \in \text{Núcleo}(\varphi)$, portanto $\text{Núcleo}(\varphi)$ é um subgrupo de G.

Em (1) usamos a Proposição 12 item (ii).

(ii)($\Longrightarrow$:) Suponhamos que φ seja injetora. Seja $a \in \text{Núcleo}(\varphi)$. Então, $\varphi(a) = e_{G'} = \varphi(e_G)$, seguindo a última igualdade da Proposição 12 item (i). Como φ é injetora, segue que $a = e_G$. Logo, $\text{Núcleo}(\varphi) = \{e_G\}$.

(ii)($\Longleftarrow$:) Suponhamos que $\text{Núcleo}(\varphi) = \{e_G\}$. Sejam $a, b \in G$ tais que $\varphi(a) = \varphi(b)$. Então, $e_{G'} \overset{(2)}{=} \varphi(a) \star (\varphi(b))^{-1} \overset{(3)}{=} \varphi(a) \star \varphi(b^{-1}) \overset{(4)}{=} \varphi(a \cdot b^{-1})$. Portanto, $a \cdot b^{-1} \in \text{Núcleo}(\varphi) = \{e_G\}$. Logo, $a \cdot b^{-1} = e_G$, que nos dá $a = b$. Então, φ é injetora. $\blacksquare$

Em (2) usamos o cancelamento em G'; em (3), o item (ii) da Proposição 12 e em (4), que φ é homomorfismo de grupos.

Definição 14 (Isomorfismo de grupos)
Sejam $(G,\cdot)$ e $(G',\star)$ grupos. A função $\varphi : G \longrightarrow G'$ é um *isomorfismo de grupos* se, e somente se, φ é um homomorfismo de grupos bijetor.

Definição 15 (Grupos isomorfos)
Os grupos $(G,\cdot)$ e $(G',\star)$ são *grupos isomorfos* se, e somente se, existe $\varphi : G \longrightarrow G'$ isomorfismo de grupos.

Exemplo 33
Os grupos $(\mathbb{R}^+,\cdot)$ e $(\mathbb{R},+)$ são isomorfos, pois a função $\varphi : \mathbb{R}^+ \longrightarrow \mathbb{R}$ definida por $\varphi(x) = \log x$ é um isomorfismo de grupos.

Verifique

Proposição 15
Sejam $(G,\cdot)$ e $(G',\star)$ grupos e $\varphi : G \longrightarrow G'$ um isomorfismo de grupos. Então, a função ψ, inversa de φ, é um isomorfismo de grupos.

Demonstração: Como φ é uma função bijetora, existe $\psi : G' \longrightarrow G$ a função inversa de φ. Temos que $\varphi \circ \psi = I_{G'}$ e $\psi \circ \varphi = I_G$. Dessas composições segue, respectivamente, que ψ é função injetora e sobrejetora.

Verifique.

Para cada $b' \in G'$ temos que existe $b \in G$ tal que $\varphi(b) = b'$, pois φ é sobrejetora, e b é único porque φ é injetora. Assim, a função ψ é definida por:

$$\psi(b') = b \text{ se, e somente se, } \varphi(b) = b'.$$

Vamos mostrar que ψ é um homomorfismo de grupos.

Sejam $a', b' \in G'$ e $a, b \in G$ tais que $\psi(a') = a$ e $\psi(b') = b$. Então, $\varphi(a) = a'$, $\varphi(b) = b'$ e

$$\begin{aligned}
\psi(a' \star b') &= \psi\big(\varphi(a) \star \varphi(b)\big) \\
&\overset{(1)}{=} \psi\big(\varphi(a \cdot b)\big) \\
&\overset{(2)}{=} (\psi \circ \varphi)(a \cdot b) \\
&\overset{(3)}{=} a \cdot b \\
&= \psi(a') \cdot \psi(b') \quad \blacksquare
\end{aligned}$$

Em (1) usamos que φ é homomorfismo de grupos; em (2), a definição de composição de funções e em (3), que $\psi \circ \varphi = I_G$.

Definição 16 (Automorfismo)
Seja $(G,\cdot)$ um grupo. Um *automorfismo* de G é um isomorfismo $\varphi : G \longrightarrow G$.

Veremos agora um resultado muito importante.

Teorema 5 (Cayley)
Sejam $(G,\cdot)$ um grupo, $S_G = \{\sigma : G \longrightarrow G \ ; \ \sigma \text{ é uma bijeção } \}$ e $(S_G, \circ)$ o grupo das bijeções de G. Então, G é isomorfo a um subgrupo de S_G.

Demonstração: Vamos construir φ, um homomorfismo injetor de grupos de G em S_G. Assim, pela Proposição 12 item (iii), a imagem de φ é um subgrupo de S_G e é isomorfo a G.

Para cada $a \in G$ seja $\sigma_a : G \longrightarrow G$ a função definida por $\sigma_a(x) = a \cdot x$. Então, para $x, y \in G$,

$$\begin{array}{rll} \sigma_a(x) = \sigma_a(y) & \text{se, e somente se,} & a \cdot x = a \cdot y \\ & \text{se, e somente se,} & x = y. \end{array}$$

Logo, σ_a é uma função injetora. Além disso, para cada $b \in G$, temos que $b = a \cdot (a^{-1} \cdot b) = \sigma_a(a^{-1} \cdot b)$, mostrando que σ_a é uma função sobrejetora. Portanto, $\sigma_a \in S_G$, para cada $a \in G$.

Definimos $\varphi : G \longrightarrow S_G$ por $\varphi(a) = \sigma_a$.

Vamos mostrar que φ é um homomorfismo de grupos injetor.

Sejam $a, b \in G$. Temos que $\varphi(a \cdot b) = \sigma_{a \cdot b}$. Quem é $\sigma_{a \cdot b}$? Para entendermos esta função devemos aplicá-la nos elementos do seu domínio. Para isto, seja $x \in G$. Então,

$$\begin{array}{rcl} \sigma_{a \cdot b}(x) & \overset{(1)}{=} & (a \cdot b) \cdot x \\ & \overset{(2)}{=} & a \cdot (b \cdot x) \\ & \overset{(3)}{=} & \sigma_a(\sigma_b(x)) \\ & \overset{(4)}{=} & (\sigma_a \circ \sigma_b)(x). \end{array}$$

Em (1) usamos a definição de $\sigma_{a \cdot b}$; em (2), a associatividade da operação de G; em (3), as definições de σ_b e σ_a e em (4), a definição de composição.

Portanto, $\sigma_{a \cdot b} = \sigma_a \circ \sigma_b$. Logo, $\varphi(a \cdot b) = \sigma_{a \cdot b} = \sigma_a \circ \sigma_b = \varphi(a) \circ \varphi(b)$, mostrando que φ é homomorfismo de grupos.

Para mostrar que φ é injetora, vamos determinar o seu núcleo.

$$\begin{array}{rcl} \text{Núcleo}(\varphi) & = & \{a \in G \,;\, \varphi(a) = I_G\} \\ & = & \{a \in G \,;\, \sigma_a = I_G\} \\ & = & \{a \in G \,;\ \text{para todo } x \in G,\ a \cdot x = x\} \\ & = & \{a = e_G\}. \quad \blacksquare \end{array}$$

Corolário 3

Seja $(G, \cdot)$ um grupo com n elementos. Então, G é isomorfo a um subgrupo de S_n.

Demonstração: Basta observar que se G é um grupo com n elementos, então S_G é isomorfo a S_n. $\blacksquare$

Os grupos finitos são realizados como subgrupos de S_n. Portanto, S_n deve ser estudado mais atentamente, o que será feito na próxima Seção.

Observação:

(1) Os grupos de ordem 4, conforme visto na Seção 2, são o grupo cíclico de ordem 4 e o grupo de Klein, que são isomorfos a $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$, respectivamente.

(2) Os grupos de ordem 8 são, a menos de isomorfismo, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_8$, todos esses grupos abelianos, e os grupos não-abelianos dos quatérnios $\mathcal{Q}$ e o diedral D_4.

Veja Elementos de Álgebra de Arnaldo Garcia e Yves Lequain.

(3) Conhecemos dois exemplos de grupos com 6 elementos: cíclico e S_3. Encerramos essa Seção mostrando que, a menos de isomorfismo, o único grupo não-cíclico de ordem 6 é S_3.

De fato, seja $(G, \cdot)$ um grupo não-cíclico com 6 elementos. Pelo Teorema de Lagrange, para cada $x \in G$, temos que $\circ(x)$ divide 6 e, como $\circ(x) \neq 6$, logo $\circ(x) \in \{1, 2, 3\}$.

Afirmamos que G tem elemento de ordem 3. De fato, suponhamos, por absurdo, que todo elemento de G diferente de e_G tenha ordem 2. Então, para todo $x \in G$, temos que $x^2 = e_G$. Pelo Exercício 15 da Seção 1, G é um grupo abeliano. Escolhendo $x, y \in G \backslash \{e_G\}$ tais que $x \neq y$ temos que $H = \{e_G, x, y, x \cdot y\}$ é um subgrupo de G com $|H| = 4$, contradizendo o Teorema de Lagrange.

Seja $b \in G$ um elemento de ordem 3. Então, $\langle b \rangle = \{e_G, b, b^2\} \subsetneq G$. Existe $a \in G$ tal que $a \notin \langle b \rangle$.

Afirmamos que a ordem de a é 2. De fato, se $\circ(a) = 3$, então e_G, b, b^2, a, a^2, $b \cdot a$, $b \cdot a^2$, $b^2 \cdot a$ e $b^2 \cdot a^2$ são elementos de G distintos (verifique), contradizendo o fato de $|G| = 6$.

Portanto, $a^2 = e_G$ e $\{e_G, b, b^2, a, a \cdot b, a \cdot b^2\} \subset G$. Como os elementos do conjunto à esquerda são distintos temos que

$$G = \{e_G, b, b^2, a, a \cdot b, a \cdot b^2\}.$$

Afirmamos que $a \cdot b \neq b \cdot a$. De fato, se $a \cdot b = b \cdot a$, então $c = a \cdot b$ é um elemento de G de ordem 6, visto que $\text{mdc}(\circ(a), \circ(b)) = \text{mdc}(2, 3) = 1$, contradizendo o fato de G não ser grupo cíclico.

Veja Exercício 11, itens (a) e (b), da Seção 2.

Como $b \cdot a$ é diferente de e_G, b, b^2, a e de $a \cdot b$, a única possibilidade é $b \cdot a = a \cdot b^2$. Assim,

$$G = \{e_G, b, b^2, a, a \cdot b, a \cdot b^2 \,;\, b \cdot a = a \cdot b^2, a^2 = e_G, b^3 = e_G\},$$

Construindo o único isomorfismo $\varphi : G \longrightarrow S_3$ definido por $\varphi(a) = \sigma$

e $\varphi(b) = \tau$, mostramos que G é isomorfo a S_3 .

Exercícios

1. Sejam $(G, \cdot)$, $(G', \star)$ grupos e $\varphi : G \longrightarrow G'$ um homomorfismo de grupos. Mostre que $\varphi(G) = \{\varphi(a)\ ;\ a \in G\}$ é um subgrupo de G'.

2. Verifique quais das aplicações são homomorfismos de grupos e, no caso afirmativo, determine o núcleo e a imagem:

   (a) $\varphi : (\mathbb{R}^*, \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$, $x \longmapsto x^2$

   (b) $\varphi : (\mathbb{R}^*, \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$, $x \longmapsto 2^x$

   (c) $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \cdot)$, $x \longmapsto 2^x$

   (d) $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$, $x \longmapsto x + 1$

3. Sejam $(G, \cdot)$, $(G', \star)$ e $(G'', \star')$ grupos, $\varphi : G \longrightarrow G'$ e $\psi : G' \longrightarrow G''$ isomorfismos de grupos. Mostre que $\psi \circ \varphi : G \longrightarrow G''$ é um isomorfismo de grupos.

4. Seja $(G, \cdot)$ um grupo e fixe $a \in G$. Mostre que φ_a é um automorfismo de G, onde

$$\varphi_a : (G, \cdot) \longrightarrow (G, \cdot), \quad x \longmapsto axa^{-1}.$$

5. Seja $(G, \cdot)$ um grupo. Seja

$$\mathrm{Aut}(G) = \{\varphi : G \longrightarrow G\ ;\ \varphi \text{ é um automorfismo do grupo } G\}.$$

   (a) Mostre que $(\mathrm{Aut}(G), \circ)$ é um grupo, onde $\circ$ é a composição de funções.

   (b) Mostre que $(\mathrm{Aut}(\mathbb{Z}), \circ)$ é isomorfo a $(\{1, -1\}, \cdot)$.

6. Sejam $(G, \cdot)$, $(G', \star)$ grupos e $\varphi : G \longrightarrow G'$ um isomorfismo de grupos.

   (a) Mostre que se $a \in G$ e $\circ(a) = \infty$, então $\circ\big(\varphi(a)\big) = \infty$.

   (b) Mostre que se $a \in G$ e $\circ(a) = n$, então $\circ\big(\varphi(a)\big) = \circ(a)$.

7. Seja $(G, \cdot)$ um grupo cíclico infinito gerado por a.

(a) Mostre que $\varphi : (\mathbb{Z}, +) \longrightarrow (G, \cdot)$ definida por $\varphi(n) = a^n$ é um isomorfismo de grupos.

(b) Mostre que quaisquer dois grupos cíclicos infinitos são isomorfos.

8. Mostre que se $(G, \cdot)$ é um grupo cíclico de ordem n gerado por a, então G é isomorfo ao grupo $(\mathbb{Z}_n, +_{\mod n})$.

9. Seja $(G, \cdot)$ um grupo abeliano finito com $|\, G \,|$ elementos.

   Seja n um inteiro com $\text{mdc}(|\, G \,|, n) = 1$. Mostre que φ é um automorfismo, onde

$$\begin{array}{rccc} \varphi : & (G, \cdot) & \longrightarrow & (G, \cdot) \\ & x & \longmapsto & x^n. \end{array}$$

10. Seja $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \; ; \; a^2 + b^2 \neq 0, a, b \in \mathbb{R} \right\}$.

(a) Mostre que G é um grupo com a multiplicação usual de matrizes.

(b) Mostre que G é um grupo isomorfo a $(C^*, \cdot)$.

11. Determine quais das aplicações são automorfismos de grupos:

(a) $\varphi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ definida por $\varphi(x) = -x$.

(b) $\varphi : (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}^+, \cdot)$ definida por $\varphi(x) = x^2$.

(c) $\varphi : (\mathbb{R}^*, \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$ definida por $\varphi(x) = x^{-1}$.

(d) $\varphi : (S_3, \circ) \longrightarrow (S_3, \circ)$ definida por $\varphi(x) = x^{-1}$.

(e) $(G, \cdot)$ é um grupo cíclico de ordem 12 e $\varphi : (G, \cdot) \longrightarrow (G, \cdot)$ é definida por $\varphi(x) = x^3$.

(f) $(G, \cdot)$ é um grupo cíclico de ordem 12 e $\varphi : (G, \cdot) \longrightarrow (G, \cdot)$ é definida por $\varphi(x) = x^5$.

12. Mostre que $\mathbb{Z}_2 \times \mathbb{Z}_3$ é um grupo cíclico.

13. Mostre que $\mathbb{Z}_2 \times \mathbb{Z}_3$ e $\mathbb{Z}_6$ são grupos isomorfos.

14. Sejam m, n inteiros positivos primos entre si. Mostre $\mathbb{Z}_m \times \mathbb{Z}_n$ e $\mathbb{Z}_{m \cdot n}$ são grupos isomorfos.

15. Mostre que os grupos $\mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_4$ não são isomorfos.

16. Mostre que o grupo dos quatérnios e o grupo D_4 não são isomorfos.

17. Mostre que os grupos $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ e $\mathbb{Z}_8$ não são isomorfos.

18. Sejam $(G, \circ)$ e $(G', \cdot)$ os grupos dos Exercícios 5 e 16 da Seção 1. Mostre que a função $\varphi : (G', \cdot) \longrightarrow (G, \circ)$ definida por $\varphi(a, b) = \sigma_{a,b}$ é um isomorfismo de grupos.

O Grupo S_n

Pelo Teorema de Cayley, um grupo finito G pode ser visto como um subgrupo de S_n, onde $n = |G|$. Isso motiva o estudo mais detalhado de S_n, o grupo das permutações de $\{1, \ldots, n\}$.

Para estudar $S_n = \{\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\} \ ; \ \sigma \text{ é uma bijeção } \}$ vamos definir uma relação de equivalência no conjunto $S = \{1, \ldots, n\}$, a partir de um elemento σ de S_n fixado.

Definição 17 (Congruência módulo σ)
Seja $\sigma \in S_n$ fixado. Para $a, b \in S$, dizemos que a é *congruente a* b *módulo* σ se, e somente se, $b = \sigma^j(a)$, para algum $j \in \mathbb{Z}$. Nesse caso, escrevemos $a \equiv_\sigma b$.

$$a \equiv_\sigma b \iff b = \sigma^j(a), \text{ para algum } j \in \mathbb{Z}.$$

Proposição 16
A congruência módulo σ é uma relação de equivalência em $S = \{1, \ldots, n\}$.

Demonstração: Como $I_S = \sigma^0$, para cada $a \in S$, temos $a = I_S(a) = \sigma^0(a)$, logo $a \equiv_\sigma a$.

Se $a, b \in S$ e $a \equiv_\sigma b$, então existe $j \in \mathbb{Z}$ tal que $b = \sigma^j(a)$, logo $-j \in \mathbb{Z}$ e $\sigma^{-j}(b) = \sigma^{-j}(\sigma^j(a)) = (\sigma^{-j} \circ \sigma^j)(a) = a$, mostrando que $b \equiv_\sigma a$.

Finalmente, se $a, b, c \in S$, $a \equiv_\sigma b$ e $b \equiv_\sigma c$, então existem $i, j \in \mathbb{Z}$ tais que $b = \sigma^i(a)$ e $c = \sigma^j(b)$, logo $c = \sigma^j(\sigma^i(a)) = (\sigma^j \circ \sigma^i)(a) = \sigma^{j+i}(a)$, com $j + i \in \mathbb{Z}$. Portanto, $a \equiv_\sigma c$.

Como a congruência módulo σ é reflexiva, simétrica e transitiva, concluímos que é uma relação de equivalência. ■

Toda relação de equivalência em um conjunto define uma decomposição do conjunto em subconjuntos disjuntos, tais subconjuntos são as classes de equivalência.

Quem são as classes de equivalência da congruência módulo σ?

Para cada $a \in S$,

$$\begin{aligned} \text{classe de } a &= \{b \in S \ ; \ b = \sigma^j(a), \text{para algum } j \in \mathbb{Z}\} \\ &= \{\sigma^j(a) \ ; \ j \in \mathbb{Z}\}. \end{aligned}$$

Definição 18 (Órbita de a por σ)
Para cada $a \in S$, chamamos a classe de equivalência de a módulo σ de *órbita de* a *por* σ.

Observação: Antes de vermos um exemplo, convém observar que para cada $a \in S$ existe $\ell = \ell_a \geq 1$ tal que $\sigma^\ell(a) = a$.

De fato, $\{\sigma^j(a)\ ;\ j \in \mathbb{Z}\} \subset S$. Logo, a órbita de a por σ tem um número finito de elementos. Em particular $\{\sigma^j(a)\ ;\ j \in \mathbb{Z},\ j \geq 1\}$ é finito. Portanto, existem inteiros i, j, com $1 \leq i < j$, tais que $\sigma^i(a) = \sigma^j(a)$. Aplicando σ^{-i}, em ambos os lados dessa igualdade, obtemos $a = \sigma^{j-i}(a)$, com $j - i \geq 1$. Portanto, o conjunto $C = \{j \in \mathbb{Z}\ ;\ j \geq 1 \text{ e } \sigma^j(a) = a\}$ é um subconjunto não-vazio de inteiros limitado inferiormente. Pelo Princípio da Boa Ordenação, C tem um menor elemento, digamos ℓ. Então, $\sigma^\ell(a) = a$. ■

$\ell = \ell_a$ depende de $a \in S$.

Proposição 17 (Propriedade da órbita de a por σ)
A órbita de a por σ é $\{a, \sigma(a), \ldots, \sigma^{\ell-1}(a)\}$, onde $\ell = \ell_a$ é o menor inteiro positivo j tal que $\sigma^j(a) = a$. Mais ainda, se b está na órbita de a por σ, então $\sigma(b)$ também está na órbita de a por σ.

Demonstração: Seja $\ell = \ell(a)$ o menor inteiro positivo tal que $\sigma^j(a) = a$.

Primeiramente, observamos que $\sigma^{\ell \cdot q}(a) = a$, para todo $q \in \mathbb{Z}$. A demonstração é por indução sobre q. De fato, se $q = 0$, então $\sigma^0 = I$ e $\sigma^0(a) = a$. Suponhamos que $q \geq 0$ e $\sigma^{q \cdot \ell}(a) = a$. Então,

$$\sigma^{\ell \cdot (q+1)}(a) = \sigma^{\ell + \ell \cdot q}(a) = (\sigma^\ell \circ \sigma^{\ell \cdot q})(a) = \sigma^\ell(\sigma^{\ell \cdot q}(a)) \overset{(\star)}{=} \sigma^\ell(a) = a.$$

Em $(\star)$ usamos a hipótese de indução.

Logo, $\sigma^{\ell \cdot q}(a) = a$, para todo $q \geq 0$.

Se $q < 0$, então $-q > 0$, $\ell \cdot q = (-\ell)(-q)$ e $\sigma^{\ell \cdot q} = \sigma^{(-\ell)\cdot(-q)}$. Como $\sigma^\ell(a) = a$ se, e somente se, $a = \sigma^{-\ell}(a)$, pelo caso já demonstrado, obtemos $\sigma^{(-\ell)\cdot(-q)}(a) = a$.

Seja $i \in \mathbb{Z}$ e $\sigma^i(a)$ na órbita de a por σ. Pela divisão euclidiana de i por ℓ, existem inteiros q, r, univocamente determinados, tais que $i = q \cdot \ell + r$, onde $0 \leq r \leq \ell - 1$. Então,

$$\sigma^i(a) = \sigma^{q \cdot \ell + r}(a) = (\sigma^r \circ \sigma^{\ell \cdot q})(a) = \sigma^r(\sigma^{\ell \cdot q}(a)) = \sigma^r(a).$$

Portanto, a órbita de a por σ é

$$\begin{aligned} \{\sigma^i(a)\ ;\ i \in \mathbb{Z}\} &= \{\sigma^r(a)\ ;\ 0 \leq r \leq \ell - 1\} \\ &= \{a, \sigma(a), \ldots, \sigma^{\ell-1}(a)\}. \end{aligned}$$

Se b está na órbita de a por σ, então $b = \sigma^j(a)$, para algum $j \in \mathbb{Z}$, logo $\sigma(b) = \sigma(\sigma^j(a)) = \sigma^{j+1}(a)$ também está na órbita de a por σ. ■

Exemplo 34
Vamos determinar a órbita de a por σ, para cada $a \in \{1,2,3,4,5,6\}$, onde $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$.
órbita de $1 = \{\sigma(1) = 2,\ \sigma^2(1) = \sigma(\sigma(1)) = \sigma(2) = 1\} \Longrightarrow \ell_1 = 2$;
órbita de $3 = \{\sigma(3) = 3\} \Longrightarrow \ell_3 = 1$;
órbita de $4 = \{\sigma(4) = 5, \sigma^2(4) = \sigma(5) = 6, \sigma^3(4) = \sigma(\sigma^2(4)) = \sigma(6) = 4\} \Longrightarrow \ell_4 = 3$.
As classes de equivalência da congruência módulo σ, isto é, as órbitas de σ, são $\{1,2\}$, $\{3\}$ e $\{4,5,6\}$.

$S = \{1,2,3,4,5,6\}$

1 2	3	4 5 6

A órbita de a por σ tem as imagens por σ de todos os elementos da órbita.

Definição 19 (Ciclo de a por σ)
Dados $a \in S = \{1,\ldots,n\}$, $\sigma \in S_n$ e $\{a, \sigma(a), \ldots, \sigma^{\ell_a - 1}(a)\}$, a órbita de a por σ, chamamos $\big(a, \sigma(a), \ldots, \sigma^{\ell_a - 1}(a)\big)$, ou qualquer permutação circular, de *um ciclo de* σ.

Exemplo 35
Os ciclos de σ no Exemplo anterior são $(1,2)$, (3), $(4,5,6)$.

Exemplo 36
Consideremos $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 6 & 7 & 2 & 5 \end{pmatrix}$.
Os seguintes ciclos são ciclos de τ: $(1,3)$, $(2,4,6)$, $(5,7)$.

Veremos que conhecendo os ciclos de σ, conhecemos a função σ.

Definição 20 (r-ciclo)
Sejam $r \geq 2$ e $\{a_1,\ldots,a_r\} \subset S = \{1,\ldots,n\}$. Por um r-ciclo $(a_1,\ldots,a_r)$ entendemos uma permutação $\sigma : S \longrightarrow S$ definida por: $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\ldots$, $\sigma(a_{r-1}) = a_r$, $\sigma(a_r) = a_1$ e σ fixa todos os outros elementos de S.

Por um 1-ciclo (a) entendemos a permutação $I : S \longrightarrow S$.

Observação: Qualquer permutação circular do r-ciclo $(a_1, a_2, \ldots, a_r)$ define a mesma bijeção de S.

Exemplo 37

Seja $n = 9$ e consideremos o 5-ciclo $(1,3,4,2,6)$. Esse ciclo corresponde à permutação $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 2 & 5 & 1 & 7 & 8 & 9 \end{pmatrix}$.

É claro que $(3,4,2,6,1) = \sigma$, assim como qualquer permutação circular do 5-ciclo $(1,3,4,2,6)$, começando em qualquer um desses elementos.

Exemplo 38

Seja $n = 9$ e consideremos a permutação $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 2 & 3 & 7 & 8 & 6 & 5 & 9 \end{pmatrix}$.

Os ciclos de σ são $(1,4,3,2)$ $(5,7,6,8)$ e (9).

Observe que $\sigma = \varphi \circ \psi = \psi \circ \varphi$, onde $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 2 & 3 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} =$ $(1,4,3,2)$ e $\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 7 & 8 & 6 & 5 & 9 \end{pmatrix} = (5,7,6,8)$

Definição 21 (Multiplicação de ciclos)

Sejam $S = \{1, \ldots, n\}$, $\{i_1, \ldots, i_r\} \subset S$ e $\{j_1, \ldots, j_s\} \subset S$. Definimos o produto dos ciclos $\sigma = (i_1, \ldots, i_r)$ e $\tau = (j_1, \ldots, j_s)$ de S_n como a composição das permutações de S_n que eles representam, a saber,

$$(i_1, \ldots, i_r)(j_1, \ldots, j_s) = \sigma \circ \tau.$$

Exemplo 39

Vamos calcular os produtos de alguns ciclos de S_7.

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

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

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

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

Exemplo 40

Vamos determinar os ciclos de σ, para cada $\sigma \in S_8$.

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 \end{pmatrix}$

Os ciclos de σ são $(1,2,3,8,5,6,4)$ e (7).

Temos $\sigma = (1,2,3,8,5,6,4)$.

(b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \end{pmatrix}$

Os ciclos de σ são $(1,3,5,7)$ e $(2,4,6,8)$.

Temos $\sigma = (1,3,5,7)(2,4,6,8)$.

Definição 22 (Ciclos disjuntos)

Sejam $S = \{1,\ldots,n\}$, $\{i_1,\ldots,i_r\} \subset S$ e $\{j_1,\ldots,j_s\} \subset S$.

Dizemos que $(i_1,\ldots,i_r)$ e $(j_1,\ldots,j_s)$ são *ciclos disjuntos* se, e somente se, $\{i_1,\ldots,i_r\} \cap \{j_1,\ldots,j_s\} = \emptyset$.

Exemplo 41

Sejam $\sigma \in S_n$ e $a, b \in S = \{1,\ldots,n\}$.

Se b não está na órbita de a por σ, então (órbita de a) $\cap$ (órbita de b) $= \emptyset$ e os ciclos $\big(a, \sigma(a), \ldots, \sigma^{\ell_a - 1}(a)\big)$ e $\big(b, \sigma(b), \ldots, \sigma^{\ell_b - 1}(b)\big)$ são ciclos disjuntos.

Se (órbita de a) $\cap$ (órbita de b) $\neq \emptyset$, então a órbita de a e a órbita de b são as mesmas e $\big(b, \sigma(b), \ldots, \sigma^{\ell_b - 1}(b)\big)$ é uma permutação circular de $\big(a, \sigma(a), \ldots, \sigma^{\ell_a - 1}(a)\big)$, com $\ell_b = \ell_a$.

No Exemplo 39 vimos que $(1,4,3)(2,5,7) = (2,5,7)(1,4,3)$. Essa é uma propriedade válida para todos os ciclos disjuntos.

Proposição 18 (Propriedade de ciclos disjuntos)

Se $\sigma = (i_1,\ldots,i_r)$ e $\tau = (j_1,\ldots,j_s)$ são ciclos de S_n disjuntos, então $\sigma \circ \tau = \tau \circ \sigma$.

Demonstração: De fato, sejam $A = \{i_1,\ldots,i_r\}$ e $B = \{j_1,\ldots,j_s\}$, tais que $A \cap B = \emptyset$ e $S = \{1,\ldots,n\}$. Se $j \in S \backslash (A \cup B)$, então e σ e τ fixam j, logo $\sigma(\tau(j)) = j = \tau(\sigma(j))$. Se $j \in A$, então $j = i_k$, $\sigma(i_k) = i_\ell$, $\tau(j) = j$ e $\tau(i_\ell) = i_\ell$, assim $\sigma(\tau(j)) = \sigma(j) = i_\ell$ e $\tau(\sigma(j)) = \tau(i_\ell) = i_\ell$. Se $j \in B$, então $j = j_k$, $\tau(j_k) = j_\ell$, $\sigma(j) = j$ e $\sigma(j_\ell) = j_\ell$, assim $\tau(\sigma(j)) = \tau(j) = j_\ell$ e $\sigma(\tau(j)) = \sigma(j_\ell) = j_\ell$. Portanto, $\sigma \circ \tau = \tau \circ \sigma$. ■

Proposição 19

Toda permutação σ em S_n se escreve, de modo único, a menos da ordem, como produto dos seus ciclos.

Demonstração: Seja $\sigma \in S_n$. Para cada $a \in S$, o ciclo de a por σ é da forma $\big(a, \sigma(a), \ldots, \sigma^{\ell_a - 1}(a)\big)$, para algum $\ell_a \geq 1$ e os ciclos de σ são disjuntos. Seja ψ a permutação que é o produto dos ciclos de σ. Então, $\psi(b) = \sigma(b)$, pois cada $b \in S$ ocorre em um único ciclo de σ. ■

Nesse caso, $n \geq 2$.

Corolário 4

Toda permutação $\sigma \in S_n$, $\sigma \neq I$, se escreve, de modo único, a menos da ordem, como produto de r-ciclos disjuntos, onde $r \geq 2$.

Demonstração: Como $\sigma \neq I$, existe $a \in S$ tal que $\sigma(a) \neq a$, logo há órbitas com pelo menos 2 elementos. Consideremos os ciclos de σ provenientes dessas órbitas. Esses ciclos determinam σ e são r-ciclos com $r \geq 2$. ■

Exemplo 42

Vamos escrever as seguintes permutações de S_{10} como produto de r-ciclos disjuntos com $r \geq 2$.

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 & 10 & 8 & 9 \end{pmatrix} \\ &= (1,3,5,7)(2,4,6)(8,10,9)\end{aligned}$$

$$\begin{aligned}\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 9 & 7 & 2 & 1 & 5 & 3 & 6 & 10 & 4 \end{pmatrix} \\ &= (1,8,6,5)(2,9,10,4)(3,7)\end{aligned}$$

$$\begin{aligned}\psi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 5 & 1 & 8 & 9 & 6 & 10 & 3 & 2 & 7 \end{pmatrix} \\ &= (1,4,8,3)(2,5,9)(6)(7,10) \\ &= (1,4,8,3)(2,5,9)(7,10)\end{aligned}$$

Consideremos o r-ciclo $(1,2,\ldots,r)$ com $r \geq 2$.

Observamos que $(1,2,\ldots,r) = (1,r)(1,r-1)\cdots(1,3)(1,2)$.

Em geral, $(i_1,\ldots i_r) = (i_1,i_r)(i_1,i_{r-1})\cdots(i_1,i_3)(i_1,i_2)$.

Exemplo 43

$(2,4,5,3) = (2,3)(2,5)(2,4)$

$(1,3,2,7,6) = (1,6)(1,7)(1,2)(1,3)$

$(1,3,2) = (1,2)(1,3)$ e $(1,3,2) = (1,2,3)(1,2,3) = (1,3)(1,2)(1,3)(1,2)$.

Lema 2

Seja $n \geq 2$. Toda permutação em S_n é o produto de 2-ciclos.

Demonstração: Seja $\sigma \in S_n$, onde $n \geq 2$. Se $\sigma \neq I$, escreva σ como o produto dos seus r-ciclos disjuntos, onde $r \geq 2$. Escrevendo cada r-ciclo como produto de 2-ciclos, obtemos o resultado.

Temos $I = (1,2)(1,2)$. Logo, I é produto de dois 2-ciclos. Se $n > 2$ há outras maneiras de escrever I como produto de 2-ciclos. ■

Corolário 5

S_n, $n \geq 2$, é gerado pelo conjunto de todos os 2-ciclos.

Definição 23 (Transposições)

Os 2-ciclos em S_n são chamados de *transposições*.

Observação: No Exemplo 43, escrevemos $(1,3,2)$ como produto de transposições de duas maneiras distintas, entretanto, em ambas as escritas, utilizamos um número par de transposições.

Exemplo 44

Todo r-ciclo, com $r \geq 2$ é o produto de $r-1$ transposições.

De fato, $(i_1,\ldots,i_r) = \underbrace{(i_1,i_r)\cdots(i_1,i_3)(i_1,i_2)}_{r-1 \text{ transposições}}$.

Definição 24 (Permutação par ou permutação ímpar)

Uma permutação $\sigma \in S_n$ é chamada *permutação par* se, e somente se, σ é um produto de um número par de transposições. Caso contrário, σ é chamada de uma *permutação ímpar*.

Vamos mostrar que a definição acima faz sentido, isto é, escrevendo $\sigma \in S_n$ como produto de transposições, podemos obter fatorações com o número de transposições diferente, mas será sempre um número par ou sempre um número ímpar.

Para isto, consideremos o polinômio $p(x_1,\ldots,x_n) = \prod_{1\leq i<j\leq n}(x_i - x_j)$.

Os fatores são construídos com todos os subconjuntos $\{x_i, x_j\}$ possíveis, tomando $i < j$.

Dada $\sigma \in S_n$, σ age no polinômio por

$$\sigma(p(x_1,\ldots,x_n)) = \prod_{1\leq i<j\leq n}\left(x_{\sigma(i)} - x_{\sigma(j)}\right).$$

$\{x_1,\ldots,x_n\} = \{x_{\sigma(1)},\ldots,x_{\sigma(n)}\}$.

Temos que $\sigma(p(x_1,\ldots,x_n)) = \pm p(x_1,\ldots,x_n)$.

Por exemplo, sejam $\sigma = (1,3,2)$ e $\tau = (1,2)$ em S_3.

Seja $p(x_1,x_2,x_3) = (x_1-x_2)(x_1-x_3)(x_2-x_3)$, então

$$\begin{aligned}
\sigma(p(x_1,x_2,x_3)) &= (x_{\sigma(1)}-x_{\sigma(2)})(x_{\sigma(1)}-x_{\sigma(3)})(x_{\sigma(2)}-x_{\sigma(3)}) \\
&= (x_3-x_1)(x_3-x_2)(x_1-x_2) \\
&= p(x_1,x_2,x_3) \text{ e} \\
\tau(p(x_1,x_2,x_3)) &= (x_{\tau(1)}-x_{\tau(2)})(x_{\tau(1)}-x_{\tau(3)})(x_{\tau(2)}-x_{\tau(3)}) \\
&= (x_2-x_1)(x_2-x_3)(x_1-x_3) \\
&= -p(x_1,x_2,x_3).
\end{aligned}$$

Proposição 20

Se σ é uma transposição de S_n, então $\sigma(p(x_1,\ldots,x_n)) = -p(x_1,\ldots,x_n)$.

Demonstração: Seja $\sigma = (i_1, i_2) \in S_n$, com $i_1 < i_2$. Então, $\sigma(i_1) = i_2$, $\sigma(i_2) = i_1$ e $\sigma(\ell) = \ell$, para todo $\ell \neq i_1$ e $\ell \neq i_2$.

Vamos analisar a ação de σ em cada fator $x_i - x_j$ de $p(x_1,\ldots,x_n)$, com $1 \leq i < j \leq n$.

A ação de σ em $x_i - x_j$ é $x_{\sigma(i)} - x_{\sigma(j)}$. Na tabela a seguir, denotaremos essa ação por $x_i - x_j \overset{\sigma}{\longmapsto} x_{\sigma(i)} - x_{\sigma(j)}$ e veremos se há troca de sinal no fator $x_{\sigma(i)} - x_{\sigma(j)}$ de $\sigma(p(x_1,\ldots,x_n))$.

$i \neq i_1, j \neq i_2$	$x_i - x_j \overset{\sigma}{\longmapsto} x_i - x_j$	não há troca de sinal
$i = i_1 < j = i_2$	$x_{i_1} - x_{i_2} \overset{\sigma}{\longmapsto} x_{i_2} - x_{i_1}$	1 troca de sinal (I)
$i = i_1 < j < i_2$	$x_{i_1} - x_j \overset{\sigma}{\longmapsto} x_{i_2} - x_j$	há troca de sinal (II)
$i = i_1 < i_2 < j$	$x_{i_1} - x_j \overset{\sigma}{\longmapsto} x_{i_2} - x_j$	não há troca de sinal
$i < j = i_1 < i_2$	$x_i - x_{i_1} \overset{\sigma}{\longmapsto} x_i - x_{i_2}$	não há troca de sinal
$i_1 < i = i_2 < j$	$x_{i_2} - x_j \overset{\sigma}{\longmapsto} x_{i_1} - x_j$	não há troca de sinal
$i < i_1 < i_2 = j$	$x_i - x_{i_2} \overset{\sigma}{\longmapsto} x_i - x_{i_1}$	não há troca de sinal
$i_1 < i < i_2 = j$	$x_i - x_{i_2} \overset{\sigma}{\longmapsto} x_i - x_{i_1}$	há troca de sinal (III)

Começam em $i = i_1$ e $j \neq i_2$.

Terminam em i_1.

Começam em i_2.

Terminam em i_2 e $i \neq i_1$.

Precisamos contar quantas trocas de sinal temos em (II) e em (III), que é equivalente a contar os valores possíveis para j e i, respectivamente.

Em (II) temos $i_2 - i_1 - 1$ valores possíveis para j e em (III), também $i_2 - i_1 - 1$ valores possíveis para i. Logo, no total temos

$$(I) + (II) + (III) = 1 + 2(i_2 - i_1 - 1)$$

trocas de sinal. Então, $\sigma(p(x_1,\ldots,x_n)) = -p(x_1,\ldots,x_n)$. ■

Uma definição alternativa para permutações pares e ímpares é

$$\begin{aligned} \sigma \text{ é par} &\iff \sigma(p(x_1,\ldots,x_n)) = p(x_1,\ldots,x_n) \\ \sigma \text{ é ímpar} &\iff \sigma(p(x_1,\ldots,x_n)) = -p(x_1,\ldots,x_n) \end{aligned}$$

Exemplo 45

Como o r-ciclo $\sigma = (i_1, i_2, \ldots, i_r) = (i_1, i_r)\cdots(i_1, i_2)$ é o produto de $r-1$ tansposições, então σ é par se, e somente se, r é ímpar.

O produto de duas permutações pares é par, I é par e a inversa de uma permutação par é par, então o conjunto das permutações pares é um subgrupo de S_n.

Definição 25 (Grupo Alternado)
Seja $A_n = \{\sigma \in S_n \ ; \ \sigma \text{ é permutação par }\}$. A_n é chamado de *grupo alternado.*

Quantos elementos A_n tem?

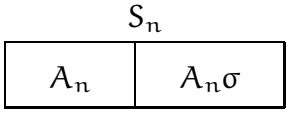
A congruência módulo A_n define uma partição de S_n em dois subconjuntos disjuntos, as classes de equivalência módulo A_n, onde uma das classes é A_n e a outra é $A_n\sigma$, onde σ é qualquer permutação ímpar.

De fato, dadas σ e τ em S_n temos:

$$\begin{aligned} \sigma \equiv \tau \mod A_n &\iff \sigma \circ \tau^{-1} \in A_n \\ &\iff \sigma \text{ e } \tau^{-1} \text{ são ambas pares ou ambas ímpares} \\ &\iff \sigma \text{ e } \tau \text{ são ambas pares ou ambas ímpares} \end{aligned}$$

τ é par $\iff \tau^{-1}$ é par
τ é ímpar $\iff \tau^{-1}$ é ímpar.

Assim, duas permutações estão na mesma classe se, e somente se, são ambas pares ou ambas ímpares. Tomando σ ímpar, temos que $A_n\sigma$ só tem permutações ímpares, $A_n\sigma \neq A_n$, a classe das permutações pares.



Portanto, $n! = |S_n| = 2 \cdot |A_n|$, isto é, $|A_n| = \frac{n!}{2}$.

Lembre que se G é um grupo finito e H é um subgrupo de G, então as classes de H em G têm o mesmo número de elementos de H.

Finalizamos com o seguinte resultado importante.

Proposição 21
Para todo $n \geq 2$, os ciclos $(1,2)$ e $(1,2,\ldots,n)$ geram S_n.

Demonstração: Sejam $\sigma = (1,2)$, $\tau = (1,2,\ldots,n)$ e $G = \langle \sigma, \tau \rangle$. Vamos mostrar que se $1 \leq r \neq s \leq n$, então qualquer transposição $(r,s) \in G$, seguindo do Corolário 5 que $S_n \subset G$. Como $G \subset S_n$, obtemos $G = S_n$.

Temos em G as seguintes transposições:

$\tau\sigma\tau^{-1} = (2,3)$, $\tau^2\sigma\tau^{-2} = (3,4)$, $\ldots$, $\tau^{r-1}\sigma\tau^{-(r-1)} = (r, r+1)$.

Portanto, G contém também as seguintes transposições:

$(1,2)(2,3)(1,2) = (1,3)$,

$(1,3)(3,4)(1,3) = (1,4)$,

$\vdots$

$(1,r-1)(r-1,r)(1,r-1) = (1,r)$.

Daí segue que para quaisquer r, s com $1 < r \neq s \leq n$ temos que

$$(1,r)(1,s)(1,r) = (r,s). \qquad \blacksquare$$

Exercícios

1. Decomponha as seguintes permutações em produto de ciclos disjuntos e, em seguida, escreva-as como produto de transposições:

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

2. Diga se são pares ou ímpares as seguintes permutações:

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}.$$

3. Determine os elementos pares e os elementos ímpares de S_3. Determine A_3.

4. (a) Escreva os elementos de S_4 como produto de ciclos disjuntos.
   (b) Determine os elementos pares e os elementos ímpares de S_4. Determine A_4.

5. Mostre que:
   (a) um r-ciclo é par se, e somente se, r é ímpar;
   (b) um r-ciclo é ímpar se, e somente se, r é par.

6. Mostre que:
   (a) a inversa de uma permutação ímpar é uma permutação ímpar;
   (b) a inversa de uma permutação par é uma permutação par.

7. Se $n > 2$ mostre que todo elemento de A_n é o produto de um certo número de 3-ciclos.

   Sugestão: $(i,j)(j,k) = (i,j,k)$ e $(i,j)(k,t) = (k,j,i)(k,t,i)$.