
Universidade Federal de São Paulo

Instituto de Ciência e Tecnologia



**Mestrado Profissional em Matemática
em Rede Nacional - PROFMAT**

**Teoria de grupos e permutações:
fundamentos e aplicações didáticas no jogo
do Quinze e nos sólidos platônicos**

Luis Felipe Fernandes de Pádua Leite

Orientadora: Prof^ª. Dr^ª. Fernanda de Andrade Pereira

São José dos Campos
Fevereiro, 2026



PROFMAT

Título: *Teoria de grupos e permutações: fundamentos e aplicações didáticas no jogo do Quinze e nos sólidos platônicos*

Dissertação apresentada ao Instituto de Ciência e Tecnologia da UNIFESP, campus São José dos Campos/SP, como parte dos requisitos exigidos para a obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

São José dos Campos
Fevereiro, 2026

Sobrenome, nome

Teoria de grupos e permutações: fundamentos e aplicações didáticas no jogo do Quinze e nos sólidos platônicos, Luis Felipe Fernandes de Pádua Leite – São José dos Campos, 2026.
ix, 114f.

Dissertação (Mestrado) – Universidade Federal de São Paulo. Instituto de Ciência e Tecnologia. Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT).

Title

1. Teoria de Grupos. 2. Permutações. 3. Jogo do 15. 4. Sólidos platônicos. 5. Sequência didática.

UNIVERSIDADE FEDERAL DE SÃO PAULO
INSTITUTO DE CIÊNCIA E TECNOLOGIA

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Chefe de departamento:

Prof. Dr. Marcelo Cristino Gama

Coordenador do Programa de Pós-Graduação:

Profa. Dra. Cláudia Aline Azevedo dos Santos Mesquita

LUIS FELIPE FERNANDES DE PÁDUA LEITE

TEORIA DE GRUPOS E PERMUTAÇÕES: FUNDAMENTOS E
APLICAÇÕES DIDÁTICAS NO JOGO DO QUINZE E NOS
SÓLIDOS PLATÔNICOS

Presidente da banca: Prof^ª. Dr^ª. Fernanda de Andrade Pereira

Banca examinadora:

Prof^ª. Dr^ª Grasiele Cristiane Jorge

Prof. Dr. Vanderley Alves Ferreira Junior

Prof. Dr. Luiz Felipe Nobili França

Data da Defesa: 20 de Fevereiro de 2026

Nada de desgosto, nem de desânimo; se acabas de fracassar, recomeça.

AGRADECIMENTOS

A conclusão desta dissertação representa muito mais do que o fechamento de uma etapa acadêmica; é também um marco profundo em minha vida pessoal. Ao olhar para trás, vejo que cada página escrita só foi possível graças a pessoas que estiveram ao meu lado, oferecendo apoio, inspiração e coragem para seguir em frente. É a elas que dedico estas palavras de gratidão.

Aos meus pais, que são e sempre serão o alicerce da minha existência, deixo um agradecimento que nenhuma frase consegue traduzir por completo. O amor incondicional, a força nos momentos de dificuldade e o exemplo diário de coragem e dedicação moldaram quem eu sou. Vocês me ensinaram não só a sonhar alto, mas também a transformar cada sonho em um caminho concreto. Esta vitória é minha, mas também é, em igual medida, de vocês.

À minha orientadora, professora Fernanda, vai minha admiração e reconhecimento. Sua paciência, generosidade e rigor acadêmico foram fundamentais em cada passo desta jornada. Com suas observações cuidadosas, mostrou-me como a pesquisa é também um exercício de humildade e curiosidade. Obrigado por acreditar no meu potencial e por me incentivar a buscar sempre mais do que eu mesmo acreditava ser capaz.

À professora Grasielle, registro meu sincero agradecimento. Sua capacidade de organizar, liderar e acolher foi essencial para que todo este processo acontecesse com clareza e firmeza. A dedicação com que conduz cada desafio é um exemplo que levo comigo, não apenas para a vida acadêmica, mas também para o cotidiano.

Um reconhecimento especial ao jornalista Julio Buzzi, que acompanha minha caminhada com atenção e sensibilidade. Suas reportagens não apenas relatam fatos, mas capturam a essência dos caminhos percorridos, transformando conquistas pessoais em mensagens de estímulo para muitos outros. Obrigado por dar voz e luz a estas histórias que, de outra forma, talvez passassem despercebidas.

Por fim, estendo minha gratidão a todos os amigos, colegas e familiares que, de algum modo, estiveram presentes nesta trajetória. Cada palavra de incentivo, cada troca de ideias, cada gesto de carinho foi um sopro de energia nos dias em que o cansaço parecia maior do que a vontade de continuar.

Esta dissertação, portanto, não é apenas fruto de esforço individual. Ela reflete uma rede de afeto, inspiração e apoio que me sustentou ao longo do caminho. A cada um de vocês, deixo não só um “obrigado”, mas a certeza de que esta conquista é também parte da história que escrevemos juntos.

RESUMO

A teoria de grupos ocupa posição de destaque na matemática contemporânea por explicitar relações entre estruturas algébricas abstratas e situações concretas. Nesse quadro, ideias como permutações, ciclos, invariantes e subgrupos tornam-se particularmente nítidas quando examinadas em problemas clássicos de simetria e em jogos matemáticos. Nesta dissertação, essa articulação é conduzida a partir de dois focos: a análise do jogo do 15 e o estudo das simetrias dos sólidos platônicos, com ênfase em como o formalismo algébrico descreve e organiza regularidades observáveis.

No desenvolvimento do trabalho, são apresentados tópicos basilares da teoria de grupos, tais como classes de equivalência, homomorfismos e decomposições em classes laterais, sempre acompanhados de exemplos que sustentam a intuição e o rigor conceitual. Na sequência, expõe-se uma análise minuciosa do jogo do 15, na qual propriedades algébricas e combinatórias são empregadas para fundamentar critérios de alcançabilidade e procedimentos de transformação. Em paralelo, investigam-se as simetrias dos sólidos platônicos, destacando a estrutura de seus grupos de rotações e o modo como essas ações podem ser interpretadas como permutações de elementos associados ao sólido.

Como desdobramento aplicado, propõe-se uma abordagem pedagógica direcionada a estudantes dos anos finais do ensino fundamental, estruturada em sequências didáticas que introduzem noções de álgebra por meio de atividades com o jogo do 15 e com modelos dos sólidos platônicos. Pretende-se, com isso, favorecer o raciocínio lógico e a argumentação matemática, convertendo conceitos abstratos em experiências manipuláveis, passíveis de discussão e verificáveis no ambiente escolar.

O eixo central da pesquisa é a articulação entre teoria e prática, oferecendo ao docente um percurso para tratar conteúdos avançados com rigor, sem prescindir de contextos lúdicos e acessíveis. Ao vincular resultados formais a situações concretas, busca-se contribuir para um ensino de álgebra mais significativo, em que a estrutura conceitual seja compreendida como instrumento de interpretação e não apenas como técnica operacional.

Palavras-chave: 1. Teoria de Grupos. 2. Permutações. 3. Jogo do 15. 4. Sólidos platônicos. 5. Sequência didática.

ABSTRACT

Group theory holds a prominent place in contemporary mathematics because it makes explicit the relationships between abstract algebraic structures and concrete situations. In this context, ideas such as permutations, cycles, invariants, and subgroups become particularly clear when examined through classical problems of symmetry and mathematical games. In this dissertation, this articulation is developed through two main focuses: the analysis of the 15-puzzle and the study of the symmetries of the Platonic solids, with emphasis on how algebraic formalism describes and organizes observable regularities.

Throughout the development of this work, foundational topics in group theory are presented, such as equivalence classes, homomorphisms, and decompositions into cosets, always accompanied by examples that support both intuition and conceptual rigor. Next, a thorough analysis of the 15-puzzle is provided, in which algebraic and combinatorial properties are employed to establish criteria of reachability and transformation procedures. In parallel, the symmetries of the Platonic solids are investigated, highlighting the structure of their rotation groups and the way these actions may be interpreted as permutations of elements associated with the solid.

As an applied development, a pedagogical approach aimed at students in the final years of elementary school is proposed, structured through didactic sequences that introduce notions of algebra by means of activities involving the 15-puzzle and models of the Platonic solids. The intention is therefore to foster logical reasoning and mathematical argumentation, transforming abstract concepts into manipulable experiences that can be discussed and verified in the school environment.

The central axis of this research is the articulation between theory and practice, offering teachers a pathway for addressing advanced content with rigor, without dispensing with playful and accessible contexts. By linking formal results to concrete situations, the study seeks to contribute to a more meaningful teaching of algebra, in which conceptual structure is understood as an instrument of interpretation rather than merely as an operational technique.

Keywords: 1. Group Theory. 2. Permutations. 3. 15 puzzle. 4. Platonic solids. 5. Instructional sequence.

SUMÁRIO

INTRODUÇÃO	3
1 GRUPOS	4
1.1 Classe de equivalência	4
1.2 Grupos	6
1.2.1 Exemplos de grupo	10
1.3 Subgrupos	16
1.3.1 Exemplos de subgrupos	18
1.3.2 Classificação dos Subgrupos de $(\mathbb{Z}, +)$	21
1.4 Subgrupo gerado por um subconjunto	21
1.4.1 Ordem de grupos e elementos	25
1.5 Classes laterais e teorema de Lagrange	28
1.6 Subgrupos normais e grupos quocientes	36
1.7 Introdução aos morfismos de grupos	44
1.8 Isomorfismos de grupos	52
2 GRUPO DE PERMUTAÇÃO	57
2.1 A notação de ciclos	57
2.2 Decomposição de uma permutação em ciclos disjuntos	59
2.3 Permutações pares e ímpares	66
2.4 O grupo alternado	68
3 JOGO DO 15	73
3.1 Configurações, reversibilidade e a questão central	74
3.2 Popularidade	74
3.3 O desafio de Sam Loyd e sua impossibilidade	75
3.4 Contagem de configurações	75
3.5 Enumeração das casas e codificação do estado	76
3.6 Composição de permutações e paridade	77
3.6.1 Ordem de composição e não comutatividade	77
3.6.2 Algoritmo de decomposição: ideia geral e exemplo	78
3.7 Movimentos válidos e transposições	79
3.7.1 Exemplo: atualização de estado e inversão de paridade	80
3.7.2 Sequências de movimentos e efeito cumulativo	80
3.8 Configurações equivalentes e o papel da cor da casa do vazio	81
3.9 Critério de equivalência: condições necessárias e suficientes	81

4	O JOGO DO 15 NA SALA DE AULA: POR QUÊ E PARA QUÊ?	85
4.1	Visão geral da sequência	86
4.2	Fundamentação pedagógica	86
4.3	Roteiro da Aula 1	88
4.4	Roteiro da Aula 2	89
4.5	Materiais de aplicação e anexos didáticos	91
4.6	Conclusão	93
4.7	Recomendações finais ao(à) professor(a)	93
5	NOTAS INTRODUTÓRIAS AO ESTUDO DOS SÓLIDOS PLATÔNICOS	94
5.1	Sólidos platônicos	95
5.1.1	Definições e caracterização dos sólidos platônicos	96
5.1.2	O grupo de rotações do tetraedro	98
5.1.3	O grupo de rotações do cubo	100
5.1.4	O grupo de rotações do dodecaedro	102
5.2	Considerações finais	103
6	OS SÓLIDOS PLATÔNICOS NA SALA DE AULA: POR QUÊ E PARA QUÊ?	105
6.1	Visão geral da sequência	106
6.2	Fundamentação pedagógica	107
6.3	Roteiro da Aula 1	108
6.4	Roteiro da Aula 2	109
6.5	Materiais de aplicação e anexos didáticos	112
6.6	Conclusão	113
6.7	Recomendações finais ao(à) professor(a)	113

INTRODUÇÃO

A teoria de grupos constitui um dos pilares da álgebra moderna, oferecendo uma linguagem para descrever estruturas que aparecem em diferentes áreas da matemática. Ao formalizar a noção de simetria e de transformação, é possível identificar padrões, invariantes e regularidades em sistemas variados, conectando aspectos abstratos a representações concretas.

Este trabalho toma como fio condutor duas situações matemáticas com forte apelo intuitivo: o jogo do 15 e as simetrias dos sólidos platônicos. Em ambos os casos, a intenção é evidenciar como conceitos como permutações, ciclos e subgrupos surgem naturalmente quando se descrevem movimentos, composições e ações sobre conjuntos finitos.

A exposição inicia-se com a revisão de noções fundamentais, incluindo a definição de grupo e propriedades básicas, além de construções e resultados usuais como classes laterais, subgrupos normais e isomorfismos. Esses elementos fornecem o vocabulário necessário para a modelagem algébrica adotada nas análises posteriores.

No jogo do 15, considera-se um tabuleiro com quinze peças numeradas e uma casa vazia, no qual movimentos válidos correspondem ao deslizamento de uma peça adjacente para a posição livre. A passagem de uma configuração a outra pode ser descrita por permutações induzidas por sequências de movimentos, de modo que a composição dessas transformações organiza um quadro algébrico adequado para discutir alcançabilidade e estrutura das configurações.

No estudo dos sólidos platônicos, investigam-se as rotações que preservam o sólido e a ação dessas rotações sobre elementos associados, como faces, arestas ou vértices. Essa perspectiva conduz naturalmente a grupos finitos de simetria e à interpretação dessas ações como permutações, permitindo comparar, classificar e relacionar as estruturas obtidas.

Além da análise teórica, o trabalho propõe sequências didáticas voltadas ao ensino médio, articuladas em atividades com o jogo do 15 e com modelos dos sólidos platônicos. Busca-se favorecer o desenvolvimento do raciocínio lógico e da argumentação matemática, aproximando a linguagem algébrica de situações manipuláveis e discutíveis em sala de aula.

Ao final, espera-se que a articulação entre teoria e aplicações contribua para um ensino de álgebra mais significativo, no qual a formalização seja percebida como instrumento de compreensão. A proposta é oferecer ao professor um percurso didático que preserve o rigor, ao mesmo tempo em que explora contextos acessíveis para introduzir ideias de simetria, permutação e estrutura algébrica.

GRUPOS

Neste capítulo, apresentamos os fundamentos da teoria de grupos: grupos, subgrupos, classes laterais, subgrupos normais, grupos quociente, morfismos e isomorfismos de grupos. O texto é desenvolvido de forma autossuficiente, com a inclusão de diversos exemplos e das principais demonstrações, de modo a torná-lo acessível mesmo a leitores sem contato prévio com o tema. As principais referências utilizadas são [8, 5, 7, 6, 1].

1.1 CLASSE DE EQUIVALÊNCIA

Antes de introduzirmos o conceito de grupos, é essencial possuir a compreensão de um conceito fundamental e intrínseco da matemática: o de classes de equivalências. Tal conceito trata de uma forma de agrupar elementos de um conjunto segundo uma relação que associa de forma significativa os seus elementos. Nesse sentido, um exemplar clássico é a relação de congruência entre os números inteiros, que permite classificar os números em subconjuntos formados por aqueles que possuem o mesmo resto em uma divisão. Essa forma de perceber os elementos é uma ferramenta poderosa para simplificar estruturas e analisar problemas com maior clareza e objetividade.

Definição 1.1.1. *Seja X um conjunto e seja R uma relação binária em X . Dizemos que R é uma **relação de equivalência** em X se satisfaz as seguintes propriedades, para quaisquer $x, y, z \in X$:*

1. **Reflexiva:** $x R x$.
2. **Simétrica:** se $x R y$, então $y R x$.
3. **Transitiva:** se $x R y$ e $y R z$, então $x R z$.

Definição 1.1.2. *Seja R uma relação de equivalência em X e seja $a \in X$. A **classe de equivalência** de a (com respeito a R), denotada por $[a]$, é o subconjunto de X definido por*

$$[a] = \{ x \in X \mid x R a \}.$$

Ou seja, $[a]$ é o conjunto de todos os elementos de X que estão relacionados com a pela relação R .

As classes de equivalência assim definidas apresentam propriedades fundamentais que descrevemos a seguir.

Em primeiro lugar, as classes de equivalência induzidas por R formam uma **partição** de X . Isto significa que cada elemento $x \in X$ pertence a exatamente uma dessas classes, de modo que não há sobreposição entre classes distintas. Mais precisamente:

1. Cada elemento $x \in X$ pertence à sua própria classe $[x]$, de modo que nenhuma classe é vazia.
2. A união de todas as classes de equivalência é o conjunto X , isto é,

$$\bigcup_{a \in X} [a] = X.$$

3. As classes são mutuamente disjuntas: se $[a] \cap [b] \neq \emptyset$, então necessariamente $[a] = [b]$.

Proposição 1.1.3. *Seja R uma relação de equivalência em A e seja $a \in A$. Então $a \in [a]$.*

Demonstração. Seja R uma relação de equivalência em A e $a \in A$. Queremos demonstrar que $a \in [a]$, onde a classe de equivalência de a é definida por $[a] = \{x \in A \mid x R a\}$. Pela definição de relação de equivalência, R é reflexiva, simétrica e transitiva. Em particular, a reflexividade garante que, para qualquer $a \in A$, temos $a R a$. Isso significa que a está relacionado a si mesmo pela relação R . Agora, pela definição de classe de equivalência, um elemento x pertence à classe de equivalência $[a]$ se, e somente se, $x R a$. Como a reflexividade de R nos assegura que $a R a$, segue que $a \in [a]$. $\square$

Proposição 1.1.4. *Seja R uma relação de equivalência em A , e sejam $a, b \in A$. Então $a R b$ se, e somente se, $[a] = [b]$.*

Demonstração. Seja R uma relação de equivalência em A e sejam $a, b \in A$. Queremos demonstrar que $a R b$ se, e somente se, $[a] = [b]$, onde as classes de equivalência são definidas como $[a] = \{x \in A \mid x R a\}$ e $[b] = \{x \in A \mid x R b\}$.

Suponha que $a R b$. Se $a R b$, pela transitividade e simetria da relação R , qualquer elemento $x \in [a]$ também estará em $[b]$, e vice-versa. De fato, seja $x \in [a]$. Por definição de classe de equivalência, $x R a$. Como $a R b$ e R é transitiva, segue que $x R b$. Assim, $x \in [b]$. Reciprocamente, seja $y \in [b]$. Por definição, $y R b$. Como $b R a$ (pela simetria de R) e R é transitiva, segue que $y R a$. Assim, $y \in [a]$. Logo, $[a] \subseteq [b]$ e $[b] \subseteq [a]$, o que implica $[a] = [b]$.

Suponha que $[a] = [b]$. Se $[a] = [b]$, então, em particular, $b \in [a]$, pois $b \in [b]$. Pela definição de $[a]$, isso implica que $b R a$. Como R é simétrica, segue que $a R b$. $\square$

Proposição 1.1.5. *Se R é uma relação de equivalência em A , e $a, x, y \in A$ são tais que $x \in [a]$ e $y \in [a]$, então $x R y$.*

Demonstração. Seja R uma relação de equivalência em A , e sejam $a, x, y \in A$ tais que $x \in [a]$ e $y \in [a]$. Pela definição de classe de equivalência, temos que $[a] = \{z \in A \mid z R a\}$.

Assim, $x \in [a]$ implica que $x R a$, e $y \in [a]$ implica que $y R a$. Como R é uma relação de equivalência, ela é transitiva. Dessa forma, $x R a$ e $y R a$ implicam, pela simetria, que $a R y$ e, pela transitividade, que $x R y$. Portanto, demonstramos que, se $x, y \in [a]$, então $x R y$. $\square$

Proposição 1.1.6. *Seja R relação de equivalência em A , e suponha que $[a] \cap [b] \neq \emptyset$. Então, $[a] = [b]$.*

Demonstração. Seja R uma relação de equivalência definida em um conjunto A . Sabemos que R é reflexiva, simétrica e transitiva, e que, para qualquer elemento $a \in A$, a classe de equivalência de a , denotada por $[a]$, é o conjunto dado por $[a] = \{x \in A \mid x R a\}$. Suponha agora que $[a] \cap [b] \neq \emptyset$, ou seja, as classes de equivalência de a e b possuem pelo menos um elemento em comum. Seja $x \in [a] \cap [b]$. Por definição de classe de equivalência, isso implica que $x R a$ e $x R b$. Como R é simétrica, de $x R a$, temos que $a R x$. Usando a transitividade de R , como $a R x$ e $x R b$, concluímos que $a R b$. Isso significa que a e b estão relacionados por R . Para mostrar que $[a] = [b]$, devemos provar que todo elemento de $[a]$ pertence a $[b]$ e vice-versa. Seja $y \in [a]$. Por definição, isso significa que $y R a$. Como $a R b$ e $y R a$, pela transitividade de R , temos que $y R b$, o que implica $y \in [b]$. Portanto, $[a] \subseteq [b]$. De maneira análoga, seja $z \in [b]$. Então, $z R b$. Como $b R a$ e $z R b$, pela transitividade de R , temos $z R a$, o que implica $z \in [a]$. Assim, $[b] \subseteq [a]$. Concluímos que $[a] = [b]$. $\square$

1.2 GRUPOS

As classes de equivalência permitem reunir elementos que são considerados “iguais” segundo um determinado critério. Essa ideia está ligada ao conceito de simetria, que aparece em figuras geométricas, em padrões da natureza e até em leis da Física. Ao estudar as transformações que preservam essas simetrias, chegamos naturalmente ao conceito de grupo.

De forma geral, um grupo é uma estrutura matemática que expressa o comportamento das simetrias e das transformações. Rigorosamente, definimos um grupo como um conjunto munido de uma operação que satisfaz três propriedades: associatividade, existência de um elemento neutro e existência de elementos inversos. Apesar da abstração, a teoria de grupos tem aplicações bastante concretas e efetivas, como na resolução de equações algébricas, desenvolvimento de sistemas de criptografia e até na análise de jogos e quebra-cabeças, como o sudoku, o cubo mágico e o jogo do 15.

O estudo de grupos assume um papel central na matemática, pois oferece uma linguagem universal e unifica em termos de descrição simétricas e suas transformações nos mais diversificados contextos. Nesse viés, a estrutura permite que diversas áreas do conhecimento sejam analisadas sob uma ótica comum, o que promove uma generalização maior nos seus resultados. Dessa forma, técnicas e ideias desenvolvidas em uma esfera específica

de conhecimento podem ser transferidas e compreendidas para outros campos de estudo, o que permite um escopo de aplicação maior.

Definição 1.2.1. *Seja G um conjunto não vazio. Uma função $*$: $G \times G \rightarrow G$ é chamada de uma operação binária sobre G . A imagem de (x, y) pela operação binária $*$ é escrita como $x * y$, em vez de $*(x, y)$.*

Observação 1.2.2. *Uma operação binária em S associa a cada par ordenado de elementos de S exatamente um elemento de S . Como uma operação é uma função, deve-se garantir que ela esteja bem definida. Isso significa que, se $(a, b) = (c, d)$ em $S \times S$ (ou seja, $a = c$ e $b = d$), então $a * b = c * d$. Em outras palavras, $*$ está bem definida se:*

$$\forall a, b, c, d \in S, a = c \text{ e } b = d \implies a * b = c * d.$$

Exemplo 1.2.3. *A adição em $\mathbb{Z}$ e a multiplicação em $\mathbb{R}$:*

$$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad \cdot : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R},$$

são operações binárias.

Definição 1.2.4. *Seja X um conjunto. Denotamos por $\mathcal{P}(X)$ o conjunto das partes de X , definido por*

$$\mathcal{P}(X) = \{ A \mid A \subseteq X \}.$$

Em outras palavras, $\mathcal{P}(X)$ é o conjunto formado por todos os subconjuntos de X , incluindo o subconjunto vazio $\emptyset$ e o próprio X .

Exemplo 1.2.5. *Sejam $A, B \subseteq X$. Então $A \cup B$, $A \cap B$ e $A - B$ são subconjuntos de X . Assim, união, interseção e diferença são operações binárias em $\mathcal{P}(X)$.*

Exemplo 1.2.6. *Seja X um conjunto qualquer. O conjunto de todas as bijeções de X em X é denotado por $\text{Bij}(X)$, isto é,*

$$\text{Bij}(X) = \{ f \mid f : X \rightarrow X \text{ é uma função bijetora} \}.$$

Dadas duas funções $f, g \in \text{Bij}(X)$, a sua composição $f \circ g : X \rightarrow X$, definida por $(f \circ g)(x) = f(g(x))$ para todo $x \in X$, é também uma função bijetora de X em X (pois a composição de bijeções é uma bijeção). Portanto, a composição é uma operação interna em $\text{Bij}(X)$, ou seja, $f \circ g \in \text{Bij}(X)$.

Definição 1.2.7. *Um grupo é uma estrutura algébrica formada por um conjunto G juntamente com uma operação binária*

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a * b \end{aligned}$$

satisfazendo as seguintes condições:

1. Associatividade: Para todos os elementos $a, b, c \in G$, vale que $(a * b) * c = a * (b * c)$.
2. Elemento neutro: Existe um elemento $e \in G$ tal que, para todo $a \in G$, $a * e = e * a = a$.
3. Elemento inverso: Para cada elemento $a \in G$, existe um elemento $b \in G$ tal que $a * b = b * a = e$, onde e é o elemento neutro.

Observação 1.2.8. *Se, adicionalmente, a operação $*$ for comutativa, ou seja, $a * b = b * a$ para todos os $a, b \in G$, o grupo é denominado abeliano ou comutativo.*

Observação 1.2.9. *Seja $(G, \cdot)$ um grupo.*

1. A cardinalidade do conjunto G é chamada de ordem do grupo e é denotada por $|G|$.
2. Se $|G| < \infty$, o grupo é chamado de finito. Caso contrário, é dito infinito.
3. Quando não houver possibilidade de confusão, podemos omitir o símbolo da operação, escrevendo ab em vez de $a \cdot b$.
4. Por outro lado, quando utilizamos a notação aditiva $(+)$, sempre escrevemos $a + b$.

Proposição 1.2.10. *O elemento neutro em G é único.*

Demonstração. Considere dois elementos neutros e_1 e e_2 em G . Por definição, e_1 satisfaz $e_1 \cdot a = a$ e $a \cdot e_1 = a$ para todo $a \in G$, e e_2 satisfaz $e_2 \cdot a = a$ e $a \cdot e_2 = a$ para todo $a \in G$.

Tomando $a = e_2$ na definição de e_1 , temos $e_1 \cdot e_2 = e_2$. De forma similar, tomando $a = e_1$ na definição de e_2 , temos $e_1 \cdot e_2 = e_1$. Logo, $e_1 = e_2$. $\square$

Proposição 1.2.11. *Para cada $a \in G$, existe um único inverso de a em G , denotado por a^{-1} .*

Demonstração. A existência decorre diretamente da definição de grupo, que garante que, para todo $a \in G$, existe $a^{-1} \in G$ tal que $a \cdot a^{-1} = e$ e $a^{-1} \cdot a = e$, onde e é o elemento neutro.

Para demonstrar a unicidade, suponha que b e c sejam dois inversos de a . Então, $a \cdot b = e$ e $a \cdot c = e$. Multiplicando à esquerda a equação $a \cdot b = e$ pelo elemento c , temos $c \cdot (a \cdot b) = c \cdot e$.

Usando a associatividade, $(c \cdot a) \cdot b = c$, e como $c \cdot a = e$, segue $e \cdot b = c$. Como $e \cdot b = b$, temos $b = c$, provando que o inverso de a é único. $\square$

Proposição 1.2.12. *Seja $(G, \cdot)$ um grupo. Para quaisquer $a, b, c \in G$, se $c \cdot a = b$, então:*

$$c = b \cdot a^{-1}.$$

Demonstração. Sejam $a, b, c \in G$ tais que $c \cdot a = b$. Mostraremos que $c = b \cdot a^{-1}$.

A partir da igualdade $c \cdot a = b$, multiplicamos ambos os lados da equação à direita pelo inverso de a , a^{-1} , obtendo $(c \cdot a) \cdot a^{-1} = b \cdot a^{-1}$.

Pela associatividade, $c \cdot (a \cdot a^{-1}) = b \cdot a^{-1}$. Sabemos que $a \cdot a^{-1} = e$, de modo que $c \cdot e = b \cdot a^{-1}$. Como $c \cdot e = c$, segue que $c = b \cdot a^{-1}$. Assim, a proposição é demonstrada. $\square$

Proposição 1.2.13. *Seja $(G, \cdot)$ um grupo. Para quaisquer $a, b \in G$, então $(ab)^{-1} = b^{-1}a^{-1}$.*

Demonstração. Sejam $a, b \in G$. Queremos mostrar que $(ab)^{-1} = b^{-1}a^{-1}$. Para isso, basta verificar que $b^{-1}a^{-1}$ é o inverso de ab , ou seja, que $(ab) \cdot (b^{-1}a^{-1}) = e$, assim como $(b^{-1}a^{-1}) \cdot (ab) = e$, onde e é o elemento neutro de G . Como o inverso de um elemento é único, basta verificar essas igualdades.

Calculamos $(ab) \cdot (b^{-1}a^{-1})$. Usando a associatividade da operação do grupo, temos

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

Como $b \cdot b^{-1} = e$, isso se reduz a $a \cdot e \cdot a^{-1} = a \cdot a^{-1}$. E, como $a \cdot a^{-1} = e$, concluímos que $(ab) \cdot (b^{-1}a^{-1}) = e$.

Agora, calculamos $(b^{-1}a^{-1}) \cdot (ab)$. Novamente, usando a associatividade, temos

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

Como $a^{-1} \cdot a = e$, isso se reduz a $b^{-1} \cdot e \cdot b = b^{-1} \cdot b$. E, como $b^{-1} \cdot b = e$, concluímos que $(b^{-1}a^{-1}) \cdot (ab) = e$.

Portanto, $b^{-1}a^{-1}$ é o inverso de ab . Assim, segue que $(ab)^{-1} = b^{-1}a^{-1}$, como queríamos demonstrar. $\square$

Proposição 1.2.14 (Lei do Cancelamento). *Seja $(G, \cdot)$ um grupo. Para todos $a, b, c \in G$, valem as implicações:*

$$a \cdot b = a \cdot c \implies b = c \quad e \quad b \cdot a = c \cdot a \implies b = c.$$

Demonstração. Suponha que $a \cdot b = a \cdot c$. Como G é um grupo, o elemento a possui um inverso $a^{-1} \in G$. Multiplicando ambos os membros da igualdade à esquerda por a^{-1} , obtemos:

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

Pela propriedade associativa da operação do grupo, podemos reescrever ambos os lados como:

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

Por definição de inverso, temos $a^{-1} \cdot a = e$, onde e é o elemento neutro de G . Logo, a igualdade torna-se:

$$e \cdot b = e \cdot c.$$

Uma vez que e é o elemento neutro, segue que $e \cdot b = b$ e $e \cdot c = c$, o que implica:

$$b = c.$$

Isso estabelece a lei do cancelamento à esquerda.

A demonstração do cancelamento à direita é similar. Suponha agora que $b \cdot a = c \cdot a$. Multiplicando ambos os lados à direita por a^{-1} , temos:

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

Novamente, pela associatividade, obtemos:

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

Como $a \cdot a^{-1} = e$, segue que:

$$b \cdot e = c \cdot e.$$

Dado que e é o elemento neutro, $b \cdot e = b$ e $c \cdot e = c$, donde concluímos:

$$b = c,$$

completando a demonstração da lei do cancelamento à direita. □

1.2.1 Exemplos de grupo

1. $(\mathbb{Z}_n, \oplus)$ é um grupo abeliano finito com n elementos.

Seja $n \in \mathbb{N}$, com $n \geq 2$. Define-se em $\mathbb{Z}$ a relação de congruência módulo n por:

$$a \equiv b \pmod{n} \quad \text{se, e somente se,} \quad n \mid (a - b),$$

para quaisquer $a, b \in \mathbb{Z}$. Esta relação é uma relação de equivalência. O conjunto de todas as classes de equivalência é denotado por $\mathbb{Z}/n\mathbb{Z}$ ou simplesmente $\mathbb{Z}_n$, e seus elementos são:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\},$$

onde $\bar{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$ é a classe de equivalência de a . Os elementos de $\mathbb{Z}_n$ são chamados de classes residuais módulo n . Além disso, se p é um número primo, o conjunto das classes não nulas em $\mathbb{Z}_p$, com a operação de multiplicação módulo p , forma um grupo abeliano, frequentemente denotado por $((\mathbb{Z}_p) \setminus \{0\}, \odot)$.

Em $\mathbb{Z}_n$, definem-se as operações de adição $\oplus$ e multiplicação $\odot$ pondo:

$$\bar{a} \oplus \bar{b} = \overline{a + b} \quad \text{e} \quad \bar{a} \odot \bar{b} = \overline{a \cdot b},$$

para quaisquer $\bar{a}, \bar{b} \in \mathbb{Z}_n$. Pode-se verificar que estas operações estão bem definidas, isto é, não dependem dos representantes escolhidos para as classes.

O conjunto $\mathbb{Z}_n$ é um exemplo importante de estrutura com duas operações. Por exemplo, para $n = 6$, temos $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. A adição e a multiplicação são realizadas módulo 6. Assim,

$$\bar{5} \oplus \bar{4} = \overline{5+4} = \bar{9} = \bar{3}, \quad \text{pois } 9 \equiv 3 \pmod{6}.$$

$$\bar{3} \odot \bar{4} = \overline{3 \cdot 4} = \bar{12} = \bar{0}, \quad \text{pois } 12 \equiv 0 \pmod{6}.$$

Note que, neste caso, o resultado da multiplicação de duas classes não nulas ($\bar{3}$ e $\bar{4}$) é a classe nula ($\bar{0}$). O elemento neutro de $\odot$ é $\bar{1}$ e não existe inverso de $\bar{3}$ em relação a $\odot$, portanto $(\mathbb{Z}_6^*, \odot)$ não é um grupo.

2. Os conjuntos $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$ formam grupos abelianos sob a adição. Da mesma forma, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ e $(\mathbb{C} \setminus \{0\}, \cdot)$ constituem grupos abelianos quando munidos da multiplicação.

Exemplo 1.2.15. Se $K = \mathbb{R}$ e $n = 2$, então:

$$GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}.$$

Aqui, $ad - bc$ é o determinante da matriz, e a condição $ad - bc \neq 0$ garante que a matriz é invertível.

3. Seja $\mathbb{Z}_n^\times$ o conjunto dos elementos inversíveis de $\mathbb{Z}_n$ com respeito à multiplicação, isto é, das classes $\bar{r}$ para as quais existe $\bar{s} \in \mathbb{Z}_n$ tal que $\bar{r} \cdot \bar{s} = \bar{1}$. Então, $(\mathbb{Z}_n^\times, \cdot)$ forma um grupo de ordem $\varphi(n)$, em que $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ denota a função de Euler, definida por $\varphi(n) = \#\{r \in \{1, \dots, n\} : \text{mdc}(r, n) = 1\}$.

Demonstração. A operação é associativa e tem $\bar{1}$ como elemento neutro. Considere um elemento $x \in \mathbb{Z}_n^\times$. Ele é invertível se existe $y \in \mathbb{Z}_n$ tal que $x \cdot y \equiv 1 \pmod{n}$. Isso significa que existe um inteiro k tal que $x \cdot y - kn = 1$. Esse é o enunciado de uma combinação linear entre x e n que resulta em 1. Assim, x será invertível em $\mathbb{Z}_n$ se, e somente se, essa equação puder ser satisfeita.

- Se $\text{mdc}(x, n) = 1$, então x é invertível:

Pelo Teorema de Bézout, se $\text{mdc}(x, n) = 1$, existem inteiros a e b tais que $a \cdot x + b \cdot n = 1$. Reduzindo essa equação módulo n , obtemos $a \cdot x \equiv 1 \pmod{n}$, ou seja, a é o inverso multiplicativo de x em $\mathbb{Z}_n$. Logo, x é invertível em $\mathbb{Z}_n$.

- Se x é invertível, então $\text{mdc}(x, n) = 1$:

Suponha que x seja invertível em $\mathbb{Z}_n$, ou seja, existe um $y \in \mathbb{Z}_n$ tal que $x \cdot y \equiv 1 \pmod{n}$, o que implica $x \cdot y - kn = 1$. Essa é uma combinação linear de x e n que resulta em 1. Como $\text{mdc}(x, n)$ divide qualquer combinação linear de x e n , segue que $\text{mdc}(x, n)$ divide 1. O único divisor positivo de 1 é 1, portanto, $\text{mdc}(x, n) = 1$.

□

4. Seja X um conjunto qualquer. O conjunto $\text{Bij}(X) = \{f : X \rightarrow X \mid f \text{ é uma bijeção}\}$ é definido como o conjunto de todas as funções bijetoras de X em X . $(\text{Bij}(X), \circ)$ é um grupo, não abeliano em geral, onde a operação $\circ$ é a composição de funções. Observe que o grupo $\text{Bij}(X)$ será abeliano se o conjunto X tiver um ou dois elementos.

Caso o conjunto C tenha um número finito n de elementos, $\text{Bij}(C)$ será denotado por S_n e será chamado grupo simétrico ou grupo das permutações de n letras. Temos que $|S_n| = n!$.

Demonstração. Seja X um conjunto não-vazio. Considere

$$\begin{aligned} \circ : \text{Bij}(X) \times \text{Bij}(X) &\rightarrow \text{Bij}(X) \\ (\sigma, \tau) &\mapsto \tau \circ \sigma \end{aligned}$$

Primeiro, vamos mostrar que a operação de composição está bem definida. Sejam $\sigma, \tau \in \text{Bij}(X)$. Precisamos mostrar que $\tau \circ \sigma \in \text{Bij}(X)$. Para isso, verificamos que $\tau \circ \sigma$ é injetora e sobrejetora. A função $\tau \circ \sigma$ é injetora pois, se $\tau \circ \sigma(x) = \tau \circ \sigma(y)$, então $\tau(\sigma(x)) = \tau(\sigma(y))$. Como τ é injetora, temos $\sigma(x) = \sigma(y)$, e como σ é injetora, concluímos que $x = y$. Além disso, $\tau \circ \sigma$ é sobrejetora pois, para qualquer $z \in X$, como τ é sobrejetora, existe $y \in X$ tal que $\tau(y) = z$, e como σ é sobrejetora, existe $x \in X$ tal que $\sigma(x) = y$. Portanto, $\tau \circ \sigma(x) = \tau(\sigma(x)) = \tau(y) = z$, o que mostra que $\tau \circ \sigma$ é sobrejetora. Assim, $\tau \circ \sigma \in \text{Bij}(X)$, e a operação de composição está bem definida.

Agora, vamos verificar a associatividade. A composição de funções é sempre associativa. Para $\sigma, \tau, \rho \in \text{Bij}(X)$, temos $(\rho \circ \tau) \circ \sigma = \rho \circ (\tau \circ \sigma)$. Isso ocorre porque, para qualquer $x \in X$, vale $(\rho \circ \tau) \circ \sigma(x) = \rho(\tau(\sigma(x))) = \rho \circ (\tau \circ \sigma)(x)$. Portanto, a operação $\circ$ é associativa.

O elemento neutro de $\text{Bij}(X)$ é a função identidade $\text{id}_X : X \rightarrow X$, definida por $\text{id}_X(x) = x$ para todo $x \in X$. Para qualquer $\sigma \in \text{Bij}(X)$, temos $\sigma \circ \text{id}_X = \sigma$ e $\text{id}_X \circ \sigma = \sigma$. Isso mostra que id_X é o elemento neutro da operação de composição.

Por fim, todo elemento de $\text{Bij}(X)$ tem um inverso. Dada uma bijeção $\sigma \in \text{Bij}(X)$, sua inversa $\sigma^{-1} : X \rightarrow X$ também é uma bijeção e satisfaz $\sigma \circ \sigma^{-1} = \text{id}_X$ e $\sigma^{-1} \circ \sigma = \text{id}_X$. Portanto, σ^{-1} é o inverso de σ .

□

5. O grupo S_3 :

$$S_3 = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\},$$

onde a notação $\begin{pmatrix} 123 \\ abc \end{pmatrix}$ representa a função definida da seguinte maneira: $f(1) = a$, $f(2) = b$ e $f(3) = c$.

Sejam $\alpha = \begin{pmatrix} 123 \\ 231 \end{pmatrix}$ e $\beta = \begin{pmatrix} 123 \\ 213 \end{pmatrix}$; temos

$$\alpha^2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \quad \alpha^3 = id, \quad \beta^2 = id,$$

$$\beta\alpha = \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \quad \alpha\beta = \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \quad \alpha^2\beta = \begin{pmatrix} 123 \\ 132 \end{pmatrix}.$$

Observe que foi verificado acima que α e β geram o grupo S_3 , ou seja, todos os elementos do grupo são produtos finitos de fatores iguais a α ou β ; foi também verificado que $\alpha^3 = id$, $\beta^2 = id$ e que $\beta\alpha = \alpha^2\beta \neq \alpha\beta$.

6. O grupo S_Δ das simetrias espaciais de um triângulo equilátero:

Seja $P_1P_2P_3$ um triângulo equilátero. Coloque o centro de gravidade do triângulo na origem 0 do espaço e chame de D_1, D_2, D_3 as retas do espaço determinadas pelas medianas do triângulo. As transformações espaciais que preservam o triângulo são:

- $id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}$: as rotações planas centradas em 0, no sentido anti-horário, de ângulos zero, $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$, respectivamente.
- R_1, R_2, R_3 : as rotações espaciais de ângulo π com eixos D_1, D_2, D_3 , respectivamente.

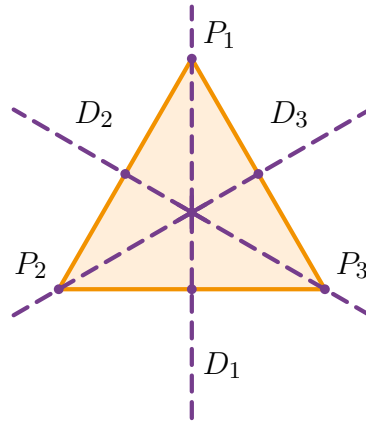


Figura 1: Os eixos de reflexão de um triângulo equilátero.

O conjunto definido pelas rotações planas e espaciais

$$S_{\Delta} := \{id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}$$

com a composição de funções é um grupo.

O grupo não é abeliano, pois temos:

$$R_1 \circ R_2 = R_{\frac{2\pi}{3}} \quad \text{e} \quad R_2 \circ R_1 = R_{\frac{4\pi}{3}}.$$

Os elementos $R_{\frac{2\pi}{3}}$ e R_1 geram o grupo S_{Δ} , isto é, todo elemento de S_{Δ} pode ser expresso como uma composição finita de $R_{\frac{2\pi}{3}}$ e R_1 .

$\circ$	id	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
id	id	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	id	R_3	R_1	R_2
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	id	$R_{\frac{2\pi}{3}}$	R_2	R_3	R_1
R_1	R_1	R_2	R_3	id	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$
R_2	R_2	R_3	R_1	$R_{\frac{4\pi}{3}}$	id	$R_{\frac{2\pi}{3}}$
R_3	R_3	R_1	R_2	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	id

7. Produto Direto de Grupos:

Sejam $(G_1, \cdot)$ e $(G_2, \cdot)$ dois grupos. No conjunto $G_1 \times G_2$ defina a operação

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2).$$

$(G_1 \times G_2, \cdot)$ é um grupo (chamado produto direto de G_1 com G_2); o elemento neutro de $G_1 \times G_2$ é (e_1, e_2) , onde e_i é o elemento neutro de G_i , $i = 1, 2$; o elemento inverso de (g_1, g_2) é (g_1^{-1}, g_2^{-1}) . Além disso, $(G_1 \times G_2, \cdot)$ é um grupo abeliano se e somente se $(G_1, \cdot)$ e $(G_2, \cdot)$ são grupos abelianos.

Mais geralmente, dados grupos $(G_1, \cdot), \dots, (G_n, \cdot)$, definimos a noção de produto direto $G_1 \times G_2 \times \dots \times G_n$.

Proposição 1.2.16. *Seja $\{G_i\}_{i \in I}$ uma coleção arbitrária de grupos, com $I \subseteq \mathbb{N}$. Definimos o conjunto produto por*

$$\prod_{i \in I} G_i = \{(a_i)_{i \in I} \mid a_i \in G_i, \forall i \in I\}.$$

Considere a função

$$\cdot : \left(\prod_{i \in I} G_i \right) \times \left(\prod_{i \in I} G_i \right) \longrightarrow \prod_{i \in I} G_i$$

dada por

$$\left((a_i)_{i \in I}, (b_i)_{i \in I}\right) \mapsto (a_i b_i)_{i \in I}.$$

Para cada $(a_i)_{i \in I}, (b_i)_{i \in I} \in \prod_{i \in I} G_i$, definimos a operação ponto a ponto dada por:

$$(a_i)_{i \in I} \cdot (b_i)_{i \in I} = (a_i \cdot b_i)_{i \in I},$$

onde a operação $a_i \cdot b_i$ é aquela definida em G_i . Então, $\left(\prod_{i \in I} G_i, \cdot\right)$ é um grupo, chamado de produto direto da família $\{G_i\}_{i \in I}$. Além disso, se cada G_i for abeliano para todo $i \in I$, então $\prod_{i \in I} G_i$ também é um grupo abeliano.

Demonstração. Para demonstrar que $(\prod_{i \in I} G_i, \cdot)$ é um grupo, seguimos uma estrutura semelhante à da imagem, utilizando $a = (a_i)_{i \in I}$, $b = (b_i)_{i \in I}$, e $c = (c_i)_{i \in I}$ como seqüências em $\prod_{i \in I} G_i$.

(1) Associatividade: Queremos mostrar que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Pela definição da operação ponto a ponto, temos:

$$a \cdot (b \cdot c) = (a_i)_{i \in I} \cdot (b_i \cdot c_i)_{i \in I} = (a_i \cdot (b_i \cdot c_i))_{i \in I}.$$

Por outro lado:

$$(a \cdot b) \cdot c = (a_i \cdot b_i)_{i \in I} \cdot (c_i)_{i \in I} = ((a_i \cdot b_i) \cdot c_i)_{i \in I}.$$

Como cada G_i é um grupo, a operação em G_i é associativa, ou seja, $a_i \cdot (b_i \cdot c_i) = (a_i \cdot b_i) \cdot c_i$ para todo $i \in I$. Portanto:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(2) Elemento neutro: Definimos o elemento neutro $e = (e_i)_{i \in I}$, onde e_i é o elemento neutro de G_i para cada $i \in I$. Para qualquer $a = (a_i)_{i \in I} \in \prod_{i \in I} G_i$, temos:

$$a \cdot e = (a_i \cdot e_i)_{i \in I} = (a_i)_{i \in I} = a,$$

e

$$e \cdot a = (e_i \cdot a_i)_{i \in I} = (a_i)_{i \in I} = a.$$

Logo, e é o elemento neutro de $\prod_{i \in I} G_i$.

(3) Inverso: Para cada $a = (a_i)_{i \in I} \in \prod_{i \in I} G_i$, definimos o inverso como $a^{-1} = (a_i^{-1})_{i \in I}$, onde a_i^{-1} é o inverso de a_i em G_i . Então:

$$a \cdot a^{-1} = (a_i \cdot a_i^{-1})_{i \in I} = (e_i)_{i \in I} = e,$$

e

$$a^{-1} \cdot a = (a_i^{-1} \cdot a_i)_{i \in I} = (e_i)_{i \in I} = e.$$

Portanto, todo elemento de $\prod_{i \in I} G_i$ possui um inverso.

(4) Comutatividade (se cada G_i for abeliano): Suponha que cada G_i seja abeliano. Sejam $a = (a_i)_{i \in I}$ e $b = (b_i)_{i \in I} \in \prod_{i \in I} G_i$. Então:

$$a \cdot b = (a_i \cdot b_i)_{i \in I} = (b_i \cdot a_i)_{i \in I} = b \cdot a,$$

onde a igualdade central segue da comutatividade de cada G_i . Portanto, $\prod_{i \in I} G_i$ é abeliano.

Concluimos que $(\prod_{i \in I} G_i, \cdot)$ é um grupo, e se cada G_i for abeliano, então $\prod_{i \in I} G_i$ também é abeliano. $\square$

Exemplo 1.2.17. Seja $I = \{1, 2\}$ e considere os grupos $G_1 = \mathbb{Z}_2$ com adição módulo 2 e $G_2 = \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ com adição módulo 3. O produto direto $\prod_{i \in I} G_i = G_1 \times G_2$ consiste em todos os pares ordenados (a_1, a_2) , onde $a_1 \in \mathbb{Z}_2$ e $a_2 \in \mathbb{Z}_3$, cujos elementos são:

$$\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$

A operação é definida coordenada a coordenada, ou seja, dados (a_1, a_2) e (b_1, b_2) , temos $(a_1, a_2) \cdot (b_1, b_2) = (a_1 + b_1 \bmod 2, a_2 + b_2 \bmod 3)$. Por exemplo, para $\mathbf{a} = (1, 2)$ e $\mathbf{b} = (0, 1)$, a operação resulta em $\mathbf{a} \cdot \mathbf{b} = (1, 0)$. O elemento neutro é $(0, 0)$, e o inverso de (a_1, a_2) é $(-a_1 \bmod 2, -a_2 \bmod 3)$, como no caso de $(1, 2)$, cujo inverso é $(1, 1)$.

1.3 SUBGRUPOS

Nesta seção, apresentaremos o conceito de subgrupo. De maneira geral, podemos imaginar um grupo como um sistema matemático no qual os elementos interagem segundo regras que estão bem definidas. Um subgrupo, constitui um subconjunto desse sistema que, apesar de conter menos elementos, preserva integralmente as propriedades da estrutura original.

A ideia para o estudo dos subgrupos está em analisar a estrutura interna de um grupo. Assim, desejamos identificar subconjuntos que preservam as mesmas propriedades de um conjunto maior. Por exemplo, o conjunto dos números pares formam um subgrupo do grupo dos inteiros com a operação de adição, pois é fechado sob essa operação, contém o elemento neutro e é fechado sob o inverso aditivo.

Além de sua importância na estrutura interna dos grupos, os subgrupos estão intrinsicamente relacionados a conceitos mais sofisticados, como homomorfismos e grupos quocientes. O subgrupo, como ferramenta para o ensino de álgebra abstrata, é indispensável para analisar simetrias e classificar estruturas algébricas.

Definição 1.3.1. Seja $(G, \cdot)$ um grupo. Um subconjunto não vazio H de G é um subgrupo de G (denotamos $H < G$) quando, com a operação de G , o conjunto H é um grupo, ou seja, quando as seguintes condições são satisfeitas:

1. $h_1 \cdot h_2 \in H, \quad \forall h_1, h_2 \in H.$

2. $h_1 \cdot (h_2 \cdot h_3) = (h_1 \cdot h_2) \cdot h_3, \quad \forall h_1, h_2, h_3 \in H.$
3. Existe $e_H \in H$ tal que $e_H \cdot h = h \cdot e_H = h, \quad \forall h \in H.$
4. Para cada $h \in H$, existe $k \in H$ tal que $h \cdot k = k \cdot h = e_H.$

Observação 1.3.2. A condição 2 é sempre satisfeita, pois a igualdade $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ é válida para todos os elementos de G . O elemento neutro e_H de H é necessariamente igual ao elemento neutro e de G . Dado $h \in H$, o inverso de h em H é necessariamente igual ao inverso de h em G . Veremos a seguir a demonstração dessas afirmações.

Proposição 1.3.3. Seja H um subgrupo de G . Se $e_H \in H$ é o elemento neutro de H e e_G é o elemento neutro de G , então $e_H = e_G$.

Demonstração. Para demonstrar que $e_H = e_G$, considere que H é um subgrupo de G , e portanto, H herda a operação de grupo de G . Como e_H é o elemento neutro de H , temos que para qualquer $h \in H$, $e_H \cdot h = h \cdot e_H = h$. Em particular, tomando $h = e_H$, obtemos $e_H \cdot e_H = e_H$. Por outro lado, como e_G é o elemento neutro de G , temos que $e_G \cdot e_H = e_H$. Comparando as duas igualdades, $e_H \cdot e_H = e_H$ e $e_G \cdot e_H = e_H$, concluímos que $e_H \cdot e_H = e_G \cdot e_H$. Pela lei do cancelamento em grupos, podemos cancelar e_H dos dois lados, obtendo $e_H = e_G$. Portanto, o elemento neutro de H é igual ao elemento neutro de G . $\square$

Proposição 1.3.4. Seja H um subgrupo de G . Seja $h \in H$. Se $h' \in H$ é o inverso de h em H e $g \in G$ é o inverso de h em G , então $h' = g$.

Demonstração. Para demonstrar que $h' = g$, observe que H é um subgrupo de G , e portanto, a operação de inverso em H é a mesma que em G . Como h' é o inverso de h em H , temos $h \cdot h' = h' \cdot h = e_H$, onde e_H é o elemento neutro de H . Pelo resultado anterior, sabemos que $e_H = e_G$, onde e_G é o elemento neutro de G . Assim, $h \cdot h' = e_G$. Por outro lado, g é o inverso de h em G , logo $h \cdot g = g \cdot h = e_G$. Comparando as duas igualdades, $h \cdot h' = e_G$ e $h \cdot g = e_G$, concluímos que $h \cdot h' = h \cdot g$. Pela lei do cancelamento em grupos, podemos cancelar h dos dois lados, obtendo $h' = g$. Portanto, o inverso de h em H é igual ao inverso de h em G . $\square$

Proposição 1.3.5. Se G é um grupo abeliano e H é um subgrupo de G , então H é um grupo abeliano.

Demonstração. Se G é abeliano e H é um subgrupo de G , então para quaisquer $h_1, h_2 \in H$, temos $h_1 \cdot h_2 = h_2 \cdot h_1$, pois $H \subseteq G$ e a comutatividade vale em G . Como H herda a operação de G , é fechado sob a operação, contém o elemento neutro e os inversos, e a associatividade é mantida, concluímos que H é abeliano. $\square$

Proposição 1.3.6. Seja H um subconjunto não vazio do grupo G . Então H é um subgrupo de G se e somente se as duas condições seguintes são satisfeitas:

1. Para quaisquer elementos $h_1, h_2 \in H$, o produto $h_1 \cdot h_2$ pertence a H .
2. Para todo $h \in H$, o elemento inverso h^{-1} também pertence a H .

Demonstração. Suponha que H seja um subgrupo de G . A primeira propriedade decorre diretamente do fato de que a operação do grupo G é fechada em H . Além disso, dado $h \in H$, como H é um grupo, o inverso de h , que denotamos por h^{-1} , também pertence a H . De acordo com a observação esse inverso coincide com o inverso de h em G , ou seja, $h^{-1} \in H$, o que confirma a validade da segunda propriedade.

Para o recíproco, suponha que H satisfaça as condições 1) e 2). Como a Definição V.2.1 exige que um subgrupo seja um subconjunto não vazio fechado para a operação e inversão, verifica-se que $e \in H$, pois tomando qualquer $h \in H$, temos $h^{-1} \in H$ pela condição 2) e, assim, $e = hh^{-1} \in H$ pela condição 1). Consequentemente, H contém a identidade de G e é fechado para a operação e inversão, o que implica que H é um subgrupo de G . $\square$

Observação 1.3.7. Na prática, para verificar se um subconjunto H de G é um subgrupo, é suficiente confirmar as propriedades 1) e 2) acima, conforme estabelecido pela Proposição anterior.

Proposição 1.3.8. Se $\{H_\alpha\}_{\alpha \in I}$ é uma família de subgrupos de G , então $\bigcap_{\alpha \in I} H_\alpha$ é um subgrupo de G .

Demonstração. Para demonstrar que $\bigcap_{\alpha \in I} H_\alpha$ é um subgrupo de G , observe que, como cada H_α é um subgrupo de G , o elemento neutro e pertence a todos os H_α , logo $e \in \bigcap_{\alpha \in I} H_\alpha$. Além disso, se $x \in \bigcap_{\alpha \in I} H_\alpha$, então $x \in H_\alpha$ para todo $\alpha \in I$, e como cada H_α é fechado sob inversos, $x^{-1} \in H_\alpha$ para todo $\alpha \in I$, implicando $x^{-1} \in \bigcap_{\alpha \in I} H_\alpha$. Finalmente, se $x, y \in \bigcap_{\alpha \in I} H_\alpha$, então $x, y \in H_\alpha$ para todo $\alpha \in I$, e como H_α é fechado sob a operação de grupo, $x \cdot y \in H_\alpha$ para todo $\alpha \in I$, logo $x \cdot y \in \bigcap_{\alpha \in I} H_\alpha$. Portanto, $\bigcap_{\alpha \in I} H_\alpha$ é um subgrupo de G . $\square$

1.3.1 Exemplos de subgrupos

1. Para qualquer grupo G , os conjuntos $\{e\}$ e G são subgrupos triviais de G .

Demonstração. Para demonstrar que $\{e\}$ e G são subgrupos triviais de G , começamos com $\{e\}$: o elemento neutro e pertence a $\{e\}$, e como $e \cdot e = e$, o conjunto é fechado sob a operação de grupo, além de conter o inverso de e , que é o próprio e . Portanto, $\{e\}$ satisfaz as condições de subgrupo. Já G é, por definição, um grupo, o que implica que ele é fechado sob a operação de grupo, contém o elemento neutro e , e todo elemento de G possui um inverso em G , tornando G um subgrupo de si mesmo. Assim, tanto $\{e\}$ quanto G são subgrupos triviais de G . $\square$

2. O conjunto dos múltiplos de 2, $2\mathbb{Z}$, constitui um subgrupo do grupo aditivo dos inteiros $(\mathbb{Z}, +)$. De maneira mais geral, para qualquer inteiro n , o conjunto $n\mathbb{Z}$ forma um subgrupo de $(\mathbb{Z}, +)$.

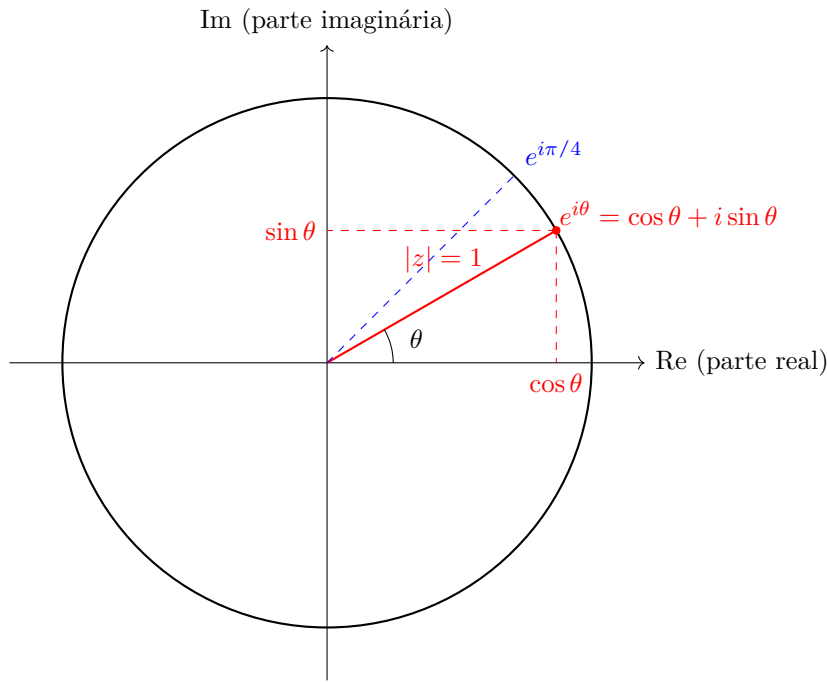
Demonstração. Para demonstrar que $n\mathbb{Z}$ é um subgrupo do grupo aditivo $(\mathbb{Z}, +)$, observe que $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Primeiro, o elemento neutro da adição, 0, pertence a $n\mathbb{Z}$, pois $0 = n \cdot 0$. Em segundo lugar, para quaisquer $a, b \in n\mathbb{Z}$, existem inteiros $k_1, k_2 \in \mathbb{Z}$ tais que $a = nk_1$ e $b = nk_2$; assim, $a + b = nk_1 + nk_2 = n(k_1 + k_2)$, o que mostra que $a + b \in n\mathbb{Z}$, garantindo o fechamento sob a adição. Por fim, para qualquer $a = nk \in n\mathbb{Z}$, o inverso aditivo de a é $-a = n(-k)$, que também pertence a $n\mathbb{Z}$. Portanto, $n\mathbb{Z}$ satisfaz as condições de subgrupo de $(\mathbb{Z}, +)$. $\square$

3. Seja G um grupo. Definimos $Z(G) := \{g \in G \mid gh = hg, \forall h \in G\}$, chamado de centro do grupo G . Ele consiste em todos os elementos de G que comutam com todos os outros elementos do grupo. $Z(G)$ é um subgrupo de G .
4. No grupo de simetrias S_Δ de um triângulo equilátero, os subconjuntos $\{id, R_1\}$ e $\{id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}\}$ constituem subgrupos.
5. No grupo $D_\square$ das simetrias do quadrado, os subconjuntos $\{id, R_\pi\}$ e $\{id, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}\}$ são subgrupos.
6. Seja $U_n = \{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \dots, e^{\frac{2(n-1)\pi i}{n}}\}$ o grupo multiplicativo das raízes n -ésimas da unidade. Temos a seguinte cadeia de subgrupos de $\mathbb{C} - \{0\}$, com a multiplicação:

$$U_n \subset \bigcup_{n \in \mathbb{N}} U_n = \{\text{raízes da unidade}\} \subset S^1 \subset \mathbb{C} - \{0\},$$

onde S^1 é o grupo dos números complexos de norma 1, ou seja, S^1 é o círculo unitário no plano complexo.

Demonstração. Mostraremos agora apenas que $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ é um subgrupo dos números complexos sem o zero $(\mathbb{C} \setminus \{0\})$, pois as demonstrações dos demais casos são análogas. Primeiro, observe que $1 \in S^1$, pois $|1| = 1$, e portanto S^1 contém o elemento neutro. Agora, sejam $z, w \in S^1$. Como $|z| = 1$ e $|w| = 1$, temos $|z \cdot w| = |z| \cdot |w| = 1 \cdot 1 = 1$, o que mostra que $z \cdot w \in S^1$, garantindo o fechamento sob a multiplicação. Além disso, se $z \in S^1$, então $|z^{-1}| = \frac{1}{|z|} = 1$, o que implica que $z^{-1} \in S^1$. Portanto, S^1 é fechado sob a operação de multiplicação, contém o elemento neutro e os inversos, sendo assim um subgrupo de $\mathbb{C} \setminus \{0\}$. $\square$



Observação 1.3.9. Para demonstrar que $|z^{-1}| = \frac{1}{|z|}$, considere um número complexo $z \neq 0$. O inverso de z é dado por $z^{-1} = \frac{\bar{z}}{|z|^2}$, onde $\bar{z}$ é o conjugado de z . O módulo de z^{-1} é então calculado como:

$$|z^{-1}| = \left| \frac{\bar{z}}{|z|^2} \right|.$$

Como o módulo de um quociente é o quociente dos módulos, temos:

$$|z^{-1}| = \frac{|\bar{z}|}{|z|^2}.$$

Sabemos que $|\bar{z}| = |z|$, pois o módulo de um número complexo é igual ao módulo do seu conjugado. Portanto:

$$|z^{-1}| = \frac{|z|}{|z|^2} = \frac{1}{|z|}.$$

Assim, concluímos que $|z^{-1}| = \frac{1}{|z|}$.

7. Seja D_4 o seguinte subconjunto de S_4 :

$$D_4 = \left\{ \begin{pmatrix} 1234 \\ 1234 \end{pmatrix}, \begin{pmatrix} 1234 \\ 2341 \end{pmatrix}, \begin{pmatrix} 1234 \\ 3412 \end{pmatrix}, \begin{pmatrix} 1234 \\ 4123 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1234 \\ 4321 \end{pmatrix}, \begin{pmatrix} 1234 \\ 2143 \end{pmatrix}, \begin{pmatrix} 1234 \\ 1432 \end{pmatrix}, \begin{pmatrix} 1234 \\ 3214 \end{pmatrix} \right\}.$$

D_4 é um subgrupo de S_4 .

Observação 1.3.10. Um grupo G é abeliano se, e somente se, $Z(G) = G$. Isso ocorre porque, por definição, G é abeliano quando todos os seus elementos comutam entre si, ou seja, $g \cdot h = h \cdot g$ para quaisquer $g, h \in G$. O centro $Z(G)$ é o conjunto de elementos que comutam com todos os outros elementos de G . Se G é abeliano, todos os elementos pertencem a $Z(G)$, logo $Z(G) = G$. Reciprocamente, se $Z(G) = G$, todos os elementos comutam entre si, o que implica que G é abeliano. Portanto, G é abeliano se, e somente se, $Z(G) = G$.

1.3.2 Classificação dos Subgrupos de $(\mathbb{Z}, +)$

É sabido que os conjuntos $n\mathbb{Z}$, para $n \in \mathbb{N}$, constituem subgrupos do grupo aditivo dos inteiros $(\mathbb{Z}, +)$. Vamos demonstrar que esses são os únicos subgrupos possíveis.

Demonstração. Seja H um subgrupo qualquer de $\mathbb{Z}$. Se $H = \{0\}$, então claramente $H = 0\mathbb{Z}$. Suponha agora que $H \neq \{0\}$ e seja n o menor elemento positivo de H , isto é, $n = \min\{x \in H \mid x > 0\}$. Como $n \in H$ e H é fechado para a adição e para a inversão, temos que $n\mathbb{Z} \subseteq H$.

Para a inclusão recíproca, seja $h \in H$. Pelo algoritmo da divisão de Euclides, existem $q, r \in \mathbb{Z}$ tais que $h = qn + r$, com $0 \leq r < n$. Como $h, n \in H$ e H é fechado para operações internas, segue que $r = h - qn \in H$. Pela escolha mínima de n , a única possibilidade é $r = 0$, ou seja, $h \in n\mathbb{Z}$. De fato se $r > 0$, teríamos r um elemento maior ou igual a n , pois n é o mínimo dos elementos positivos de H , um absurdo. Assim, temos que $h = qn \in n\mathbb{Z}$, ou seja, $H \subseteq n\mathbb{Z}$. Logo $H = n\mathbb{Z}$, o que conclui a demonstração. $\square$

1.4 SUBGRUPO GERADO POR UM SUBCONJUNTO

Definição 1.4.1. Sejam G um grupo e $S \subseteq G$. Definimos $\langle S \rangle$ como o conjunto de todos os elementos $g \in G$ para os quais existem $n \in \mathbb{N}$ e $a_1, \dots, a_n \in G$ tais que $g = a_1 \dots a_n$ e para todo $i \in \{1, \dots, n\}$, $a_i \in S$ ou $a_i^{-1} \in S$. Assim, temos

$$\langle S \rangle = \{a_1 a_2 \dots a_n \mid n \in \mathbb{N}, a_i \in S \text{ ou } a_i \in S^{-1}\}.$$

Observação 1.4.2. Definimos $\langle S \rangle$ como o conjunto de todos os elementos que podem ser escritos como produtos finitos de elementos de S e de seus inversos.

Observação 1.4.3. Se S for um conjunto finito, digamos $S = \{\alpha_1, \alpha_2, \dots, \alpha_r\}$, utilizamos a notação $\langle \alpha_1, \alpha_2, \dots, \alpha_r \rangle$ para representar $\langle S \rangle$.

Exemplo 1.4.4. No grupo aditivo $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, o subgrupo gerado pelo elemento 2, denotado por $\langle 2 \rangle$, consiste em todas as somas finitas de 2 e seu inverso 4 (já que $-2 \equiv 4 \pmod{6}$), resultando em $\langle 2 \rangle = \{0, 2, 4\}$. Esse conjunto forma um subgrupo de ordem 3, pois

é fechado sob a operação de adição, contém o elemento neutro 0 e os inversos de cada elemento (o inverso de 2 é 4).

Lema 1.4.5. Se H é um subgrupo de G e $a_1, \dots, a_r \in H$ então $a_1 \cdots a_r \in H$

Demonstração. Vamos começar com o caso base $r = 1$, que é trivial, pois podemos observar que $a_1 \in H$. Suponha, por hipótese de indução, que o resultado é verdadeiro para $r = k$, ou seja, $a_1 \cdots a_k \in H$, então, para $r = k + 1$, temos $(a_1 \cdots a_k) \cdot a_{k+1}$, que é o produto de dois elementos de H (pois $a_1 \cdots a_k \in H$ pela hipótese de indução e $a_{k+1} \in H$ por definição). Como H é fechado sob a operação do grupo, concluímos que $a_1 \cdots a_{k+1} \in H$. $\square$

Proposição 1.4.6. Sejam G um grupo e $S \subseteq G$, $S \neq \emptyset$. Então $\langle S \rangle$ é um subgrupo de G . Além disso,

$$\langle S \rangle = \bigcap_{H \in V(S)} H, \quad \text{onde } V(S) = \{H \mid H \text{ é subgrupo de } G \text{ e } S \subseteq H\}.$$

Em particular, $\langle S \rangle$ é o menor subgrupo de G que contém S . Mais precisamente, se H é um subgrupo de G tal que $S \subseteq H$ então $\langle S \rangle \subseteq H$.

Demonstração. $\langle S \rangle$ é um subgrupo de G . O elemento $e \in \langle S \rangle$. De fato, como $S \neq \emptyset$, então existe $a \in S$. Por definição, $aa^{-1} \in \langle S \rangle$ implica que $e \in \langle S \rangle$.

Vamos mostrar que $\langle S \rangle$ é fechado para a operação de G . Sejam $x, y \in \langle S \rangle$. Daí existem $r, s \in \mathbb{N}$ e $a_1, \dots, a_r, b_1, \dots, b_s \in G$ tais que $x = a_1 \dots a_r$ com $a_i \in S$ ou $a_i^{-1} \in S, \forall i \in \{1, \dots, r\}$ e $y = b_1 \dots b_s$ com $b_j \in S$ ou $b_j^{-1} \in S, \forall j \in \{1, \dots, s\}$. Logo, $xy = a_1 \dots a_r b_1 \dots b_s$, onde por definição, $xy \in \langle S \rangle$.

Vamos mostrar a existência do elemento inverso. Seja $x \in \langle S \rangle$. Daí existem $r \in \mathbb{N}$ e $a_1, \dots, a_r \in G$ tais que $x = a_1 \dots a_r$ com $a_i \in S$ ou $a_i^{-1} \in S, \forall i \in \{1, \dots, r\}$. Assim: $x^{-1} = a_r^{-1} \dots a_1^{-1}$ onde $a_j^{-1} \in S$ ou $(a_j^{-1})^{-1} = a_j \in S, \forall j \in \{1, \dots, r\}$. Logo, $x^{-1} \in \langle S \rangle$ por definição. Portanto, $\langle S \rangle$ é subgrupo de G .

Agora mostraremos que $\langle S \rangle = \bigcap_{H \in V(S)} H, \forall H \in V(S)$.

Primeiramente demonstraremos a primeira inclusão, isto é, $\langle S \rangle \subseteq H, \forall H \in V(S)$. Seja $H \in V(S)$. Seja $x \in \langle S \rangle$ qualquer. Daí existem $a_1, \dots, a_r \in G$ tais que $x = a_1 \cdots a_r$ e $(a_i \in S \text{ ou } a_i^{-1} \in S), \forall i \in \{1, \dots, r\}$.

Devemos mostrar que $a_i \in H, \forall i \in \{1, \dots, r\}$. De fato, seja $i \in \{1, \dots, r\}$. Se $a_i \in S$, como $S \subseteq H$, então $a_i \in H$. Suponha que $a_i^{-1} \in S$. Como $S \subseteq H$ então $a_i^{-1} \in H$. Como H é um subgrupo de G então $(a_i^{-1})^{-1} \in H$, ou seja, $a_i \in H$. Assim, uma vez que H é subgrupo de G , então $a_1 \cdots a_r \in H$, isto é, $x \in H$. Logo, $\langle S \rangle \subseteq H, \forall H \in V(S)$.

Reciprocamente, seja $x \in \bigcap_{H \in V(S)} H$. Como $\langle S \rangle$ é um subgrupo de G que contém S , então $\langle S \rangle \in V(S)$. Em particular, $x \in \langle S \rangle$. Portanto, $\bigcap_{H \in V(S)} H \subseteq \langle S \rangle$ $\square$

Observação 1.4.7. O subgrupo $\langle S \rangle$ pode ser obtido como a interseção de todos os subgrupos de G que contêm S . Isso confirma que $\langle S \rangle$ é a menor estrutura com as propriedades

desejadas, garantindo que qualquer outra construção que contenha S seja necessariamente mais ampla ou igual a $\langle S \rangle$.

Definição 1.4.8. *Seja G um grupo. Dizemos que G é um grupo finitamente gerado se existe $S \subseteq G$ finito tal que $G = \langle S \rangle$*

Definição 1.4.9. *Um grupo G é cíclico se pode ser gerado por um único elemento, ou seja, se $G = \langle g \rangle$ para algum $g \in G$.*

Proposição 1.4.10. *Sejam G um grupo e $g \in G$. Então $\langle g \rangle = \{g^t \mid t \in \mathbb{Z}\}$.*

Demonstração. Seja $L = \{g^t \mid t \in \mathbb{Z}\}$. É imediato que $L \subseteq \langle g \rangle$, pois cada elemento g^t pode ser expresso como: $g^t = e$ se $t = 0$, $g^t = \underbrace{g \cdots g}_{t \text{ vezes}}$ se $t > 0$, e $g^t = (g^{-1})^{-t}$ se $t < 0$, sendo que todas essas formas pertencem ao subgrupo gerado por g , uma vez que $\langle g \rangle$ contém g , seu inverso g^{-1} , e todas as potências inteiras deles.

Afirmção: Se $a_1, \dots, a_n$ são tais que $a_i = g$ ou $a_i^{-1} = g$, $\forall i \in \{1, \dots, n\}$ então $a_1, \dots, a_n \in L$.

Vamos demonstrar a afirmação por indução sobre n . Para $n = 1$, se $a_1 = g$ então $a_1 = g^1 \in L$, e se $a_1^{-1} = g$ então $a_1 = g^{-1} \in L$. Suponha que $n > 1$ e que $a_1, \dots, a_{n-1} \in L$. Daí existe $t \in \mathbb{Z}$ tal que $a_1 \cdots a_{n-1} = g^t$. Se $a_n = g$ então $a_1 \cdots a_n = (a_1 \cdots a_{n-1}) \cdot a_n = g^t \cdot g = g^{t+1} \in L$. Se $a_n^{-1} = g$ então $a_n = g^{-1}$ e daí temos que $a_1 \cdots a_n = (a_1 \cdots a_{n-1}) \cdot a_n = g^t \cdot g^{-1} = g^{t-1} \in L$. Portanto, o resultado segue para n , concluindo a demonstração por indução. Assim, $\langle g \rangle \subseteq L$. Portanto $\langle g \rangle = L = \{g^t \mid t \in \mathbb{Z}\}$. $\square$

Exemplo 1.4.11. *O grupo $(\mathbb{Z}, +)$ é cíclico infinito gerado pelo elemento 1, isto é, $\mathbb{Z} = \langle 1 \rangle$. Devemos adaptar a noção de potência para a adição, as potências de 1 correspondem a múltiplos inteiros: para todo $t \in \mathbb{Z}$, temos $1^t := t \cdot 1$, onde $1^0 = id = 0$, $1^t = \underbrace{1 + \cdots + 1}_{t \text{ vezes}}$ se $t > 0$, e $1^t = \underbrace{(-1) + \cdots + (-1)}_{|t| \text{ vezes}}$ se $t < 0$. Assim, $\langle 1 \rangle = \{1^t \mid t \in \mathbb{Z}\} = \mathbb{Z}$, conforme a estrutura geral de grupos cíclicos.*

Exemplo 1.4.12. *Considere o grupo $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ com a operação $\oplus$ (soma módulo n), onde $a \oplus b = (a + b) \bmod n$. Este grupo é cíclico e gerado pelo elemento 1, pois todo elemento $k \in \mathbb{Z}_n$ pode ser escrito como:*

$$k = \underbrace{1 \oplus 1 \oplus \cdots \oplus 1}_{k \text{ vezes}}.$$

A estrutura $(\mathbb{Z}_n, \oplus)$ é o protótipo de grupo cíclico finito de ordem n , essencial para classificar grupos abelianos finitos.

Exemplo 1.4.13. *O conjunto $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$, formado pelas raízes n -ésimas da unidade, é um subconjunto notável do grupo multiplicativo $\mathbb{C}^\times$. Para demonstrar que U_n é um grupo cíclico, considere o número complexo:*

$$\xi = e^{i\frac{2\pi}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right).$$

Observe que $\xi^n = 1$, logo $\xi \in U_n$. Além disso, as potências ξ^k , para $k = 0, 1, \dots, n-1$, são todas distintas e satisfazem $(\xi^k)^n = 1$, o que implica $U_n = \{1, \xi, \xi^2, \dots, \xi^{n-1}\}$.

Como ξ gera todos os elementos de U_n por exponenciação, temos $U_n \subseteq \langle \xi \rangle$. Por outro lado, como $\xi \in U_n$ e U_n é fechado sob multiplicação e inversos, segue que $\langle \xi \rangle \subseteq U_n$. Portanto, concluímos que:

$$U_n = \langle \xi \rangle,$$

o que mostra que U_n é um grupo cíclico de ordem n , gerado por ξ .

Proposição 1.4.14. *Se G é um grupo cíclico então G é um grupo abeliano.*

Demonstração. Como G é cíclico, existe $g \in G$ tal que $G = \langle g \rangle$. Sejam $x, y \in G$. Então existem, $n, m \in \mathbb{Z}$ tais que $x = g^n$ e $y = g^m$. Logo, $x \cdot y = g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n = y \cdot x$. Portanto, G é um grupo abeliano $\square$

Exemplo 1.4.15. *O grupo $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$ com adição módulo 2 não é cíclico, como mostra a análise de seus subgrupos geradores a seguir:*

- $\langle (0,0) \rangle = \{(0,0)\}$
- $\langle (1,0) \rangle = \{(0,0), (1,0)\}$
- $\langle (0,1) \rangle = \{(0,0), (0,1)\}$
- $\langle (1,1) \rangle = \{(0,0), (1,1)\}$

Definição 1.4.16. *Dado um grupo G e dois elementos quaisquer $x, y \in G$, define-se o comutador de x e y como o elemento*

$$[x, y] = xyx^{-1}y^{-1}.$$

Esta medida quantifica o grau de não comutatividade entre os elementos x e y , sendo trivial $[x, y] = e$ se e somente se x e y comutarem.

Proposição 1.4.17. *Dois elementos $x, y \in G$ comutam se, e somente se, $[x, y] = e$.*

Demonstração. Vamos mostrar que dois elementos comutam se, e somente se, o comutador entre eles é a identidade. Em outras palavras, $x \cdot y = y \cdot x$ se, e somente se, $[x, y] = e$. Sejam $x, y \in G$ tal que $x \cdot y = y \cdot x$. Assim, multiplicando à direita ambos os lados por x^{-1} temos que $x \cdot y \cdot x^{-1} = y$. Além disso, multiplicando à direita ambos os lados por y^{-1} chegamos que $x \cdot y \cdot x^{-1} \cdot y^{-1} = e$, ou seja, $[x, y] = e$. Reciprocamente, suponha que $[x, y] = e$. Então $x \cdot y \cdot x^{-1} \cdot y^{-1} = e$. Multiplicando à direita ambos os lados por y , obtemos $x \cdot y \cdot x^{-1} = y$. Multiplicando novamente à direita ambos os lados por x , segue que $x \cdot y = y \cdot x$. Portanto, x e y comutam se, e somente se, $[x, y] = e$. $\square$

Definição 1.4.18. *Seja G um grupo. O subgrupo dos comutadores de G é definido como $G' = \langle \{[x, y] \mid x, y \in G\} \rangle$.*

Proposição 1.4.19. *Sejam G um grupo. Então G é abeliano se, e somente se, $G' = \{e\}$.*

Demonstração. Para mostrar a primeira inclusão, suponha que G é abeliano. Então $[x, y] = e$, para todo $x, y \in G$. Logo $G' = \langle e \rangle = \{e\}$. Reciprocamente, supondo que $G' = \{e\}$, escolha arbitrariamente $x, y \in G$. Por definição, temos que $[x, y] \in G'$ e $G' = \{e\}$, onde concluímos que o comutador entre x e y é a identidade, isto é, $[x, y] = e$. Assim, obtemos $x \cdot y = y \cdot x$, completando que G é um grupo abeliano. $\square$

Proposição 1.4.20. *Seja $n \in \mathbb{N}$, $n \geq 2$, e $m \in \mathbb{N}$. Então, m gera o grupo $(\mathbb{Z}_n, \oplus)$, se e somente se, $\text{mdc}(m, n) = 1$.*

Demonstração. Suponha primeiro que $\overline{m}$ gera $\mathbb{Z}_n$. Nesse caso, toda classe de $\mathbb{Z}_n$ pode ser escrita como combinação inteira de $\overline{m}$, em particular a classe $\overline{1}$. Assim, existe $k \in \mathbb{Z}$ tal que $\overline{1} = k \odot \overline{m} = \overline{km}$. Em termos de congruência, isso significa que $km \equiv 1 \pmod{n}$. Pela definição de congruência módulo n , existem $q \in \mathbb{Z}$ tal que $km - 1 = qn$, isto é, $km - qn = 1$. Essa igualdade mostra que 1 é uma combinação linear inteira de m e n . Pelo teorema de Bézout, o máximo divisor comum entre m e n é precisamente 1, isto é, $\text{mdc}(m, n) = 1$.

Reciprocamente, suponha que $\text{mdc}(m, n) = 1$. Pelo teorema de Bézout, existem inteiros $u, v \in \mathbb{Z}$ tais que $um + vn = 1$. Passando a igualdade para o contexto de congruência módulo n , obtém-se $um + vn \equiv 1 \pmod{n}$. Como $vn \equiv 0 \pmod{n}$, conclui-se que $um \equiv 1 \pmod{n}$, ou seja, $\overline{um} = \overline{1}$. Por outro lado, $\overline{um} = u \odot \overline{m}$, de modo que $\overline{1} \in \langle \overline{m} \rangle$. Como se sabe que $\overline{1}$ gera todo o grupo $\mathbb{Z}_n$, tem-se $\mathbb{Z}_n = \langle \overline{1} \rangle \subseteq \langle \overline{m} \rangle$. Por definição, $\langle \overline{m} \rangle$ é um subgrupo de $\mathbb{Z}_n$, logo $\langle \overline{m} \rangle \subseteq \mathbb{Z}_n$. Dessa forma, as duas inclusões conduzem à igualdade $\langle \overline{m} \rangle = \mathbb{Z}_n$. Conclui-se, portanto, que $\overline{m}$ gera o grupo $(\mathbb{Z}_n, \oplus)$ se, e somente se, $\text{mdc}(m, n) = 1$, o que completa a demonstração. $\square$

1.4.1 Ordem de grupos e elementos

Definição 1.4.21. *Sejam G um grupo. A ordem de um elemento $a \in G$ é definida como a cardinalidade do subgrupo cíclico gerado por a . Formalmente:*

$$\mathcal{O}(a) := |\langle a \rangle|.$$

Observação 1.4.22. *Caso $\langle a \rangle$ seja infinito, dizemos que a possui ordem infinita. Esta noção quantifica o menor número de vezes que o elemento deve ser operado consigo mesmo para retornar ao elemento neutro do grupo.*

Proposição 1.4.23. *O subgrupo cíclico $\langle a \rangle$ é finito se, e somente se, existe $t \in \mathbb{N}^*$ tal que $a^t = e$. Além disso, se a ordem $\mathcal{O}(a) = n$ para algum $n \in \mathbb{N}^*$, então n é o menor inteiro positivo satisfazendo $a^n = e$, ou seja, $n = \min\{t \in \mathbb{N} \mid a^t = e\}$, onde $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$, com $|\langle a \rangle| = n$.*

Demonstração. Considere a função

$$\begin{aligned}\varphi: \mathbb{Z} &\rightarrow \langle a \rangle \\ t &\mapsto a^t.\end{aligned}$$

($\Rightarrow$) Uma vez que $\mathbb{Z}$ é infinito e por hipótese $\langle a \rangle$ é finito, então φ não é injetiva. Nesse viés, existem $t', s \in \mathbb{Z}$, com $t' < s$ tais que $\varphi(t') = \varphi(s)$. Logo, $a^{t'} = a^s$. Operando $a^{-t'}$ a direita chegamos em $a^{t'} \cdot a^{-t'} = a^s \cdot a^{-t'} = e$, o que nos fornece $a^{s-t'} = e$. Escolha $t = s - t' \in \mathbb{N}$ e então $a^t = e$.

($\Leftarrow$) Vamos mostrar a recíproca da proposição e a sentença adicional. Para isso, suponha que exista $t \in \mathbb{N}$ tal que $a^t = e$. Tome $n := \min\{t \in \mathbb{N} \mid a^t = e\}$. Por hipótese temos que $n \neq 0$. Em particular, $a^n = e$. Mostraremos que $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$. Para a primeira inclusão seja $m \in \mathbb{Z}$ qualquer. Pelo algoritmo da divisão existem $q, r \in \mathbb{Z}$ tais que $m = qn + r$ onde $0 \leq r < n$. Assim,

$$a^m = a^{qn+r} = (a^n)^q \cdot a^r = e \cdot a^r \in \{e, a, \dots, a^{n-1}\}.$$

A segunda inclusão é imediata, pois as potências de a estão em $\langle a \rangle$. Portanto, $\langle a \rangle$ é finito.

Suponha por absurdo que $\mathcal{O}(a) < n$. Daí existem $t, s \in \{0, 1, \dots, n-1\}$ com $t < s$ tais que $a^t = a^s$. Multiplicando pelo inverso a^t a direita chegamos em $a^{s-t} = e$. Como $s, t \in \{0, \dots, n-1\}$, então $s - t < n$. Por outro lado, como $s - t \in \mathbb{N}$ e $a^{s-t} = e$, donde concluímos que $s - t \geq n$, absurdo. Agora como $\langle a \rangle$ tem no máximo n elementos, a única possibilidade é que $\mathcal{O}(a)$ tenha exatamente n elementos.

□

Observação 1.4.24. *Esta proposição estabelece uma relação fundamental entre a finitude do subgrupo gerado por um elemento a e a existência de uma potência positiva que retorna ao elemento neutro e . Quando tal potência t existe, a ordem $\mathcal{O}(a)$ corresponde exatamente ao menor expoente natural n para o qual $a^n = e$, determinando completamente a estrutura do subgrupo cíclico $\langle a \rangle$ como o conjunto $\{e, a, \dots, a^{n-1}\}$ com exatamente n elementos distintos.*

Proposição 1.4.25. *Sejam G um grupo e $\alpha \in G$, $\alpha \neq e$. Então:*

1. $\mathcal{O}(\alpha) = 2$ se, e somente se, $\alpha = \alpha^{-1}$.
2. Se $\mathcal{O}(\alpha) = mn$, então $\mathcal{O}(\alpha^m) = n$.
3. $\mathcal{O}(\alpha^{-1}) = \mathcal{O}(\alpha)$.
4. Se $\mathcal{O}(\alpha) = 2$ para todo $\alpha \neq e$, então G é abeliano.

Demonstração. 1. ($\Rightarrow$) Suponha que α tem ordem 2, ou seja, $\alpha^2 = e$. Multiplicando ambos os lados por α^{-1} , obtemos:

$$\alpha = \alpha^{-1}.$$

($\Leftarrow$) Suponha que $\alpha = \alpha^{-1}$. Então, multiplicando ambos os lados por α , temos:

$$\alpha^2 = e.$$

Como $\alpha \neq e$, $2 = \min\{t \in \mathbb{N} / \alpha^t = e\}$. Portanto, $\mathcal{O}(\alpha) = 2$.

2. Suponha que $\mathcal{O}(\alpha) = mn$. Queremos mostrar que $\mathcal{O}(\alpha^m) = n$. Tome $L := \{r \in \mathbb{N} / (a^m)^r = e\}$. Temos que, $\mathcal{O}(\alpha^m) = \min L$. Observe que:

$$(\alpha^m)^n = \alpha^{mn} = (\alpha^{\mathcal{O}(\alpha)}) = e.$$

Perceba que o elemento n está em L . Suponha, por absurdo, que $n \neq \min L$. Isso significa que existe $l \in \mathbb{N}$ com $l < n$ tal que $(a^m)^l = e$. Assim, $a^{ml} = e$, e como $\mathcal{O}(a) = mn$, então, devido à minimalidade da ordem, temos $mn \leq ml$, isto é, $n \leq l$. Logo, $l \geq n$, o que é um absurdo. Portanto, $n = \min L = \mathcal{O}(\alpha^m)$.

3. Defina

$$\begin{aligned} \varphi: \langle a \rangle &\rightarrow \langle a^{-1} \rangle \\ x &\mapsto x^{-1}. \end{aligned}$$

Mostraremos que φ está bem definida, ou seja, que não há ambiguidade na construção da função. De fato, se $x \in \langle a \rangle$ então $x = a^t$, para algum $t \in \mathbb{Z}$. Assim, $x^{-1} = (a^t)^{-1} = (a^{-1})^t \in \langle a^{-1} \rangle$.

Ainda é necessário verificar que diferentes representações de um mesmo elemento no domínio levam ao mesmo resultado no contradomínio. Como todo $x \in \langle a \rangle$ pode ser expresso como $x = a^t$ para algum inteiro t , surge a questão: se x admitir duas representações distintas $x = a^t = a^s$, a função ainda produzirá a mesma imagem? Observe que $a^t = a^s$ implica $a^{t-s} = e$ ao multiplicarmos por a^{-s} . Calculando as inversas, temos $(a^t)^{-1} = a^{-t}$ e $(a^s)^{-1} = a^{-s}$. A igualdade $a^{-t} = a^{-s}$ decorre de $a^{-t} = a^{-s} \cdot a^{s-t} = a^{-s} \cdot e = a^{-s}$, onde usamos $a^{t-s} = e$. Consequentemente, $\varphi(a^t) = \varphi(a^s)$, demonstrando que a função está corretamente definida, pois associa a cada elemento uma única inversa, independentemente de sua representação como potência de a .

A função $\varphi: \langle a \rangle \rightarrow \langle a^{-1} \rangle$ definida por $\varphi(x) = x^{-1}$ é uma bijeção. Para verificar a injetividade, suponha que $\varphi(x_1) = \varphi(x_2)$, ou seja, $x_1^{-1} = x_2^{-1}$. Tomando a inversa de ambos os lados, obtemos $x_1 = x_2$, o que prova que φ é injetora. Quanto à sobrejetividade, dado qualquer elemento $y \in \langle a^{-1} \rangle$, existe $t \in \mathbb{Z}$ tal que $y =$

$(a^{-1})^t = (a^t)^{-1} = \varphi(a^t)$, mostrando que todo elemento do contradomínio é imagem de algum elemento do domínio.

Logo $|\langle a \rangle| = |\langle a^{-1} \rangle|$, o que implica em $\mathcal{O}(a) = \mathcal{O}(a^{-1})$

4. Suponha que $\mathcal{O}(\alpha) = 2$ para todo $\alpha \neq e$. Queremos mostrar que G é abeliano. Dados $\alpha, \beta \in G$, temos:

$$(\alpha\beta)^2 = e.$$

Expandindo, obtemos:

$$\alpha\beta\alpha\beta = e.$$

Multiplicando ambos os lados por $\beta^{-1}\alpha^{-1}$ à direita, temos:

$$\alpha\beta = \beta^{-1}\alpha^{-1}.$$

Como $\mathcal{O}(\alpha) = 2$ e $\mathcal{O}(\beta) = 2$, temos $\alpha^{-1} = \alpha$ e $\beta^{-1} = \beta$. Portanto:

$$\alpha\beta = \beta\alpha.$$

Assim, G é abeliano. □

Exemplo 1.4.26. Seja G um grupo abeliano e defina $T(G) := \{a \in G \mid \mathcal{O}(a) < \infty\}$, onde $\mathcal{O}(a)$ representa a ordem do elemento a . Então, $T(G)$ é um subgrupo (chamado de torção) de G .

Demonstração. Como $\langle e \rangle = \{e\}$ então $\mathcal{O}(e) = 1$, que implica em $e \in T(G)$. Sejam $a, b \in T(G)$. Assim, $\mathcal{O}(a) < \infty$ e $\mathcal{O}(b) < \infty$ e existem, $t, s \in \mathbb{N}$ tais que $a^t = e$ e $b^s = e$. Logo $(ab)^{ts} = a^{ts} \cdot b^{ts} = (a^t)^s \cdot (b^s)^t = e^t \cdot e^s = e$ e segue que $\mathcal{O}(ab) < \infty$, implicando que $ab \in T(G)$. Para finalizar, seja $a \in T(G)$. Assim, chegamos que $\mathcal{O}(a) < \infty$ e como $\mathcal{O}(a^{-1}) = \mathcal{O}(a)$ então $\mathcal{O}(a^{-1}) < \infty$, ou seja, $a^{-1} \in T(G)$. □

Observação 1.4.27. Se $G = \mathbb{C} \setminus \{0\}$, então $T(\mathbb{C} \setminus \{0\}) = \{\alpha \in \mathbb{C} \setminus \{0\} \mid \mathcal{O}(\alpha) < \infty\} = \{\text{raízes da unidade}\}$, com a operação de multiplicação.

1.5 CLASSES LATERAIS E TEOREMA DE LAGRANGE

Definição 1.5.1. Seja G um grupo e H um subgrupo de G . Defina a relação de equivalência $\sim$ em G da seguinte forma:

$$y \underset{H}{\sim} x \iff \exists h \in H \text{ tal que } y = xh.$$

Definição 1.5.2. A relação $\sim$ é de fato uma relação de equivalência.

Demonstração. Para mostrar que $\underset{H}{\sim}$ é uma relação de equivalência, verificamos as três propriedades necessárias: reflexividade, simetria e transitividade.

- Reflexividade: Para todo $x \in G$, temos $x = x \cdot e$, onde $e \in H$ é o elemento neutro, logo $x \underset{H}{\sim} x$.
- Simetria: Se $x \underset{H}{\sim} y$, existe $h \in H$ tal que $x = yh$. Como H é subgrupo, $h^{-1} \in H$, logo $y = xh^{-1}$, o que implica $y \underset{H}{\sim} x$.
- Transitividade: Se $x \underset{H}{\sim} y$ e $y \underset{H}{\sim} z$, existem $h_1, h_2 \in H$ tais que $x = yh_1$ e $y = zh_2$. Substituindo, obtemos $x = z(h_2h_1)$, e como $h_2h_1 \in H$, concluímos $x \underset{H}{\sim} z$. Portanto, $\underset{H}{\sim}$ é uma relação de equivalência em G .

□

Definição 1.5.3. Para cada $x \in G$, denotamos $xH := \{y \in G \mid y \underset{H}{\sim} x\}$, que é chamado classe lateral à esquerda de H pelo representante x , e denotamos $\frac{G}{H} := \frac{G}{\underset{H}{\sim}} = \{xH \mid x \in G\}$ chamado conjunto das classes laterais à esquerda de x ou conjunto quociente de G por H .

Observação 1.5.4. Para todo $x \in G$, $xH = \{xh \mid h \in H\}$. Note que $y \in xH$ se, e somente se, $y \underset{H}{\sim} x$, se, e somente se, existe $h \in H$ tal que $y = xh$.

A classe de equivalência que contém um elemento x de um grupo G em relação a um subgrupo H é definida como o conjunto $xH = \{y \in G \mid y \underset{H}{\sim} x\}$, onde a relação $y \underset{H}{\sim} x$ significa que existe algum $h \in H$ tal que $y = xh$. Esse conjunto, chamado de classe lateral à esquerda de H em G que contém x , pode ser interpretado como todas as combinações de x com os elementos de H multiplicados à direita.

De forma simples, quando não há ambiguidade, nos referimos a ele apenas como a classe lateral de x à esquerda. Um caso particular importante é quando x é o elemento neutro e , pois a classe lateral correspondente é o próprio subgrupo H .

Vale notar que y pertence a xH se, e somente se, as classes laterais de y e x coincidirem, ou seja, $yH = xH$. De maneira análoga, podemos definir uma relação de equivalência à direita, onde $y \underset{H}{\sim} x$ se existe $h \in H$ tal que $y = hx$, gerando as classes laterais à direita $Hx = \{hx \mid h \in H\}$, que representam as multiplicações dos elementos de H por x à esquerda.

Definição 1.5.5. A cardinalidade do conjunto das classes laterais à esquerda é chamada de índice de H em G e é denotada por $(G : H) = \left| \frac{G}{H} \right|$.

Definição 1.5.6. (Projeção Canônica) Seja H um subgrupo de um grupo G . A projeção canônica (ou função quociente) é a aplicação:

$$\begin{aligned} \pi : G &\rightarrow G/H \\ x &\mapsto xH \end{aligned} ,$$

onde G/H denota o conjunto das classes laterais à esquerda de H em G .

Observação 1.5.7. A função π é sempre sobrejetora, pois toda classe lateral em G/H é da forma xH para algum $x \in G$. Isso decorre diretamente da construção do conjunto quociente, garantindo que cada elemento de G/H seja imagem de pelo menos um elemento de G .

Proposição 1.5.8. Seja G um grupo e H um subgrupo de G . As seguintes afirmações são equivalentes:

I. $H = \{e\}$, onde e é o elemento neutro de G ;

II. A projeção canônica

$$\pi: G \rightarrow G/H, \quad \pi(x) = xH,$$

é uma bijeção;

Além disso, se $H = \{e\}$, o índice de H em G , denotado por $(G : H)$, coincide com a ordem de G , ou seja:

$$(G : \{e\}) = |G|.$$

Demonstração. Suponha que $H = \{e\}$. Resta mostrar que π é injetiva. Sejam $x, y \in G$ tais que $\pi(x) = \pi(y)$. Assim, $xH = yH$, ou seja, $x \in yH$ implicando na existência de $h \in H$ tal que $x = yh$. Como $H = \{e\}$ então $h = e$. Consequentemente $x = yh = ye = y$. Logo π é um bijeção.

Reciprocamente, suponha que π seja uma bijeção. Claro que $\{e\} \subseteq H$. Reciprocamente, se $x \in H$ então $x \in eH$. Consequentemente $xH = eH$, ou seja, $\pi(x) = \pi(e)$ e como π é injetiva então $x = e$. Portanto, $H = \{e\}$. $\square$

Observação 1.5.9. Se G é um grupo abeliano e H é um subgrupo de G então $xH = Hx$.

Demonstração. De fato, $xH = \{xh \mid h \in H\} = \{hx \mid h \in H\} = Hx$ $\square$

Proposição 1.5.10. (Princípio Multiplicativo) Sejam G um grupo, H subgrupo de G e K subgrupo de H . Então $(G : K) = (G : H) \cdot (H : K)$.

Demonstração. Sejam G um grupo e H, K subgrupos de G com $K \subseteq H \subseteq G$. Queremos demonstrar que o índice $(G : K)$ é igual ao produto dos índices $(G : H)$ e $(H : K)$. Para isso, utilizamos o Axioma da Escolha para construir representantes de classes laterais e uma bijeção explícita entre os conjuntos envolvidos.

Pelo Axioma da Escolha, existe uma função

$$\phi: \frac{G}{H} \longrightarrow \bigcup_{\alpha \in \frac{G}{H}} \alpha \subseteq H$$

tal que, para cada classe lateral $\alpha \in \frac{G}{H}$, temos $\phi(\alpha) \in \alpha$. Definimos $x_\alpha := \phi(\alpha) \in G$ para cada $\alpha \in \frac{G}{H}$, de modo que $x_\alpha H = \alpha$.

Analogamente, aplicando o Axioma da Escolha ao quociente $\frac{H}{K}$, obtemos uma função

$$\delta : \frac{H}{K} \longrightarrow \bigcup_{\beta \in \frac{H}{K}} \beta \subseteq H$$

tal que $\delta(\beta) \in \beta$ para todo $\beta \in \frac{H}{K}$. Denotamos $y_\beta := \delta(\beta) \in H$, e assim $y_\beta K = \beta$.

Definimos agora a função

$$\eta : \frac{G}{H} \times \frac{H}{K} \longrightarrow \frac{G}{K}$$

por $\eta(\alpha, \beta) := (x_\alpha y_\beta)K$. Mostraremos que essa função é injetiva e sobrejetiva, portanto uma bijeção.

Injetividade. Suponha que $\eta(\alpha_1, \beta_1) = \eta(\alpha_2, \beta_2)$. Isso significa que

$$(x_{\alpha_1} y_{\beta_1})K = (x_{\alpha_2} y_{\beta_2})K,$$

ou seja, existe $z \in K$ tal que $x_{\alpha_1} y_{\beta_1} = x_{\alpha_2} y_{\beta_2} z$.

Como $K \subseteq H$, podemos reescrever:

$$x_{\alpha_1} = x_{\alpha_2} (y_{\beta_2} z y_{\beta_1}^{-1}).$$

Note que o termo $y_{\beta_2} z y_{\beta_1}^{-1} \in H$, pois $y_{\beta_2}, y_{\beta_1} \in H$ e $z \in K \subseteq H$. Assim, temos que x_{α_1} e x_{α_2} pertencem à mesma classe lateral à esquerda de H , ou seja,

$$x_{\alpha_1} H = x_{\alpha_2} H \Rightarrow \alpha_1 = \alpha_2.$$

Com isso, voltamos à equação inicial e aplicamos a igualdade $x_{\alpha_1} = x_{\alpha_2}$, obtendo:

$$y_{\beta_1} = y_{\beta_2} z.$$

Portanto, $y_{\beta_1} K = y_{\beta_2} K$, ou seja, $\beta_1 = \beta_2$. Concluimos que $(\alpha_1, \beta_1) = (\alpha_2, \beta_2)$, o que mostra que η é injetiva.

Sobrejetividade. Seja $\mu \in \frac{G}{K}$. Então existe $x \in G$ tal que $\mu = xK$. Tomamos $\alpha := xH \in \frac{G}{H}$. Como $x_\alpha \in \alpha = xH$, segue que $x \in x_\alpha H$, ou seja, existe $h \in H$ tal que $x = x_\alpha h$.

Tomamos $\beta := hK \in \frac{H}{K}$. Como $y_\beta \in \beta = hK$, então $h \in y_\beta K$, o que implica que existe $z \in K$ tal que $h = y_\beta z$. Substituindo, temos:

$$x = x_\alpha h = x_\alpha y_\beta z.$$

Logo, $xK = (x_\alpha y_\beta)K$, isto é,

$$\mu = xK = (x_\alpha y_\beta)K = \eta(\alpha, \beta).$$

Portanto, η é sobrejetiva.

Concluimos que η é uma bijeção entre $\frac{G}{H} \times \frac{H}{K}$ e $\frac{G}{K}$. Assim, temos:

$$(G : K) = \left| \frac{G}{K} \right| = \left| \frac{G}{H} \times \frac{H}{K} \right| = (G : H) \cdot (H : K).$$

□

Observação 1.5.11. *O índice de H em G também é igual à cardinalidade do conjunto das classes laterais à direita de H em G , pois a aplicação ϕ abaixo é uma bijeção bem definida.*

$$\phi : \{\text{classes laterais à esquerda}\} \rightarrow \{\text{classes laterais à direita}\}, \quad xH \mapsto Hx^{-1}.$$

Definição 1.5.12. *Dada uma partição de um conjunto, um sistema de representantes é um conjunto $\{x_\alpha\}_{\alpha \in \Gamma}$ que contém exatamente um elemento de cada subconjunto da partição. Em particular, a cardinalidade de qualquer sistema de representantes das classes laterais à esquerda de H em G é igual a $(G : H)$.*

Proposição 1.5.13. *Todas as classes laterais de H em G têm a mesma cardinalidade, igual à cardinalidade de H .*

Demonstração. Seja $H \leq G$ um subgrupo de um grupo G . Para cada $x \in G$, define-se a classe lateral à esquerda de H por x como

$$xH = \{xh \mid h \in H\}.$$

Afirma-se que, para todo $x \in G$, vale $|xH| = |H|$. Essa igualdade decorre da existência de uma bijeção natural entre H e xH , dada por:

$$\varphi_x : H \rightarrow xH, \quad \varphi_x(h) = xh.$$

A aplicação φ_x é bem definida e:

Injetiva: Suponha que $\varphi_x(h_1) = \varphi_x(h_2)$, ou seja, $xh_1 = xh_2$. Multiplicando ambos os lados à esquerda por x^{-1} , temos $h_1 = h_2$, logo φ_x é injetiva.

Sobrejetiva: Para todo $y \in xH$, existe $h \in H$ tal que $y = xh$, isto é, $y = \varphi_x(h)$, logo φ_x é sobrejetiva.

Portanto, φ_x é uma bijeção entre H e xH , o que garante que $|xH| = |H|$. □

Teorema 1.5.14. *(Teorema de Lagrange). Sejam G um grupo finito e H um subgrupo de G . Então $|G| = (G : H) \cdot |H|$. Em particular, a ordem e o índice de H dividem a ordem de G .*

Demonstração. Tome $K = \{e\}$. Pelo princípio multiplicativo temos que

$$|G| = (G : \{e\}) = (G : H) \cdot (H : \{e\}) = (G : H) \cdot |H|.$$

□

Corolário 1.5.15. *Se G é um grupo finito e $\alpha \in G$ então $\mathcal{O}(\alpha)$ divide $|G|$. Em particular, $\alpha^{|G|} = e$.*

Demonstração. Como $\langle \alpha \rangle$ é um subgrupo de G e G é finito então a igualdade $|G| = (G : \langle \alpha \rangle) \cdot |\langle \alpha \rangle|$ implica que $|\langle \alpha \rangle|$ divide $|G|$, isto é, $\mathcal{O}(\alpha) \mid |G|$.

Assim, existe $r \in \mathbb{N}$ tal que $|G| = r \cdot \mathcal{O}(\alpha)$. Logo, $\alpha^{|G|} = (\alpha^{\mathcal{O}(\alpha)})^r = e^r = e$. □

Corolário 1.5.16. *(Pequeno Teorema de Fermat). Seja $p \in \mathbb{N}$ um número primo. Então $a^{p-1} \equiv 1 \pmod{p}$, $\forall a \in \mathbb{Z}$ com $p \nmid a$.*

Demonstração. Sabemos que $\left(\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*, \cdot\right)$ é um grupo multiplicativo de ordem $p-1$ elementos. Se $a \in \mathbb{Z}$ com $p \nmid a$ então $\bar{a} \neq \bar{0}$ módulo p . Assim, $\bar{a} \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ e pelo corolário anterior segue que $\bar{a}^{p-1} = \bar{1}$, isto é, $\overline{a^{p-1}} = \bar{1}$ e portanto $a^{p-1} \equiv 1 \pmod{p}$. □

Corolário 1.5.17. *Se p é um número primo, então, para cada $a \in \mathbb{Z}$, temos $a^p \equiv a \pmod{p}$.*

Corolário 1.5.18. *(Euler). Sejam x e n dois inteiros relativamente primos. Então $x^{\Phi(n)} \equiv 1 \pmod{n}$, onde Φ é a função de Euler.*

Demonstração. Já sabemos que $\left|\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*\right| = \Phi(n)$. Como $x \in \mathbb{N}$ tal que $\text{mdc}(x, n) = 1$ então $\bar{x} \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \Rightarrow \bar{x}^{\Phi(n)} = \bar{1} \Rightarrow x^{\Phi(n)} \equiv 1 \pmod{n}$. □

Corolário 1.5.19. *Seja G um grupo de ordem prima. Então G é cíclico.*

Demonstração. Seja G um grupo finito cuja ordem $|G|$ é um número primo p . Vamos mostrar que G é necessariamente cíclico. Como p é primo, temos $p \geq 2$, e portanto G contém pelo menos um elemento diferente da identidade. Seja $\alpha \in G$ tal que $\alpha \neq e$, onde e denota o elemento neutro de G .

Considere o subgrupo gerado por α , denotado por $\langle \alpha \rangle$. Pelo Teorema de Lagrange, a ordem de $\langle \alpha \rangle$ deve dividir a ordem de G , ou seja, $|\langle \alpha \rangle|$ divide p . Como p é primo, seus únicos divisores positivos são 1 e p . Mas $\alpha \neq e$, logo a ordem de α é maior que 1. Portanto, $|\langle \alpha \rangle|$ não pode ser 1, restando apenas $|\langle \alpha \rangle| = p$. Isso implica que $\langle \alpha \rangle$ é um subgrupo de G com exatamente p elementos. Como G é finito e tem a mesma cardinalidade, segue que $\langle \alpha \rangle = G$. Concluimos assim, que G é gerado por α , ou seja, G é um grupo cíclico. □

Proposição 1.5.20. *Seja G um grupo e $\alpha \in G$ um elemento de ordem finita. Se $n \in \mathbb{Z}$ é tal que $\alpha^n = e$, então a ordem de α divide n .*

Demonstração. Seja $\mathcal{O}(\alpha) = r$ (a ordem de α). Por definição, r é o menor inteiro positivo tal que $\alpha^r = e$.

Pelo algoritmo da divisão de Euclides, existem inteiros q e s tais que:

$$n = q \cdot r + s \quad \text{com} \quad 0 \leq s < r.$$

Substituindo n na equação $\alpha^n = e$, temos:

$$\alpha^n = \alpha^{q \cdot r + s} = (\alpha^r)^q \cdot \alpha^s = e^q \cdot \alpha^s = \alpha^s = e.$$

Assim, $\alpha^s = e$, com $0 \leq s < r$.

Como r é o menor inteiro positivo que satisfaz $\alpha^r = e$, a única possibilidade é $s = 0$. Caso contrário, se $s > 0$, teríamos um inteiro positivo menor que r satisfazendo $\alpha^s = e$, uma contradição para a minimalidade de r .

Portanto, $s = 0$, e a equação da divisão torna-se $n = q \cdot r$, o que implica $r \mid n$. $\square$

Proposição 1.5.21. *Seja G um grupo abeliano. Se $a, b \in G$ são dois elementos de ordem finita tais que $\text{mdc}(\mathcal{O}(a), \mathcal{O}(b)) = 1$, então $\mathcal{O}(ab) = \mathcal{O}(a) \cdot \mathcal{O}(b)$.*

Demonstração. Sejam $\mathcal{O}(a) = n$ e $\mathcal{O}(b) = m$. Mostraremos que $\mathcal{O}(ab) = n \cdot m$.

Como $ab = ba$, temos:

$$(ab)^{n \cdot m} = a^{n \cdot m} \cdot b^{n \cdot m} = (a^n)^m \cdot (b^m)^n = e^m \cdot e^n = e.$$

Logo, $\mathcal{O}(ab) \mid n \cdot m$.

Seja $\mathcal{O}(ab) = s$. Então:

$$(ab)^s = a^s \cdot b^s = e \implies a^s = b^{-s}.$$

Como $a^s \in \langle a \rangle$ e $b^{-s} \in \langle b \rangle$, segue que $a^s = b^{-s} \in \langle a \rangle \cap \langle b \rangle$.

Pelo Teorema de Lagrange, $|\langle a \rangle \cap \langle b \rangle|$ divide $|\langle a \rangle|$ e $|\langle a \rangle \cap \langle b \rangle|$ divide $|\langle b \rangle|$, o que implica $|\langle a \rangle \cap \langle b \rangle|$ é um divisor comum de n e m . Assim, $|\langle a \rangle \cap \langle b \rangle|$ divide $\text{mdc}(n, m) = 1$. Portanto, $\langle a \rangle \cap \langle b \rangle = \{e\}$, o que implica:

$$a^s = e \implies \mathcal{O}(a) \mid s, \quad \text{e} \quad b^s = e \implies \mathcal{O}(b) \mid s.$$

Como $\text{mdc}(n, m) = 1$, temos $\mathcal{O}(a) \cdot \mathcal{O}(b) \mid s$.

Já que $s \mid n \cdot m$ e $n \cdot m \mid s$, concluímos que $s = n \cdot m$, isto é, $\mathcal{O}(ab) = \mathcal{O}(a) \cdot \mathcal{O}(b)$. $\square$

Proposição 1.5.22. *Sejam G um grupo abeliano e $a, b \in G$ elementos de ordem finita. Então, existe $c \in G$ tal que $\mathcal{O}(c) = \text{mmc}(\mathcal{O}(a), \mathcal{O}(b))$.*

Demonstração. Sejam $\mathcal{O}(a) = n$ e $\mathcal{O}(b) = m$. Pelo Teorema Fundamental da Aritmética, podemos escrever:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

onde $p_1, \dots, p_k$ são primos distintos e $\alpha_i, \beta_i \geq 0$ para todo i .

As expressões para o máximo divisor comum e o mínimo múltiplo comum são:

$$\begin{aligned} \text{mdc}(n, m) &= p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}, \\ \text{mmc}(n, m) &= p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}. \end{aligned}$$

Reordenando os primos, podemos assumir que existe ℓ tal que:

$$\alpha_i \leq \beta_i \text{ para } 1 \leq i \leq \ell, \quad \alpha_i > \beta_i \text{ para } \ell + 1 \leq i \leq k.$$

Definimos os seguintes produtos:

$$s := p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}, \quad t := p_{\ell+1}^{\beta_{\ell+1}} \cdots p_k^{\beta_k}, \quad s' := p_{\ell+1}^{\alpha_{\ell+1}} \cdots p_k^{\alpha_k}, \quad t' := p_1^{\beta_1} \cdots p_\ell^{\beta_\ell}.$$

Note que:

$$n = s \cdot s', \quad m = t \cdot t', \quad \text{e} \quad \text{mdc}(s', t') = 1.$$

Considere agora:

$$a' := a^s, \quad b' := b^t.$$

Como $\mathcal{O}(a) = s \cdot s'$, temos:

$$(a')^{s'} = (a^s)^{s'} = a^{s \cdot s'} = a^n = e,$$

e s' é o menor inteiro positivo com essa propriedade. Logo,

$$\mathcal{O}(a') = s'.$$

De forma análoga, como $\mathcal{O}(b) = t \cdot t'$, temos:

$$(b')^{t'} = (b^t)^{t'} = b^{t \cdot t'} = b^m = e \Rightarrow \mathcal{O}(b') = t'.$$

Como G é abeliano e $\text{mdc}(s', t') = 1$, segue do resultado sobre ordens de produtos de elementos com ordens coprimas que:

$$\mathcal{O}(a'b') = s' \cdot t' = \text{mmc}(n, m).$$

Logo, tomando $c := a'b'$, temos $\mathcal{O}(c) = \text{mmc}(\mathcal{O}(a), \mathcal{O}(b))$, como desejado. $\square$

Proposição 1.5.23. *Seja G um grupo abeliano. Se $r := \sup\{\mathcal{O}(g) \mid g \in G\}$ é finito, então $\mathcal{O}(x)$ divide r para cada $x \in G$.*

Demonstração. Suponha que $r := \sup\{\mathcal{O}(g) \mid g \in G\}$ seja finito e tome $y \in G$ tal que $\mathcal{O}(y) = r$. Se existisse $x \in G$ com $\mathcal{O}(x)$ não dividindo r , então $s := \text{MMC}(\mathcal{O}(x), \mathcal{O}(y)) >$

r , e pela afirmação anterior, existiria $c \in G$ com $\mathcal{O}(c) = s > r$, contradizendo a definição de r . Portanto, $\mathcal{O}(x)$ divide r . $\square$

1.6 SUBGRUPOS NORMAIS E GRUPOS QUOCIENTES

Sejam G um grupo e $H \leq G$ um subgrupo. Podemos considerar o conjunto das classes laterais à esquerda de H em G , denotado por

$$G/H = \{xH \mid x \in G\}.$$

Uma ideia natural da álgebra é investigar a possibilidade em definir uma estrutura algébrica sobre G/H , mais precisamente uma estrutura de grupo, de forma que a operação em G/H esteja relacionada à operação original em G .

A tentativa mais direta e lógica de definirmos um produto entre duas classes xH e yH em G/H é por meio da seguinte regra:

$$xH \cdot yH := (xy)H.$$

Essa definição é motivada pela noção de que, como G já possui uma operação $\cdot$, a forma mais razoável de desenvolver um produto entre classes laterais é através da multiplicação dos representantes correspondentes.

Toda via, essa definição tem uma dependência da escolha dos representantes x e y . Para que a operação acima seja bem definida, é necessário assegurar que, se $xH = x'H$ e $yH = y'H$, então $(xy)H = (x'y')H$. Isto é, a definição deve ser independente da escolha dos representantes de classe. Em outras palavras, queremos verificar se a operação

$$(xH, yH) \mapsto xyH$$

é bem definida.

Sejam $x_1, x_2, y_1, y_2 \in G$ tais que $(x_1H, y_1H) = (x_2H, y_2H)$, ou seja,

$$x_1H = x_2H \quad \text{e} \quad y_1H = y_2H.$$

Então, existem $h_1, h_2 \in H$ tais que

$$x_2 = x_1h_1 \quad \text{e} \quad y_2 = y_1h_2.$$

Desejamos garantir que:

$$x_1y_1H = x_2y_2H.$$

Substituindo as expressões de x_2 e y_2 , temos:

$$x_2y_2 = (x_1h_1)(y_1h_2) = x_1(h_1y_1)h_2.$$

Logo, a igualdade desejada se traduz em:

$$x_1 y_1 H = x_1 (h_1 y_1) h_2 H.$$

Multiplicando ambos os lados à esquerda por x_1^{-1} , obtemos:

$$y_1 H = (h_1 y_1) h_2 H.$$

Multiplicando ambos os lados à esquerda por y_1^{-1} , temos:

$$H = y_1^{-1} h_1 y_1 h_2 H.$$

Observe que $h_2 \in H$ e então $eH = h_2 H$, ou seja, $H = h_2 H$. Assim:

$$H = eH = y_1^{-1} h_1 y_1 H.$$

Portanto, para que a igualdade das classes seja garantida independentemente dos representantes escolhidos, é necessário que

$$y^{-1} h y \in H \quad \text{para todo } y \in G \text{ e } h \in H.$$

Isto equivale a exigir que

$$gHg^{-1} \subseteq H, \quad \forall g \in G.$$

Como essa inclusão vale para todo $g \in G$, ela também vale para g^{-1} . Assim,

$$g^{-1} H g \subseteq H.$$

Multiplicando essa inclusão à esquerda por g e à direita por g^{-1} , obtemos

$$H = g g^{-1} H g g^{-1} \subseteq g H g^{-1}.$$

Logo,

$$H \subseteq g H g^{-1}.$$

Juntando com a inclusão anterior $g H g^{-1} \subseteq H$, concluímos que

$$g H g^{-1} = H, \quad \forall g \in G.$$

Definição 1.6.1. Dizemos que um subgrupo $H \leq G$ é normal em G , e escrevemos $H \trianglelefteq G$, se

$$g h g^{-1} \in H, \quad \forall g \in G.$$

Observação 1.6.2. Para reforçar a diferença entre subgrupos normais e subgrupos arbitrários, utiliza-se a notação $H \trianglelefteq G$, graficamente semelhante ao símbolo de inclusão,

mas com um triângulo à esquerda que indica a normalidade. Essa notação é particularmente útil para enfatizar propriedades de invariância, principalmente em contextos onde há múltiplos subgrupos envolvidos.

Proposição 1.6.3. *Sejam G um grupo e $H \leq G$ um subgrupo. As seguintes afirmações são equivalentes:*

- (i) $gHg^{-1} \subseteq H$ para todo $g \in G$;
- (ii) $gHg^{-1} = H$ para todo $g \in G$;
- (iii) $gH = Hg$ para todo $g \in G$.

Demonstração. Por definição, se $H \trianglelefteq G$, então para todo $g \in G$ e todo $h \in H$, tem-se $ghg^{-1} \in H$. Como $h \in H$ foi arbitrário, isso implica $gHg^{-1} \subseteq H$.

(i) $\Rightarrow$ (ii): Se $gHg^{-1} \subseteq H$ para todo $g \in G$, então tomando g^{-1} no lugar de g , temos também $g^{-1}Hg \subseteq H$. Seja $h \in H$ e tome $l := g^{-1}hg \in g^{-1}Hg \subseteq H$, o que implica $l \in H$. Note que $gl = g(g^{-1}hg) = hg$. Assim:

$$glg^{-1} = (hg)g^{-1} = h \Rightarrow h = glg^{-1} \in gHg^{-1}$$

Logo, $gHg^{-1} \subseteq H$ e $H \subseteq gHg^{-1}$, o que implica

$$gHg^{-1} = H.$$

(ii) $\Rightarrow$ (iii): Assuma que $gHg^{-1} = H$ para todo $g \in G$.

Primeira inclusão ($gH \subseteq Hg$): Seja $x \in gH$. Então, existe $h \in H$ tal que $x = gh$. Multiplicando à direita por g^{-1} , obtemos:

$$xg^{-1} = ghg^{-1} \in gHg^{-1}.$$

Pela hipótese (ii), $gHg^{-1} = H$, logo $xg^{-1} \in H$. Assim, existe $h' \in H$ tal que $xg^{-1} = h'$. Portanto,

$$x = h'g \in Hg.$$

Isso mostra que $gH \subseteq Hg$.

Segunda inclusão ($Hg \subseteq gH$). Seja $y \in Hg$. Então, existe $h \in H$ tal que $y = hg$. Reescrevendo, temos:

$$g^{-1}y = g^{-1}hg \in g^{-1}Hg.$$

Pela hipótese (ii), $g^{-1}Hg = H$, logo $g^{-1}y \in H$. Assim, existe $h'' \in H$ tal que $g^{-1}y = h''$. Portanto,

$$y = gh'' \in gH.$$

Isso mostra que $Hg \subseteq gH$.

Como ambas as inclusões estão verificadas, concluímos que $gH = Hg$ para todo $g \in G$.

(iii) $\Rightarrow$ (i) Suponha que $gH = Hg$, para todo $g \in G$. Queremos mostrar que $gHg^{-1} \subseteq H$.

Seja $g \in G$ fixado e considere um elemento arbitrário $y \in gHg^{-1}$. Então, existe $h \in H$ tal que

$$y = ghg^{-1}.$$

Seja $c := gh \in gH$. Como, por hipótese, $gH = Hg$, então existe $l \in H$ tal que

$$c = lg.$$

Substituindo, temos:

$$y = (gh)g^{-1} = cg^{-1} = (lg)g^{-1} = l(gg^{-1}) = l \cdot e = l.$$

Portanto, $y \in H$, e como $y \in gHg^{-1}$ foi arbitrário, concluímos que

$$gHg^{-1} \subseteq H.$$

□

Exemplos de Subgrupos Normais

A definição de subgrupo normal nos permite identificar dois exemplos que sempre ocorrem em qualquer grupo, e que por isso são chamados de exemplos *triviais*.

- O próprio grupo G é um subgrupo normal de si mesmo. De fato, para todo $g \in G$ e todo $h \in G$, tem-se $ghg^{-1} \in G$, pois G é fechado sob a operação do grupo. Assim, $G \trianglelefteq G$.
- O subgrupo trivial $\{e\}$, onde e é o elemento neutro de G , também é um subgrupo normal. De fato, para todo $g \in G$, temos:

$$g\{e\}g^{-1} = \{geg^{-1}\} = \{gg^{-1}\} = \{e\},$$

portanto $g\{e\}g^{-1} = \{e\} \subseteq \{e\}$, o que mostra que $\{e\} \trianglelefteq G$.

Estes dois exemplos evidenciam que, em qualquer grupo G , sempre existem pelo menos dois subgrupos normais: o próprio grupo G e o subgrupo trivial $\{e\}$.

Corolário 1.6.4. *O centro de um grupo G é um subgrupo normal de G , ou seja, $Z(G) \trianglelefteq G$.*

Demonstração. Basta aplicar a proposição anterior ao subgrupo $H = Z(G)$, observando que $Z(G) \subseteq Z(G)$ trivialmente. □

Nosso objetivo é demonstrar que o subgrupo dos comutadores $G' \trianglelefteq G$.

Para isso, faremos uso do seguinte lema auxiliar:

Lema 1.6.5. *Seja G um grupo e $S \subseteq G$. Suponha que, para todo $s \in S$ e $g \in G$, tanto $gsg^{-1} \in \langle S \rangle$ quanto $gs^{-1}g^{-1} \in \langle S \rangle$. Então o subgrupo $\langle S \rangle$ gerado por S é normal em G .*

Demonstração. Seja $h \in \langle S \rangle$. Por definição de subgrupo gerado, existe uma expressão:

$$h = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_r^{\varepsilon_r}, \quad \text{com } s_i \in S, \varepsilon_i = \pm 1.$$

Seja $g \in G$. Queremos mostrar que $ghg^{-1} \in \langle S \rangle$. Utilizando a associatividade e inserindo identidades estrategicamente, temos:

$$ghg^{-1} = (gs_1^{\varepsilon_1}g^{-1})(gs_2^{\varepsilon_2}g^{-1}) \cdots (gs_r^{\varepsilon_r}g^{-1}).$$

Cada fator $gs_i^{\varepsilon_i}g^{-1} \in \langle S \rangle$ por hipótese. Como $\langle S \rangle$ é subgrupo, e portanto fechado sob o produto, conclui-se que $ghg^{-1} \in \langle S \rangle$. Assim, $\langle S \rangle \trianglelefteq G$. $\square$

Proposição 1.6.6. *Se G é um grupo então G' é um subgrupo normal de G .*

Demonstração. Agora, aplicamos o lema anterior ao conjunto dos comutadores. Seja:

$$S = \{[x, y] = xyx^{-1}y^{-1} \mid x, y \in G\}.$$

Queremos mostrar que $\langle S \rangle = G'$ é um subgrupo normal de G .

Seja $s = [x, y] \in S$ e $g \in G$. Temos:

$$gsg^{-1} = g(xy x^{-1} y^{-1})g^{-1} = (g x g^{-1})(g y g^{-1})(g x g^{-1})^{-1}(g y g^{-1})^{-1} = [g x g^{-1}, g y g^{-1}].$$

Como $g x g^{-1}, g y g^{-1} \in G$, então $gsg^{-1} \in S \subseteq \langle S \rangle$.

De modo análogo, seja $s^{-1} = [x, y]^{-1} = y x y^{-1} x^{-1} = [y, x]$. Assim,

$$gs^{-1}g^{-1} = g[y, x]g^{-1} = [g y g^{-1}, g x g^{-1}] \in S \subseteq \langle S \rangle.$$

Portanto, ambos os requisitos do lema estão satisfeitos, e concluímos que:

$$G' = \langle S \rangle \trianglelefteq G.$$

$\square$

Proposição 1.6.7. *Seja G um grupo abeliano. Então, todo subgrupo $H \subseteq G$ é normal em G .*

Demonstração. Como G é abeliano, todo elemento de G comuta com qualquer outro elemento de G . Logo, o centro de G coincide com o próprio grupo, isto é,

$$Z(G) = G.$$

Seja agora $H \leq G$. Da igualdade acima, obtemos $H \leq Z(G)$. Pela proposição que afirma que todo subgrupo contido no centro é normal, isto é,

$$H \leq Z(G) \implies H \trianglelefteq G,$$

segue que $H \trianglelefteq G$. Portanto, todo subgrupo de G é normal em G . $\square$

Proposição 1.6.8. *Se G é um grupo e H é um subgrupo de G com $(G : H) = 2$ então $H \triangleleft G$.*

Demonstração. Vamos mostrar que $gH = Hg$, $\forall g \in G$.

1. Se $g \in H$: Neste caso, $gH = H$ (pois g é um elemento de H e H é fechado sob a operação do grupo) e $Hg = H$ (pela mesma razão). Logo, $gH = H = Hg$.
2. Se $g \notin H$: Como $(G : H) = 2$, existem exatamente dois conjuntos laterais à esquerda e dois conjuntos laterais à direita distintos. Podemos escrever os conjuntos laterais à esquerda como $G/H = \{eH, xH\}$ para algum $x \in G \setminus H$. Equivalentemente, $G = eH \dot{\cup} xH = H \dot{\cup} xH$, onde $\dot{\cup}$ denota união disjunta.

Observamos que $xH = G \setminus H$.

($\subseteq$) Suponha, por contradição, que $xH \not\subseteq G \setminus H$. Então, existe $h \in H$ tal que $xh \in H$, pois H é subgrupo. Se $xh \in H$, então $x = (xh)h^{-1} \in H$. Como $h^{-1} \in H$, temos $x \in H$, o que é um absurdo, pois escolhemos $x \notin H$. Portanto, $xH \subseteq G \setminus H$.

($\supseteq$) Se $g \in G \setminus H$, como $G = H \dot{\cup} xH$, e $g \notin H$, necessariamente $g \in xH$.

Assim, $xH = G \setminus H$.

Analogamente, podemos escrever os conjuntos laterais à direita como $H/G = \{He, Hx\}$. Novamente, $G = He \dot{\cup} Hx = H \dot{\cup} Hx$. Similarmente, $Hx = G \setminus H$.

Portanto, como $xH = G \setminus H$ e $Hx = G \setminus H$, temos $xH = Hx$.

Finalmente, dado $g \in G$:

- Se $g \in H$, já vimos que $gH = H = Hg$.
- Se $g \notin H$, então, como $G = H \dot{\cup} xH = H \dot{\cup} Hx$, necessariamente $g \in xH$ e $g \in Hx$. Se $g \in xH$, então $gH = xH$. Se $g \in Hx$, então $Hg = Hx$. Como demonstramos que $xH = Hx$, segue que $gH = Hg$.

Em ambos os casos ($g \in H$ e $g \notin H$), temos $gH = Hg$. Portanto, $H \triangleleft G$. $\square$

Definição 1.6.9. *Seja G um grupo e seja $H \triangleleft G$ um subgrupo normal. Podemos considerar o conjunto das classes laterais de G módulo H , denotado por G/H , onde cada classe lateral à esquerda tem a forma $gH = \{gh : h \in H\}$.*

Definimos a operação binária em G/H da seguinte maneira:

$$(gH)(g'H) = (gg')H,$$

para quaisquer $g, g' \in G$.

Observação 1.6.10. Esta operação é chamada de operação quociente e é bem definida justamente porque H é normal em G .

- **Associatividade:** Como a operação em G é associativa, temos para quaisquer $xH, yH, zH \in G/H$:

$$(xH)(yH)(zH) = ((xy)H)(zH) = (xyz)H = (xH)((yz)H) = (xH)((yH)(zH)).$$

Assim, a operação em G/H é associativa.

- **Elemento neutro:** A classe lateral $eH = H$, onde e é o elemento neutro de G , atua como identidade em G/H , pois para todo $x \in G$:

$$(eH)(xH) = (ex)H = xH, \quad (xH)(eH) = (xe)H = xH.$$

- **Inverso:** Para todo $x \in G$, temos que $(xH)(x^{-1}H) = (xx^{-1})H = eH = H$. Logo, o inverso da classe xH é a classe $x^{-1}H$.

Portanto, G/H com essa operação é um grupo, chamado **grupo quociente** de G por H .

Observação 1.6.11. Se G é abeliano, então G/H também é abeliano. De fato, para quaisquer $x, y \in G$:

$$(xH)(yH) = (xy)H = (yx)H = (yH)(xH).$$

Assim, a comutatividade de G se transmite ao quociente.

Proposição 1.6.12. Seja G um grupo qualquer. O subgrupo comutador $G' = \langle [x, y] = x^{-1}y^{-1}xy \mid x, y \in G \rangle$ é o menor subgrupo normal de G tal que o quociente G/G' é abeliano.

Demonstração. Primeiramente, mostramos que G/G' é um grupo abeliano. Como já provamos que G' é normal em G , a construção do grupo quociente G/G' é válida.

Sejam $xG', yG' \in G/G'$ quaisquer. Temos:

$$(xG')(yG') = xyG', \quad \text{e} \quad (yG')(xG') = yxG'.$$

Queremos mostrar que $xyG' = yxG'$. Para isso, notamos que:

$$xyG' = yxG' \iff (yx)^{-1}(xy) \in G'.$$

De fato,

$$(yx)^{-1}(xy) = x^{-1}y^{-1}xy = [x, y] \in G',$$

por definição de G' . Logo, $xyG' = yxG'$, e portanto G/G' é abeliano.

Agora mostramos que G' é o menor subgrupo normal de G com essa propriedade. Seja $H \triangleleft G$ tal que G/H é abeliano. Vamos provar que $G' \subseteq H$.

Basta verificar que todos os geradores de G' estão contidos em H . Como G' é gerado pelos comutadores $[x, y]$ com $x, y \in G$, mostramos que $[x, y] \in H$.

Como G/H é abeliano, temos $xH \cdot yH = yH \cdot xH$, ou seja,

$$xyH = yxH \iff (yx)^{-1}xy \in H \iff [x, y] \in H.$$

Logo, todo comutador $[x, y]$ pertence a H , e como G' é gerado por esses elementos, segue que $G' \subseteq H$.

Portanto, G' é o menor subgrupo normal de G tal que G/G' é abeliano, o que conclui a demonstração. $\square$

Proposição 1.6.13. *Seja G um grupo. Se o grupo quociente $G/Z(G)$ é cíclico, então G é abeliano. Em particular, se G é finito, então o índice $(G : Z(G))$ nunca é um número primo.*

Demonstração. Como o centro $Z(G)$ é um subgrupo normal de G , o quociente $G/Z(G)$ é um grupo. Suponha que $G/Z(G)$ seja cíclico. Então, existe um elemento $y \in G$ tal que $G/Z(G)$ é gerado pela classe $\bar{y}$ de y em $G/Z(G)$, ou seja,

$$G/Z(G) = \langle \bar{y} \rangle.$$

Dado $g_1, g_2 \in G$, como $\bar{g}_1, \bar{g}_2 \in G/Z(G)$, existem inteiros r_1, r_2 tais que:

$$\bar{g}_1 = \bar{y}^{r_1}, \quad \bar{g}_2 = \bar{y}^{r_2}.$$

Ou seja, existem $z_1, z_2 \in Z(G)$ tais que:

$$g_1 = y^{r_1} z_1, \quad g_2 = y^{r_2} z_2.$$

Então:

$$g_1 g_2 = (y^{r_1} z_1)(y^{r_2} z_2) = y^{r_1} y^{r_2} z_1 z_2 = y^{r_1+r_2} z_1 z_2,$$

pois os elementos do centro comutam com todos os elementos de G . Analogamente:

$$g_2 g_1 = (y^{r_2} z_2)(y^{r_1} z_1) = y^{r_2+r_1} z_2 z_1 = y^{r_1+r_2} z_1 z_2,$$

pois $z_1 z_2 = z_2 z_1$. Portanto, $g_1 g_2 = g_2 g_1$, e como g_1, g_2 foram arbitrários, segue que G é abeliano.

Agora, suponha por absurdo que $(G : Z(G)) = p$, com p primo. Como $Z(G)$ é normal em G , $G/Z(G)$ é um grupo de ordem p . Pelo corolário 1.5.19, qualquer grupo de ordem prima é cíclico. Logo, $G/Z(G)$ é cíclico. Pelo que já foi demonstrado, isso implica que G é abeliano.

Se G é abeliano, então $Z(G) = G$, pois o centro de um grupo abeliano é o próprio grupo. Portanto,

$$(G : Z(G)) = (G : G) = 1,$$

o que contradiz a suposição de que $(G : Z(G)) = p$ com p primo. Logo, $(G : Z(G))$ não pode ser primo.

□

1.7 INTRODUÇÃO AOS MORFISMOS DE GRUPOS

Em várias áreas da matemática, quando tratamos de estruturas algébricas, é imprescindível compreender a forma que diferentes objetos dessa natureza podem ser ou estar relacionados entre si. Tal entendimento não está limitado à análise dos conjuntos implícitos, mas requer em essência, o estudo das estruturas internas que caracterizam a identidade a esses objetos. Nesse viés, surgem o que chamamos de *morfismos*, que são funções algébricas que mantêm, de forma adequada, as operações que definem essas estruturas.

No contexto de álgebra linear, as transformações lineares são funções entre espaços vetoriais que preservam a operação de adição de vetores e a multiplicação por escalares. Para entender e comparar estruturas semelhantes, é conveniente dispor de funções que, além de operar nos conjuntos subjacentes, respeitem as operações definidas nessas estruturas.

Trazendo essa ideia para o contexto de Grupos, almejamos estudar e entender funções que preservem a operação, assim como propriedades norteadoras que fundamentarão o conteúdo. Considerando que um grupo é uma estrutura algébrica formada por um conjunto munido de uma operação binária associativa, que admite elemento neutro e inversos, é natural pensarmos que as funções de interesse sejam aquelas que respeitam essa operação.

Definição 1.7.1. *Sejam G e H grupos. Uma função $f : G \rightarrow H$ é chamada de morfismo de grupos (ou homomorfismo de grupos) se, para todos os elementos $x, y \in G$, tem-se:*

$$f(xy) = f(x)f(y),$$

onde a multiplicação xy no domínio é realizada com a operação do grupo G , e o produto $f(x)f(y)$ no contradomínio ocorre com a operação do grupo H .

A condição anterior assegura que f preserva a estrutura algébrica de G , no entendimento que a imagem do produto de dois elementos coincide com o produto das imagens.

Embora toda função estabeleça uma correspondência entre conjuntos, apenas aquelas que respeitam as operações internas dos grupos envolvidos são consideradas morfismos de grupos.

Podemos notar que nem toda função entre dois grupos satisfaz essa propriedade. Por exemplo, considere a função $f : \mathbb{Z} \rightarrow \mathbb{Z}$ definida por $f(n) = n^2$. Embora bem definida sobre $\mathbb{Z}$, essa função não é um morfismo de grupos com respeito à adição, pois, em geral:

$$f(m+n) = (m+n)^2 \neq m^2 + n^2 = f(m) + f(n).$$

Exemplo 1.7.2. *Seja G um grupo qualquer. A função identidade $\text{id}_G : G \rightarrow G$, definida por $\text{id}_G(x) = x$ para todo $x \in G$, é um morfismo de grupos.*

De fato, para quaisquer $x, y \in G$, temos:

$$\text{id}_G(xy) = xy = \text{id}_G(x) \cdot \text{id}_G(y),$$

onde a operação $\cdot$ é a operação do grupo G . Uma vez que a função identidade simplesmente devolve o próprio elemento, obviamente temos a operação do grupo preservada. Este é um exemplo trivial de morfismo, mas necessária, pois toda estrutura algébrica admite sua própria identidade como um automorfismo.

Exemplo 1.7.3. *Sejam G e H grupos. Seja e_H o elemento neutro de H . A função constante $f : G \rightarrow H$, definida por $f(x) = e_H$ para todo $x \in G$, é chamada de morfismo trivial.*

Para quaisquer $x, y \in G$, temos:

$$f(xy) = e_H = e_H \cdot e_H = f(x) \cdot f(y).$$

Ou seja, mesmo sendo constante, a função preserva a operação, pois o elemento neutro multiplicado por si mesmo continua sendo o neutro. O morfismo trivial é um exemplo onde nenhuma informação estrutural de G é transportada para H , mas ainda assim a definição é realizada.

Exemplo 1.7.4. *Seja G um grupo abeliano e $n \in \mathbb{Z}$ um número fixado. Define-se a função $\varphi_n : G \rightarrow G$ por:*

$$\varphi_n(x) = x^n, \quad \text{para todo } x \in G,$$

onde x^n denota a operação iterada de x com ele mesmo n vezes (utilizando inversos, se $n < 0$).

Como G é abeliano, temos, para quaisquer $x, y \in G$,

$$\varphi_n(xy) = (xy)^n = x^n y^n = \varphi_n(x) \cdot \varphi_n(y),$$

onde a igualdade $(xy)^n = x^n y^n$ decorre do fato de G ser abeliano. Assim, φ_n é um morfismo de grupos.

Exemplo 1.7.5. No caso particular em que $G = (\mathbb{Z}, +)$, o grupo aditivo dos inteiros, e $n \in \mathbb{Z}$, a função

$$\varphi_n : \mathbb{Z} \rightarrow \mathbb{Z}, \quad \varphi_n(m) = nm,$$

define um morfismo de grupos. Neste contexto, como a operação do grupo é a adição, a potenciação se traduz em multiplicação escalar. De fato, para quaisquer $m_1, m_2 \in \mathbb{Z}$,

$$\varphi_n(m_1 + m_2) = n(m_1 + m_2) = nm_1 + nm_2 = \varphi_n(m_1) + \varphi_n(m_2).$$

Portanto, φ_n preserva a operação aditiva e é um morfismo de grupos.

Exemplo 1.7.6. Seja H um subgrupo de um grupo G . A aplicação natural

$$\iota_H : H \hookrightarrow G, \quad x \mapsto x,$$

chamada de função inclusão, é um morfismo de grupos. Como $H \subseteq G$ e a operação de H é a restrição da operação de G , temos que, para quaisquer $x, y \in H$,

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

onde a operação à esquerda é tomada em H e, à direita, em G . No entanto, como H é subgrupo de G , ambas as operações coincidem. Portanto, ι_H preserva a operação do grupo e é, por definição, um morfismo de grupos.

Exemplo 1.7.7 (Morfismo quociente). Seja $H \trianglelefteq G$ um subgrupo normal. A aplicação

$$\pi_H : G \rightarrow G/H, \quad x \mapsto xH,$$

que associa a cada elemento sua classe lateral à esquerda, é chamada de projeção canônica ou morfismo quociente.

De fato, para quaisquer $x, y \in G$, pela definição da operação no grupo quociente G/H , tem-se:

$$\pi_H(xy) = (xy)H = xH \cdot yH = \pi_H(x)\pi_H(y),$$

onde o produto à direita é tomado em G/H . Assim, π_H preserva a estrutura algébrica e, portanto, é um morfismo de grupos.

Observação 1.7.8. A projeção canônica π_H também pode ser referida como função quociente ou morfismo de grupos.

Proposição 1.7.9. Seja $\varphi : G \rightarrow H$ um homomorfismo de grupos. Então:

1. $\varphi(e_G) = e_H$;

2. Para todo $x \in G$, tem-se $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Demonstração. (a) Como φ é um homomorfismo de grupos, temos:

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G).$$

Multiplicando ambos os lados à direita por $\varphi(e_G)^{-1} \in H$, obtemos:

$$\varphi(e_G) \cdot \varphi(e_G) \cdot \varphi(e_G)^{-1} = \varphi(e_G) \cdot e_H.$$

Utilizando a associatividade da operação em H e a definição de elemento inverso, temos:

$$(\varphi(e_G) \cdot \varphi(e_G)) \cdot \varphi(e_G)^{-1} = \varphi(e_G) \cdot \varphi(e_G)^{-1} = e_H.$$

Portanto, $\varphi(e_G) = e_H$, como queríamos demonstrar.

(b) Seja $x \in G$. Como φ preserva a operação, temos:

$$\varphi(x) \cdot \varphi(x^{-1}) = \varphi(x \cdot x^{-1}) = \varphi(e_G) = e_H,$$

pela parte (a). Assim, $\varphi(x^{-1})$ é um elemento de H tal que, multiplicado à direita por $\varphi(x)$, resulta no elemento neutro de H . Isso mostra que $\varphi(x^{-1})$ é o inverso de $\varphi(x)$ em H , ou seja,

$$\varphi(x^{-1}) = \varphi(x)^{-1}.$$

A demonstração está concluída. □

Definição 1.7.10. *Sejam G e H dois grupos e $\varphi : G \rightarrow H$ um morfismo de grupos. O núcleo de φ , denotado por $\ker \varphi$, é o subconjunto de G formado pelos elementos cuja imagem é o elemento neutro de H :*

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_H\},$$

onde e_H representa o elemento neutro do grupo H .

Definição 1.7.11. *A imagem de um morfismo de grupos $\varphi : G \rightarrow H$ é o subconjunto de H constituído pelos elementos que são imagem de algum elemento de G via φ , ou seja:*

$$\text{Im}(\varphi) = \{\varphi(g) \in H \mid g \in G\}.$$

Proposição 1.7.12. *Seja $\pi : G \rightarrow G/H$ o morfismo quociente definido por $\pi(g) = gH$, com $H \trianglelefteq G$. Então:*

1. π é sobrejetivo;

2. $\ker \pi = H$.

Demonstração. A sobrejetividade de π decorre do fato de que, para qualquer classe lateral $gH \in G/H$, existe $g \in G$ tal que $\pi(g) = gH$, ou seja, todo elemento do quociente está na imagem de π .

Quanto ao núcleo, note que:

$$g \in \ker \pi \iff \pi(g) = H \iff gH = H \iff g \in H.$$

Logo, $\ker \pi = H$. □

Proposição 1.7.13. *Seja $\varphi : G \rightarrow H$ um morfismo de grupos. Então o núcleo de φ , denotado por $\ker \varphi$, é um subgrupo normal de G .*

Demonstração. Começemos por mostrar que $\ker \varphi \subseteq G$ é um subgrupo.

- **Elemento neutro:** Como φ é um homomorfismo de grupos, temos $\varphi(e_G) = e_H$. Logo, $e_G \in \ker \varphi$, e o núcleo não é vazio.
- **Fechamento para o produto:** Sejam $x, y \in \ker \varphi$. Por definição, isso significa que $\varphi(x) = e_H$ e $\varphi(y) = e_H$. Como φ preserva a operação do grupo, segue que:

$$\varphi(xy) = \varphi(x) \cdot \varphi(y) = e_H \cdot e_H = e_H,$$

o que implica $xy \in \ker \varphi$.

- **Fechamento para o inverso:** Seja $x \in \ker \varphi$. Temos $\varphi(x) = e_H$, e como $\varphi(x^{-1}) = \varphi(x)^{-1}$ (proposição anterior), então:

$$\varphi(x^{-1}) = (\varphi(x))^{-1} = (e_H)^{-1} = e_H.$$

Portanto, $x^{-1} \in \ker \varphi$.

Assim, $\ker \varphi$ é de fato um subgrupo de G .

Agora, vamos provar que $\ker \varphi$ é um subgrupo *normal* de G . Seja $g \in G$ arbitrário e $x \in \ker \varphi$. Devemos mostrar que o conjugado $gxg^{-1} \in \ker \varphi$. Como φ é um homomorfismo, temos:

$$\varphi(gxg^{-1}) = \varphi(g) \cdot \varphi(x) \cdot \varphi(g^{-1}).$$

Como $x \in \ker \varphi$, então $\varphi(x) = e_H$, e sabemos que $\varphi(g^{-1}) = \varphi(g)^{-1}$. Assim,

$$\varphi(gxg^{-1}) = \varphi(g) \cdot e_H \cdot \varphi(g)^{-1} = \varphi(g) \cdot \varphi(g)^{-1} = e_H.$$

Logo, $gxg^{-1} \in \ker \varphi$. Como $g \in G$ e $x \in \ker \varphi$ foram arbitrários, isso prova que $\ker \varphi$ é normal em G . □

Proposição 1.7.14. *Sejam G e H grupos e seja $f : G \rightarrow H$ um homomorfismo de grupos. Então, f é injetivo se, e somente se, $\ker f = \{e_G\}$, onde e_G é o elemento neutro de G .*

Demonstração. Suponha inicialmente que f seja injetivo. Como $\ker f \subseteq G$, temos que $e_G \in \ker f$, pois $f(e_G) = e_H$, sendo e_H o elemento neutro de H . Portanto, $\{e_G\} \subseteq \ker f$.

Queremos agora mostrar a inclusão inversa, isto é, que se $x \in \ker f$, então necessariamente $x = e_G$. De fato, se $x \in \ker f$, então $f(x) = e_H$. Como $f(e_G) = e_H$, temos $f(x) = f(e_G)$. Pela hipótese de que f é injetivo, segue-se que $x = e_G$, como queríamos demonstrar.

Assim, $\ker f = \{e_G\}$.

Para a recíproca, suponha que $\ker f = \{e_G\}$, e provemos que f é injetivo. Sejam $x, y \in G$ tais que $f(x) = f(y)$. Então,

$$f(x)f(y)^{-1} = e_H.$$

Utilizando que $f(y^{-1}) = f(y)^{-1}$ (pois f é um homomorfismo), podemos reescrever a equação acima como:

$$f(xy^{-1}) = e_H.$$

Ou seja, $xy^{-1} \in \ker f$. Pela hipótese, $\ker f = \{e_G\}$, logo $xy^{-1} = e_G$. Multiplicando ambos os lados à direita por y , obtemos:

$$xy^{-1}y = e_Gy \Rightarrow x = y.$$

Portanto, f é injetivo. □

Proposição 1.7.15. *Seja $f : G \rightarrow H$ um homomorfismo de grupos. Então, a imagem de f , denotada por $\text{Im}(f) = f(G)$, é um subgrupo de H .*

Demonstração. Como f é homomorfismo, temos $f(e_G) = e_H$. Logo, $e_H \in \text{Im}(f)$, e portanto a imagem de f é não vazia.

Sejam $x, y \in \text{Im}(f)$. Então, existem $a, b \in G$ tais que $x = f(a)$ e $y = f(b)$. Assim,

$$xy^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}).$$

Como $ab^{-1} \in G$, segue que $xy^{-1} \in \text{Im}(f)$.

Portanto, pelo critério de subgrupo, $\text{Im}(f)$ é um subgrupo de H . □

Proposição 1.7.16. *Seja $f : G \rightarrow H$ um homomorfismo de grupos, e seja $K \trianglelefteq G$ um subgrupo normal de G . Então, $f(K) \trianglelefteq \text{Im}(f)$.*

Demonstração. Já vimos anteriormente (Proposição 1.7.15) que, se $K \leq G$, então $f(K) \leq H$, e, em particular, $f(K) \leq \text{Im}(f)$, pois $f(K) \subseteq f(G)$. Assim, $f(K)$ é de fato um subgrupo de $\text{Im}(f)$.

Resta verificar que $f(K)$ é normal em $\text{Im}(f)$. Para isso, seja $g \in \text{Im}(f)$ e $x \in f(K)$. Queremos mostrar que $gxg^{-1} \in f(K)$.

Como $g \in \text{Im}(f)$, existe $g_0 \in G$ tal que $f(g_0) = g$. Da mesma forma, como $x \in f(K)$, existe $x_0 \in K$ tal que $f(x_0) = x$.

Como $K \trianglelefteq G$, temos que $g_0x_0g_0^{-1} \in K$. Aplicando o homomorfismo f a esse elemento, obtemos:

$$gxg^{-1} = f(g_0)f(x_0)f(g_0)^{-1} = f(g_0x_0g_0^{-1}).$$

Como $g_0x_0g_0^{-1} \in K$, então $f(g_0x_0g_0^{-1}) \in f(K)$. Portanto, $gxg^{-1} \in f(K)$, o que mostra que $f(K)$ é fechado sob conjugação por elementos da imagem de f .

Assim, $f(K) \trianglelefteq \text{Im}(f)$, como queríamos demonstrar. $\square$

Proposição 1.7.17. *Seja $f : G \rightarrow H$ um homomorfismo de grupos e seja $L \leq H$ um subgrupo de H . Então:*

- (i) $f^{-1}(L) \leq G$;
- (ii) $\ker f \subseteq f^{-1}(L)$;
- (iii) $f(f^{-1}(L)) = L \cap \text{Im}(f)$;
- (iv) Se $L \trianglelefteq \text{Im}(f)$, então $f^{-1}(L) \trianglelefteq G$.

Demonstração. (i) Mostremos que $f^{-1}(L) \leq G$.

Como $L \leq H$, o elemento neutro $e_H \in L$. Como $f(e_G) = e_H$, segue que $e_G \in f^{-1}(L)$, de modo que o conjunto não é vazio.

Sejam $x, y \in f^{-1}(L)$. Então $f(x), f(y) \in L$, e como L é um subgrupo, $f(x)f(y) \in L$. Como f é um homomorfismo, $f(xy) = f(x)f(y) \in L$, logo $xy \in f^{-1}(L)$, provando o fechamento sob o produto.

Para o inverso, seja $x \in f^{-1}(L)$. Como $f(x) \in L$ e $L \leq H$, então $f(x)^{-1} \in L$. Como $f(x^{-1}) = f(x)^{-1}$, segue que $x^{-1} \in f^{-1}(L)$. Assim, $f^{-1}(L)$ é um subgrupo de G .

(ii) Como $\ker f = f^{-1}(\{e_H\})$, e $\{e_H\} \subseteq L$, segue da preservação de inclusões pela imagem inversa que:

$$\ker f = f^{-1}(\{e_H\}) \subseteq f^{-1}(L).$$

(iii) Mostremos que:

$$f(f^{-1}(L)) = L \cap \text{Im}(f).$$

(Inclusão $\subseteq$): Seja $x \in f(f^{-1}(L))$. Então existe $g \in G$ tal que $f(g) = x$ e $f(g) \in L$, ou seja, $x \in L$ e $x \in \text{Im}(f)$. Logo, $x \in L \cap \text{Im}(f)$.

(Inclusão $\supseteq$): Seja $y \in L \cap \text{Im}(f)$. Então existe $g \in G$ tal que $f(g) = y$. Como $y \in L$, temos $f(g) \in L$, ou seja, $g \in f^{-1}(L)$, e portanto $y = f(g) \in f(f^{-1}(L))$.

Assim, temos a igualdade:

$$f(f^{-1}(L)) = L \cap \text{Im}(f).$$

(iv) Suponha agora que $L \leq \text{Im}(f)$, e provemos que $f^{-1}(L) \leq G$.

Sejam $g \in G$ e $x \in f^{-1}(L)$. Queremos mostrar que $gxg^{-1} \in f^{-1}(L)$, ou seja, que $f(gxg^{-1}) \in L$.

Note que $f(gxg^{-1}) = f(g)f(x)f(g)^{-1}$. Como $f(x) \in L$ (por definição de $f^{-1}(L)$) e $f(g) \in \text{Im}(f)$, e como $L \leq \text{Im}(f)$, segue que:

$$f(g)f(x)f(g)^{-1} \in L.$$

Portanto, $f(gxg^{-1}) \in L$, e assim $gxg^{-1} \in f^{-1}(L)$, provando que $f^{-1}(L)$ é fechado sob conjugação por elementos de G .

Consequentemente, $f^{-1}(L) \leq G$, como queríamos demonstrar. $\square$

Proposição 1.7.18. *Seja $f : G \rightarrow H$ um homomorfismo de grupos e seja $x \in G$ um elemento de ordem finita. Então $f(x) \in H$ também tem ordem finita, e mais precisamente,*

$$\mathcal{O}(f(x)) \mid \mathcal{O}(x).$$

Demonstração. Seja $n = \mathcal{O}(x)$, ou seja, $x^n = e_G$, e n é o menor inteiro positivo com essa propriedade.

Como f é um homomorfismo de grupos, temos:

$$f(x^n) = f(x)^n = f(e_G) = e_H.$$

Portanto, $f(x)^n = e_H$, o que mostra que $f(x)$ é um elemento de ordem finita.

Além disso, como $f(x)^n = e_H$, segue que a ordem de $f(x)$, denotada por $m = \mathcal{O}(f(x))$, é o menor inteiro positivo tal que $f(x)^m = e_H$. Como $f(x)^n = e_H$, segue que $m \mid n$.

Ou seja,

$$\mathcal{O}(f(x)) \mid \mathcal{O}(x),$$

conforme queríamos demonstrar. $\square$

Lema 1.7.19. *Se $f : G \rightarrow H$ é um homomorfismo de grupos, então para todo $x \in G$ e todo $r \in \mathbb{Z}$, vale:*

$$f(x^r) = f(x)^r.$$

Demonstração. Para $r = 0$, temos $x^0 = e_G$, então $f(x^0) = f(e_G) = e_H = f(x)^0$. Para $r = 1$, a igualdade é trivial. Suponha por indução que $f(x^r) = f(x)^r$ para algum $r \geq 1$. Então:

$$f(x^{r+1}) = f(x^r \cdot x) = f(x^r)f(x) = f(x)^r f(x) = f(x)^{r+1}.$$

Para $r < 0$, escrevemos $x^r = (x^{-1})^{-r}$ e usamos que $f(x^{-1}) = f(x)^{-1}$ (já que f é homomorfismo). Então:

$$f(x^r) = f((x^{-1})^{-r}) = f(x^{-1})^{-r} = f(x)^{-1 \cdot (-r)} = f(x)^r.$$

Assim, o lema está demonstrado. $\square$

Proposição 1.7.20. *Seja $f : G \rightarrow H$ um homomorfismo de grupos. Suponha que f é injetivo. Então, para todo $x \in G$, vale*

$$\mathcal{O}(f(x)) = \mathcal{O}(x),$$

independentemente de $\mathcal{O}(x)$ ser finita ou infinita.

Demonstração. Fixemos $x \in G$. Considere os subgrupos $\langle x \rangle \subseteq G$ e $\langle f(x) \rangle \subseteq H$, gerados por x e $f(x)$, respectivamente.

Definimos a aplicação

$$\varphi : \langle x \rangle \rightarrow \langle f(x) \rangle, \quad \varphi(g) = f(g).$$

Queremos mostrar que φ é uma bijeção de grupos, o que nos permitirá concluir que $\mathcal{O}(f(x)) = \mathcal{O}(x)$, pois a ordem de um elemento é, por definição, a cardinalidade do subgrupo que ele gera.

Note que todo elemento $g \in \langle x \rangle$ pode ser escrito como $g = x^t$ para algum $t \in \mathbb{Z}$. Como f é um homomorfismo, segue do lema abaixo que:

$$f(x^t) = f(x)^t.$$

Portanto, $f(g) = f(x^t) = f(x)^t \in \langle f(x) \rangle$, o que mostra que $\varphi(g) \in \langle f(x) \rangle$, e assim φ está bem definida.

Injetividade de φ : Suponha $\varphi(g_1) = \varphi(g_2)$, ou seja, $f(g_1) = f(g_2)$. Como f é injetiva, segue que $g_1 = g_2$. Logo, φ é injetiva.

Sobrejetividade de φ : Seja $y \in \langle f(x) \rangle$. Então, existe $t \in \mathbb{Z}$ tal que $y = f(x)^t = f(x^t) = f(x^t) = \varphi(x^t)$, e $x^t \in \langle x \rangle$. Assim, $y \in \text{Im}(\varphi)$, e portanto φ é sobrejetiva.

Conclusão: Como $\varphi : \langle x \rangle \rightarrow \langle f(x) \rangle$ é bijetiva, os subgrupos têm a mesma cardinalidade. Assim,

$$\mathcal{O}(f(x)) = |\langle f(x) \rangle| = |\langle x \rangle| = \mathcal{O}(x),$$

como queríamos demonstrar. $\square$

1.8 ISOMORFISMOS DE GRUPOS

A essência do conceito de *isomorfismo* entre grupos tem como elemento principal a noção de que dois grupos são *a mesma estrutura* quando se pode estabelecer entre eles uma cor-

respondência que preserve integralmente a operação de grupo. Essa ideia é amplamente utilizada em diversas áreas da álgebra, como na teoria de anéis e espaços vetoriais, permitindo uma comparação entre estruturas aparentemente diferentes mas que essencialmente são indissociáveis quanto a operação.

Definição 1.8.1. *Sejam G e H dois grupos. Um isomorfismo de grupos entre G e H é um morfismo de grupos $f : G \rightarrow H$ tal que existe um morfismo de grupos $g : H \rightarrow G$ satisfazendo:*

$$g \circ f = id_G \quad e \quad f \circ g = id_H,$$

onde id_G e id_H são os morfismos identidade dos grupos G e H , respectivamente. Nesse caso, dizemos que G e H são isomorfos e escrevemos $G \cong H$.

Naturalmente, a existência de um isomorfismo entre dois grupos nos mostra que não existe distinção significativa entre eles no que se refere à estrutura de grupo. Ainda que os conjuntos subjacentes ou a origem dos elementos possam ser diferentes, a forma como esses elementos se comportam é perfeitamente conservada.

Proposição 1.8.2. *Um morfismo de grupos $f : G \rightarrow H$ é um isomorfismo se, e somente se, f é bijetora.*

Demonstração. ($\Rightarrow$) Suponha que $f : G \rightarrow H$ seja um isomorfismo. Então, por definição, existe um morfismo de grupos $g : H \rightarrow G$ tal que $g \circ f = id_G$ e $f \circ g = id_H$. Essas duas equações mostram que f é inversível com inversa g , ou seja, f é bijetora.

($\Leftarrow$) Suponha agora que $f : G \rightarrow H$ seja um morfismo de grupos bijetor. Então, a função f admite uma inversa de conjuntos $f^{-1} : H \rightarrow G$. Devemos mostrar que essa inversa $g := f^{-1}$ é também um morfismo de grupos.

Sejam $x, y \in H$. Como f é uma bijeção, existem $a, b \in G$ tais que $f(a) = x$ e $f(b) = y$. Então,

$$g(xy) = f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)f^{-1}(y) = g(x)g(y),$$

onde utilizamos o fato de que f preserva a operação do grupo e que f^{-1} reverte essa operação. Portanto, g também preserva a operação de grupo, o que implica que g é um morfismo de grupos.

Assim, f possui uma inversa que é também um morfismo de grupos, e portanto, f é um isomorfismo. $\square$

Teorema 1.8.3. *Sejam G e H grupos, $f : G \rightarrow H$ um homomorfismo de grupos, e $L \trianglelefteq G$ um subgrupo normal contido no núcleo de f , ou seja, $L \subseteq \ker(f)$. Então, existe um único homomorfismo de grupos*

$$\bar{f} : G/L \rightarrow H$$

tal que o diagrama abaixo comuta:

$$\begin{array}{ccc}
 G & \xrightarrow{f} & H \\
 \pi_L \downarrow & \nearrow \bar{f} & \\
 G/L & &
 \end{array}$$

Mais precisamente, $\bar{f} \circ \pi_L = f$, onde $\pi_L : G \rightarrow G/L$ é a projeção canônica que envia um elemento $x \in G$ para a sua classe $xL \in G/L$.

Demonstração. Definimos $\bar{f} : G/L \rightarrow H$ da seguinte forma: para cada classe $xL \in G/L$, tomamos

$$\bar{f}(xL) = f(x).$$

É necessário verificar que $\bar{f}$ está bem definida, ou seja, que a definição acima não depende do representante x da classe. Suponha que $xL = yL$, ou seja, $x^{-1}y \in L$. Como $L \subseteq \ker(f)$, então $f(x^{-1}y) = e_H$, e como f é um homomorfismo, isso implica

$$f(x^{-1})f(y) = e_H \Rightarrow f(x) = f(y).$$

Logo, $\bar{f}(xL) = f(x) = f(y) = \bar{f}(yL)$, e portanto $\bar{f}$ está bem definida.

Agora, mostramos que $\bar{f}$ é um homomorfismo. Sejam $xL, yL \in G/L$, então:

$$\bar{f}(xL \cdot yL) = \bar{f}((xy)L) = f(xy) = f(x)f(y) = \bar{f}(xL) \cdot \bar{f}(yL).$$

Assim, $\bar{f}$ preserva a operação de grupo e é, portanto, um homomorfismo.

Verifiquemos que o diagrama comuta:

$$(\bar{f} \circ \pi_L)(x) = \bar{f}(xL) = f(x), \quad \forall x \in G.$$

Logo, $\bar{f} \circ \pi_L = f$.

Por fim, mostramos a unicidade. Suponha que exista outro homomorfismo $g : G/L \rightarrow H$ tal que $g \circ \pi_L = f$. Então, para todo $x \in G$, temos:

$$g(xL) = (g \circ \pi_L)(x) = f(x) = \bar{f}(xL).$$

Portanto, $g = \bar{f}$, e a unicidade está demonstrada. □

Teorema 1.8.4 (Teorema do Isomorfismo para Grupos). *Sejam G e H grupos e seja $\varphi : G \rightarrow H$ um homomorfismo de grupos. Então, o núcleo de φ , denotado por $\ker(\varphi)$, é um subgrupo normal de G , e o grupo quociente $G/\ker(\varphi)$ é isomorfo à imagem de φ . Mais precisamente, existe um isomorfismo de grupos*

$$\bar{\varphi} : G/\ker(\varphi) \rightarrow \varphi(G)$$

tal que, para todo $x \in G$, tem-se

$$\bar{\varphi}([x]) = \varphi(x),$$

onde $[x]$ denota a classe lateral de x módulo $\ker(\varphi)$.

Demonstração. Como o núcleo de qualquer homomorfismo de grupos é um subgrupo normal, temos $\ker(\varphi) \trianglelefteq G$, o que garante que o quociente $G/\ker(\varphi)$ está bem definido como grupo.

Consideremos o mapeamento $\bar{\varphi} : G/\ker(\varphi) \rightarrow \varphi(G)$ definido por

$$\bar{\varphi}([x]) = \varphi(x).$$

Devemos verificar que essa aplicação é bem definida. De fato, se $[x] = [y]$, então $x^{-1}y \in \ker(\varphi)$, o que implica que $\varphi(x^{-1}y) = e_H$, ou seja, $\varphi(x)^{-1}\varphi(y) = e_H$, logo $\varphi(x) = \varphi(y)$. Portanto, $\bar{\varphi}$ é bem definida.

É imediato que $\bar{\varphi}$ é um homomorfismo de grupos, pois

$$\bar{\varphi}([x][y]) = \bar{\varphi}([xy]) = \varphi(xy) = \varphi(x)\varphi(y) = \bar{\varphi}([x])\bar{\varphi}([y]).$$

Mostremos que $\bar{\varphi}$ é sobrejetora. Como $\varphi(G)$ é, por definição, a imagem de φ , para todo $h \in \varphi(G)$, existe $x \in G$ tal que $\varphi(x) = h$, ou seja, $h = \bar{\varphi}([x])$, o que prova a sobrejetividade.

Por fim, resta mostrar que $\bar{\varphi}$ é injetora. Seja $[x] \in \ker(\bar{\varphi})$, ou seja,

$$\bar{\varphi}([x]) = \varphi(x) = e_H.$$

Então $x \in \ker(\varphi)$, o que implica que $[x] = [e_G]$. Assim, o núcleo de $\bar{\varphi}$ é trivial, e $\bar{\varphi}$ é injetora.

Portanto, $\bar{\varphi}$ é um isomorfismo de grupos entre $G/\ker(\varphi)$ e $\varphi(G)$. $\square$

Exemplo 1.8.5. Seja $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ o círculo unitário no plano complexo, munido da multiplicação usual de números complexos. Trata-se de um subgrupo de $\mathbb{C}^\times$, o grupo multiplicativo dos complexos não nulos. Nosso objetivo é demonstrar que

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

Para isso, consideremos o grupo aditivo dos números reais, $(\mathbb{R}, +)$, e o homomorfismo de grupos

$$\varphi : \mathbb{R} \longrightarrow S^1, \quad \varphi(t) = e^{2\pi it}.$$

Essa aplicação está bem definida, pois para todo $t \in \mathbb{R}$, o número complexo $e^{2\pi it}$ tem módulo 1, e portanto pertence a S^1 .

Verifiquemos que φ é um homomorfismo: dados $t, s \in \mathbb{R}$,

$$\varphi(t+s) = e^{2\pi i(t+s)} = e^{2\pi it} \cdot e^{2\pi is} = \varphi(t) \cdot \varphi(s),$$

mostrando que φ preserva a operação de grupo, isto é, é um homomorfismo de grupos de $(\mathbb{R}, +)$ em $(S^1, \cdot)$.

Além disso, φ é sobrejetora: dado $z \in S^1$, podemos escrever $z = \cos(\theta) + i \sin(\theta) = e^{i\theta}$, para algum $\theta \in \mathbb{R}$. Assim, basta tomar $t = \theta/(2\pi)$, de modo que $\varphi(t) = e^{2\pi it} = e^{i\theta} = z$. Logo, φ é sobrejetiva.

Vamos agora determinar o núcleo de φ . Observamos que:

$$t \in \ker(\varphi) \iff \varphi(t) = 1 \iff e^{2\pi it} = 1.$$

Como $e^{2\pi it} = 1$ se e somente se $2\pi it \in 2\pi i\mathbb{Z}$, segue que $t \in \mathbb{Z}$. Portanto, temos:

$$\ker(\varphi) = \mathbb{Z}.$$

Concluimos que φ é um homomorfismo sobrejetivo com núcleo $\mathbb{Z}$. Pelo Primeiro Teorema de Isomorfismo, temos então um isomorfismo de grupos:

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

GRUPO DE PERMUTAÇÃO

Neste capítulo trabalharemos com o grupo simétrico S_n , isto é, o conjunto de todas as permutações do conjunto $\{1, 2, \dots, n\}$ munido da operação de composição (ver Seção 1.2.1). As principais referências utilizadas são [8, 5, 7, 6, 1].

2.1 A NOTAÇÃO DE CICLOS

Definição 2.1.1. *Sejam $n \geq 2$ e $r \geq 2$. Uma permutação $\alpha \in S_n$ é chamada de r -ciclo se existem elementos $a_1, a_2, \dots, a_r \in \{1, 2, \dots, n\}$ dois a dois distintos tais que*

$$\alpha(a_i) = a_{i+1} \quad (i = 1, 2, \dots, r-1), \quad \alpha(a_r) = a_1,$$

e, além disso, $\alpha(j) = j$ para todo $j \in \{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_r\}$. Nesse caso, escrevemos

$$\alpha = (a_1 a_2 \cdots a_r).$$

Quando $r = 2$, o ciclo $(a_1 a_2)$ é chamado de transposição (ou 2-ciclo).

Exemplo 2.1.2. *O 2-ciclo (transposição) em S_4 : Considere $\alpha = (12)$. Aqui, $\alpha(1) = 2$, $\alpha(2) = 1$, e $\alpha(3) = 3$, $\alpha(4) = 4$. Isso significa que α troca os elementos 1 e 2, enquanto deixa 3 e 4 fixos.*

Exemplo 2.1.3. *O 3-ciclo em S_5 : Considere $\beta = (245)$. Aqui, $\beta(2) = 4$, $\beta(4) = 5$, $\beta(5) = 2$, e $\beta(1) = 1$, $\beta(3) = 3$. Isso significa que β cicla os elementos 2, 4 e 5, enquanto deixa 1 e 3 fixos.*

Esses exemplos ilustram como os ciclos funcionam, movendo alguns elementos e deixando outros inalterados.

Lema 2.1.4. *Seja $\alpha = (a_1 \dots a_r) \in S_n$ um r -ciclo. Então $\alpha^i(a_1) = a_{i+1}$, $\forall i \in \{1, \dots, r-1\}$.*

Demonstração. Seja $\alpha = (a_1 a_2 \dots a_r)$ um r -ciclo em S_n . Queremos mostrar que $\alpha^i(a_1) = a_{i+1}$ para todo $i \in \{1, \dots, r-1\}$. Vamos provar isso por indução em i .

Base da indução ($i = 1$): Para $i = 1$, temos $\alpha^1(a_1) = \alpha(a_1)$. Pela definição de α como um r -ciclo, sabemos que $\alpha(a_1) = a_2$. Portanto, $\alpha^1(a_1) = a_2$, o que verifica a base da indução.

Hipótese de indução: Suponha que, para algum $k \in \{1, \dots, r-2\}$, a afirmação seja válida, ou seja, $\alpha^k(a_1) = a_{k+1}$.

Passo indutivo ($i = k + 1$): Agora, vamos mostrar que a afirmação também é válida para $i = k + 1$. Temos:

$$\alpha^{k+1}(a_1) = \alpha(\alpha^k(a_1)).$$

Pela hipótese de indução, $\alpha^k(a_1) = a_{k+1}$. Portanto:

$$\alpha^{k+1}(a_1) = \alpha(a_{k+1}).$$

Pela definição de α como um r -ciclo, sabemos que $\alpha(a_{k+1}) = a_{k+2}$, desde que $k + 1 \leq r - 1$. Assim:

$$\alpha^{k+1}(a_1) = a_{k+2}.$$

Isso completa o passo indutivo.

Pelo princípio da indução matemática, concluímos que $\alpha^i(a_1) = a_{i+1}$ para todo $i \in \{1, \dots, r - 1\}$. □

Proposição 2.1.5. *Se $\alpha \in S_n$ é um r -ciclo então $\mathcal{O}(\alpha) = r$.*

Demonstração. Seja $\alpha = (a_1 a_2 \dots a_r)$ um r -ciclo em S_n . Queremos mostrar que a ordem de α , denotada por $\mathcal{O}(\alpha)$, é igual a r , ou seja, $\mathcal{O}(\alpha) = r$. A ordem de α é o menor inteiro positivo k tal que $\alpha^k = \text{id}$, onde id é a permutação identidade.

Primeiro, considere a ação de α sobre os elementos $a_1, a_2, \dots, a_r$. Pela definição de α como um r -ciclo, temos $\alpha(a_i) = a_{i+1}$ para $i \in \{1, \dots, r - 1\}$ e $\alpha(a_r) = a_1$. Além disso, $\alpha(j) = j$ para todo $j \in \{1, \dots, n\} \setminus \{a_1, \dots, a_r\}$. Vamos aplicar α repetidamente a um elemento a_1 . Pela proposição anterior, temos $\alpha^i(a_1) = a_{i+1}$ para $i \in \{1, \dots, r - 1\}$. Em particular, $\alpha^{r-1}(a_1) = a_r$. Aplicando α mais uma vez, obtemos $\alpha^r(a_1) = \alpha(a_r) = a_1$. Para os outros elementos $a_2, \dots, a_r$, Utilizando indução finita, obtemos $\alpha^r(a_i) = a_i$, $\forall i \in \{1, 2, \dots, n\}$. Portanto, $\alpha^r = \text{id}$.

Agora, vamos mostrar que $\alpha^k \neq \text{id}$ para $k \in \{1, \dots, r - 1\}$. Suponha, por contradição, que exista $k \in \{1, \dots, r - 1\}$ tal que $\alpha^k = \text{id}$. Então, $\alpha^k(a_1) = a_1$. No entanto, pela proposição anterior, $\alpha^k(a_1) = a_{k+1}$. Como $k + 1 \leq r$, temos $a_{k+1} \neq a_1$, a menos que $k + 1 = r + 1$, o que não é possível pois $k \leq r - 1$. Portanto, $\alpha^k \neq \text{id}$ para $k \in \{1, \dots, r - 1\}$.

Concluímos que $\mathcal{O}(\alpha) = r$, pois $\alpha^r = \text{id}$ e $\alpha^k \neq \text{id}$ para $k \in \{1, \dots, r - 1\}$. □

Definição 2.1.6. *Sejam $\alpha, \beta \in S_n$ ciclos. Dizemos que α e β são ciclos disjuntos se para todo $j \in \{1, \dots, n\}$ tem-se que $\alpha(j) = j$ ou $\beta(j) = j$.*

Proposição 2.1.7. *Sejam $\alpha, \beta \in S_n$ ciclos disjuntos. Então $\alpha\beta = \beta\alpha$.*

Demonstração. Sejam α e β ciclos disjuntos em S_n . Isso significa que os conjuntos de elementos movidos por α e β são disjuntos. Vamos mostrar que $\alpha\beta = \beta\alpha$.

Considere um elemento $x \in \{1, 2, \dots, n\}$. Se x não é movido por α nem por β . Neste caso, $\alpha(x) = x$ e $\beta(x) = x$. Portanto, $\alpha\beta(x) = \alpha(x) = x$ e $\beta\alpha(x) = \beta(x) = x$. Logo, $\alpha\beta(x) = \beta\alpha(x)$. Se x é movido por α mas não por β . Neste caso, $\alpha(x) \neq x$ e $\beta(x) = x$. Como α e β são disjuntos, $\alpha(x)$ não é movido por β , ou seja, $\beta(\alpha(x)) = \alpha(x)$. Portanto, $\alpha\beta(x) = \alpha(x)$ e $\beta\alpha(x) = \beta(\alpha(x)) = \alpha(x)$. Logo, $\alpha\beta(x) = \beta\alpha(x)$. Se x é movido por β mas não por α . Este caso é análogo ao Caso 2. Temos $\beta(x) \neq x$ e $\alpha(x) = x$. Como α e β são disjuntos, $\beta(x)$ não é movido por α , ou seja, $\alpha(\beta(x)) = \beta(x)$. Portanto, $\alpha\beta(x) = \alpha(\beta(x)) = \beta(x)$ e $\beta\alpha(x) = \beta(x)$. Logo, $\alpha\beta(x) = \beta\alpha(x)$.

Como $\alpha\beta(x) = \beta\alpha(x)$ para todo $x \in \{1, 2, \dots, n\}$, concluímos que $\alpha\beta = \beta\alpha$.

□

Proposição 2.1.8. *Sejam $\alpha_1, \dots, \alpha_t \in S_n$ ciclos dois a dois disjuntos de comprimentos $r_1, \dots, r_t$, respectivamente. Então $\mathcal{O}(\alpha_1 \cdots \alpha_t) = \text{mmc}(r_1, \dots, r_t) = \text{mmc}(\mathcal{O}(\alpha_1), \dots, \mathcal{O}(\alpha_t))$.*

Demonstração. Sejam $\alpha_1, \dots, \alpha_t \in S_n$ ciclos dois a dois disjuntos de comprimentos $r_1, \dots, r_t$, respectivamente. Queremos mostrar que a ordem do produto $\alpha_1 \cdots \alpha_t$ é igual ao mínimo múltiplo comum (mmc) dos comprimentos $r_1, \dots, r_t$, ou seja, $\mathcal{O}(\alpha_1 \cdots \alpha_t) = \text{mmc}(r_1, \dots, r_t)$. Como a ordem de cada ciclo α_i é $\mathcal{O}(\alpha_i) = r_i$, isso também pode ser escrito como $\mathcal{O}(\alpha_1 \cdots \alpha_t) = \text{mmc}(\mathcal{O}(\alpha_1), \dots, \mathcal{O}(\alpha_t))$.

Primeiro, observe que, como os ciclos $\alpha_1, \dots, \alpha_t$ são disjuntos, eles comutam entre si, ou seja, $\alpha_i \alpha_j = \alpha_j \alpha_i$ para quaisquer $i, j \in \{1, \dots, t\}$. Isso implica que, para qualquer inteiro $k \geq 1$, temos $(\alpha_1 \cdots \alpha_t)^k = \alpha_1^k \cdots \alpha_t^k$.

Agora, seja $m = \text{mmc}(r_1, \dots, r_t)$. Queremos mostrar que m é a ordem de $\alpha_1 \cdots \alpha_t$. Para isso, precisamos mostrar que $(\alpha_1 \cdots \alpha_t)^m = \text{id}$ e que m é o menor inteiro positivo com essa propriedade.

Vamos mostrar que $(\alpha_1 \cdots \alpha_t)^m = \text{id}$. Como m é o mmc de $r_1, \dots, r_t$, temos que m é múltiplo de cada r_i . Portanto, $\alpha_i^m = \text{id}$ para cada $i \in \{1, \dots, t\}$, pois $\mathcal{O}(\alpha_i) = r_i$. Assim, $(\alpha_1 \cdots \alpha_t)^m = \alpha_1^m \cdots \alpha_t^m = \text{id} \cdots \text{id} = \text{id}$.

Vamos mostrar que m é o menor inteiro positivo com essa propriedade. Suponha que exista um inteiro positivo $k < m$ tal que $(\alpha_1 \cdots \alpha_t)^k = \text{id}$. Então, $\alpha_1^k \cdots \alpha_t^k = \text{id}$. Como os ciclos são disjuntos, isso implica que $\alpha_i^k = \text{id}$ para cada $i \in \{1, \dots, t\}$. Portanto, k deve ser múltiplo de cada r_i , ou seja, k é um múltiplo comum de $r_1, \dots, r_t$. No entanto, como $k < m$ e m é o mmc de $r_1, \dots, r_t$, isso é uma contradição. Logo, m é o menor inteiro positivo tal que $(\alpha_1 \cdots \alpha_t)^m = \text{id}$.

Concluímos que $\mathcal{O}(\alpha_1 \cdots \alpha_t) = \text{mmc}(r_1, \dots, r_t) = \text{mmc}(\mathcal{O}(\alpha_1), \dots, \mathcal{O}(\alpha_t))$. □ □

2.2 DECOMPOSIÇÃO DE UMA PERMUTAÇÃO EM CICLOS DISJUNTOS

Considere a permutação $\tau \in S_8$ dada, na notação de ciclos disjuntos, por

$$\tau = (1 \ 3 \ 5)(2 \ 4)(6 \ 7 \ 8). \quad (1)$$

Essa escrita já explicita a dinâmica da ação de τ : no ciclo $(1\ 3\ 5)$, por exemplo, tem-se $1 \mapsto 3$, $3 \mapsto 5$ e $5 \mapsto 1$. De modo análogo, $(2\ 4)$ determina a transposição $2 \mapsto 4$ e $4 \mapsto 2$, enquanto $(6\ 7\ 8)$ descreve o deslocamento cíclico $6 \mapsto 7$, $7 \mapsto 8$ e $8 \mapsto 6$.

Uma forma equivalente de codificar essas imagens é a notação matricial

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 2 & 1 & 7 & 8 & 6 \end{pmatrix}. \quad (2)$$

De fato, ao ler a segunda linha como a lista das imagens dos elementos da primeira, recupera-se imediatamente o comportamento imposto pelos ciclos: 1 é enviado em 3, 3 em 5, 5 em 1; do mesmo modo, 2 e 4 permutam-se, e o bloco $\{6, 7, 8\}$ gira segundo $6 \mapsto 7 \mapsto 8 \mapsto 6$. Evidencia-se, portanto, que as duas representações são consistentes e descrevem a mesma permutação.

Vale notar que os ciclos são disjuntos no sentido estrito: não há sobreposição de suportes. Essa independência permite articular a decomposição como um produto de componentes que atuam em subconjuntos distintos, de modo que a ordem dos fatores não altera a transformação global. É precisamente esse tipo de decomposição que será formalizado a seguir, quando se estabelece a unicidade da escrita em ciclos disjuntos, salvo reordenações e a escolha do ponto de partida em cada ciclo. Omitiremos a demonstração que pode ser encontrada em [6]

Teorema 2.2.1. *Toda permutação $\sigma \in S_n$ admite uma decomposição como produto de ciclos dois a dois disjuntos. Além disso, essa decomposição é única, a menos da ordem dos ciclos e de rotações dentro de cada ciclo.*

Lema 2.2.2. *Dados $n, r \in \mathbb{N}$, com $r \geq 2$, e elementos $a_1, \dots, a_r \in \{1, \dots, n\}$ distintos dois a dois, o ciclo $(a_1\ a_2\ \dots\ a_r)$ pode ser expresso como um produto de transposições da forma:*

$$(a_1\ a_2\ \dots\ a_r) = (a_1\ a_r)(a_1\ a_{r-1}) \cdots (a_1\ a_2).$$

Demonstração. Vamos analisar a ação de ambos os lados da igualdade sobre um elemento $x \in \{1, \dots, n\}$. Consideraremos dois casos: $x \notin \{a_1, \dots, a_r\}$ e $x \in \{a_1, \dots, a_r\}$. Suponha que $x \notin \{a_1, \dots, a_r\}$. Se x não pertence ao conjunto $\{a_1, \dots, a_r\}$, então x é um ponto fixo tanto do ciclo $(a_1\ a_2\ \dots\ a_r)$ quanto de cada transposição $(a_1\ a_i)$. Portanto, a ação do ciclo e do produto de transposições sobre x é a identidade:

$$(a_1\ a_2\ \dots\ a_r)(x) = x \quad \text{e} \quad (a_1\ a_r)(a_1\ a_{r-1}) \cdots (a_1\ a_2)(x) = x.$$

Assim, ambos os lados da igualdade coincidem para $x \notin \{a_1, \dots, a_r\}$. Suponhamos que $x \in \{a_1, \dots, a_r\}$. Agora, analisaremos a ação sobre os elementos $a_1, \dots, a_r$. Para

isso, consideremos cada elemento a_i separadamente. Começemos com $x = a_1$. Aplicando o ciclo $(a_1 a_2 \dots a_r)$ sobre a_1 , temos:

$$(a_1 a_2 \dots a_r)(a_1) = a_2.$$

Agora, aplicando o produto de transposições $(a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_2)$ sobre a_1 : A primeira transposição $(a_1 a_2)$ leva a_1 para a_2 , as transposições subsequentes $(a_1 a_3) \dots (a_1 a_r)$ não afetam a_2 , pois $a_2 \neq a_1$. Portanto, o produto de transposições também leva a_1 para a_2 :

$$(a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_2)(a_1) = a_2.$$

Suponhamos que $x = a_2$. Aplicando o ciclo $(a_1 a_2 \dots a_r)$ sobre a_2 , temos:

$$(a_1 a_2 \dots a_r)(a_2) = a_3.$$

Agora, aplicando o produto de transposições sobre a_2 : A primeira transposição $(a_1 a_2)$ leva a_2 para a_1 , a segunda transposição $(a_1 a_3)$ leva a_1 para a_3 , as transposições subsequentes $(a_1 a_4) \dots (a_1 a_r)$ não afetam a_3 . Portanto, o produto de transposições leva a_2 para a_3 :

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

Suponha que $x = a_i$ para $3 \leq i \leq r-1$. Para $x = a_i$ com $3 \leq i \leq r-1$, aplicando o ciclo $(a_1 a_2 \dots a_r)$, temos:

$$(a_1 a_2 \dots a_r)(a_i) = a_{i+1}.$$

Agora, aplicando o produto de transposições sobre a_i : As transposições $(a_1 a_2) \dots (a_1 a_{i-1})$ não afetam a_i , pois $a_i \neq a_1$, a transposição $(a_1 a_i)$ leva a_i para a_1 , a transposição $(a_1 a_{i+1})$ leva a_1 para a_{i+1} , as transposições subsequentes $(a_1 a_{i+2}) \dots (a_1 a_r)$ não afetam a_{i+1} . Portanto, o produto de transposições leva a_i para a_{i+1} :

$$(a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_2)(a_i) = a_{i+1}.$$

Considere $x = a_r$. Finalmente, para $x = a_r$, aplicando o ciclo $(a_1 a_2 \dots a_r)$, temos:

$$(a_1 a_2 \dots a_r)(a_r) = a_1.$$

Agora, aplicando o produto de transposições sobre a_r : As transposições $(a_1 a_2) \dots (a_1 a_{r-1})$ não afetam a_r , a última transposição $(a_1 a_r)$ leva a_r para a_1 . Portanto, o produto de transposições leva a_r para a_1 :

$$(a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_2)(a_r) = a_1.$$

Assim, em todos os casos, a ação do ciclo $(a_1 a_2 \dots a_r)$ coincide com a ação do produto de transposições $(a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_2)$. Portanto, concluímos que:

$$(a_1 a_2 \dots a_r) = (a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_2)$$

como afirmado no lema. $\square$

Proposição 2.2.3. *Se $n \in \mathbb{N}$ então $S_n = \langle \{\text{transposições}\} \rangle$.*

Demonstração. Para demonstrar que $S_n = \langle \{\text{transposições}\} \rangle$, ou seja, que o grupo simétrico S_n é gerado por transposições, usemos o lema anterior. Sabemos que toda permutação em S_n pode ser escrita como um produto de ciclos disjuntos (pela decomposição em ciclos). Pelo lema, cada ciclo $(a_1, a_2, \dots, a_r)$ pode ser expresso como um produto de transposições: $(a_1, a_2, \dots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_2)$. Como toda permutação é um produto de ciclos e cada ciclo é um produto de transposições, segue que toda permutação em S_n pode ser escrita como um produto de transposições. Portanto, S_n é gerado por transposições, ou seja, $S_n = \langle \{\text{transposições}\} \rangle$. $\square$

Lema 2.2.4. *Sejam $n \in \mathbb{N}$ e $a, b \in \{1, 2, \dots, n\}$, $a \neq b$. Então $(a b) = (1 a)(1 b)(1 a)$.*

Demonstração. Para demonstrar que $(a b) = (1 a)(1 b)(1 a)$, onde $a, b \in \{1, 2, \dots, n\}$ com $a \neq b$, verificamos a ação de ambos os lados da igualdade em cada elemento de $\{1, 2, \dots, n\}$. Primeiro, a transposição $(a b)$ troca a e b e deixa os demais elementos fixos. Agora, aplicamos $(1 a)(1 b)(1 a)$: se $x = 1$, $(1 a)$ leva 1 para a , $(1 b)$ deixa a fixo, e $(1 a)$ leva a de volta para 1. Se $x = a$, $(1 a)$ leva a para 1, $(1 b)$ leva 1 para b , e $(1 a)$ deixa b fixo. Se $x = b$, $(1 a)$ deixa b fixo, $(1 b)$ leva b para 1, e $(1 a)$ leva 1 para a . Para $x \neq 1, a, b$, ambos os lados deixam x fixo. Portanto, $(a b) = (1 a)(1 b)(1 a)$. $\square$

Proposição 2.2.5. *Se $n \in \mathbb{N}$, então $S_n = \langle (1 2), \dots, (1 n) \rangle$.*

Demonstração. Já sabemos que $S_n = \langle \text{2-ciclos} \rangle$. Para mostrar que $S_n = \langle (1 2), \dots, (1 n) \rangle$, basta provar que $\langle \text{2-ciclos} \rangle \subseteq \langle (1 2), \dots, (1 n) \rangle$. Seja $\tau \in S_n$ um 2-ciclo, escrito como $\tau = (a b)$, com $a, b \in \{1, \dots, n\}$ e $a \neq b$. Se $a = 1$, então $\tau = (1 b) \in \langle (1 2), \dots, (1 n) \rangle$. Se $b = 1$, então $\tau = (a 1) = (1 a) \in \langle (1 2), \dots, (1 n) \rangle$. Se $a \neq 1$ e $b \neq 1$, pelo lema anterior, $\tau = (a b) = (1 a)(1 b)(1 a) \in \langle (1 2), \dots, (1 n) \rangle$. Portanto, $\langle \text{2-ciclos} \rangle \subseteq \langle (1 2), \dots, (1 n) \rangle$, e como $S_n = \langle \text{2-ciclos} \rangle$, segue que $S_n = \langle (1 2), \dots, (1 n) \rangle$. $\square$

Lema 2.2.6. *Se $n \in \mathbb{N}$ e $a \in \{1, \dots, n-1\}$, então $(1 a+1) = (1 a)(a a+1)(1 a)$.*

Demonstração. Seja $x \notin \{1, a, a+1\}$. Temos que

$$(1 a+1)(x) = x = (1 a)(a a+1)(1 a)(x),$$

pois todas as transposições deixam x fixo. Para $x = 1$, temos

$$(1 a)(a a+1)(1 a)(1) = (1 a)(a a+1)(a) = (1 a)(a+1) = a+1 = (1 a+1)(1).$$

Para $x = a$, temos

$$(1\ a)(a\ a+1)(1\ a)(a) = (1\ a)(a\ a+1)(1) = (1\ a)(1) = a = (1\ a+1)(a).$$

Portanto,

$$(1\ a+1) = (1\ a)(a\ a+1)(1\ a)$$

para todos os casos. $\square$

Proposição 2.2.7. *Se $n \in \mathbb{N}$, então $S_n = \langle (1\ 2), (2\ 3), \dots, (n-1\ n) \rangle$.*

Demonstração. Sabemos que $S_n = \langle (1\ 2), \dots, (1\ n) \rangle$, ou seja, o grupo simétrico S_n é gerado pelas transposições $(1\ 2), (1\ 3), \dots, (1\ n)$. Para mostrar que $S_n = \langle (1\ 2), (2\ 3), \dots, (n-1\ n) \rangle$, basta provar que todas as transposições $(1\ j)$ (para $j \in \{2, \dots, n\}$) podem ser geradas pelo conjunto $X = \{(1\ 2), (2\ 3), \dots, (n-1\ n)\}$. Faremos isso por indução sobre j .

Caso base ($j = 2$): Para $j = 2$, a transposição $(1\ 2)$ já pertence ao conjunto X . Portanto, $(1\ 2) \in \langle X \rangle$.

Hipótese indutiva: Suponha que, para algum j tal que $2 \leq j < n$, a transposição $(1\ j-1)$ pertença a $\langle X \rangle$, ou seja, $(1\ j-1)$ pode ser escrita como um produto de elementos de X .

Passo indutivo (j): Queremos mostrar que $(1\ j) \in \langle X \rangle$. Para isso, observe que:

$$(1\ j) = (1\ j-1) \cdot (j-1\ j) \cdot (1\ j-1).$$

Pela hipótese indutiva, $(1\ j-1) \in \langle X \rangle$.

Além disso, $(j-1\ j) \in X$, pois X contém todas as transposições da forma $(k\ k+1)$ para $k \in \{1, \dots, n-1\}$.

Portanto, $(1\ j)$ é um produto de elementos de $\langle X \rangle$, o que implica $(1\ j) \in \langle X \rangle$.

Pelo princípio da indução, $(1\ j) \in \langle X \rangle$ para todo $j \in \{2, \dots, n\}$. Como $S_n = \langle (1\ 2), \dots, (1\ n) \rangle$, segue que:

$$\langle (1\ 2), \dots, (1\ n) \rangle \subseteq \langle X \rangle.$$

Por outro lado, como $X \subseteq S_n$, temos:

$$\langle X \rangle \subseteq S_n.$$

Portanto, concluímos que:

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

$\square$

Lema 2.2.8. *Se $\sigma \in S_n$ é um n -ciclo então $\sigma(x) \neq x, \forall x \in \{1, \dots, n\}$.*

Demonstração. Por hipótese, seja $\sigma = (a_1 a_2 \dots a_n)$ um n -ciclo em S_n . Então, para cada $a_i \in \{1, \dots, n\}$, temos $\sigma(a_i) = a_{i+1}$ (com $a_{n+1} = a_1$). Como os elementos $\{a_1, \dots, a_n\}$ são todos distintos e σ é um ciclo de comprimento n , segue que $\sigma(a_i) \neq a_i$ para todo $i \in \{1, \dots, n\}$. Portanto, $\sigma(x) \neq x$ para todo $x \in \{1, \dots, n\}$. $\square$

Proposição 2.2.9. *Se $t \in \mathbb{N}$ e $\sigma_1, \sigma_2, \dots, \sigma_t \in S_n$ são n -ciclos dois a dois disjuntos, então $t = 1$.*

Demonstração. Suponha por absurdo que $t \geq 2$. Como $1 \in \{1, 2, \dots, n\}$ e σ_1 e σ_2 são ciclos disjuntos, então $\sigma_1(1) = 1$ ou $\sigma_2(1) = 1$. Por outro lado, como $\sigma_1, \sigma_2 \in S_n$ são n -ciclos então pelo lema anterior $\sigma_1(1) \neq 1$ e $\sigma_2(1) \neq 1$, absurdo. Portanto, $t = 1$. $\square$

Exemplo 2.2.10. *Sejam $p \in \mathbb{N}$ um número primo e $n \in \mathbb{N}$.*

- a) *Se $\sigma \in S_p$ e $\mathcal{O}(\sigma) = p$, então σ é um p -ciclo;*
- b) *Se $\tau \in S_p$, então $\mathcal{O}(\tau) \neq kp, \forall k \in \mathbb{Z}, k \geq 2$.*
- c) *Seja $t \in \mathbb{N}$. Então: S_n admite um elemento de ordem $p^t \iff p^t \leq n$.*

Demonstração. (a) Seja $p \in \mathbb{N}$ um número primo e considere $\sigma \in S_p$ tal que $\mathcal{O}(\sigma) = p$. Então, σ é necessariamente um p -ciclo.

Pelo Teorema da Decomposição em ciclos disjuntos 2.2.1, podemos escrever

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_t,$$

onde cada σ_i é um ciclo de comprimento $r_i \geq 2$ e os ciclos são dois a dois disjuntos. Além disso, a ordem de σ é dada por

$$\mathcal{O}(\sigma) = \text{mmc}(r_1, r_2, \dots, r_t).$$

Como $\mathcal{O}(\sigma) = p$ e p é primo, segue que cada r_i divide p , de modo que $r_i \in \{1, p\}$. No entanto, pela construção da decomposição, cada $r_i \geq 2$, logo $r_i = p$ para todo i .

Assim, todos os ciclos $\sigma_1, \dots, \sigma_t$ são p -ciclos dois a dois disjuntos. Ora, dois p -ciclos disjuntos em S_p exigiriam pelo menos $2p$ elementos distintos, o que é impossível, pois S_p atua apenas sobre p elementos. Portanto, deve-se ter $t = 1$.

Concluimos que σ é exatamente um p -ciclo, como queríamos demonstrar.

(b) Sejam $p \in \mathbb{N}$ um número primo e $\tau \in S_p$. Então,

$$\mathcal{O}(\tau) \neq kp, \quad \forall k \in \mathbb{Z}, k \geq 2.$$

Suponha, por contradição, que $\mathcal{O}(\tau) = kp$ para algum $k \geq 2$. Pelo Teorema da Decomposição em ciclos disjuntos, escrevemos

$$\tau = \tau_1 \tau_2 \cdots \tau_t,$$

onde cada τ_i é um ciclo de comprimento $r_i \geq 2$ e os τ_i são dois a dois disjuntos. Assim,

$$\mathcal{O}(\tau) = \text{mmc}(r_1, r_2, \dots, r_t).$$

Logo, cada r_i divide kp .

Por hipótese, $\mathcal{O}(\tau) = kp$, de modo que

$$\mathcal{O}(\tau^k) = \frac{\mathcal{O}(\tau)}{\text{mdc}(\mathcal{O}(\tau), k)} = \frac{kp}{k} = p.$$

Portanto, $\tau^k \in S_p$ tem ordem p . Pelo Item A, isso implica que τ^k é um p -ciclo.

Em particular, τ^k não fixa nenhum elemento do conjunto $\{1, 2, \dots, p\}$, pois um p -ciclo atua ciclicamente em todos os p elementos.

Agora, suponha que exista algum j tal que $r_j < p$. Como $r_j \geq 2$ e $r_j \mid kp$, segue que $\text{mdc}(r_j, p) = 1$, já que p é primo. Consequentemente, $r_j \mid k$.

Isso implica que $\tau_j^k = \text{id}$, isto é, τ_j^k fixa todo elemento do suporte de τ_j .

Contudo, os demais ciclos τ_ℓ ($\ell \neq j$) são disjuntos de τ_j e, portanto, fixam cada ponto do suporte de τ_j . Assim, τ^k fixaria os pontos de τ_j , o que contradiz o fato de que τ^k é um p -ciclo.

Portanto, não é possível que exista $r_j < p$. Concluimos que $r_i = p$ para todo $i = 1, \dots, t$.

Assim, τ é produto de p -ciclos dois a dois disjuntos. No entanto, em S_p não podem existir dois p -ciclos disjuntos, pois isso exigiria ao menos $2p$ elementos distintos. Portanto, $t = 1$, e τ é um único p -ciclo, de ordem p .

Logo, $\mathcal{O}(\tau) = p$, e a suposição inicial de que $\mathcal{O}(\tau) = kp$ com $k \geq 2$ leva a contradição.

(c) Sejam $p \in \mathbb{N}$ um número primo, $n \in \mathbb{N}$ e $t \in \mathbb{N}$. Então,

$$S_n \text{ admite um elemento de ordem } p^t \iff p^t \leq n.$$

($\Rightarrow$) Suponha que exista $\tau \in S_n$ tal que $\mathcal{O}(\tau) = p^t$. Pelo Teorema da Decomposição em ciclos disjuntos 2.2.1, podemos escrever

$$\tau = \tau_1 \tau_2 \cdots \tau_s,$$

onde cada τ_i é um ciclo de comprimento $r_i \geq 2$, dois a dois disjuntos. Nesse caso, a ordem de τ é

$$\mathcal{O}(\tau) = \text{mmc}(r_1, r_2, \dots, r_s).$$

Como $\mathcal{O}(\tau) = p^t$, segue que cada r_i é um divisor de p^t . Portanto, necessariamente $r_i = p^{t_i}$ para algum $t_i \in \mathbb{N}$ com $t_i \geq 1$.

Além disso,

$$p^t = \text{mmc}(p^{t_1}, p^{t_2}, \dots, p^{t_s}) = p^{\max\{t_1, \dots, t_s\}}.$$

Logo, existe algum índice j tal que $t = t_j$ e, portanto, $r_j = p^t$.

Como r_j é o comprimento do ciclo τ_j , e todo ciclo em S_n tem comprimento no máximo n , obtemos

$$p^t = r_j \leq n.$$

($\Leftarrow$) Reciprocamente, suponha que $p^t \leq n$. Considere o ciclo

$$\sigma = (1 \ 2 \ \cdots \ p^t) \in S_n.$$

Este é um p^t -ciclo, e portanto sua ordem é exatamente p^t . Assim, S_n contém um elemento de ordem p^t .

Concluimos que S_n admite um elemento de ordem p^t se, e somente se, $p^t \leq n$. $\square$

2.3 PERMUTAÇÕES PARES E ÍMPARES

Um aspecto fundamental no estudo das permutações é a noção de *paridade*, isto é, a classificação de uma permutação como *par* ou *ímpar*. Essa distinção será feita a partir da ação das permutações sobre um polinômio especial, conhecido como *polinômio de Vandermonde*.

Definição 2.3.1. *Seja $n \in \mathbb{N}$ e considere o polinômio em n variáveis*

$$V(X_1, X_2, \dots, X_n) = \prod_{1 \leq i < j \leq n} (X_j - X_i).$$

Chamamos V de polinômio de Vandermonde.

Note que V é produto de todas as diferenças possíveis $X_j - X_i$, com $j > i$, de modo que cada fator sempre tem o índice maior à esquerda.

Dada uma permutação $\sigma \in S_n$, definimos a sua ação em V substituindo cada variável X_i por $X_{\sigma(i)}$, ou seja:

$$\sigma \cdot V(X_1, \dots, X_n) = \prod_{1 \leq i < j \leq n} (X_{\sigma(j)} - X_{\sigma(i)}).$$

Observação 2.3.2. *Fixe $n \in \mathbb{N}$ e*

$$g := \prod_{1 \leq i < j \leq n} (X_j - X_i) \in \mathbb{Z}[X_1, \dots, X_n].$$

Se $\alpha \in S_n$, então

$$\hat{\alpha}(g) = \prod_{1 \leq i < j \leq n} (X_{\alpha(j)} - X_{\alpha(i)})$$

satisfaz

$$\hat{\alpha}(g) = g \quad \text{ou} \quad \hat{\alpha}(g) = -g.$$

Demonstração. Seja $\alpha \in S_n$. Por definição,

$$\hat{\alpha}(g) = \prod_{1 \leq i < j \leq n} (X_{\alpha(j)} - X_{\alpha(i)}).$$

Observe que cada termo $X_{\alpha(j)} - X_{\alpha(i)}$ corresponde a um único fator de g , possivelmente com a ordem invertida. Se $\alpha(j) > \alpha(i)$, então $X_{\alpha(j)} - X_{\alpha(i)} = X_k - X_l$ com $k > l$, que é um termo de g . Caso contrário, se $\alpha(j) < \alpha(i)$, então

$$X_{\alpha(j)} - X_{\alpha(i)} = -(X_{\alpha(i)} - X_{\alpha(j)}),$$

e $X_{\alpha(i)} - X_{\alpha(j)}$ é um termo de g (pois $\alpha(i) > \alpha(j)$). Assim, cada fator de $\hat{\alpha}(g)$ é igual a um fator de g ou a seu simétrico.

O número de inversões de ordem é exatamente o número de pares (i, j) com $i < j$ e $\alpha(j) < \alpha(i)$, denotado por $\psi(\alpha)$. Cada inversão contribui com um fator -1 . Portanto,

$$\hat{\alpha}(g) = (-1)^{\psi(\alpha)} \prod_{1 \leq i < j \leq n} (X_j - X_i) = (-1)^{\psi(\alpha)} g.$$

Como $(-1)^{\psi(\alpha)} \in \{1, -1\}$, segue que

$$\hat{\alpha}(g) = g \quad \text{ou} \quad \hat{\alpha}(g) = -g,$$

conforme $\psi(\alpha)$ seja par ou ímpar, respectivamente. □

Exemplo 2.3.3. Considere a transposição $\sigma = (1 \ 2) \in S_3$, que em notação de matriz é :

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

Aplicando σ $g = (X_3 - X_1)(X_2 - X_1)(X_3 - X_2)$, obtemos:

$$\hat{\sigma}(g) = (X_3 - X_2)(X_1 - X_2)(X_3 - X_1).$$

Observe que:

$$\hat{\sigma}(g) = (X_3 - X_2)(X_1 - X_2)(X_3 - X_1).$$

Comparando com g , notemos que:

$$\hat{\sigma}(g) = (-1)^2 \cdot (X_2 - X_3)(X_2 - X_1)(X_3 - X_1),$$

mas, rearranjando os fatores para coincidir com a ordem de g :

$$\hat{\sigma}(g) = (X_3 - X_1)(X_2 - X_1)(X_3 - X_2) \cdot (-1) = -g.$$

Portanto, diremos que σ é uma permutação ímpar pois o rearranjo nos forneceu a mesma ordem de g com o sinal negativo.

Definição 2.3.4. Dizemos que $\alpha \in S_n$ é uma permutação par se

$$\hat{\alpha}(g) = \prod_{1 \leq i < j \leq n} (X_{\alpha(j)} - X_{\alpha(i)}) = \prod_{1 \leq i < j \leq n} (X_j - X_i)$$

Definição 2.3.5. Dizemos que $\alpha \in S_n$ é ímpar se

$$\hat{\alpha}(g) = \prod_{1 \leq i < j \leq n} (X_{\alpha(j)} - X_{\alpha(i)}) = (-1) \cdot \prod_{1 \leq i < j \leq n} (X_j - X_i).$$

Defina $\psi : S_n \rightarrow \{-1, 1\}$ dada por

$$\psi(\alpha) := \begin{cases} 1, & \text{se } \alpha \text{ é par,} \\ -1, & \text{se } \alpha \text{ é ímpar.} \end{cases}$$

2.4 O GRUPO ALTERNADO

Proposição 2.4.1. A função $\psi : S_n \rightarrow \{-1, 1\}$ definida por

$$\psi(\alpha) = \begin{cases} 1, & \text{se } \alpha \text{ é par,} \\ -1, & \text{se } \alpha \text{ é ímpar,} \end{cases}$$

é um homomorfismo de grupos. Em particular, o conjunto

$$A_n := \ker \psi = \{\alpha \in S_n \mid \psi(\alpha) = 1\} = \{\alpha \in S_n \mid \alpha \text{ é par}\}$$

é um subgrupo normal de S_n .

Demonstração. Seja $g = \prod_{1 \leq i < j \leq n} (X_i - X_j)$ o polinômio de Vandermonde. Para qualquer $\alpha \in S_n$, a ação de α sobre g é dada por:

$$\hat{\alpha}(g) = \prod_{1 \leq i < j \leq n} (X_{\alpha(i)} - X_{\alpha(j)}) = \psi(\alpha) \cdot g.$$

Agora, considere $\alpha, \beta \in S_n$. Queremos mostrar que $\psi(\alpha\beta) = \psi(\alpha) \cdot \psi(\beta)$. Observe que:

$$\hat{\beta}(g) = \prod_{1 \leq i < j \leq n} (X_{\beta(j)} - X_{\beta(i)}) = \psi(\beta) \cdot \prod_{1 \leq i < j \leq n} (X_j - X_i)$$

Além disso:

$$\widehat{\alpha\beta}(g) = \prod_{1 \leq i < j \leq n} (X_{\alpha(\beta(j))} - X_{\alpha(\beta(i))}) = \hat{\alpha} \left(\psi(\beta) \cdot \prod_{i < j \leq n} (X_j - X_i) \right)$$

Assim:

$$\widehat{\alpha\beta}(g) = \psi(\alpha\beta) \cdot g.$$

Por outro lado, temos:

$$\widehat{\alpha\beta}(g) = \hat{\alpha}(\hat{\beta}(g)) = \hat{\alpha}(\psi(\beta) \cdot g).$$

Como $\hat{\alpha}$ fixa os inteiros, em particular $\psi(\beta)$, segue que

$$\hat{\alpha}(\psi(\beta) \cdot g) = \psi(\beta) \cdot \hat{\alpha}(g) = \psi(\beta) \cdot \psi(\alpha) \cdot g.$$

Portanto, comparando as duas expressões para $\widehat{\alpha\beta}(g)$, obtemos:

$$\psi(\alpha\beta) \cdot g = \psi(\beta) \cdot \psi(\alpha) \cdot g.$$

Como $g \neq 0$ e estamos trabalhando em $\mathbb{Z}$, segue da igualdade acima que

$$\psi(\alpha\beta) = \psi(\alpha) \cdot \psi(\beta).$$

o que conclui a demonstração de que ψ é um homomorfismo de grupos. $\square$

Lema 2.4.2. *Seja $k \in \{1, 2, \dots, n-1\}$. Então, a transposição $\tau = (k \ k+1)$ tem sinal -1 , ou seja,*

$$\psi(\tau) = -1.$$

Demonstração. Seja $g = \prod_{1 \leq i < j \leq n} (X_i - X_j)$ o polinômio discriminante. Queremos calcular a ação de τ sobre g , isto é, $\hat{\tau}(g)$. Note que τ apenas troca k e $k+1$, deixando os outros índices fixos. Podemos decompor o produto g em fatores que envolvem ou não os índices k e $k+1$:

$$g = \left(\prod_{\substack{1 \leq i < j \leq n \\ i, j \notin \{k, k+1\}}} (X_i - X_j) \right) \cdot \left(\prod_{\substack{1 \leq i \leq n \\ i \notin \{k, k+1\}}} (X_i - X_k)(X_i - X_{k+1}) \right) \cdot (X_k - X_{k+1}).$$

A ação de τ nos fatores que não envolvem k ou $k+1$ é trivial. Nos fatores que envolvem um índice fora de $\{k, k+1\}$ e um dentro, temos:

$$\hat{\tau}(X_i - X_k) = X_i - X_{k+1}, \quad \hat{\tau}(X_i - X_{k+1}) = X_i - X_k.$$

Portanto, o produto

$$\prod_{\substack{1 \leq i \leq n \\ i \notin \{k, k+1\}}} (X_i - X_k)(X_i - X_{k+1})$$

é invariante sob τ , pois os fatores são apenas permutados.

Resta analisar o fator $(X_k - X_{k+1})$. Temos:

$$\hat{\tau}(X_k - X_{k+1}) = X_{k+1} - X_k = -(X_k - X_{k+1}).$$

Assim, a ação de τ sobre g é:

$$\hat{\tau}(g) = \left(\prod_{\substack{1 \leq i < j \leq n \\ i, j \notin \{k, k+1\}}} (X_i - X_j) \right) \cdot \left(\prod_{\substack{1 \leq i \leq n \\ i \notin \{k, k+1\}}} (X_i - X_k)(X_i - X_{k+1}) \right) \cdot (-(X_k - X_{k+1})) = -g.$$

Logo, $\psi(\tau) = -1$. □

Proposição 2.4.3. *Seja $t \in S_n$ uma transposição. Então, $\psi(t) = -1$.*

Demonstração. Primeiro, note que já demonstramos no lema anterior que transposições de elementos consecutivos, ou seja, da forma $(k \ k+1)$ para $k \in \{1, 2, \dots, n-1\}$, satisfazem $\psi((k \ k+1)) = -1$.

Agora, seja $t = (a \ b)$ uma transposição arbitrária, com $a, b \in \{1, 2, \dots, n\}$ e $a < b$. Queremos mostrar que $\psi(t) = -1$. Para isso, expressamos t como um produto de transposições consecutivas. De fato, pode-se verificar que:

$$(a \ b) = (a \ a+1)(a+1 \ a+2) \cdots (b-2 \ b-1)(b-1 \ b)(b-2 \ b-1) \cdots (a+1 \ a+2)(a \ a+1).$$

Essa decomposição é conhecida e pode ser verificada diretamente pela ação nos elementos $a, a+1, \dots, b$. Note que o número de transposições consecutivas neste produto é $2(b-a) - 1$, que é ímpar.

Como cada transposição consecutiva tem sinal -1 e ψ é um homomorfismo, temos:

$$\begin{aligned} \psi(t) &= \psi((a \ a+1)) \cdot \psi((a+1 \ a+2)) \cdots \psi((b-1 \ b)) \cdots \psi((a \ a+1)) \\ &= (-1)^{2(b-a)-1} \\ &= -1, \end{aligned}$$

pois o expoente é ímpar. Alternativamente, podemos usar uma decomposição mais eficiente:

$$(a \ b) = (a \ a+1)(a+1 \ a+2) \cdots (b-1 \ b)(b-2 \ b-1) \cdots (a+1 \ a+2)(a \ a+1),$$

que também consiste em um número ímpar de transposições consecutivas. Em qualquer caso, o sinal é -1 .

Portanto, toda transposição tem sinal -1 . □

Proposição 2.4.4. *Seja $\alpha \in S_n$. Então existem transposições duas a duas disjuntas $\alpha_1, \dots, \alpha_t \in S_n$ tais que $\alpha = \alpha_1 \cdots \alpha_t$ se, e somente se, $\mathcal{O}(\alpha) = 2$.*

Demonstração. Sabemos que $\mathcal{O}(\alpha) = \text{mmc}\{\mathcal{O}(\alpha_1), \dots, \mathcal{O}(\alpha_t)\} = \text{mmc}\{2, \dots, 2\} = 2$.

Podemos escrever $\alpha = \alpha_1 \cdots \alpha_t$, onde $\alpha_1, \dots, \alpha_t$ são ciclos dois a dois disjuntos onde $r_i = \mathcal{O}(\alpha_i) \geq 2, \forall i \in \{1, \dots, t\}$.

Como $2 = \mathcal{O}(\alpha) = \text{mmc}\{r_1, \dots, r_t\}$ então $r_i \mid 2, \forall i \in \{1, \dots, t\}$. Como $r_i \geq 2, \forall i \in \{1, \dots, t\}$ então $r_i = 2, \forall i \in \{1, \dots, t\}$, então α_i é um 2-ciclo, $\forall i \in \{1, \dots, t\}$. $\square$

Teorema 2.4.5. *Seja $\alpha \in S_n$ e sejam $\tau_1, \dots, \tau_t \in S_n$ transposições tais que $\alpha = \tau_1 \cdots \tau_t$. Então:*

1. $\psi(\alpha) = (-1)^t$.

2. Se $\mu_1, \dots, \mu_r \in S_n$ são transposições tais que $\alpha = \mu_1 \cdots \mu_r$, então $r \equiv t \pmod{2}$.

Demonstração. (a) Como ψ é um homomorfismo e $\psi(\tau) = -1$ para toda transposição τ (conforme demonstrado anteriormente), temos:

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

(b) Se $\alpha = \mu_1 \cdots \mu_r$ é outra decomposição em transposições, então, pelo item (a),

$$\psi(\alpha) = (-1)^t = (-1)^r.$$

Portanto, $(-1)^t = (-1)^r$, o que implica $t \equiv r \pmod{2}$. $\square$

Uma permutação $\sigma \in S_n$ é dita par quando pode ser escrita como produto de uma quantidade par de transposições, isto é, existe $k \in \mathbb{N}$ tal que $\sigma = \tau_1 \tau_2 \cdots \tau_{2k}$, onde cada τ_i é uma transposição.

Corolário 2.4.6. *Se $n \in \mathbb{N}$, então A_n é um subgrupo de S_n com índice $[S_n : A_n] = 2$. Em particular, $A_n \trianglelefteq S_n$.*

Demonstração. Considere o homomorfismo sobrejetor

$$\psi : S_n \rightarrow \{-1, 1\}, \quad \psi(\sigma) = \begin{cases} 1, & \text{se } \sigma \text{ é par,} \\ -1, & \text{se } \sigma \text{ é ímpar,} \end{cases}$$

definido usando o polinômio de Vondermonde ou a decomposição em transposições. Como ψ é sobrejetor (pois $\psi(\text{id}) = 1$ e $\psi((1 \ 2)) = -1$), e $\ker \psi = A_n$, pelo Teorema do Isomorfismo para Grupos 1.8.4,

$$S_n/A_n \cong \{-1, 1\}.$$

Logo, $[S_n : A_n] = |S_n/A_n| = |\{-1, 1\}| = 2$. Além disso, como A_n é o núcleo de um homomorfismo, segue que $A_n \trianglelefteq S_n$. $\square$

Proposição 2.4.7. *Seja H um subgrupo de S_n . Então H é um subgrupo de A_n ou $[H : H \cap A_n] = 2$.*

Demonstração. Considere a restrição do homomorfismo $\psi : S_n \rightarrow \{-1, 1\}$ a H , denotada por $\psi|_H : H \rightarrow \{-1, 1\}$. Temos duas possibilidades:

CASO 1: $\psi|_H$ é trivial, isto é, $\psi(h) = 1$ para todo $h \in H$. Então $H \subseteq \ker \psi = A_n$, logo H é um subgrupo de A_n .

CASO 2: $\psi|_H$ não é trivial. Então existe $h_0 \in H$ tal que $\psi(h_0) = -1$. Como $\psi|_H$ é um homomorfismo não trivial, sua imagem é $\{-1, 1\}$. Pelo Primeiro Teorema do Isomorfismo,

$$H / \ker(\psi|_H) \cong \{-1, 1\}.$$

Note que $\ker(\psi|_H) = H \cap \ker \psi = H \cap A_n$. Portanto,

$$|H / (H \cap A_n)| = |\{-1, 1\}| = 2,$$

ou seja, $[H : H \cap A_n] = 2$. □

Exemplo 2.4.8. Seja $H = \{id, (1\ 2)\} \subset S_3$. Então $H \cap A_3 = \{id\}$, e

$$[H : H \cap A_3] = |H| / |H \cap A_3| = 2/1 = 2,$$

o que corresponde ao segundo caso.

Exemplo 2.4.9. Seja $H = S_n$. Então $H \cap A_n = A_n$, e

$$[S_n : A_n] = 2,$$

como já conhecido.

JOGO DO 15

Este capítulo se fundamenta no artigo de Dutenhefner [4], do qual se aproveitam a motivação e parte da abordagem didática, com adaptações quando necessário.

O jogo do 15 é um quebra-cabeça deslizante disposto em um tabuleiro 4×4 , com quinze peças numeradas e uma casa vazia. Um movimento válido consiste em deslocar, horizontal ou verticalmente, uma peça adjacente para o espaço livre. O objetivo clássico é alcançar a posição normal, na qual as peças aparecem em ordem crescente, da esquerda para a direita e de cima para baixo, com o vazio situado no canto inferior direito.

Esse problema recreativo possui uma estrutura combinatória bastante rica e pode ser analisado por meio de noções elementares da Teoria de Grupos, em particular das permutações e de sua paridade. Em termos históricos, o quebra-cabeça atualmente conhecido como jogo do 15 é atribuído a Noyes Chapman, por volta de 1874, embora tenha se tornado amplamente popular também por causa da configuração divulgada por Sam Loyd, obtida pela troca das peças 14 e 15 na posição normal.

De maneira geral, interpretamos cada configuração do tabuleiro como uma permutação de 16 símbolos, representando a casa vazia pelo número 16. Com essa convenção, a posição normal corresponde à identidade, enquanto a configuração atribuída a Sam Loyd difere dela pela transposição das peças 14 e 15. Assim, torna-se natural investigar quais configurações podem ser obtidas a partir de sequências de movimentos válidos e quais não podem.

A ideia central será associar a cada movimento uma transformação da permutação correspondente e estudar uma quantidade que permanece invariante ao longo do processo. Isso permitirá explicar, de forma precisa, por que certas configurações são alcançáveis e por que outras se mostram impossíveis sem violar as regras do jogo. Em particular, veremos que o espaço de estados se divide em duas componentes disjuntas, determinadas por critérios de paridade.

Nesse sentido, adotamos uma abordagem teórica que privilegia a formulação algébrica do problema. A partir de definições e propriedades básicas do grupo simétrico, estabeleceremos critérios necessários e suficientes para a equivalência de tabuleiros, relacionando a decomposição em transposições, a paridade e o número de cruzamentos de uma permutação. Com isso, mostraremos que toda configuração pode ser reduzida, por movimentos válidos, a uma forma canônica pertencente a uma de duas classes: a da posição normal ou a da posição atribuída a Sam Loyd.

3.1 CONFIGURAÇÕES, REVERSIBILIDADE E A QUESTÃO CENTRAL

Para fixar ideias, considere o tabuleiro 4×4 com quinze peças numeradas e uma casa vazia. A Figura 2 ilustra, à esquerda, uma configuração inicial típica; à direita, apresenta-se a *posição normal*, objetivo clássico do jogo. Observa-se que um movimento válido consiste em deslizar uma peça adjacente (horizontal ou verticalmente) para o espaço vazio, invertendo as posições da peça e do vazio. *Mutatis mutandis*, a sequência inversa de movimentos reverte qualquer transformação realizada, de modo que, partindo de uma configuração A e chegando a B , pode-se retornar de B a A percorrendo a sequência inversa. Essa reversibilidade simples, mas fundamental, sugere que o problema relevante não é a direção “inicial $\rightarrow$ final”, e sim a *conectividade* entre configurações sob movimentos válidos.

Configuração inicial

7	1	8	
11	10	3	14
6	4	5	2
15	12	9	13

Posição normal

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Figura 2: Uma configuração inicial e a posição usual do jogo do 15.

Nesse sentido, formula-se a pergunta essencial que orienta a análise dessa dissertação: *dada duas configurações arbitrárias do tabuleiro, é possível transformar uma na outra por meio de uma sequência de movimentos válidos?* A Figura 3 exibe um par de configurações ilustrativas. Nas próximas seções, apresentaremos critérios necessários que respondem a essa pergunta central.

Configuração A

	13	1	3
14	2	9	11
5	8	4	6
10	7	12	15

Configuração B

3	15	5	8
1	9	2	12
7		14	13
11	4	10	6

Figura 3: Duas configurações de referência para a questão de conectividade.

3.2 POPULARIDADE

Ainda que a criação do quebra-cabeça seja comumente atribuída a Noyes Chapman, foi Sam Loyd quem desempenhou o papel decisivo na sua propagação internacional. De maneira geral, os relatos indicam que Loyd ofereceu um prêmio de mil dólares, um valor substancial para o ano de 1870, à pessoa que apresentasse uma sequência de movimentos válidos capaz de *apenas* trocar as peças 14 e 15 a partir da posição usual. A proposta, formulada de forma simples e sedutora, alcançou grande repercussão pública, promovendo

tentativas em larga escala, o que resultou na popularização do jogo em ambos os lados do Atlântico. Esse percurso histórico, como se verá, está intrinsicamente ligado à solução matemática que demonstra a impossibilidade desse feito dentro das regras do jogo.

3.3 O DESAFIO DE SAM LOYD E SUA IMPOSSIBILIDADE

A divulgação em massa do *jogo do 15* esteve fortemente vinculadas às ações publicitárias de Sam Loyd, que popularizou uma expressão particularmente sedutora: partindo da posição normal, realizar exclusivamente a troca das peças 14 e 15 através de movimentos válidos. Relatos históricos nos mostram que o problema rapidamente se espalhou pela Europa e pelas Américas, com ampla repercussão em jornais e círculos recreativos, impulsionado pela promessa de uma recompensa financeira para a primeira solução apresentada.

Sob a perspectiva matemática, observa-se que o desafio disseminado é insolúvel quando se respeitam integralmente as regras do tabuleiro. Em outras palavras, não existe uma sequência de deslizamentos legais que produza a troca de posição apenas das peças 14 e 15; para tal propósito, seria necessário violar as regras do jogo (por exemplo, retirando peças e recolocando-as no tabuleiro), o que descaracteriza o problema original.

É razoável supor que Loyd conhecesse a natureza insolúvel do quebra-cabeça; ainda que não haja documentação histórica definitiva que comprove tal fato, a hipótese contribui em compreender o impacto social do enunciado e a admiração constante que o acompanha desde então.

3.4 CONTAGEM DE CONFIGURAÇÕES

O tabuleiro 4×4 contém 16 casas. Considerando as quinze peças numeradas e a casa vazia como um décimo sexto símbolo, o número total de arranjos possíveis é

$$16! = 20.922.789.888.000,$$

consequência direta do princípio multiplicativo. Para dimensionar essa grandeza, podemos comparar com o jogo da loteria, a Mega-Sena. Ao escolher 6 números dentre 60, obtêm-se 50.063.860 resultados diferentes, isto é, uma quantidade insignificante quando equiparada com o total de configurações do *jogo do 15*.

Nesse viés, anuncia-se um dos fatos que centralizam a análise dessa dissertação: exatamente *metade* das configurações iniciais são solúveis sob as regras do jogo, enquanto a outra metade não pode ser conectada à posição normal por movimentos válidos. De forma estimada, temos a ordem de dez trilhões de estados solúveis e dez trilhões de estados insolúveis. A posição divulgada por Loyd, com a troca isolada das peças 14 e 15, ilustra um caso sem solução.

3.5 ENUMERAÇÃO DAS CASAS E CODIFICAÇÃO DO ESTADO

Inicialmente, vamos enumerar as casas do tabuleiro de 1 a 16, em ordem da esquerda para a direita e de cima para baixo, como é habitual em representações matriciais. Essa convenção nos ajuda a fixar o referencial do tabuleiro, uma vez que as casas não se deslocam, são as peças que deslizam entre elas. De forma geral, podemos considerar que as quinze peças numeradas recebem a identificação $1, 2, \dots, 15$, enquanto a casa vazia será representada pelo símbolo 16.

Assim, cada configuração do tabuleiro é codificada por uma permutação matricial que chamaremos pela letra σ de $\{1, \dots, 16\}$ na notação de duas linhas

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & 16 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(16) \end{pmatrix},$$

onde $\sigma(i)$ indica *qual peça* ocupa a posição i . Observa-se que a primeira linha permanece sempre organizada, pois referencia as posições fixas do tabuleiro, ou seja, não haverá alterações na primeira linha da matriz; a segunda linha registra o arranjo das peças no tabuleiro (incluindo o vazio). Nota-se, portanto, que a posição normal corresponde à identidade id (o elemento neutro), enquanto outras configurações são obtidas por permutações aleatórias desses símbolos.

A fim de ilustrar um exemplar considere um arranjo em que o vazio ocupa a casa 11 e as demais peças se distribuem conforme a figura abaixo. A codificação por permutação assume a forma

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 12 & 3 & 15 & 7 & 1 & 14 & 10 & 6 & 8 & 5 & 16 & 13 & 4 & 11 & 2 & 9 \end{pmatrix}.$$

Nessa análise, por exemplo, a casa 1 contém a peça 12, a casa 2 contém a peça 3 e assim sucessivamente. Veja que a casa 11 contém o vazio, representado pelo 16. Essa exposição resume, em notação compacta, toda a informação do tabuleiro.

Sabemos que cada deslizamento legal troca a posição do vazio com a de uma peça adjacente. Em termos de permutações, se a matriz σ representa o estado atual e a peça movida possui o rótulo n , então o novo estado é designado por

$$\sigma' = (n \ 16) \circ \sigma,$$

isto é, compõe-se à esquerda com a transposição que permuta o elemento n e 16. Em particular, cada movimento modifica a paridade da permutação associada ao arranjo.

Para tornar a ideia mais intuitiva e concreta, vamos retomar o exemplo anterior e deslizar a peça 5 para a casa vazia. A permutação resultante é

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 12 & 3 & 15 & 7 & 1 & 14 & 10 & 6 & 8 & 16 & 5 & 13 & 4 & 11 & 2 & 9 \end{pmatrix}$$

obtida, pela transposição (5 16) aplicada ao estado anterior (as posições 10 e 11 trocam os valores 5 e 16). Note que a natureza do movimento no tabuleiro aparece, como uma transposição que compreende necessariamente o símbolo 16. Tal fato será fundamental nas seções seguintes, quando a paridade for utilizada como invariante para decidir a relação entre as configurações.

Relembrando que, conforme visto no Capítulo 2, denominamos transposição a permutação que inverte a posição de exatamente dois elementos, atuando como identidade sobre todos os demais. Por exemplo, a aplicação

$$\tau = (3 \ 12)$$

$$\tau = (3 \ 12)$$

troca as posições associadas aos elementos 3 e 12 e deixa inalterados os demais elementos. As transposições serão os blocos fundamentais na descrição dos movimentos válidos do tabuleiro, uma vez que cada deslizamento válido pode ser compreendido precisamente como a composição com uma transposição que envolve o símbolo do vazio.

3.6 COMPOSIÇÃO DE PERMUTAÇÕES E PARIDADE

3.6.1 Ordem de composição e não comutatividade

Adota-se, neste trabalho, a convenção funcional para composições: dado $\alpha, \beta \in S_n$, a aplicação $\alpha\beta$ significa “primeiro agir por β , depois por α ”. Em particular, a avaliação ponto a ponto é feita da direita para a esquerda, à semelhança do que ocorre na composição de funções. Para tornar essa convenção explícita, considere-se as transposições $\tau_1 = (4 \ 13)$ e $\tau_2 = (10 \ 13)$. Então:

$$\begin{aligned} (\tau_1\tau_2)(4) &= \tau_1(\tau_2(4)) = \tau_1(4) = 13, \\ (\tau_1\tau_2)(10) &= \tau_1(\tau_2(10)) = \tau_1(13) = 4, \\ (\tau_1\tau_2)(13) &= \tau_1(\tau_2(13)) = \tau_1(10) = 10, \end{aligned}$$

de modo que, restringindo-nos a $\{4, 10, 13\}$, tem-se

$$\tau_1\tau_2 = \begin{pmatrix} 4 & 10 & 13 \\ 13 & 4 & 10 \end{pmatrix}, \quad \text{e a identidade nos demais símbolos.}$$

Se, por outro lado, invertemos a ordem,

$$\begin{aligned} (\tau_2\tau_1)(4) &= \tau_2(\tau_1(4)) = \tau_2(13) = 10, \\ (\tau_2\tau_1)(10) &= \tau_2(\tau_1(10)) = \tau_2(10) = 13, \\ (\tau_2\tau_1)(13) &= \tau_2(\tau_1(13)) = \tau_2(4) = 4, \end{aligned}$$

obtemos

$$\tau_2\tau_1 = \begin{pmatrix} 4 & 10 & 13 \\ 10 & 13 & 4 \end{pmatrix},$$

o que evidencia a não comutatividade em S_n : em geral, $\tau_1\tau_2 \neq \tau_2\tau_1$.

3.6.2 Algoritmo de decomposição: ideia geral e exemplo

Para efeitos práticos, convém explicitar um procedimento sistemático para escrever uma permutação como produto de transposições. De modo geral, corrige-se a configuração “da esquerda para a direita”: a cada passo, escolhe-se uma transposição que coloca, na coluna atualmente analisada, o símbolo correto, de modo que o resultado vá se aproximando da identidade. Prossegue-se da primeira para a última coluna até que todas estejam corretas. Ao final, como a inversa de cada transposição coincide com ela própria, basta reverter a sequência de transposições aplicada para obter a fatoração desejada.

Exemplo 3.6.1.

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

Passo 1. Ajuste da primeira coluna: tomar $\tau_1 = (1\ 6)$ e compor à esquerda:

$$\tau_1\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 2 & 3 \end{pmatrix}.$$

Passo 2. Ajuste da segunda coluna: tomar $\tau_2 = (2\ 6)$:

$$\tau_2\tau_1\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix}.$$

Passo 3. Ajuste da terceira coluna: tomar $\tau_3 = (3\ 5)$:

$$\tau_3\tau_2\tau_1\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix}.$$

Passo 4. A quarta coluna já está correta; ajusta-se a quinta com $\tau_4 = (5\ 6)$:

$$\tau_4\tau_3\tau_2\tau_1\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \text{id.}$$

Logo,

$$\sigma = \tau_1\tau_2\tau_3\tau_4 = (1\ 6)(2\ 6)(3\ 5)(5\ 6),$$

o que evidencia que σ é uma permutação par (produto de quatro transposições).

Exemplo 3.6.2. *Agora, considere*

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

Passo 1. *Corrigir a primeira coluna com $\tau_1 = (1\ 6)$:*

$$\tau_1\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 6 & 2 & 3 \end{pmatrix}.$$

Passo 2. *Corrigir a segunda coluna com $\tau_2 = (2\ 4)$:*

$$\tau_2\tau_1\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 6 & 4 & 3 \end{pmatrix}.$$

Passo 3. *Corrigir a terceira coluna com $\tau_3 = (3\ 5)$:*

$$\tau_3\tau_2\tau_1\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 4 & 5 \end{pmatrix}.$$

Passo 4. *Corrigir a quarta coluna com $\tau_4 = (4\ 6)$:*

$$\tau_4\tau_3\tau_2\tau_1\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix}.$$

Passo 5. *Ajustar a quinta coluna com $\tau_5 = (5\ 6)$:*

$$\tau_5\tau_4\tau_3\tau_2\tau_1\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \text{id}.$$

Conclui-se, portanto, que

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

decomposição que envolve cinco transposições; logo, σ é ímpar.

3.7 MOVIMENTOS VÁLIDOS E TRANSPOSIÇÕES

Nesta etapa, conecta-se a dinâmica do *jogo dos 15* à estrutura algébrica previamente introduzida. A correspondência é direta: cada deslizamento legal realiza a troca entre a peça movimentada e o vazio; em notação de permutações, esse efeito é modelado pela composição, à esquerda, com uma transposição que envolve necessariamente o símbolo 16. Como consequência imediata, *todo* movimento altera a paridade da permutação que codifica o tabuleiro, invertendo-a de par para ímpar ou de ímpar para par. Essa observação

servirá de base para os critérios de equivalência e de solubilidade a serem apresentados mais adiante.

3.7.1 Exemplo: atualização de estado e inversão de paridade

Considere a configuração A exibida na Figura 4, na qual o vazio ocupa a casa 11 (numeração por linhas). Sua codificação por permutação, tomando o vazio como símbolo 16, é

$$\sigma_A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 4 & 13 & 2 & 9 & 1 & 12 & 7 & 15 & 10 & 6 & 16 & 5 & 14 & 3 & 11 & 8 \end{pmatrix}.$$

Deslizando a peça 11 para cima, isto é, trocando-a com o vazio, obtém-se a configuração B (Figura 4), cuja codificação é

$$\sigma_B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 4 & 13 & 2 & 9 & 1 & 12 & 7 & 15 & 10 & 6 & 11 & 5 & 14 & 3 & 16 & 8 \end{pmatrix}.$$

Comparando as duas expressões, verifica-se que a única alteração é a inversão dos símbolos 11 e 16. Em termos algébricos, $\sigma_B = \tau \circ \sigma_A$ com $\tau = (11 \ 16)$. Em particular, a paridade passa a ser a oposta: se σ_A era par, σ_B torna-se ímpar, e vice-versa.

4	13	2	9		→ (mover 11 para cima)	4	13	2	9
1	12	7	15			1	12	7	15
10	6		5			10	6	11	5
14	3	11	8			14	3		8

Figura 4: Configuração A com o vazio na casa 11.

Observação 3.7.1. *Note que cada movimento corresponde à transposição entre a peça e o vazio*

3.7.2 Sequências de movimentos e efeito cumulativo

Generalizando o caso anterior, suponha que a partir de A se executem k movimentos válidos, invertendo sucessivamente as peças $n_1, n_2, \dots, n_k$ com o vazio. Denotando

$$\tau_i = (n_i \ 16) \quad (i = 1, \dots, k),$$

o estado final B é descrito por

$$\sigma_B = \tau_k \cdots \tau_2 \tau_1 \sigma_A.$$

Como cada τ_i é uma transposição, conclui-se que:

- se k é par, σ_A e σ_B têm a mesma paridade;

- se k é ímpar, σ_A e σ_B têm paridades opostas.

Esse controle fino do efeito cumulativo dos movimentos, isto é, a alternância inevitável da paridade a cada deslizamento, será decisivo para a classificação das configurações em classes de equivalência e, em particular, para a prova de que o espaço de estados se biparte em dois conjuntos que não se comunicam por movimentos legais.

3.8 CONFIGURAÇÕES EQUIVALENTES E O PAPEL DA COR DA CASA DO VAZIO

Definição 3.8.1 (Equivalência de configurações). *Duas configurações do jogo dos 15 dizem-se equivalentes quando existe uma sequência finita de movimentos válidos que transforma uma na outra. Trata-se, portanto, de uma relação reflexiva, simétrica e transitiva, a qual particiona o conjunto de todos os tabuleiros em classes de equivalência.*

A pergunta natural que se manifesta, nessa ótica, é a seguinte: *como caracterizar, quando duas configurações pertencem à mesma classe?* Para avançarmos nessa direção, é vantajoso fixar uma coloração xadrez no tabuleiro, alternando casa a casa, preservando a numeração por linhas de 1 a 16. Essa convenção permite um acompanhamento, de forma controlada, para com a posição do vazio e uma associação mais direta com a paridade da permutação através da configuração do tabuleiro.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Figura 5: Coloração e numeração das casas do tabuleiro do jogo dos 15.

Considere uma configuração A , obtida por uma permutação σ_A de $\{1, \dots, 16\}$, e uma configuração B tomada a partir de A por k movimentos válidos. Cada deslizamento legal realiza a transposição entre o símbolo 16 e a peça movimentada. Note que a paridade da permutação é invertida a cada passo e a cor da casa do vazio alterna entre preto e branco.

3.9 CRITÉRIO DE EQUIVALÊNCIA: CONDIÇÕES NECESSÁRIAS E SUFICIENTES

Teorema 3.9.1. *Sejam A e B duas configurações do tabuleiro do jogo dos 15, representadas por permutações $\sigma_A, \sigma_B \in S_{16}$. Então, A e B são equivalentes, isto é, há uma sequência finita de movimentos válidos transformando A em B se, e somente se, verifica-se uma das alternativas:*

1. σ_A e σ_B possuem a mesma paridade e, simultaneamente, os vazios estão em casas de mesma cor; ou
2. σ_A e σ_B possuem paridades distintas e, simultaneamente, os vazios estão em casas de cores diferentes.

Em particular, quando as duas afirmações acima são falsas, conclui-se que as configurações não são equivalentes, o que implica a impossibilidade de obter uma a partir da outra por deslizamentos legais.

Com essa ideia, compreende-se a razão pela qual o enunciado clássico de Sam Loyd é insolúvel sob as regras do jogo. A configuração obtida pela troca isolada dos símbolos 14 e 15 é descrita por uma transposição, que é uma permutação *ímpar*, mantendo o vazio na mesma cor. Como, nesse caso, a paridade difere e a cor do vazio não muda (a configuração inicial corresponde a identidade - que é par), nenhuma sequência de movimentos válidos pode conectar as duas posições.

Exemplo 3.9.2. *Considere as três configurações apresentadas a seguir. Adota-se a numeração por linhas e a coloração xadrez previamente fixadas, de modo a controlar a posição do vazio.*

A				B				C			
7	11	10	4	7	11	8	12	1	9	12	10
1	12	14	8	2	6	14		5	11	7	15
2		9	3	9	10	5	3	6	3		4
13	5	15	6	13	1	15	4	8	14	13	2

Figura 6: Configurações A, B e C do tabuleiro.

Codificação por permutações e paridades

Comparando com a coloração da Figura 3.8, verifica-se que, na configuração A, o vazio ocupa uma casa *preta*. A permutação correspondente é

$$\sigma_A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 7 & 11 & 10 & 4 & 1 & 12 & 14 & 8 & 2 & 16 & 9 & 3 & 13 & 5 & 15 & 6 \end{pmatrix}.$$

Uma decomposição de σ_A em transposições é dada por

$$\sigma_A = (3 \ 10)(10 \ 12)(6 \ 10)(10 \ 16)(1 \ 5)(1 \ 14)(1 \ 7)(2 \ 9)(2 \ 11),$$

que contém nove fatores; logo, σ_A é *ímpar*.

Na configuração B , o vazio encontra-se em uma casa *branca* e a codificação é

$$\sigma_B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 7 & 11 & 8 & 12 & 2 & 6 & 14 & 16 & 9 & 10 & 5 & 3 & 13 & 1 & 15 & 4 \end{pmatrix}.$$

Na configuração C , procede-se de modo análogo:

$$\sigma_C = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 9 & 12 & 10 & 5 & 11 & 7 & 15 & 6 & 3 & 16 & 4 & 8 & 14 & 13 & 2 \end{pmatrix}.$$

A partir do Teorema 3.9.1, a combinação entre paridade e cor do vazio decidirá a equivalência das três posições consideradas, como será detalhado adiante com base em decomposições adequadas.

Retomando as três configurações anteriormente, aplica-se o Teorema 3.9.1 para decidir o elo entre elas. Observe que para a configuração B , escrevemos a permutação como:

$$\sigma_B = (3\ 8)(8\ 12)(4\ 8)(8\ 16)(1\ 14)(1\ 7)(2\ 5)(2\ 11),$$

decomposição com oito fatores. Concluimos que σ_B é par. Como σ_A e σ_B possuem paridades diferentes e, simultaneamente, os vazios estão em casas de cores diferentes, segue do Teorema 3.9.1 que A e B são equivalentes. Em outras palavras, existe uma sequência de movimentos válidos que transforma uma das configurações na outra.

Agora, considere a configuração C . Comparando sua posição do vazio com a coloração xadrez, nota-se que o espaço vazio está na casa branca. A permutação associada admite a decomposição:

$$\sigma_C = (6\ 11)(9\ 11)(2\ 11)(11\ 16)(3\ 10)(3\ 4)(3\ 12)(8\ 13)(8\ 15),$$

a qual contém nove transposições; logo, a permutação σ_C é ímpar. Pelo Teorema 3.9.1, os tabuleiros A e C não são equivalentes (paridades iguais, porém cores do vazio distintas), e B e C também não são equivalentes, pois possuem paridades distintas, e mesma cor para o vazio para as configurações consideradas.

Em síntese, observa-se que o par (*paridade da permutação, cor da casa do vazio*) funciona como um invariante completo para o problema de conectividade: quando ambos se alinham conforme as alternativas do Teorema 3.9.1, as configurações são equivalentes; caso contrário, não o são.

Teorema 3.9.3. *Seja $\sigma \in S_{16}$ a permutação que codifica uma configuração inicial do jogo dos 15, tomando o vazio como símbolo 16. O problema admite solução, isto é, a posição normal pode ser alcançada por movimentos válidos se, e somente se, uma das condições abaixo se verifica:*

1. o vazio ocupa uma casa branca e σ é par;
2. o vazio ocupa uma casa preta e σ é ímpar.

Na posição normal, a permutação é a identidade (par) e o vazio encontra-se em casa branca; o enunciado acima generaliza esse caso e caracteriza completamente as configurações solúveis.

Corolário 3.9.4. *Dada qualquer configuração do tabuleiro, por meio de movimentos válidos, pode-se levar o vazio até a casa 16. Feito isso, a equivalência entre duas configurações passa a depender apenas da paridade das permutações associadas. Mais precisamente, duas configurações com o vazio na casa 16 são equivalentes se, e somente se, as permutações correspondentes têm a mesma paridade. Consequentemente, o conjunto dos estados do problema se divide em exatamente duas classes de equivalência: a classe das configurações associadas a permutações pares e a classe das configurações associadas a permutações ímpares. Como metade das permutações de S_{16} é par e a outra metade é ímpar, segue que metade das configurações iniciais do tabuleiro é solúvel e a outra metade é insolúvel.*

O JOGO DO 15 NA SALA DE AULA: POR QUÊ E PARA QUÊ?

Como prática cultural estruturada por regras, o jogo oferece metas claras, feedback imediato e um contexto significativo de resolução de problemas. Em ambiente escolar, seu potencial se realiza quando há intencionalidade pedagógica: o professor cria tarefas, orienta registros, promove comparações entre estratégias e convida os estudantes a explicarem “por que funcionou”. Nesta proposta, o jogo do 15 cumpre esse papel ao tornar visível um invariante (a ideia de que certas posições não se resolvem) e ao demandar explicações baseadas em como os movimentos transformam a posição.

Considerando os anos finais do Ensino Fundamental, esta proposta encontra respaldo em habilidades da BNCC que envolvem a construção de procedimentos, a observação de regularidades e a análise de transformações. Nesse sentido, aproxima-se da habilidade EF06MA23, ao requerer que os estudantes organizem, testem e comuniquem sequências de passos para atingir um objetivo; das habilidades EF08MA10 e EF08MA11, ao estimular a percepção de padrões e recorrências nas jogadas, bem como a elaboração de estratégias de continuidade e resolução; e da habilidade EF08MA18, uma vez que os movimentos das peças podem ser compreendidos como composições de transformações no tabuleiro. Assim, o trabalho com o jogo do 15 ultrapassa a dimensão lúdica e passa a constituir uma situação pedagógica em que os estudantes são levados a analisar procedimentos, justificar escolhas, comparar estratégias e compreender que diferentes sequências de ações produzem efeitos específicos sobre a configuração final [2].

PROCESSO DE ENSINO

O trabalho organiza-se em três momentos encadeados: lançamento do problema investigação orientada e sistematização compartilhada. Primeiro, apresenta-se um desafio concreto do jogo do 15 e pedem-se hipóteses: “é possível resolver? como saber?”. Em seguida, os grupos jogam com regras de registro (anotar sequências de movimentos e tentativas de “trocar apenas duas peças”), enquanto o professor circula, observa e intervém com perguntas que ampliam a análise (“o que mudou?”, “o que nunca muda?”). Por fim, a turma discute padrões percebidos e constrói um vocabulário comum para descrever transformações da posição, preparando o terreno para, na aula seguinte, consolidar a ideia de permutação e de composição de movimentos em linguagem acessível. O fio condutor é a mediação: transformar a experiência lúdica em compreensão conceitual progressiva.

APRENDIZAGEM

O foco é aprender com o jogo, e não medir o desempenho. Adotam-se práticas de acompanhamento leve: registros de grupo, breves discussões de metacognição (“que ideia ajudou?”) e devolutivas orais do professor. O jogo sustenta aprendizagem porque envolve regras, tomada de decisão e explicação de estratégias; com intervenção adequada, converte-se em contexto para construir conceitos, comparar raciocínios e estabilizar significados compartilhados.

4.1 VISÃO GERAL DA SEQUÊNCIA

1. Desafio inicial: apresentar uma configuração do jogo do 15; solicitar previsões de caminhos de solução e de situações “impossíveis”.
2. Exploração orientada: em duplas/grupos, jogar e registrar cada movimento realizado por meio da notação de ciclos e de sua composição, de modo a organizar a tentativa de solução e permitir a análise das transformações envolvidas.
3. Conjecturas sobre invariantes: incentivar tentativas de “trocar só duas peças” e discutir por que certas trocas não aparecem nos registros, introduzindo a ideia de que há algo que não muda ao longo dos movimentos.
4. Sistematização acessível: nomear dois modos de representar uma transformação de posição: (i) um arranjo organizado de posições descrito em texto e (ii) a apresentação por ciclos; explicitar que compor movimentos significa “fazer um depois do outro” e descrever, ainda em linguagem comum, o efeito final sobre as peças usando ambos os modos de registro.
5. Preparação para a aula seguinte: combinar que, na próxima etapa, essas descrições serão conectadas à ideia geral de permutações e suas composições, mantendo a linguagem simples e sem formalismo.

Objetivo central declarado aos estudantes: conseguir resolver configurações do jogo do 15, representar cada sequência de movimentos nas duas formas de registro acima e compor sequências (aplicar uma transformação depois da outra) verificando o efeito final sobre as peças.

4.2 FUNDAMENTAÇÃO PEDAGÓGICA

Esta proposta entende o jogo como contexto estruturado por regras e metas que favorece a formulação de estratégias, a explicitação de raciocínios e a construção de significados compartilhados. A centralidade recai sobre a mediação docente, que articula objetivos,

conteúdos, tarefas e formas de acompanhamento da aprendizagem. Nesse sentido, a didática organiza o ensino como prática intencional, convertendo finalidades educacionais em ações de sala de aula: “À didática cabe converter objetivos sociopolíticos e pedagógicos em objetivos de ensino, selecionar conteúdos e métodos em função desses objetivos e estabelecer os vínculos entre ensino e aprendizagem, tendo em vista o desenvolvimento das capacidades mentais dos alunos.” [9]

O jogo do 15 oferece um problema autêntico e investigável, no qual os estudantes podem observar padrões de transformação das posições, levantar hipóteses sobre o que muda e o que permanece e, gradualmente, nomear essas transformações com uma linguagem comum à turma. A sequência evita formalismo excessivo e foca na descrição em palavras do que cada movimento faz, preparando posteriormente a ligação com registros convencionais de transformações.

OBJETIVOS DE APRENDIZAGEM

1. Resolver configurações selecionadas do jogo do 15, explicando o raciocínio empregado.
2. Descrever, em linguagem comum, o que cada movimento faz com as peças, identificando padrões de mudança e aspectos que permanecem inalterados.
3. Representar uma transformação de posição em dois modos de registro textual: um arranjo organizado de posições e a forma por ciclos, sempre sem notação simbólica.
4. Compor transformações, isto é, aplicar uma depois da outra e descrever o efeito resultante nas peças, ainda em linguagem comum.

RECURSOS E ORGANIZAÇÃO

Tabuleiros impressos ou físicos do jogo do 15; projeção de uma configuração inicial; folhas de registro para cada grupo; cartões com exemplos de descrições por ciclos escritos em palavras; quadro para sínteses coletivas. Recomenda-se trabalho em duplas ou trios, com rodízio de papéis: quem movimenta, quem observa e narra, quem registra.

METODOLOGIA E PAPÉIS

A condução assume três momentos encadeados: lançamento do problema, investigação orientada e sistematização. O professor provoca a explicitação de estratégias e justificativas, incentiva a comparação entre abordagens dos grupos e organiza o vocabulário comum da turma. O acompanhamento da aprendizagem ocorre por meio de registros escritos, sínteses orais e perguntas de sondagem, sem atribuição de nota.

4.3 ROTEIRO DA AULA 1

1. Abertura: apresentar uma configuração inicial e perguntar se ela parece resolvível; recolher hipóteses iniciais e combinados de registro.
2. Exploração em grupos: jogar e registrar as transformações de duas maneiras em texto.
3. lista organizada de posições, indicando, em palavras, de onde para onde cada peça foi levada ao longo da tentativa;
4. forma por ciclos, descrevendo, em palavras, as voltas que as peças dão entre si ao longo de uma transformação.
5. Observação de invariantes: propor tentativas de trocar apenas duas peças e discutir por que certas trocas não aparecem nos registros; levantar a ideia de algo que não muda.
6. Sistematização parcial: construir coletivamente um pequeno glossário de termos de sala (posição, movimento, transformação, composição como fazer uma depois da outra) e registrar um exemplo curto nos dois modos de descrição textual.

NOTA PRÁTICA SOBRE O REGISTRO. Em configurações muito difíceis, o registro de todos os movimentos pode se tornar impraticável. Ajuste a exigência de acordo com a complexidade:

- em posições acessíveis, solicitar registro sequencial completo;
- em posições desafiadoras, solicitar marcos (início, dois ou três intermediários relevantes e final), um registro amostral a cada certo número de movimentos, ou a descrição apenas das mudanças estruturais, como quando um bloco de peças entra na ordem correta.

Em qualquer caso, prioriza-se a clareza da explicação sobre a exaustividade.

ENCAMINHAMENTOS PARA O PROFESSOR

Selecionar previamente ao menos duas configurações: uma de baixa complexidade para treino de registro e outra moderada para discussão de marcos e de impossibilidades aparentes. Preparar cartões de apoio com modelos de frases para as descrições por ciclos em palavras. Planejar perguntas de sondagem que ajudem os estudantes a explicitar por que uma sequência de movimentos foi escolhida e o que ela altera na posição final.

4.4 ROTEIRO DA AULA 2

1 - Retomada (5–10 min)

Recuperar termos de sala construídos na aula anterior: posição, movimento, transformação, composição como fazer uma depois da outra. Revisitar rapidamente exemplos curtos descritos nos dois modos de registro em texto.

Consolidação guiada (15–20 min)

1. Propor uma pequena sequência de movimentos já conhecida e pedir duas tarefas:
 - (a) reescrever a descrição em lista organizada de posições (em palavras, sem símbolos);
 - (b) reescrever a mesma transformação *por ciclos*, também em palavras, mostrando a “volta” que as peças dão entre si.
2. Discutir como a mesma transformação pode aparecer de modos diferentes nos registros e por que ambos são úteis: a lista ajuda a enxergar a ordem em que as peças foram deslocadas; a forma por ciclos mostra o conjunto de trocas encadeadas que acontecem ao final.
3. Introduzir a ideia de *compor* transformações: tomar duas transformações curtas e descrever, em texto, o que ocorre quando uma acontece depois da outra. Evitar qualquer notação simbólica; manter a linguagem comum, indicando claramente começo e fim.

Prática em grupos (15–20 min)

1. Cada grupo recebe uma posição-alvo e dois desafios:
 - (a) produzir um caminho de solução e descrevê-lo nos dois modos de registro em texto;
 - (b) compor duas pequenas transformações escolhidas pelo grupo e explicar o efeito resultante nas peças.
2. Orientações de registro:
 - Em posições acessíveis, registrar a sequência completa.
 - Em posições longas ou complexas, registrar *marcos*: início, dois ou três momentos intermediários relevantes e final; opcionalmente, usar amostragem (por exemplo, a cada cinco movimentos) ou descrever apenas mudanças estruturais, como quando um bloco de peças entra na ordem correta.

Socialização e síntese

Cada grupo apresenta um exemplo curto de composição de transformações, explicitando:

- o que cada transformação fazia isoladamente;
- o que mudou quando uma foi feita depois da outra;
- como isso apareceu nos dois modos de registro em texto.

Produzir, no quadro, uma síntese com três colunas: situação de partida; descrição por lista organizada; descrição por ciclos em palavras; e uma linha final explicando o efeito combinado.

NOTA PRÁTICA Quando a complexidade for alta, priorizar clareza e justificativa em vez de exaustividade. O objetivo é que os estudantes compreendam e comuniquem *o que* a transformação faz e *por que* determinadas tentativas não produzem o efeito desejado.

ESTRATÉGIAS DE MEDIAÇÃO (PERGUNTAS-GUIA)

- O que mudou nesta jogada e o que permaneceu no mesmo lugar?
- Se você fizesse esta sequência em ordem diferente, qual seria o efeito final?
- Há uma maneira mais curta de alcançar o mesmo resultado? Como você sabe?
- Em que momento um bloco de peças ficou estável e deixou de ser alterado pelas suas jogadas?
- O que sua descrição por ciclos em palavras revela que a lista organizada não mostra tão claramente, e vice-versa?

DIFERENCIAÇÃO E ACESSIBILIDADE

- Materiais em alto contraste e peças táteis para estudantes com necessidades específicas.
- Tempos estendidos para registro ou permissão de gravação de áudio como rascunho oral antes da versão escrita.
- Desafios graduados: do microcaso (poucas peças fora de lugar) ao caso moderado (vários blocos a organizar), mantendo sempre a possibilidade de registro por marcos.

Folha de registro do grupo

1. Descrição por lista organizada de posições (em palavras).

2. Descrição por ciclos em palavras (explicitar a “volta” das peças).
3. Composição de duas transformações curtas (o que cada uma faz e o que acontece quando são feitas em sequência).
4. Observações: o que não mudou ao longo das jogadas.

Cartões-modelo de frases

- “A peça que estava no lugar X foi para o lugar Y, enquanto a que estava em Y passou para Z...”
- “Ao final desta sequência, o conjunto de peças (X, Y, Z) trocou de posição em forma de volta.”
- “Depois que a primeira transformação foi aplicada, a segunda apenas reorganizou o grupo de peças já aproximado do lugar correto.”

Roteiro do(a) professor(a) para composição

- Indicar com clareza onde termina a primeira transformação e onde começa a segunda.
- Solicitar que os estudantes expliquem o efeito combinado usando as duas formas de registro em texto.
- Incentivar a comparação entre caminhos que levam ao mesmo resultado, valorizando descrições claras e justificadas.

4.5 MATERIAIS DE APLICAÇÃO E ANEXOS DIDÁTICOS

1 Folha de atividade para estudantes (modelo imprimível)

PARTE A — EXPLORAÇÃO DO JOGO DO 15

1. Descreva, em palavras, a posição inicial que o grupo recebeu.
2. Escreva um plano de tentativa: qual peça pretende mover primeiro e por quê?
3. Execute uma pequena sequência de movimentos e registre de dois modos *em texto*:
 - a) lista organizada de posições (dizer, em palavras, de onde para onde as peças foram levadas);
 - b) descrição por ciclos em palavras (indicar as “voltas” entre peças).
4. Pare e discuta: o que mudou na posição? o que permaneceu igual?

PARTE B — COMPOSIÇÃO DE TRANSFORMAÇÕES

1. Escolha duas transformações curtas já realizadas pelo grupo. Descreva cada uma separadamente nos dois modos de registro em texto.
2. Agora descreva o que acontece quando a segunda é feita depois da primeira. Indique claramente o estado inicial, o intermediário e o final.
3. Explique, em palavras, por que o efeito combinado não é necessariamente a soma óbvia dos efeitos isolados.

PARTE C — IMPOSSIBILIDADES

1. Tente realizar uma troca de apenas duas peças. O que aconteceu?
2. Dê uma justificativa *em palavras* para o resultado observado, usando a ideia de que certas características da posição não mudam ao longo dos movimentos.

ORIENTAÇÃO SOBRE REGISTROS LONGOS Em posições longas, registre *marcos* (início, dois ou três intermediários relevantes e final) ou use amostragem (por exemplo, a cada cinco movimentos). Em qualquer caso, priorize a clareza da explicação.

Roteiro de mediação para o(a) professor(a)

ANTES DA AULA Selecionar duas posições: uma acessível para treino de registro e outra moderada para composição de transformações. Preparar cartões com frases-modelo de descrição por ciclos em palavras. Planejar perguntas de sondagem alinhadas aos objetivos.

DURANTE A EXPLORAÇÃO

- Solicitar previsões e critérios: “como saberemos que estamos mais perto da solução?”
- Circular entre os grupos, pedindo que narrem *o que a jogada faz* com a posição.
- Incentivar a comparação entre caminhos distintos que levam ao mesmo resultado.
- Em casos complexos, autorizar registros por marcos e reforçar a justificativa do *porquê* das escolhas.

NA SISTEMATIZAÇÃO Construir no quadro dois modelos de registro em texto para a mesma transformação: lista organizada de posições e descrição por ciclos. Em seguida, conduzir um exemplo curto de composição, marcando claramente onde termina a primeira transformação e onde começa a segunda.

3 Indicadores de aprendizagem observáveis

- Explica, em palavras, o efeito de uma transformação sobre a posição.
- Registra a mesma transformação *em dois modos textuais* com consistência.
- Compõe duas transformações e descreve o efeito combinado com começo e fim claros.
- Identifica algo que não muda ao longo de uma sequência de movimentos e usa isso para argumentar sobre uma impossibilidade.

4.6 CONCLUSÃO

A proposta desenvolvida ao longo deste material toma o jogo do 15 como contexto didático para construir, em linguagem acessível, a compreensão de transformações de posições, a ideia de algo que não muda ao longo das jogadas e a descrição de composições de transformações. O percurso privilegia a mediação docente e a organização intencional do ensino, em que objetivos, tarefas e registros textuais se articulam para promover participação ativa e explicações fundamentadas. Ao reduzir o formalismo e insistir na clareza das descrições em palavras, cria-se uma ponte entre a experiência lúdica e conceitos que, em momentos posteriores do curso, podem ser formalizados de modo gradual.

A ênfase na comunicação do que cada movimento “faz” à posição contribui para que os estudantes comparem caminhos, avaliem decisões e justifiquem por que determinadas tentativas não alcançam o efeito desejado. Com isso, o jogo deixa de ser mera ocupação para converter-se em prática de estudo: observar, registrar, argumentar e revisar. Essa orientação está em consonância com a compreensão de que a didática organiza a passagem de finalidades pedagógicas a ações concretas de sala, papel que envolve, entre outros aspectos, a seleção de conteúdos e métodos e a vinculação entre ensino e aprendizagem (LIBÂNEO, 2013).

4.7 RECOMENDAÇÕES FINAIS AO(À) PROFESSOR(A)

Selecionar posições iniciais compatíveis com o tempo disponível; explicitar, no início de cada aula, o que será considerado um bom registro textual; manter perguntas de sondagem que obriguem a explicitar razões e não apenas procedimentos; ajustar a exigência de registro à complexidade da posição; promover socializações breves e frequentes, nas quais diferentes grupos exponham como descreveram e compuseram transformações.

NOTAS INTRODUTÓRIAS AO ESTUDO DOS SÓLIDOS PLATÔNICOS

Neste capítulo propõe-se apresentar, através de alguns exemplos, a estrutura de grupos de forma visual e geométrica. Salienta-se, que não se propõe o conceito formal de grupo na educação básica; considera-se suficiente, que o professor domine a estrutura, uma vez que ela organiza com precisão as simetrias de polígonos e poliedros, favorecendo um tratamento conceitual consistente e uma comunicação mais clara em sala de aula.

Este capítulo baseia-se principalmente no artigo [3], no qual são apresentados exemplos de grupos finitos por meio das simetrias de polígonos regulares e das rotações dos sólidos platônicos. A partir dessa referência, retomamos e adaptamos as ideias centrais para sustentar a abordagem geométrica das estruturas de grupo discutidas aqui.

Grupos cíclicos em polígonos regulares

Seja $n \in \mathbb{N}$. Considere um n -ágono regular no plano e as rotações em torno de seu centro. Denotamos por C_n o conjunto formado por todas as rotações de ângulo $2\pi k/n$, com $k \in \{0, \dots, n-1\}$. Nesse conjunto, faremos a inclusão da rotação de ângulo 0 (a transformação que deixa o polígono na mesma posição), denominada rotação trivial. A rotação de ângulo $2\pi/n$ funciona como um gerador de C_n , pois composições sucessivas dessa rotação produzem todas as demais. Se denotarmos a rotação $2\pi/n$ por a , e utilizaremos a notação multiplicativa para a composição, podemos escrever:

$$C_n = \{a^k \mid k \in \{0, \dots, n-1\}\}.$$

O caso diedral: rotações e reflexões

Incorporando também as reflexões em relação a retas adequadas, obtém-se o grupo diedral. Para tornar a descrição concreta, considere uma figura quadrada. Com base na Figura 7, é possível identificar quatro eixos de reflexão, $\overleftrightarrow{AC}$, $\overleftrightarrow{BD}$, $\overleftrightarrow{HF}$ e $\overleftrightarrow{EG}$, de onde percebemos a existência de quatro tipos de reflexões. Acrescentando as quatro rotações possíveis (de ângulos 0° , 90° , 180° e 270°), obtemos o conjunto dos oito movimentos que compõem as simetrias do quadrado.

Observe que a rotação de 90° e uma única reflexão, em relação ao eixo $\overleftrightarrow{EG}$, geram todo o conjunto de simetrias. Denotando por a a rotação de 90° , no sentido anti-horário, e por b a reflexão em relação a $\overleftrightarrow{EG}$, qualquer outra rotação ou reflexão do quadrado pode

ser obtida por composições apropriadas de a e b . A reflexão em relação a $\overleftrightarrow{AC}$ coincide com a composição ab : efetuar primeiro b e, em seguida, a produz o mesmo efeito sobre os vértices que refletir diretamente em $\overleftrightarrow{AC}$. Perceba que as posições de A e C continuam fixadas, enquanto as de B e D são trocadas.

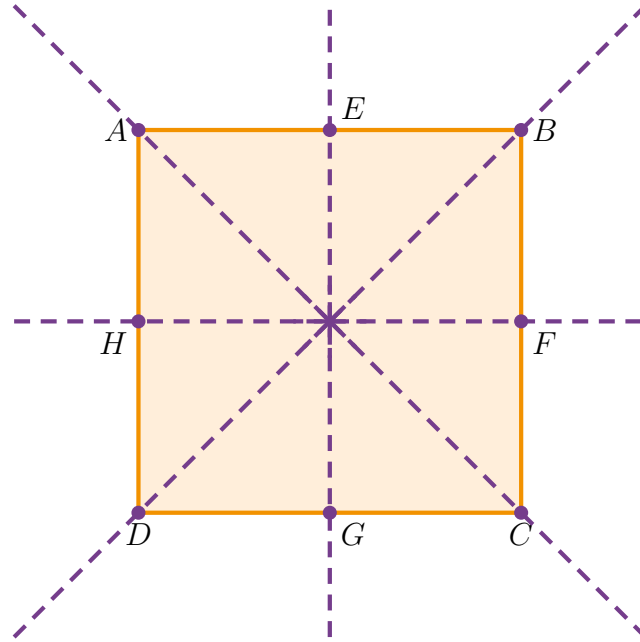


Figura 7: Os eixos de reflexão de um quadrado.

O grupo diedral no quadrado e o caso geral

No caso do quadrado, a reflexão em relação à diagonal $\overleftrightarrow{AC}$ pode ser obtida pela composição de uma reflexão b com a rotação a (no sentido anti-horário), o que denotamos por ab . De maneira análoga conseguimos obter as demais simetrias:

$$D_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\},$$

o qual recebe o nome de *grupo diedral*. O termo 4 indica o número de lados do polígono em questão, e o símbolo 1 representa a rotação trivial.

Para um n -ágono regular, o raciocínio se generaliza e resulta em

$$D_n = \{1, a, a^2, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\},$$

em que a denota a rotação de ângulo $2\pi/n$ e b representa uma reflexão em relação a um eixo fixo, que aqui tomamos como o eixo vertical.

5.1 SÓLIDOS PLATÔNICOS

Agora passamos a objetos tridimensionais com alto grau de simetria. Os exemplos emblemáticos são os cinco *sólidos platônicos*: tetraedro, cubo, octaedro, dodecaedro e icosaedro.

Esses poliedros serão a base para discutir grupos além dos cíclicos e dos diedrais, mostrando como as rotações em três dimensões organizam-se em estruturas ricas.

5.1.1 Definições e caracterização dos sólidos platônicos

Definiremos com certo grau de precisão o que se entende por *sólidos platônicos* e será apresentado algumas ideias para sua classificação.

Nesse momento pressupomos que o leitor já esteja familiarizado com o conceito de poliedro. É válido salientar que os termos sólido e poliedro serão empregados sem distinção, pois as ideias permanecem as mesmas quer consideremos o objeto como oco (apenas a casca) quer como maciço. Utilizaremos alguns exemplos clássicos, como o cubo, a pirâmide, o prisma ou o icosaedro.

Um poliedro possui faces, arestas representadas por segmentos de reta e vértices, podendo ser caracterizado, em certa forma, pela quantidade e pelo tipo desses elementos. Assim, ao descrever um icosaedro, é convencional mencionar que ele é formado por 20 faces triangulares regulares. Com vistas à construção de objetos com alto grau de simetria, denomina-se *sólido platônico* todo poliedro convexo cujas faces são formadas por polígonos regulares congruentes e o número de faces que se encontram em cada vértice é constante.

Se as faces são polígonos de n lados e m faces concorrem em cada vértice, analisam-se os possíveis valores do par ordenado (m, n) . Como estamos lidando com um sólido convexo, essa condição impõe restrições aos pares (m, n) , a partir das quais se obtém a classificação almejada.

A desigualdade no vértice e a forma $(m - 2)(n - 2) < 4$

Seja α_n o ângulo interno de um n -ágono regular:

$$\alpha_n = \frac{(n - 2) \cdot 180^\circ}{n}.$$

Considere um poliedro regular convexo cujas faces são n -gonos regulares e suponha que em cada vértice concorrem exatamente m faces. A condição de convexidade implica que a soma dos ângulos planos incidentes em torno de um vértice é *estritamente* menor que 360° , isto é,

$$m \alpha_n < 360^\circ.$$

Substituindo a expressão de α_n :

$$m \cdot \frac{(n - 2) \cdot 180^\circ}{n} < 360^\circ.$$

Dividindo ambos os lados por 180° e reorganiza:

$$\begin{aligned} m \cdot \frac{n-2}{n} < 2 &\Rightarrow m(n-2) < 2n \Rightarrow mn - 2m < 2n \\ &\Rightarrow mn - 2m - 2n < 0. \end{aligned}$$

Uma forma conveniente é escrever isso como

$$(m-2)(n-2) < 4.$$

De fato,

$$(m-2)(n-2) = mn - 2m - 2n + 4,$$

logo $mn - 2m - 2n < 0$ é equivalente a $(m-2)(n-2) < 4$.

Observa-se que, se $n = 2$, a condição é satisfeita para qualquer $m > 0$; e, simetricamente, se $m = 2$, qualquer $n > 0$ verifica a desigualdade. Excluídos os casos degenerados $m = 1$ ou $n = 1$, os pares que satisfazem com $m, n \geq 2$ são:

$$(m, 2), \quad (2, n), \quad (3, 3), \quad (3, 4), \quad (4, 3), \quad (3, 5), \quad (5, 3).$$

Embora não existam polígonos de dois lados no plano euclidiano, admite-se, para fins de visualização sobre a esfera, um “2-ágono regular” como a figura determinada por dois arcos geodésicos congruentes ligando os mesmos dois pontos (os “vértices”), de modo a formar uma faixa esférica. Nessa convenção:

- O caso $(m, 2)$ dá origem ao *hosoedro*: pode-se concebê-lo como a colagem de m dessas faixas esféricas, cujas bordas unem dois polos; os dois polos funcionam como vértices e cada faixa corresponde a uma “face” com duas “arestas”.
- O caso $(2, n)$ produz o *diedro*: Apenas duas faces se encontram em cada vértice; uma realização simples é formada por duas semiesferas (as faces), enquanto os n vértices se distribuem uniformemente no equador.

Ainda que *hosoedros* e *diedros* não sejam considerados poliedros convexos no sentido adotado nesta dissertação, eles se mostram úteis para organizar intuições e, adiante, oferecer uma visualização alternativa para os grupos do tipo diedral.

Pelos argumentos anteriores, concluímos que existem exatamente cinco possibilidades não degeneradas para o par (m, n) , e pode-se demonstrar que cada uma delas determina um único poliedro convexo regular. Dessa forma, obtêm-se os cinco *sólidos platônicos*. Para fins de síntese, reúne-se abaixo a contagem de faces, arestas e vértices tanto desses casos quanto dos dois limites esféricos discutidos anteriormente.

A partir da Tabela 1, observam-se relações de dualidade: hosoedro e diedro são duais entre si; o cubo é dual do octaedro; o dodecaedro é dual do icosaedro. Em termos geométricos, dadas as faces de um poliedro, tomam-se os seus centros como novos vértices e conectam-se centros de faces adjacentes para formar o poliedro dual. Não é casual,

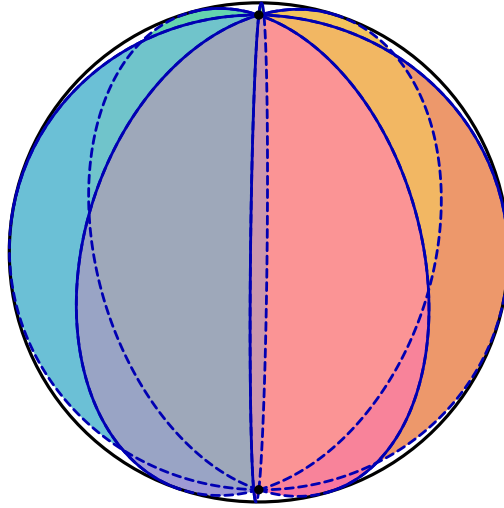


Figura 8: Hossoedro com oito faces.

Tabela 1: Contagem de faces, arestas e vértices em poliedros regulares (incluindo casos-limite).

(m, n)	Poliedro	Faces	Arestas	Vértices
$(2, n)$	diedro	2	n	n
$(m, 2)$	hossoedro	m	m	2
$(3, 3)$	tetraedro	4	6	4
$(3, 4)$	cubo	6	12	8
$(4, 3)$	octaedro	8	12	6
$(3, 5)$	dodecaedro	12	30	20
$(5, 3)$	icosaedro	20	30	12

portanto, que o número de vértices do cubo coincida com o número de faces do octaedro, e que fenômeno análogo ocorra para o par dodecaedro–icosaedro.

5.1.2 O grupo de rotações do tetraedro

Agora, denotemos por T o grupo de rotações do tetraedro regular. Identificando os vértices por 1, 2, 3, 4, cada rotação determina uma permutação desses rótulos; assim, podemos enxergar T como subgrupo de S_4 . Vale ressaltar que $A_4 \subseteq T$, onde $A_4 \subset S_4$ é o subgrupo das permutações pares; seus elementos são de dois tipos:

- **3-ciclos.** Podem ser realizados por rotações de 120° em torno do eixo que une um vértice ao centro da face oposta. Por exemplo, tomando a face $\{1, 2, 3\}$ apoiada sobre um plano horizontal, uma rotação de 120° em torno do eixo vertical produz a permutação (123) ; uma segunda rotação de 120° produz (132) .
- **Produtos de dois 2-ciclos independentes.** São obtidos por rotações de 180° em torno do eixo que une os pontos médios de *arestas opostas*. A transformação ilustrada por $(12)(34)$ é um exemplo típico desse tipo.

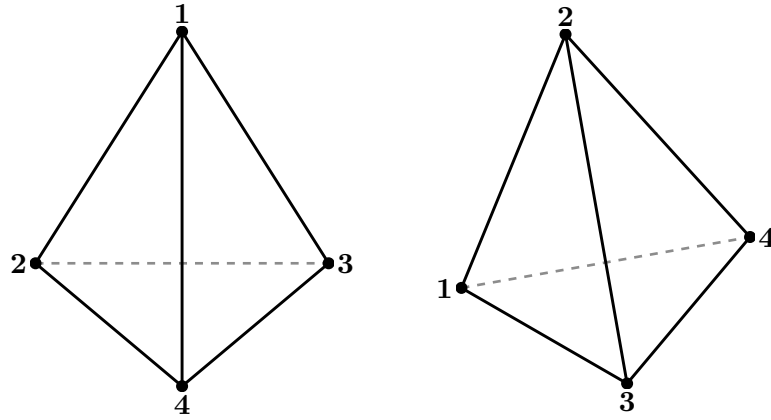


Figura 9: Tetraedros: a rotação $(12)(34) \in T$. Painel da direita com menor inclinação e topo alinhado.

Para concluir, note-se que uma permutação ímpar, como (12) , *não* pode ser realizada por qualquer rotação do tetraedro: fixando 3 e 4, a única isometria que preserva o sólido e o envia a si mesmo seria uma rotação em torno do eixo que passa por esses vértices; todavia, essa rotação troca simultaneamente 1 e 2 (quando o ângulo é 180°) ou produz um 3-ciclo envolvendo 1, 2 e um dos vértices fixados (quando o ângulo é 120°), nunca ocorrendo a transposição isolada (12) . Em particular, todas as rotações são *pares*, de modo que $T \subseteq A_4$. Combinando as inclusões $A_4 \subseteq T$ e $T \subseteq A_4$, obtém-se $T = A_4$. Além disso, $A_4 \subsetneq S_4$, uma vez que $|S_4|/|A_4| = 2$.

Para explicitar a operação interna, pode-se organizar a *tábua de multiplicação* de A_4 (tabela 2): as linhas e colunas representam as permutações do grupo (ou, de modo equivalente, as rotações do tetraedro), e cada entrada registra a composição entre os elementos da linha e da coluna. Essa tabela ilustra como os 12 elementos - a identidade, os três produtos de dois 2-ciclos independentes e os oito 3-ciclos - interagem sob composição.

A_4	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9	σ_{10}	σ_{11}	σ_{12}
$(1) = \sigma_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \sigma_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \sigma_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \sigma_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \sigma_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \sigma_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \sigma_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \sigma_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \sigma_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \sigma_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \sigma_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \sigma_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

Tabela 2: Tabela de Cayley do grupo A_4 com a enumeração $\sigma_1, \dots, \sigma_{12}$.

5.1.3 O grupo de rotações do cubo

Denotemos por O o grupo de rotações do cubo (em referência ao seu dual, o octaedro). Embora seja possível vê-lo como subgrupo de S_8 ao rotular os oito vértices, a análise torna-se mais transparente quando se acompanha a ação sobre as diagonais (isto é, os pares de vértices opostos). Para fixar uma convenção, considere o cubo apoiado sobre uma mesa e rotule os vértices da face superior, em sentido anti-horário, por 1, 2, 3, 4. Cada um desses vértices determina de modo único uma diagonal; A seguir, descrevem-se os três tipos de rotações relevantes e como eles permutam tais diagonais.

- **Eixo que liga os centros de duas faces opostas.** Em torno desse eixo, o cubo permite rotações de 90° (e seus múltiplos). Observando a ação sobre as quatro diagonais do corpo, esses giros aparecem como *ciclos de comprimento 4*. Por exemplo, escolhendo o eixo vertical, uma rotação de 90° no sentido anti-horário pode ser registrada pela permutação (1423); ao aplicar mais 90° , obtém-se (12)(34); e, com mais 90° , resulta (1324).

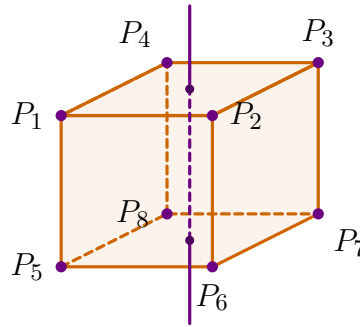


Figura 10: Cubo com os oito vértices e reta passando pelos centros de duas faces opostas.

- **Eixo que passa por dois vértices opostos.** Para esse eixo, rotações de 120° (ou de 240°) geram *ciclos de comprimento 3* na ação sobre as diagonais do corpo. A ideia é que o eixo coincide com uma das diagonais, que permanece fixa, enquanto as outras três são permutadas ciclicamente. Assim, em um sentido, um giro de 120° pode produzir, por exemplo, (234); e no sentido contrário (equivalente a 240°), obtém-se (243).
- **Eixo que une os pontos médios de duas arestas opostas.** Nesse caso, a rotação relevante é a de 180° , que mantém duas diagonais invariantes e troca as outras duas. No registro por permutações, isso aparece como uma transposição, por exemplo (14) (com as demais diagonais fixas).

Com as três famílias de eixos descritas (centros de faces opostas, vértices opostos e pontos médios de arestas opostas), verifica-se que toda rotação do cubo induz uma

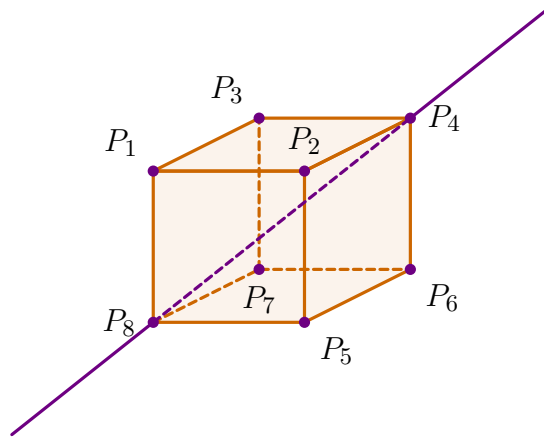


Figura 11: Cubo com a diagonal espacial determinada por dois vértices opostos.

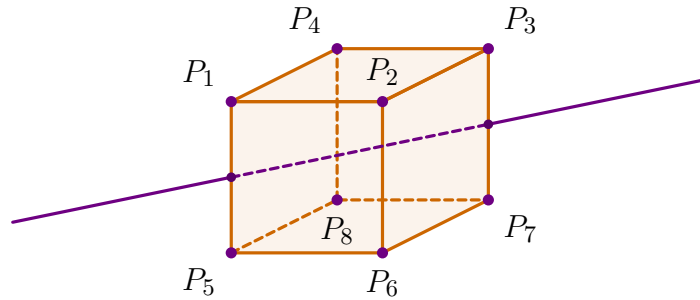


Figura 12: Reta determinada pelos pontos médios de duas arestas opostas do cubo.

permutação das quatro diagonais do corpo. Reciprocamente, cada permutação dessas diagonais é realizada por uma única rotação do sólido; caso duas rotações distintas agissem de modo igual nas diagonais, também coincidiriam na permutação dos vértices, o que não ocorre.

Dessa forma, por meio da ação natural sobre as diagonais do corpo, estabelece-se uma identificação entre o grupo de rotações do cubo O e o grupo simétrico em quatro letras: em particular, mediante um rotulamento fixo das diagonais, pode-se considerar $O \cong S_4$ (e, nessa identificação, escrever $O = S_4$).

Rotação de 180° e ação nas diagonais

No cenário em que o eixo de rotação une os pontos médios de duas arestas opostas do cubo, a rotação de 180° induz a transposição de duas diagonais do corpo e mantém as demais fixas. Em termos de rotulamento, se designarmos por V_1V_5 e V_3V_7 as diagonais trocadas, obtém-se a permutação (13) nas quatro diagonais, ao passo que as outras duas permanecem inalteradas.

TETRAEDROS INSCRITOS E INCLUSÕES DE GRUPOS

Uma visualização alternativa decorre do fato de que é possível inscrever *dois* tetraedros regulares no cubo de modo que seus vértices coincidam com vértices do cubo. Como toda rotação de um tetraedro é, ao mesmo tempo, rotação do cubo, segue a inclusão

$$A_4 = T \subset O,$$

onde T denota o grupo de rotações do tetraedro e O o do cubo. Além disso, ao permutar-se os dois tetraedros inscritos, obtém-se uma permutação *ímpar* no conjunto das diagonais do corpo; dessa forma, conclui-se que $A_4 \subsetneq O \subseteq S_4$.

5.1.4 O grupo de rotações do dodecaedro

Por referência ao dual (o icosaedro), denotaremos o grupo de rotações do dodecaedro por I . Assim como nos casos anteriores, as rotações possíveis organizam-se em torno de três famílias de eixos:

- **Eixo pelos centros de faces opostas.** Como cada face é um pentágono regular, as rotações em torno desse eixo são de ordem 5 (ângulos 72° , 144° , 216° e 288°). Existem 6 pares de faces opostas, o que perfaz $4 \cdot 6 = 24$ rotações não triviais desse tipo.
- **Eixo que une vértices opostos.** Nesse caso, as rotações são de ordem 3 (ângulos 120° e 240°). Como o dodecaedro possui 10 pares de vértices opostos, contam-se $2 \cdot 10 = 20$ rotações não triviais desta família.

Há, ainda, a família de eixos que unem os centros de duas arestas opostas do dodecaedro. As rotações correspondentes têm ângulo 180° e, portanto, ordem 2. Como existem 15 pares de arestas opostas, contam-se 15 rotações não triviais desse tipo.

Somando-se às demais famílias e à rotação trivial, obtém-se:

$$1 + 24 + 20 + 15 = 60,$$

isto é,

$$|I| = 60,$$

onde I denota o grupo de rotações do dodecaedro.

Para caracterizar I por meio de uma ação de permutação, considera-se a decomposição interna do dodecaedro em *cinco* tetraedros regulares mutuamente posicionados. Cada rotação do dodecaedro induz, de modo unívoco, uma permutação desse conjunto de cinco tetraedros; segue, então, a inclusão

$$I \subseteq S_5.$$

Por outro lado, as rotações de um tetraedro inscrito também são rotações do dodecaedro; à luz do que foi estabelecido para o tetraedro, tem-se $T = A_4 \subset I$, onde T é o grupo de rotações do tetraedro. Além disso, uma rotação de ordem 5 no dodecaedro atua ciclicamente sobre os cinco tetraedros, de modo que o subgrupo cíclico

$$C_5 = \langle (12345) \rangle$$

está contido em I .

Dessas observações, conclui-se que o produto de grupos $A_4 \cdot C_5$ encontra-se contido em I . Como

$$|A_4 \cdot C_5| = 60,$$

segue imediatamente que

$$I = A_4 \cdot C_5.$$

Note-se, ainda, que $A_4, C_5 \subset A_5$ e $|A_5| = 60$; portanto,

$$A_5 = A_4 \cdot C_5 = I.$$

Assim, o grupo de rotações do dodecaedro (e, por dualidade, do icosaedro) é isomorfo a A_5 .

5.2 CONSIDERAÇÕES FINAIS

Para sintetizar a análise desenvolvida, registra-se, na Tabela 3, as *ordens* das rotações de cada grupo. Adota-se a seguinte convenção de notação:

- n_1 : ordem da rotação cujo eixo passa por dois *vértices opostos*;
- n_2 : ordem da rotação cujo eixo passa pelos *pontos médios de duas arestas opostas*.

Adota-se a seguinte notação: n_1 é a ordem da rotação cujo eixo passa por vértices opostos; n_2 corresponde ao eixo que une os pontos médios de arestas opostas; e n_3 refere-se ao eixo que liga os centros de faces opostas. Entretanto, essa convenção precisa ser ajustada em três situações específicas:

- **Tetraedro:** como não há pares de vértices ou faces opostas, toma-se n_1 como a ordem da rotação em torno do eixo que passa por um vértice e pelo centro da face oposta. Mantém-se n_2 inalterado e define-se $n_3 = n_1$.
- **Diedro, com n ímpar:** não existem pares de vértices ou arestas opostas. Define-se n_1 usando o eixo que passa por um vértice e pelo ponto médio da aresta oposta; nessa configuração, $n_2 = n_1$ e n_3 permanece como anteriormente.

- **Hosoedro, com m ímpar:** não há pares de arestas ou faces opostas. Mantém-se n_1 ; toma-se n_2 como a ordem da rotação cujo eixo passa pelo ponto médio de uma aresta e pelo centro da “face” oposta; por simetria, $n_3 = n_2$.

Registre-se, ademais, que as ordens de rotação do hosoedro, do octaedro e do icosaedro podem ser deduzidas por dualidade, conforme discutido anteriormente.

Tabela 3: Grupos de rotações dos sólidos considerados. Aqui, $|G|$ denota a ordem do grupo G .

G	$ G $	n_1	n_2	n_3
Diedro D_n	$2n$	2	2	n
Hosoedro D_m	$2m$	m	2	2
Tetraedro A_4	12	3	2	3
Cubo S_4	24	3	2	4
Octaedro S_4	24	4	2	3
Dodecaedro A_5	60	3	2	5
Icosaedro A_5	60	5	2	3

OS SÓLIDOS PLATÔNICOS NA SALA DE AULA: POR QUÊ E PARA QUÊ?

Como prática de investigação estruturada por regras e metas, a exploração de simetrias de sólidos oferece um contexto significativo de resolução de problemas, no qual hipóteses podem ser testadas, comparadas e justificadas. Em ambiente escolar, seu potencial se realiza quando há intencionalidade pedagógica: o professor seleciona tarefas, orienta registros, promove comparações entre estratégias e convida os estudantes a explicarem “por que funcionou”. Nesta proposta, os sólidos platônicos cumprem esse papel ao tornar visível a ideia de *grupo de simetrias*: as movimentações que preservam o sólido (rotações e, quando conveniente, reflexões, conforme o recorte didático) podem ser descritas como transformações que se compõem, possuem identidade e admitem inversos. O percurso articula observação, registro e composição de movimentos, conectando ações concretas a uma linguagem básica de permutações.

Considerando os anos finais do Ensino Fundamental, essa proposta também pode ser relacionada a habilidades da BNCC que envolvem a observação e a descrição de propriedades dos sólidos, a análise de transformações e a organização de procedimentos. Em particular, aproxima-se de EF06MA17 e EF06MA18, ao mobilizar a identificação e a comparação de faces, vértices e arestas dos poliedros explorados; de EF06MA23, ao exigir que os estudantes organizem e registrem sequências de ações para realizar e descrever movimentos; de EF07MA21, ao favorecer o estudo de rotações e outras simetrias como transformações que preservam a forma do sólido; e de EF08MA18, ao permitir que composições de movimentos sejam interpretadas e analisadas como composições de transformações. Desse modo, a exploração dos sólidos platônicos em sala de aula não se limita à manipulação concreta de objetos, mas constitui uma situação pedagógica em que os estudantes observam regularidades, comparam estratégias, justificam resultados e atribuem sentido matemático às ações realizadas [2].

PROCESSO DE ENSINO

O trabalho organiza-se em três momentos encadeados: lançamento do problema, investigação orientada e sistematização compartilhada. Primeiro, apresenta-se um desafio concreto: “quais movimentos deixam o sólido com a mesma aparência? como registrar essas mudanças de modo que outra pessoa consiga repetir?”. Em seguida, os grupos investigam com regras de registro: escolhem um sólido, definem uma numeração para suas faces (ou vértices) e descrevem o efeito de rotações sobre esses rótulos. O professor circula, observa e

intervém com perguntas que ampliam a análise (“o que ficou no lugar? o que trocou?”, “qual movimento desfaz este?”, “se eu fizer um depois do outro, qual é o efeito final?”). Por fim, a turma discute padrões percebidos e constrói um vocabulário comum para descrever transformações: identidade, inverso, composição e a noção de que cada movimento pode ser registrado como uma permutação dos rótulos.

OBSERVAÇÃO PRÁTICA SOBRE ESCOLHA DE SÓLIDOS. Embora a sequência seja desenhada para ser usada com qualquer sólido platônico, o cubo e o tetraedro são particularmente indicados no início por permitirem perceber e registrar rotações com mais facilidade, além de produzirem descrições curtas e visualmente controláveis. Após estabilizar a notação com esses casos, a turma pode generalizar o procedimento para octaedro, dodecaedro e icosaedro.

APRENDIZAGEM

O foco é aprender com a investigação e com a comunicação de ideias, e não medir desempenho. Adotam-se práticas de acompanhamento leve: registros de grupo, breves discussões de metacognição (“que representação ajudou?”) e devolutivas orais do professor. A exploração sustenta aprendizagem porque envolve regras de registro, tomada de decisão e explicação de estratégias; com mediação adequada, converte-se em contexto para construir a ideia de grupo como “coleção de movimentos que se combinam” e para desenvolver o básico de notação por permutações.

6.1 VISÃO GERAL DA SEQUÊNCIA

1. **Desafio inicial:** apresentar um sólido e perguntar quais movimentos preservam sua forma e sua aparência global; solicitar previsões sobre como registrar essas mudanças sem desenhar cada etapa.
2. **Exploração orientada:** em duplas/grupos, escolher um sólido (preferencialmente cubo ou tetraedro no início), fixar uma numeração nas faces (ou nos vértices) e realizar rotações controladas, registrando:
 - (a) o movimento executado (por exemplo, “rotacionar em torno do eixo que passa pelo centro de uma face”, ou “girar em torno de um vértice”);
 - (b) o efeito do movimento nos rótulos: “para onde foi cada face” (ou cada vértice), em forma de lista organizada.
3. Conjecturas sobre fechamento e inversos: incentivar a busca do movimento que desfaz outro (“qual rotação reverte esta?”) e discutir por que certos movimentos, quando

repetidos, retornam ao ponto inicial, introduzindo a ideia de identidade e de ordem do elemento.

4. Sistematização acessível: nomear dois modos de representar uma transformação: (i) uma tabela de envio “rótulo original $\rightarrow$ rótulo final” e (ii) a escrita por ciclos; explicitar que compor movimentos significa “fazer um depois do outro” e descrever o efeito final aplicando primeiro a segunda ação e depois a primeira, de modo consistente.
5. Preparação para a aula seguinte: combinar que, na próxima etapa, essas descrições serão conectadas explicitamente ao grupo de permutações: cada rotação vira uma permutação dos rótulos e o conjunto dessas permutações forma um grupo pelo critério de fechamento, identidade, inverso e associatividade.

Objetivo central declarado aos estudantes: construir um conjunto de movimentos do sólido que preservam sua forma, registrar cada movimento como uma permutação de faces (ou vértices), e compor movimentos verificando o efeito final, desenvolvendo o básico de notação e de leitura de transformações.

6.2 FUNDAMENTAÇÃO PEDAGÓGICA

Esta proposta entende a geometria espacial como campo fértil para investigação: manipular, registrar, comparar e justificar. A centralidade recai sobre a mediação docente, que articula objetivos, conteúdos, tarefas e formas de acompanhamento da aprendizagem, convertendo finalidades educacionais em ações de sala de aula. O recorte conceitual é o desenvolvimento inicial da linguagem de grupo por meio de permutações: em vez de começar por definições abstratas, parte-se de movimentos concretos e de seus registros, estabilizando progressivamente um vocabulário comum.

Os sólidos platônicos oferecem um problema autêntico e investigável, no qual os estudantes podem observar que as rotações preservam o objeto, mas reorganizam a posição de faces e vértices. Ao numerar esses elementos e acompanhar seu deslocamento, a turma passa a representar movimentos como permutações e a compreender composição como “fazer uma transformação depois da outra”. A sequência evita formalismo excessivo no início e foca na descrição em palavras e em registros organizados, preparando posteriormente a formalização em notação simbólica.

OBJETIVOS DE APRENDIZAGEM

1. Identificar faces, arestas e vértices em um sólido platônico e estabelecer uma numeração consistente para faces ou vértices.
2. Reconhecer rotações como movimentos que preservam o sólido e descrever, em linguagem comum, o que cada rotação faz com os rótulos escolhidos.

3. Representar uma rotação em dois modos de registro: uma lista organizada “original $\rightarrow$ final” e a forma por ciclos, desenvolvendo o básico da notação.
4. Compor rotações, isto é, aplicar uma depois da outra e descrever o efeito resultante nos rótulos, mantendo a convenção de leitura da direita para a esquerda.
5. Identificar, em exemplos, a identidade e o inverso de um movimento, relacionando-os ao retorno ao estado inicial e ao “desfazer” uma rotação.

RECURSOS E ORGANIZAÇÃO

Modelos físicos de sólidos platônicos (preferencialmente cubo e tetraedro para início); etiquetas removíveis ou canetas para marcar faces/vértices; fichas de registro; cartões com exemplos de escrita “original $\rightarrow$ final” e por ciclos; quadro para sínteses. Recomenda-se trabalho em duplas ou trios, com rodízio de papéis: quem executa a rotação, quem observa e narra, quem registra.

METODOLOGIA E PAPÉIS

A condução assume três momentos encadeados: lançamento do problema, investigação orientada e sistematização. O professor provoca a explicitação de estratégias e justificativas, incentiva a comparação entre registros dos grupos e organiza o vocabulário comum. O acompanhamento ocorre por meio de registros escritos, sínteses orais e perguntas de sondagem, sem atribuição de nota.

6.3 ROTEIRO DA AULA 1

1. Abertura: apresentar um cubo ou um tetraedro e perguntar quais movimentos deixam o sólido “o mesmo”; recolher hipóteses sobre que informações precisam ser registradas para descrever uma rotação.
2. Exploração em grupos: numerar faces (ou vértices) e executar rotações curtas e controladas, escolhidas pelo grupo.
3. Registro guiado: para cada rotação, anotar o movimento em palavras e registrar o envio dos rótulos (“a face 1 foi para o lugar da 3”, etc.) em lista organizada.
4. Discussão de composição: escolher duas rotações realizadas e investigar o que acontece quando uma é feita depois da outra; comparar o resultado com a ordem invertida.

5. Sistematização parcial: construir coletivamente um glossário de termos de sala (rotação, transformação, composição, identidade como não mexer, inverso como desfazer) e registrar um exemplo curto nos dois modos de escrita (lista organizada e ciclos).

NOTA PRÁTICA SOBRE O REGISTRO. Em sólidos com muitas faces, o registro completo pode se tornar impraticável no início. Ajuste a exigência:

- no cubo e no tetraedro, solicitar registro completo dos rótulos;
- em sólidos mais complexos, permitir registro por subconjuntos (por exemplo, apenas faces afetadas) e depois ampliar para o registro completo quando a notação estiver estabilizada.

Em qualquer caso, prioriza-se a clareza e a consistência da convenção escolhida.

ENCAMINHAMENTOS PARA O PROFESSOR

Selecionar previamente o sólido inicial (cubo ou tetraedro) e preparar uma numeração padrão para facilitar comparações entre grupos. Preparar cartões de apoio com frases-modelo de descrição (“girei em torno deste eixo”, “estas faces formaram um ciclo”) e com exemplos de composição. Planejar perguntas de sondagem que ajudem os estudantes a explicitar por que a ordem importa e como identificar o inverso.

6.4 ROTEIRO DA AULA 2

1 - Retomada (5–10 min)

Recuperar termos de sala construídos na aula anterior: rotação, transformação, composição, identidade, inverso. Revisitar rapidamente um registro do cubo ou do tetraedro em lista organizada e por ciclos.

Consolidação guiada (15–20 min)

1. Tomar uma rotação padrão do sólido escolhido e reconstruir coletivamente seu registro como permutação dos rótulos.
2. Discutir como encontrar o inverso: “o que desfaz este movimento?” e verificar por composição que o resultado é a identidade.
3. Introduzir explicitamente a ideia de que o conjunto das rotações registradas pode ser visto como um conjunto de permutações, no qual a operação é a composição.
4. Destacar a convenção de leitura: ao compor duas rotações, aplica-se primeiro a segunda e depois a primeira, verificando o efeito final nos rótulos.

Prática em grupos (15–20 min)

1. Cada grupo escolhe três rotações do seu sólido e registra:
 - (a) a lista organizada “original $\rightarrow$ final”;
 - (b) a mesma rotação em forma por ciclos;
 - (c) o inverso de pelo menos uma delas e a verificação de que a composição resulta na identidade.
2. Orientações de registro:
 - Indicar claramente a convenção de numeração (faces ou vértices) e mantê-la fixa.
 - Registrar o movimento em palavras antes da notação, garantindo que a descrição seja reproduzível.

Socialização e síntese

Cada grupo apresenta um exemplo curto de composição de rotações, explicitando:

- o que cada rotação fazia isoladamente;
- o que mudou quando uma foi feita depois da outra;
- como isso apareceu na lista organizada e na forma por ciclos.

Produzir, no quadro, uma síntese com três colunas: movimento em palavras; registro em lista organizada; registro por ciclos; e uma linha final indicando a composição.

NOTA PRÁTICA Quando a complexidade for alta, priorizar clareza e justificativa em vez de exaustividade. O objetivo é que os estudantes compreendam e comuniquem *o que* cada rotação faz com os rótulos e *como* a composição determina o efeito final.

ESTRATÉGIAS DE MEDIAÇÃO (PERGUNTAS-GUIA)

- O que permanece no lugar nesta rotação e o que muda?
- Como você descreveria este movimento para alguém que não está vendo o sólido?
- Qual rotação desfaz esta? Como verificar pela composição?
- Se você fizer as duas rotações em ordem invertida, o efeito final muda? Onde isso aparece no registro?
- Como transformar sua lista organizada em uma escrita por ciclos mais compacta?

DIFERENCIAÇÃO E ACESSIBILIDADE

- Modelos em alto contraste, marcações táteis e possibilidade de manipulação lenta para estudantes com necessidades específicas.
- Tempos estendidos para registro, ou permissão de gravação de áudio como rascunho oral antes da versão escrita.
- Desafios graduados: do cubo e tetraedro (registro completo) aos demais sólidos (registro por partes e posterior ampliação).

Folha de registro do grupo

1. Numeração adotada (faces ou vértices) e desenho simples indicando os rótulos.
2. Três rotações descritas em palavras e registradas como lista organizada “original $\rightarrow$ final”.
3. As mesmas rotações escritas por ciclos.
4. Um exemplo de inverso e a verificação de que a composição produz a identidade.
5. Observações: o que a composição mostrou sobre a importância da ordem.

Cartões-modelo de frases

- “Depois da rotação, a face que estava no lugar X foi para o lugar Y.”
- “O efeito final pode ser descrito como uma volta entre as faces (X, Y, Z).”
- “O inverso é o movimento que desfaz a rotação, retornando todos os rótulos ao lugar inicial.”

Roteiro do(a) professor(a) para sistematização

- Indicar com clareza a passagem do movimento concreto para o registro organizado.
- Solicitar descrição em palavras antes da notação por permutação, estabilizando significado.
- Reforçar a convenção de composição e comparar ordens diferentes com exemplos curtos.

6.5 MATERIAIS DE APLICAÇÃO E ANEXOS DIDÁTICOS

1 Folha de atividade para estudantes (modelo imprimível)

PARTE A — EXPLORAÇÃO DE ROTAÇÕES

1. Numere as faces (ou os vértices) do sólido escolhido e registre essa numeração.
2. Execute uma rotação simples e descreva-a em palavras.
3. Registre o efeito do movimento como lista organizada “original $\rightarrow$ final”.
4. Reescreva o mesmo efeito em forma por ciclos, indicando as “voltas” entre os rótulos.

PARTE B — COMPOSIÇÃO

1. Escolha duas rotações já realizadas. Descreva cada uma em palavras e registre sua permutação.
2. Agora faça a segunda depois da primeira e registre o efeito final.
3. Explique, em palavras, por que a ordem das rotações pode alterar o resultado.

PARTE C — IDENTIDADE E INVERSO

1. Identifique um movimento que não muda o sólido (identidade) e registre-o.
2. Escolha uma rotação e encontre seu inverso. Verifique pela composição que o resultado é a identidade.

2. ROTEIRO DE MEDIAÇÃO PARA O(A) PROFESSOR(A)

ANTES DA AULA Selecionar cubo ou tetraedro como ponto de partida, preparar numeração padrão e exemplos de rotações. Planejar perguntas de sondagem alinhadas aos objetivos.

DURANTE A EXPLORAÇÃO

- Solicitar previsões: “qual face vai para onde?”
- Pedir que o grupo justifique o registro: “como você sabe que esta face foi para aquele lugar?”
- Incentivar comparação entre grupos e correção de inconsistências de numeração.
- Em casos complexos, permitir registro por faces afetadas e depois ampliar.

NA SISTEMATIZAÇÃO Construir no quadro um exemplo completo: rotação em palavras, lista organizada, ciclos e composição com outra rotação, destacando identidade e inverso.

3 Indicadores de aprendizagem observáveis

- Estabelece uma numeração consistente e a mantém ao longo dos registros.
- Descreve rotações em palavras e registra corretamente o efeito nos rótulos.
- Converte lista organizada em ciclos e interpreta ciclos em termos de movimento.
- Compõe duas rotações e prevê o efeito final com base na convenção adotada.
- Identifica identidade e inverso e verifica o resultado por composição.

Considerações didáticas

A organização intencional do ensino orienta a escolha de objetivos, conteúdos e tarefas, bem como os modos de acompanhamento da aprendizagem. Nessa perspectiva, a sequência busca articular finalidades pedagógicas e ações concretas de sala, de modo que os estudantes avancem na compreensão conceitual por meio de experiências planejadas e devidamente mediadas.

6.6 CONCLUSÃO

A proposta desenvolvida ao longo deste material toma as simetrias dos sólidos platônicos como contexto didático para construir, em linguagem acessível, a compreensão de transformações que se compõem, a importância da ordem, e o desenvolvimento inicial da notação por permutações. O percurso privilegia a mediação docente e a organização intencional do ensino, em que objetivos, tarefas e registros se articulam para promover participação ativa e explicações fundamentadas. Ao reduzir o formalismo no início e insistir na clareza das descrições em palavras, cria-se uma ponte entre a experiência concreta de rotações e a ideia de grupo como estrutura de movimentos.

6.7 RECOMENDAÇÕES FINAIS AO(A) PROFESSOR(A)

Selecionar cubo e tetraedro como casos iniciais para estabilizar a notação; explicitar, no início de cada aula, o que será considerado um bom registro; manter perguntas de sondagem que obriguem a explicitar razões e não apenas procedimentos; ajustar a exigência de registro à complexidade do sólido escolhido; promover socializações breves e frequentes, nas quais diferentes grupos exponham como registraram e compuseram rotações.

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] ARMSTRONG, Mark A. *Groups and Symmetry*. New York: Springer-Verlag, 1988. ISBN: 9780387966755.
- [2] BRASIL. Ministério da Educação. *Base Nacional Comum Curricular*. Brasília: MEC, 2018. Disponível em: https://basenacionalcomum.mec.gov.br/images/BNCC_20dez_site.pdf. Acesso em: 10 fev. 2026.
- [3] CRUZ, Guilherme da Costa. *Girando sólidos platônicos ou como visualizar grupos finitos*. *Professor de Matemática Online (PMO)*, v. 11, n. 1, 2023. DOI: 10.21711/2319023x2023/pmo1107.
- [4] DUTENHEFNER, Francisco. *O jogo dos 15*. *Professor de Matemática Online (PMO)*, v. 12, n. 3, 2024. DOI: 10.21711/2319023x2024/pmo1224.
- [5] DUMMIT, David S.; FOOTE, Richard M. *Abstract Algebra*. 3rd ed. Hoboken: John Wiley & Sons, 2004. ISBN: 9780471433347.
- [6] GARCIA, Arnaldo; LEQUAIN, Yves. *Elementos de Álgebra*. 7. ed. Rio de Janeiro: IMPA, 2022. ISBN: 9786589124108.
- [7] GONÇALVES, Adilson. *Introdução à Álgebra*. 6. ed. Rio de Janeiro: IMPA, 2017. ISBN: 9788524404306.
- [8] HERSTEIN, I. N. *Topics in Algebra*. 2nd ed. New York: John Wiley & Sons, 1975. ISBN: 9780471010906.
- [9] LIBÂNEO, José Carlos. *Didática*. 2. ed. São Paulo: Cortez, 2013.