2020: Trabalho de Conclusão de Curso do Mestrado Profissional em Matemática em Rede Nacional
Universidade Federal de São João del-Rei - UFSJ
Sociedade Brasileira de Matemática - SBM

Uso de Grupos nas Transformações Geométricas

Renata Gonçalves de Almeida[1]
Maurício Reis e Silva Junior[2]
Amanda Gonçalves Saraiva Ottoni[3]

Resumo:

Este trabalho tem por objetivo apresentar uma introdução à teoria de grupos. Para alcançar este objetivo foram abordados elementos básicos da estrutura algébrica de grupos e a relação entre a teoria de grupos com algumas transformações geométricas, destacando-se reflexões e rotações. Além disso, é apresentada uma proposta de abordagem deste assunto na estrutura curricular do ensino fundamental.

Palavras-chave: Teoria de grupos, permutações, simetria, diedral, reflexão e rotação.

Abstract: This work aims to present an introduction to group theory. In order to achieve this objective, the basic elements of the product group structure and a relationship between a group theory with some geometric transformations were approached, highlighting reflections and rotations. In addition, it is a proposal to address this issue in the curriculum structure of elementary education.

Keywords: Group theory, permutations, symmetry, dihedral, reflection and rotation.

[1]Aluno de Mestrado Profissional em Matemática em Rede Nacional, Turma 2017
Instituição: Universidade Federal de São João Del-Rei - UFSJ
E-mail: renata_rga@yahoo.com.br
[2]Orientador do Trabalho de Conclusão de Curso
Departamento de Física e Matemática - Defim, CAP-UFSJ
E-mail: mreis@ufsj.edu.br
[3]Co-Orientadora do Trabalho de Conclusão de Curso
Departamento de Física e Matemática - Defim, CAP-UFSJ
E-mail: amandagso@ufsj.edu.br

1 Introdução

A teoria de grupos, decorre do estudo de vários matemáticos na busca da solução por radicais de equações algébricas.

Segundo Domingues e Iezzi [7], entre 1500 e 1515, o matemático italiano Scipione del Ferro (1456 - 1526) descobriu um método para resolver a equação cúbica $x^3 + px = q$ $(p, q > 0)$. Del Ferro verificou que a equação dada é resolúvel por radicais. No entanto, a solução de Del Ferro apresentou um desafio para os algebristas: será que toda equação algébrica é resolúvel por radicais? Essa questão só começou a ser esclarecida genericamente na segunda metade do século XVII, através das pesquisas de Joseph-Louis Lagrange (1736 - 1813). Assim, Lagrange observou que a teoria das permutações ou simetrias era de grande relevância para a resolução de equações.

Em 1824, de acordo com Domingues e Iezzi [7] o matemático norueguês Niels Henrik Abel (1802 - 1829) mostrou que não há nenhuma fórmula geral por radicais para resolver as equações de grau igual ou maiores que 5. Contudo, uma questão permanecia em pé: por que algumas equações de grau igual ou maiores que 5 são resolúveis por radicais e, o que caracteriza esse tipo de equação?

Somente no século XIX, o jovem francês Evariste Galois (França, 1811 - 1832) mostrou que toda equação pode ser associada a um grupo característico e que as propriedades desse grupo podem ser usadas para determinar se a equação é solúvel por radicais ou não. Onde, o termo grupo foi utilizado em seu sentido atual pela primeira vez por Galois, que procurou descrever os grupos de simetrias satisfeitos pelas soluções da equação algébrica (Domingues e Iezzi, 2003)[7].

O conceito de grupo é fundamental para a álgebra abstrata, mas também possui aplicação direta outras áreas da matemática e de outras ciências. Um exemplo disso, é o grupo das simetrias que possui aplicação na cristalografia e na química, por exemplo. Na física clássica, o grupo de Galileu é usado para correlacionar simetrias do espaço com teoremas de conservação, o grupo de Lorenz é estudado na mecânica relativística e esses grupos surgem também na formalização da mecânica quântica (Sakurai e Tuan, 1994) [12]. Além desses, outros grupos clássicos são usados no estudo das álgebras que resultam em dinâmicas importantes da mecânica quântica, como a álgebra de momento angular e a álgebra anticomutativa fermiônica (Ballentine, 1998)[2].

Arthur Cayley foi um dos matemáticos ingleses mais ilustres do século XIX. Ele nasceu no ano de 1821 em Richmond, Surrey. Se formou em matemática pela Universidade de Cambridge, mas escolheu não seguir uma carreira acadêmica por causa da necessidade de se tornar um sacerdote anglicano. Ele morreu em Cambridge no dia 26 de janeiro de 1895. Durante sua vida, Cayley escreveu mais de 900 publicações. Dedicou grande parte de sua energia à teoria dos invariantes, mas sem dúvida seu trabalho de maior e o valor mais duradouro foi o da teoria das matrizes, onde ele foi pioneiro (Allenby e SLOMSON, 2011)[1].

Em 1854, Cayley publicou um artigo intitulado On The Theory of Groups as Depending on the Symbolic Equation $6^0 = 1$ (Sobre a teoria dos grupos como dependente da equação simbólica $6^0 = 1$), sendo notável por descrever provavelmente, a mais antiga definição de grupo abstrato finito. Nesse artigo também está formulado o que hoje se conhece como Teorema de Cayley que diz que todo grupo finito é isomorfo a um subgrupo de um grupo de

permutações (Baumgart, 1992) [4].

O teorema de Cayley permite descrever grupos através de uma estrutura em comum, e ajuda na classificação de grupos de acordo com seus isomorfismos. Assim, teoremas que são verdadeiros para subgrupos de grupos de permutação são verdadeiros para grupos em geral. O fato de todo o grupo poder ser representado por um grupo de permutações tem a vantagem de dar um certo caráter de concretude ao grupo em estudo por mais abstrato que ele seja.

A primeira seção motiva o estudo dos grupos. A segunda sessão apresenta a definição de grupo e alguns resultados teóricos sobre essas estruturas algébricas. Trata também dos subgrupos e apresenta critérios para saber se um determinado subconjunto não vazio de um grupo constitui um subgrupo.

As seções 3 e 4 aborda respectivamente grupo de permutações e grupo diedral abordando o tema de forma simples e depois expondo suas definições, teoremas e proposições associadas a cada grupo. A sessão 5, apresenta homomorfismo de grupos e partindo desse conceito, defini-se isomorfismo de grupos e apresenta exemplos. Dando prosseguimento à abordagem, chega-se ao Teorema de Cayley. Exibi-se algumas situações que permitem ao leitor verificar a aplicação do resultado demonstrado em exemplos explorados ao longo do trabalho. O Teorema de Cayley também dá ao leitor um vislumbre das generalizações que a Matemática, e em particular a álgebra, é capaz ao mostrar que todo grupo é isomorfo a um determinado grupo de permutações. Finalizando o trabalho é abordado uma proposta de plano de aula sugerindo uma aplicação do Teorema de Cayley em uma turma de ensino fundamental. Essa proposta consiste na troca de chaves de resolução de um código escrito.

2 Grupos

Nesta seção será definida a estrutura algébrica de grupo que é o ponto central deste trabalho, usando como referências [3, 6, 7, 8, 10, 11, 13]. Serão apresentadas algumas propriedades decorrentes da definição e uma classificação elementar de acordo com algumas propriedades que podem ou não ser observadas. Além disso também será abordado o conceito de subgrupos.

A matemática define grupos relacionando elementos de um conjunto através de uma operação binária. Do ponto de vista prático, grupos são usados para estudar as operações que podem ser realizadas e combinadas dentro de determinados contextos. Por exemplo, pode-se tratar do conjunto de operações que mudam a posição ou orientação de um sólido geométrico ou uma figura plana. O estudo do Grupo, nesse caso, pode determinar transformações que preservem propriedades do sólido ou mostrar como a posição de determinadas peças mudam de acordo com transformações aplicadas em um conjunto de peças. Em geral, portanto, grupos generalizam a ideia de transformações e com eles pode-se estudar características gerais delas.

Diz-se que um conjunto G é fechado com relação à operação $*$, se todas as combinações de dois elementos desse conjunto através da operação $*$ dada, resulta em um elemento do próprio conjunto, ou seja, $\forall\ a, b \in G$, $a * b \in G$. Um exemplo disso é o conjunto dos números inteiros ($\mathbb{Z}$) com operação de adição, pois para todo $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$. Outro exemplo em que se pode verificar o fechamento com a operação de divisão entre seus elementos é o conjunto dos números complexos não nulos ($\mathbb{C}^*$) pois para todo $a, b \in \mathbb{C}^*$ tal que $a = a_1 + a_2 i$ e $b = b_1 + b_2 i$, com $a_n, b_n \in \mathbb{R},$ com $n = \{1, 2\}$, então:

$\frac{a}{b} = \frac{a_1 + a_2 i}{b_1 + b_2 i} = \frac{(a_1 + a_2 i)}{(b_1 + b_2 i)} . \frac{(b_1 - b_2 i)}{(b_1 - b_2 i)} = \frac{a_1.b_1 - (a_1.b_2)i + (a_2.b_1)i - (a_2.b_2)i^2}{b_1^2 + (b_1.b_2)i - (b_1.b_2)i - b_2^2 i^2}$, como $i^2 = -1$, então $\frac{(a_1.b_1 + a_2.b_2) + (a_2.b_1 - a_1.b_2)i}{b_1^2 + b_2^2} = \frac{a_1.b_1 + a_2.b_2}{b_1^2 + b_2^2} + \frac{a_2.b_1 - a_1.b_2}{b_1^2 + b_2^2} i$, como $\frac{a_1.b_1 + a_2.b_2}{b_1^2 + b_2^2} \in \mathbb{R}$ e $\frac{a_2.b_1 - a_1.b_2}{b_1^2 + b_2^2} \in \mathbb{R}$ então $\frac{a}{b} \in \mathbb{C}^*$ para todo $a, b \in \mathbb{C}$.

Definição 2.1 *Seja G um conjunto não vazio. Uma operação binária sobre um conjunto G é uma função que associa a cada par ordenado $(a, b) \in G \times G$ um elemento $a * b \in G$. Uma operação binária sobre G pode ser representada da seguinte maneira:*

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

Diz-se que um conjunto G é fechado com relação à operação $*$, se $*$ é uma operação binária sobre G. Isso quer dizer que todas as combinações binárias através da operação dada resultam em elementos do conjunto.

Observe que o conjunto $\mathbb{Z}$ dos números inteiros, com a operação usual de adição possui algumas propriedades além da operação binária. Dados $a, b, c \in \mathbb{Z}$ é sabido que a operação de adição é associativa. Simbolicamente, isso significa que $(a + b) + c = a + (b + c)$. Existe um elemento $e \in \mathbb{Z}$ para o qual $a + e = e + a = a$ para todo $a \in \mathbb{Z}$. e é denominado elemento neutro e neste caso, $e = 0$. E, finalmente, para cada $a \in \mathbb{Z}$, existe um outro elemento $b \in \mathbb{Z}$, tal que $a + b = b + a = e$. Como $e = 0$, concluí-se que $b = -a$.

De modo geral, para conjuntos com essas propriedades estabelecem a seguinte definição:

Definição 2.2 *Um grupo, denotado por $(G, *)$, consiste de um conjunto não vazio G onde pode ser definida uma operação $(*)$ binária, que satisfaça as seguintes propriedades:*

1. *Associatividade: $\forall\ g_1, g_2$ e $g_3\ \in G,\ (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$;*
2. *Existência do elemento neutro: $\exists\ e \in G$ tal que $e * g = g * e = g,\ \forall\ g \in G$;*
3. *Existência do elemento inverso: $\forall\ g \in G,\ \exists\ g' \in G$ tal que $g * g' = g' * g = e$.*

Exemplo 2.1 *Prove que $GL_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) / detM \neq 0\}$ é grupo com a operação de multiplicação usual de matrizes.*

De fato.

1. $GL_n(\mathbb{R})$ é associativo.
   Dados $A, B, C \in GL_n(\mathbb{R})$, então vale a igualdade $(AB)C = A(BC)$;
2. Seja
$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \in GL_n(\mathbb{R}),$$

O elemento neutro é dado por

$$I_n = \begin{bmatrix} 1 & ... & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} \in GL_n(\mathbb{R}),$$

pois $detI_n \neq 0$ e

$$AI_n = \begin{bmatrix} a_{11} & ... & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} 1 & ... & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & ... & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} = A$$

e

$$I_nA = \begin{bmatrix} 1 & ... & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} a_{11} & ... & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} = \begin{bmatrix} a_{11} & ... & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} = A,$$

ou seja, $AI_n = A = I_nA$.

3. Dado $A \in GL_n(\mathbb{R})$, tal que $det(A) \neq 0$, existe $A' \in M_n(\mathbb{R})$ tal que $A.A' = A'A = I_n$. Para isso é suficiente mostre que $A' \in GL_n(\mathbb{R})$.

   Tem-se que $AA' = I_n$, logo $\det(A).\det(A') = \det(I_n)$. Sabe-se que $\det(I_n) = 1$ e por hipótese $\det(A) \neq 0$. Assim, $det(A') = \frac{1}{\det(A)} \neq 0$, ou seja, $A' \in GL_n(\mathbb{R})$.
   Portanto $GL_n(\mathbb{R})$ é grupo multiplicativo.

Observe que $GL_n(\mathbb{R})$ com a multiplicação usual não é comutativa.
Sejam $A = \begin{bmatrix} 3 & 1 \\ 2 & 4 \end{bmatrix} \in GL_2(\mathbb{R})$ e $B = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \in GL_2(\mathbb{R})$.
$AB = \begin{bmatrix} 3 & 1 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 5 & 10 \\ 10 & 20 \end{bmatrix}$ e $BA = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 7 & 9 \\ 14 & 18 \end{bmatrix}$.
O que implica que $AB \neq BA$.

Em um grupo, se a operação binária é uma adição conhecida, representa-se o elemento neutro por $e = 0$ e o elemento oposto $g' = -g$. Este grupo é denotado por $(G, +)$ e diz-se que um grupo G é aditivo. Outras operações como, a composição de funções, representada por $(G, \circ)$ e, operações não triviais também podem satisfazer as propriedades de Grupo. Se a operação estiver implícita ao grupo $(G, *)$, este será denotado simplesmente por grupo G.

Um grupo é multiplicativo se sua operação binária é a multiplicação, o elemento identidade é representado por $e = 1$ e este grupo é denotado por $(G, .)$. Em grupos multiplicativos, dados $g_1, g_2 \in G$, é comum escrever g_1g_2 omitindo o sinal de operação entre os elementos g_1 e g_2.

Em conjuntos finitos pequenos, a construção da tábua de operações pode facilitar a observação de algumas propriedades de grupo, tais como verificar se um conjunto com n elementos é fechado, qual é o elemento neutro, quais são os inversos de cada elemento do grupo e quais pares de elementos são comutativos.

Definição 2.3 *Uma tábua de operação $*$ definida sobre um conjunto finito $G = \{g_1, g_2, ..., g_n\}$ é uma tabela onde o resultado da operação $g_i * g_j$ é colocado na i-ésima linha e j-ésima coluna, ou seja, o resultado é obtido usando um elemento da linha operado por um elemento da coluna.*

Seja $G = g_1, g_2, ..., g_n$ com $n > 1$ um conjunto com n elementos. Toda operação sobre G é uma aplicação $f : G \times G \longrightarrow G$ que associa cada par ordenado (g_i, g_j) o elemento $g_i * g_j = g_{ij}$.

O elemento g_{ij} pode ser representado numa tabela de dupla entrada construída como na tabela 1.

Tabela 1: Tábua de operações

$*$	g_1	g_2	$\cdots$	g_n
g_1	g_{11}	g_{12}	$\cdots$	g_{1n}
g_2	g_{21}	g_{22}	$\cdots$	g_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
g_n	g_{n1}	g_{n2}	$\cdots$	g_{nn}

Observe como se pode checar as propriedades de uma operação $*$ sobre um conjunto G através de uma tábua de operações.

1. Elemento neutro.
   Observe a tábua de operações e verifique se a primeira linha da tábua (o cabeçalho) se repete em algum lugar da tábua. Caso encontre a linha, quer dizer que para algum elemento $g_i \in G$, g_ié o elemento neutro à esquerda para a operação $*$, ou seja, $g_i * g_n = g_i$ para todo $g_n \in G$. Observe novamente a tábua de operações para ver se a primeira coluna se repete em algum lugar da tábua. Ao encontrar a coluna significa que o elemento g_i é o elemento neutro à direita, ou seja, $g_n * g_i = g_i$ para todo $g_n \in g$. Portanto o elemento g_i é o elemento neutro da operação $*$.

2. Elemento inverso.
   Como g_i é o elemento neutro da operação, verifica-se na tábua quais são os pares de elementos $g_a, g_b \in G$ tais que $g_a * g_b = g_i$.

3. Propriedade Associativa.
   Não é possível verificar tal propriedade através da tábua de operações. Esta é a propriedade que exige mais trabalho, podendo ser feita de dois modos:
   1^o modo: Calculam-se todos os compostos do tipo $g_i*(g_j*g_k)$, com $i, j, k \in \{1, 2, 3, ..., n\}$ e comparar os compostos que tem os mesmos i, j e k. Esse método requer o cálculo de $2n^3$ compostos.
   2^o modo: Encontra-se um conjunto H dotado de uma operação $*$ que se sabe ser associativa de tal forma que existe uma aplicação $f : E \to F$ com as seguintes propriedades:
   (i) f é bijetora;
   (ii) $f(x * y) = f(x) * f(y)$ para todo $x, y \in E$.

Exemplo 2.2 *O conjunto finito definido pelo conjunto* $G = \{-i, -1, i, 1\} \subset \mathbb{C}$ *com a operação usual de multiplicação em* $\mathbb{C}$ *mostrada na tabela 2 é um grupo multiplicativo.*

Tabela 2: Multiplicação do conjunto G

$*$	$-i$	-1	i	1
$-i$	-1	i	1	$-i$
-1	i	1	$-i$	-1
i	1	$-i$	-1	i
1	$-i$	-1	i	1

De fato, como o conjunto $\mathbb{C}$ é associativo com relação a operação de multiplicação e como $G \subset \mathbb{C}$ então G é associativo.
Analisando a tabela, observa-se que na quinta linha a multiplicação é igual a primeira linha da tabela e na quinta coluna a multiplicação é igual a primeira coluna. Logo o elemento 1 é o elemento neutro dessa operação.
Como 1 é o elemento neutro e se encontra em todas as entradas da diagonal da tabela, os elementos inversos são:

$$(-i)' = i,\ (-1)' = -1,\ i' = -i,\ 1' = 1.$$

Logo G é um grupo multiplicativo.

A seguir, é apresentado propriedades básicas que são obtidas a partir dos axiomas da definição de grupo:

Teorema 2.1 *Se* $(G, *)$ *é um grupo então existe um único elemento neutro* $e \in G$.

Demonstração: Suponha que existam $e_1, e_2 \in G$ elementos neutros distintos em G com relação a $*$. Logo,
• Como e_1 é um elemento neutro, então $e_1 * e_2 = e_2 * e_1 = e_2$;
• Como e_2 é um elemento neutro, então $e_1 * e_2 = e_2 * e_1 = e_1$;
Deste modo,

$$e_2 = e_1 * e_2 = e_2 * e_1 = e_1.$$

Então $e_1 = e_2$, isto é, o elemento neutro é único. □

Teorema 2.2 *Para cada elemento* $g \in G$, *existe um único elemento inverso* $g' \in G$.

Demonstração: Suponha que g' e $\hat{g}$ sejam dois inversos de $g \in G$, então
• Como g' é inverso de g então, $g' * g = g * g' = e$;
• Como $\hat{g}$ é inverso de g então, $\hat{g} * g = g * \hat{g} = e$;
Deste modo,
$\hat{g} = \hat{g} * e = \hat{g} * (g * g') = (\hat{g} * g) * g' = e * g' = g'$.
Então, $\hat{g} = g'$, isto é, o inverso de cada elemento $g \in G$ é único. □

Do teorema acima observa-se que se e é o elemento neutro do grupo G, então $e * e' = e$, ou seja, $e' = e$. Em outras palavras, quer dizer que a inversa do elemento neutro é o próprio elemento neutro.

Teorema 2.3 *Se G é um grupo então $(g')' = g$.*

Demonstração: Observe, pela definição de elemento inverso, que $(g')'$ é um elemento que quando multiplicado por g' resulta em e, mas sabe-se que g é esse elemento, já que g' é inverso de g, e pelo teorema 2.2 existe a unicidade do inverso. Portanto,

$$(g')' = g.$$

□

Teorema 2.4 *Se G é um grupo tal que $g_1, g_2 \in G$ então $(g_1 * g_2)' = g_2' * g_1'$.*

Demonstração: Mostre que

$$(g_1 * g_2) * (g_2' * g_1') = (g_2' * g_1') * (g_1 * g_2) = e.$$

De fato, pela propriedade associativa da operação em G tem-se que

$$(g_1 * g_2) * (g_2' * g_1') = g_1 * (g_2 * g_2') * g_1' = g_1 * e * g_1' = g_1 * g_1' = e.$$

Analogamente, tem-se que

$$(g_2' * g_1') * (g_1 * g_2) = g_2' * (g_1' * g_1) * g_2 = g_2' * e * g_2 = (g_2' * g_2) = e.$$

□

Nem sempre a operação binária usada na definição do grupo é comutativa. Quando há comutatividade, entretanto, atribui-se ao grupo uma denominação especial, a saber, grupo abeliano.

Definição 2.4 *Um grupo $(G, *)$ é abeliano ou comutativo se, e somente se, $*$ é uma operação comutativa, ou seja, $\forall\ g_1, g_2 \in G$:*

$$g_1 * g_2 = g_2 * g_1.$$

Caso contrário, o grupo G é não comutativo ou não abeliano.

É possível verificar no exemplo 2.2 que o conjunto é comutativo. Além disso, todos os grupos aditivos e multiplicativos definidos sobre o subconjuntos dos números reais ou complexos são abelianos.

E através da tábua de operações também é possível verificar a propriedade comutativa. Para isso basta verificar se a parte da tábua que está acima da diagonal que vai do canto superior esquerdo ao inferior direito é simétrica com relação à parte que está abaixo da diagonal.

Exemplo 2.3 *Seja* $G = \{f : R \longrightarrow R \,/\, f(x) = ax + b;\ a, b \in \mathbb{R};\ a \neq 0\}$. *Verifique que* G *é grupo não abeliano com relação à composição de funções.*

Sejam $f(x) = a_1x + b_1$, $g(x) = a_2x + b_2$ e $h(x) = a_3x + b_3$ elementos de G e $a_n, b_n \in \mathbb{R}$ para $1 \leq n \leq 3$ e $a_n \neq 0$.

Primeiro para mostrar que G é associativo com a operação de composição de funções, efetua-se a composição $[f \circ (g \circ h)](x)$. Então,

$$[f \circ (g \circ h)](x) = f[g(a_3x + b_3)] = f[a_2(a_3x + b_3) + b_2] = f[a_2a_3x + a_2b_3 + b_2] = a_1(a_2a_3x + a_2b_3 + b_2) + b_1 = a_1a_2a_3x + a_1a_2b_3 + a_1b_2 + b_1$$

e

$$[(f \circ g) \circ h](x) = [f(a_2x + b_2)] \circ (a_3x + b_3) = [a_1(a_2x + b_2) + b_1] \circ (a_3x + b_3) = (a_1a_2x + a_1b_2 + b_1) \circ (a_3x + b_3) = a_1a_2(a_3x + b_3) + a_1b_2 + b_1 = a_1a_2a_3x + a_1a_2b_3 + a_1b_2 + b_1.$$

Assim verifica-se que $f \circ (g \circ h) = (f \circ g) \circ h$.

Seja $e \in G$ tal que $e(x) = e_1x + e_2$. Para encontrar $e(x) \in G$ tal que $(f \circ e)(x) = f(x)$ e $(e \circ f)(x) = f(x)$.

Fazendo a composição $(f \circ e)(x)$ obtêm-se:

$$(f \circ e)(x) = f(e_1x + e_2) = a_1(e_1x + e_2) + b_1 = a_1e_1x + a_1e_2 + b_1.$$

Como $(f \circ e) = f(x)$, então:

$$a_1e_1x + (a_1e_2 + b_1) = a_1x + b_1.$$

Pela igualdade de polinômios, forma-se o seguinte sistema:

$$\begin{cases} a_1e_1 = a_1 \\ a_1e_2 + b_1 = b_1. \end{cases}$$

Então, $e_1 = 1$ e $e_2 = 0$, $a_1 \neq 0$ e, portanto, $e(x) = x \in G$. Fazendo a composição de funções $(e \circ f)(x)$, substituindo $e(x)$ por x obtêm-se: $(e \circ f)(x) = e(a_1x + b_1) = a_1x + b_1 = f(x)$.
Portanto o elemento neutro é $e(x) = x$.

Seja $f'(x) \in G$ tal que $f'(x) = ux + v$. Para encontrar $f'(x) \in G$ basta resolver $(f \circ f')(x) = (f' \circ f)(x) = e(x)$.

Então:

$$x = e(x) = (f \circ f')(x) = f(ux + v) = a_1ux + a_1v + b_1.$$

Então, resolvendo o sistema:

$$u = \frac{1}{a_1};\ v = \frac{-b_1}{a_1},\ \text{logo}\ f'(x) = \frac{1}{a_1}x - \frac{b_1}{a_1} \in G.$$

Resta fazer $(f' \circ f)(x)$, então:

$$f'(a_1x + b_1) = \frac{1}{a_1}(a_1x + b_1) - \frac{b_1}{a_1} = x = e(x).$$

Portanto para todo $f(x) \in G$, existe $f'(x) \in G$ tal que $(f \circ f')(x) = e(x)$.
Como

$$(f \circ g)(x) = f(a_2x + b_2) = a_1(a_2x + b_2) + b_1 = a_1a_2x + (a_1b_2 + b_1)$$

e

$$(g \circ f) = g(a_1x + b_1) = a_2(a_1x + b_1) + b_2 = a_1a_2x + (a_2b_1 + b_2)\,,$$

então $(f \circ g)(x) \neq (g \circ f)(x)$. Portanto G é um grupo não abeliano.

2.1 Subgrupos

Dado um grupo, um subconjunto do conjunto original, fechado com relação a operação do grupo é chamado subgrupo se possui as propriedades da definição abaixo.

Definição 2.5 *Seja $(G; *)$ um grupo. Um subconjunto não vazio $H \subset G$ é um subgrupo de G se H for grupo com a operação de G. Isto é, H é subgrupo de G (denotado por $H < G$), quando satisfaz as seguintes condições:*
(i) Para todo x, $y \in H$ segue que $x * y \in H$;
(ii) $(H; *)$ é um grupo.

Todo grupo G possui pelo menos dois subgrupos, a saber: G e $\{e\}$, chamados de subgrupos triviais de G.

Observe que o elemento neutro e_H de H é necessariamente igual ao elemento neutro e de G.

Sejam e_H o elemento neutro de H e e_G o elemento neutro de G, então $e_H = e_G$. De fato, como e_H é o elemento neutro de H, $e_H \circ e_H = e_H$, por outro lado, como $e_H \in H \subset G$, segue que $e_H \circ e_G = e_H$. Logo,

$$e_H \circ e_H = e_H = e_H \circ e_G.$$

Assim, pela lei do cancelamento em G,

$$e_H = e_G.$$

E se $x \in H$, seu inverso em H é necessariamente igual ao inverso de x em G. Também pela lei do cancelamento segue que, para cada $x \in H$ então $x'_H = x'$, onde x'_H é o elemento inverso de x em H e x' é o elemento inverso de x em G. Com efeito,

$$x \circ x'_H = e_H = e_H = x * x'.$$

Logo, $x'_H = x'$.

Exemplo 2.4 *Considere as seguintes funções reais com domínio em $D = \{x \in \mathbb{R}^* / x \neq -1\}$,*

$$f_1(x) = x;\ f_2(x) = \frac{1}{x};\ f_3(x) = 1 - x;\ f_4(x) = \frac{x}{x-1};\ f_5(x) = \frac{1}{1-x}\ \ e\ f_6(x) = \frac{x-1}{x}.$$

Prove que o conjunto de tais funções $F = \{f_1(x), f_2(x), f_3(x), f_4(x), f_5(x), f_6(x)\}$ *com a operação de composição usual de funções, é um grupo.*

De fato, a composição de funções possui a propriedade associativa, então F é associativo. O elemento neutro do conjunto F é $f_1(x) = x$ pois $(f_1 \circ f_n)(x) = (f_n \circ f_1)(x) = f_n(x)$, $1 \leqslant n \leqslant 6$. E $f_1'(x) = f_1(x)$; $f_2'(x) = f_2(x)$; $f_3'(x) = f_3(x)$; $f_4'(x) = f_4(x)$; $f_5'(x) = f_6(x)$; $f_6'(x) = f_5(x)$. Portanto F é um grupo.

A operação de composição de funções é apresentada na tabela 3.

Tabela 3: Tábua de operações para o grupo F

$f_i(x) \circ f_j(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$
$f_1(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$
$f_2(x)$	$f_2(x)$	$f_1(x)$	$f_5(x)$	$f_6(x)$	$f_3(x)$	$f_4(x)$
$f_3(x)$	$f_3(x)$	$f_6(x)$	$f_1(x)$	$f_5(x)$	$f_4(x)$	$f_2(x)$
$f_4(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$
$f_5(x)$	$f_5(x)$	$f_4(x)$	$f_2(x)$	$f_3(x)$	$f_6(x)$	$f_1(x)$
$f_6(x)$	$f_6(x)$	$f_3(x)$	$f_4(x)$	$f_2(x)$	$f_1(x)$	$f_5(x)$

b) Identifique um subgrupo de F.

Observe que $G = \{f_1(x), f_5(x)$ e $f_6(x)\}$ forma um subgrupo do grupo original. Pela definição 2.5 analisando na tabela 3 somente os elementos $f_1(x), f_5(x)$ e $f_6(x)$ e suas respectivas composições de funções, pode-se perceber que o conjunto é fechado com a operação de composição de funções. A composição de funções é associativa, portanto G também é associativo. O elemento neutro de G é o mesmo de F, ou seja, $f_1(x)$ é tal elemento. E as inversas de $f_1(x), f_5(x)$ e $f_6(x)$ são respectivamente $f_1(x), f_6(x)$ e $f_5(x)$. Portanto G é subgrupo de F.

Teorema 2.5 *Para que um subconjunto não vazio* $H \subset G$ *seja subgrupo de um grupo* $(G; *)$*, é necessário e suficiente que para todo* $x, y \in H$*,* $x * y' \in H$*. Onde,* y' *é o elemento inverso de* y*.*

Demonstração: Primeiramente mostrar que se H um subgrupo de G, então para todo $x, y \in H$ segue que $x * y' \in H$. Por hipótese, H um subgrupo de G, então para quaisquer $x, y \in H, x \circ y \in H$. Além disso, $(H; *)$ é um grupo.

Seja $x, y \in H$, como $y \in H$ e H é um grupo a inversa $y' \in H$. Assim $x * y' \in H$ pois H é fechado.

Suponha agora, por hipótese, que para todo $x, y \in H$, $x * y' \in H$, então $(H, *)$ é um subgrupo de $(G, *)$.

De dato,

(i) $(H; *)$ é um grupo:

1. Existência de elemento identidade:

   Como por hipótese, para todo x, $y \in H$, $x * y' \in H$, segue que $e \in H$, pois $H \neq 0$, logo $\exists\ x \in H$ e $e = x * x'$; $\forall\ x \in H$.

2. Existência de elemento inverso:

   Para cada $y \in H$, $y' \in H$, pois
   $$y' = e * y' \in H.$$
   E para cada $y \in H \subset G$,
   $$y * y' = e = y' * y.$$
   Portanto, y' é o elemento inverso de y em $(H, *)$.

3. Propriedade associativa:

   Finalmente, a propriedade associativa para H é válida uma vez que G é um grupo e $H \subset G$.

(ii) Para todo $x; y \in H$ segue que $x * y \in H$. Dados $x, y \in H$, como $y' \in H$, segue por hipótese que
$$x * y = x * (y')' \in H.$$
Logo, por (i) e (ii), segue que $(H, *)$ é um subgrupo de $(G, *)$. □

Exemplo 2.5 *Sejam H_1 e H_2 subgrupos de um grupo G. A interseção $H_1 \cap H_2$ também é um subgrupo de G.*

Como H_1 e H_2 são subgrupos de G então cada um deles contém o elemento neutro $e \in G$, ou seja, $e \in H_1$ e $e \in H_2$. Logo, $e \in H_1 \cap H_2$ e, portanto, $H_1 \cap H_2 \neq \varnothing$.

Sejam $a, b \in H_1 \cap H_2$. Como H_1 é subgrupo de G, $a, b \in H_1$ então $a * b' \in H_1$. Analogamente, $a, b \in H_2$ então $a * b' \in H_2$. Portanto, $a * b' \in H_1 \cap H_2$. Logo $H_1 \cap H_2$ é um subgrupo de G.

3 Grupo de Permutações

Nesta seção será abordado os grupos de permutações, foram utilizadas como referências [6, 7, 8, 11, 13].

Para iniciar esta seção considere o conjunto formado por três figuras, a estrela, a lua e o sol, dispostos em uma determinada ordem, como pode ser visto na Figura 1.

Figura 1: Sequência de figuras iniciada pela estrela.

Fonte: elaborada pelo autor.

Pode-se perceber, que a sequência dada na Figura 1 não é a única tripla ordenada iniciada pela estrela. O leitor poderia começar a sequência com qualquer uma das três figuras, por exemplo, iniciar a sequência pela lua ao invés de começar pela estrela, bastaria posicionar a figura escolhida na primeira posição e dispor as demais figuras na ordem em que desejar. Como por exemplo na Figura 2.

Figura 2: Sequência de figuras iniciada pela lua.

Fonte: elaborada pelo autor.

Para obter a sequência que aparece na Figura 2 a partir sequência que foi dada na Figura 1, seria necessário fazer um movimento de reordenar. Neste caso, a sequência foi obtida colocando a estrela na segunda posição; a lua na primeira; e mantendo o sol na mesma posição, ou seja, terceira posição.

Para facilitar a reordenação, seja o conjunto $A = \{estrela, lua, sol\}$ correspondente respectivamente ao conjunto $B = \{E, L, S\}$, uma sequência possível para seus elementos é (E, L, S). A partir daí podemos reordenar seus elementos de diversas formas e obter as sequências $(L, E, S); (E, L, S); (L, S, E); (S, E, L); (E, S, L); (S, L, E)$ que são todas as permutações de 3 objetos. A palavra permutar significa trocar reciprocamente. Permutação é um assunto fundamental da matemática, normalmente apresentado em análise combinatória, podendo ser definida como uma bijeção de um conjunto enumerável nele mesmo.

Definição 3.1 *Seja* $E = \{1, 2, 3, ..., n\}$. *Denotado por* $S(E)$ *o conjunto de todas as permutações dos elementos de* E, *isto é, o conjunto de todas as bijeções* f *de* E *em* E,

$$S(E) = \{f : E \longrightarrow E; f \text{ é uma bijeção}\}.$$

Exemplo 3.1 *Seja* $E = \{1, 2, 3, 4\}$. *Dê um exemplo de permutação do conjunto* E.

Uma permutação desse conjunto pode ser representada por $(2, 3, 4, 1)$.
Cada sequência desse tipo determina uma função bijetiva $\sigma : E \longrightarrow E$.
Na sequência $(2, 3, 4, 1)$, por exemplo, definimos a bijeção $\sigma : E \longrightarrow E$, por $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 4$ e $\sigma(4) = 1$

3.1 Representação por Notação Matricial

Seja $E = \{1, 2, 3, ..., n\}$. O conjunto das permutações dos n elementos de E também pode ser denotado por S_n. Uma bijeção $\sigma \in S_n$ tal que

$$\begin{array}{c} 1 \mapsto \sigma(1) \\ 2 \mapsto \sigma(2) \\ 3 \mapsto \sigma(3) \\ \vdots \\ n \mapsto \sigma(n) \end{array}$$

pode ser representada por meio da seguinte notação matricial:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \sigma_1 & \sigma_2 & \sigma_3 & ... & \sigma_n \end{pmatrix},$$

onde $\sigma_i = \sigma(i)$, com $i \in \{1, 2, ..., n\}$.

A permutação identidade, e, é representada por:

$$e = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ 1 & 2 & 3 & ... & n \end{pmatrix}.$$

Nessa notação geralmente os elementos da primeira linha em ordem crescente. Com essa notação a operação de composição de duas permutações,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \sigma(1) & \sigma(2) & \sigma(3) & ... & \sigma(n) \end{pmatrix} \text{ e } \tau = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \tau(1) & \tau(2) & \tau(3) & ... & \tau(n) \end{pmatrix}$$

denotada pelo símbolo " $\circ$ " se faz da seguinte maneira:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \sigma(\tau(3)) & ... & \sigma(\tau(n)) \end{pmatrix}.$$

Exemplo 3.2 *Sejam* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$ *e* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$ *duas permutações de* S_5. *Tem-se que* $\sigma \circ \tau \neq \tau \circ \sigma$

De fato, fazendo as composições de permutações obtêm-se:

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

Observe que dado $\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \sigma_1 & \sigma_2 & \sigma_3 & ... & \sigma_n \end{pmatrix} \in S_n$, ao trocar a primeira linha (domínio de σ) com a segunda linha (as correspondentes imagens de σ), obtêm-se

$$\sigma' = \begin{pmatrix} \sigma_1 & \sigma_2 & \sigma_3 & ... & \sigma_n \\ 1 & 2 & 3 & ... & n \end{pmatrix}.$$

Para expressar σ' da maneira correta basta reordenar a matriz acima deixando a primeira linha como $1, 2, ..., n$. Então, utilizando o exemplo anterior a inversa de σ é dada por

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

e a inversa de τ é

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}.$$

3.2 Definição de Grupo de Permutações

Teorema 3.1 *Seja $E = \{1, 2, ..., n\}$ e $S_n = \{\sigma : E \longrightarrow E;$ σ é uma bijeção$\}$ com a operação de composição de funções S_n é um grupo (chamado grupo de permutações de n elementos).*

Demonstração: Sejam $f, g \in S_n$ permutações de E, ou seja, $f : E \longrightarrow E$ e $g : E \longrightarrow E$ bijeções. Deseja-se mostrar que a composta $f \circ g$ também é uma bijeção. Como f e g são bijeções, então f e g são injetiva e sobrejetiva. $f \circ g$ é injetiva. De fato, sejam x_1 e $x_2 \in E$ tais que $(g \circ f)(x_1) = (g \circ f)(x_2)$. Então $g(f(x_1)) = g(f(x_2))$;
Como g é injetiva então $f(x_1) = f(x_2)$. Como f é injetiva então $x_1 = x_2$. Portanto $f \circ g$ é injetora. $f \circ g$ é sobrejetiva. Sejam $z \in E$. Como g é sobrejetiva então existe $y \in E$ tal que $g(y) = z$. Sendo f sobrejetora, existe $x \in E$ tal que $f(x) = y$. Assim:

$$z = g(y) = g(f(x)) = (g \circ f)(x).$$

Então $g \circ f$ é sobrejetiva. Como $g \circ f$ é injetiva e sobrejetiva então é bijetiva.
Portanto S_n é fechado com a operação de composição de permutações.
A composição de funções é associativa.
O elemento neutro de S_né a bijeção identidade $e : E \longrightarrow E = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ 1 & 2 & 3 & ... & n \end{pmatrix}$.

Se f é uma bijeção, então possui inversa f' e f' também é uma bijeção, ou seja,

$$f \circ f' = f' \circ f = e.$$

Portanto S_n é grupo. □

Conforme estudado em análise combinatória, se $E = \{1, 2, ..., n\}$ tem n elementos, então o grupo S_n, das permutações de n, possui $n!$ elementos. De fato, como o conjunto de todas as permutações do conjunto S_n é finito, então para obter qualquer permutação desses n elementos, tem-se n possibilidades de preenchimento para o primeiro termo da sequência, $n-1$ possibilidades para o segundo, ..., 2 possibilidades para o $(n-1)$-ésimo e 1 possibilidade para o último. Assim, pelo princípio fundamental existem $n.(n-1).\cdots.2.1$, permutações em S_n.

Exemplo 3.3 *Seja $E = \{1, 2, 3\}$.*

O número de permutações de E é $3! = 6$. O conjunto S_3 contém os seguintes elementos:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \;\; ; \;\; \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \;\; ; \;\; \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} ;$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \;\; ; \;\; \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \;\; \text{e} \;\; \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} .$$

Os elementos nos permitem escrever a seguinte tábua de operação do grupo S_3.

Tabela 4: Tábua de operação o grupo S_3

$*$	e	σ_1	σ_2	σ_3	σ_4	σ_5
e	e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	σ_2	e	σ_5	σ_3	σ_4
σ_2	σ_2	e	σ_1	σ_4	σ_5	σ_3
σ_3	σ_3	σ_4	σ_5	e	σ_1	σ_2
σ_4	σ_4	σ_5	σ_3	σ_2	e	σ_1
σ_5	σ_5	σ_3	σ_4	σ_1	σ_2	e

Vale observar também que esse grupo não é abeliano, por exemplo:

$$\sigma_3 \circ \sigma_2 = \sigma_5 \neq \sigma_4 = \sigma_2 \circ \sigma_3.$$

Pelo exercício 3.3 e observando sua respectiva tábua de operações observa-se que o conjunto $F = \{e, \sigma_1, \sigma_2\}$ é um subgrupo do grupo S_3. De fato, verifica-se que F é fechado para composição, como pode ser observado na tábua mostrada na tabela 4. Em F, vale a associatividade herdada de S_3. O elemento neutro e está no conjunto. E as inversas de $e' = e$; $\sigma_1' = \sigma_2$; $\sigma_2' = \sigma_1$. Portanto, F é subgrupo do grupo S_3.

4 Grupos Diedrais

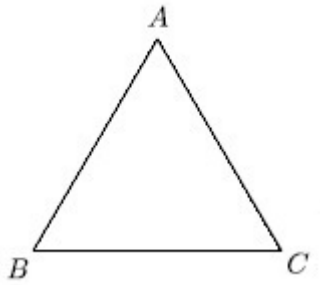
Esta seção abordará os grupos diedrais, utilizando como referência [6, 7, 8, 11, 13].

O uso de grupos é muito útil quando se trata de estudar transformações sobre figuras geométricas. Se classificar as figuras geométricas de acordo com suas propriedades de interesse, pode-se criar conjuntos e, estabelecendo operações binárias entre esses elementos, formam-se grupos relacionados àquelas características.

Rotações e reflexões são exemplos de transformações isométricas que podem ser feitas em figuras planas. Se as figuras planas em questão são polígonos regulares e o conjunto for formado de operações apenas aquelas que preservam as posições dos vértices dessas figuras, forma-se os grupos diedrais. Veja a seguinte situação.

Suponha que exista o desenho de um triângulo equilátero em uma folha de papel como o da Figura 3 e que, separadamente, exista um modelo de triângulo equilátero com os vértices identificados da mesma forma que no desenho. Assuma, ainda, que o modelo sobreponha-se exatamente ao triângulo desenhado no papel e que em sua posição inicial os vértices A, B e C do modelo estejam respectivamente sobre os vértices A, B e C do desenho.

Figura 3: Triângulo desenhado em uma folha de papel.

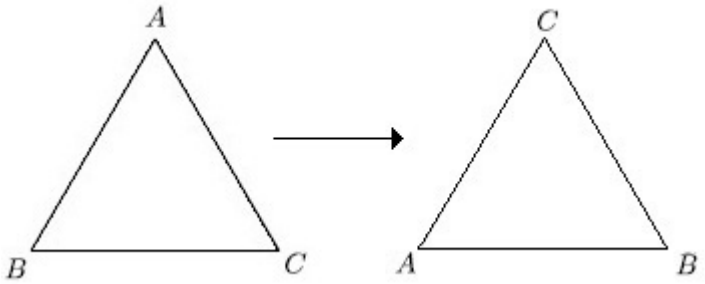


Fonte: elaborada pelo autor.

Há o interesse em saber: quais movimentos pode-se fazer, sem deformar o modelo, ou seja, sem ampliar, esticar, encolher ou sofrer qualquer tipo de deformação, de modo que, ao final do movimento, o triângulo se sobreponha ao desenho da folha de papel?

Um desses movimentos é a rotação por ângulos de 120° em torno do baricentro do triângulo, como na Figura 4. Por conveniência, sempre que se referir a uma rotação, ela será feita no sentido anti-horário e em torno do baricentro do triângulo.

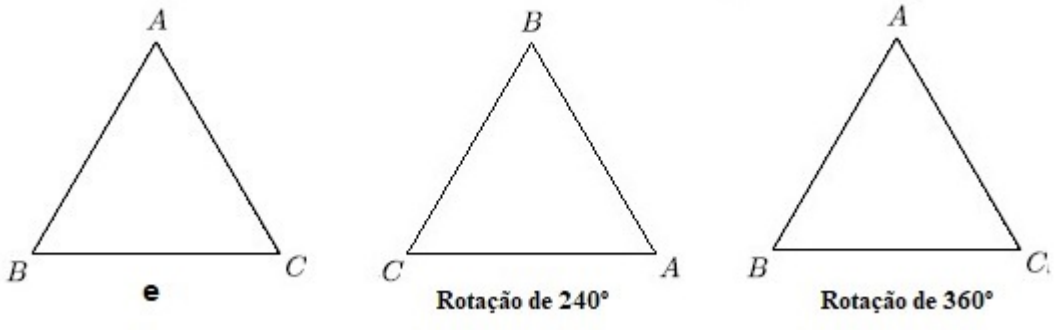
Figura 4: Triângulo equilátero rotacionado 120°.



Fonte: elaborada pelo autor.

Além dessa primeira rotação existem outras duas rotações que fazem com que o modelo se sobreponha ao desenho. A saber, tais rotações são obtidas pelos ângulos de 240° e 360° e estão apresentados na Figura 5. Observe, contudo, que a rotação de 360° gera o mesmo resultado que não fazer rotação nenhuma e esta rotação será indicada por e.

Figura 5: Triângulo rotacionado em 240° e em 360°.



Fonte: elaborada pelo autor.

Então, sob a condição de manter correspondência com o desenho na folha de papel, existe 3 rotações no sentido anti-horário e seus efeitos sobre os vértices A, B e C.

- Rotação de 0° ou de 360°; sendo denotada por e. Nesta situação o triângulo permanece inalterado após a rotação, isto é, o vértice A é levado no vértice A; o vértice B no vértice B; e o vértice C também é levado em si próprio.

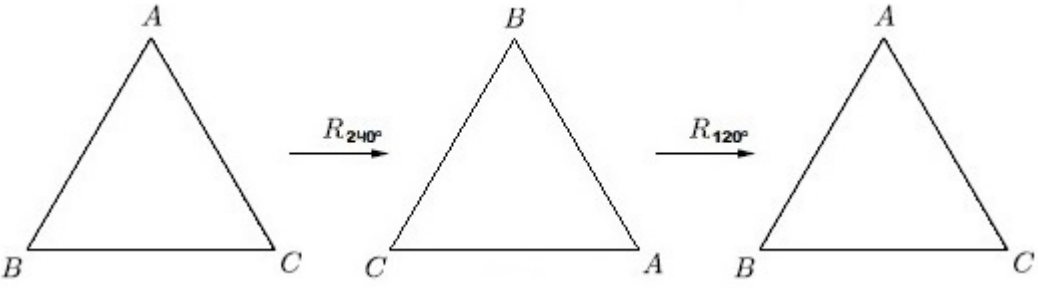
- Rotação de 120°; sendo denotada por R_{120°. Agora nesta situação, aplicando a rotação, o vértice A é levado no vértice B; o vértice B no vértice C; e o vértice C é levado no vértice A. Como pode ser visto na Figura 5.

- Rotação de 240°; sendo denotada por R_{240°. Neste caso, após a rotação, o vértice A é levado no vértice C; o vértice B no vértice A; e o vértice C é levado no vértice B.

Observe que as rotações que identificadas não são rotações quaisquer, limitam-se àquelas que preservam a correspondência com a figura original "na folha de papel".

Feita essa análise, é normal questionar o que ocorre na composição de rotações, isto é, ao fazer um movimento após o outro, ainda obtêm-se uma das rotações listadas? Observe o exemplo da composição $R_{120^\circ} \circ R_{240^\circ}$. As composições sempre serão feitas da direita para a esquerda. Portanto, nesse caso, primeiro é feita a rotação em torno de R_{240°, para só então aplicar a rotação R_{120°. Observe na Figura 6 como fica a composição dos dois movimentos.

Figura 6: Ilustração da composição $R_{120^\circ} \circ R_{240^\circ} = e$.



Fonte: elaborada pelo autor.

Observe que ao efetuar a composição $R_{120^\circ} \circ R_{240^\circ}$ obtêm-se e que também é uma rotação do triângulo equilátero como mostrado anteriormente.

O conjunto das rotações de um triângulo equilátero em torno de seu baricentro que preservam a localização de seus vértices $R_3 = \{e, R_{120^\circ}, R_{240^\circ}\}$, juntamente com a operação de composição de rotações ($\circ$), forma um grupo cuja tábua de operação é descrita na tabela 5.

Tabela 5: Tábua de operações de rotações do triângulo equilátero.

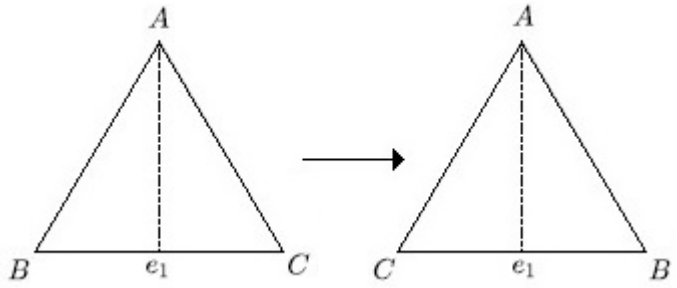
$\circ$	e	R_{120°	R_{240°
e	e	R_{120°	R_{240°
R_{120°	R_{120°	R_{240°	e
R_{240°	R_{240°	e	R_{120°

De fato, analisando a tábua de operações verifica-se que e é o elemento neutro. Além disso, é válida a associatividade, por se tratar de composição de rotações. E as inversas de e, R_{120° e R_{240° são, respectivamente, e, R_{240° e R_{120°. Portanto efetivamente se trata de um grupo.

Observe que $(R_3, \circ)$ é um grupo abeliano. De fato, pois $R_{120^\circ} \circ R_{240^\circ} = R_{240^\circ} \circ R_{120^\circ}$, $R_{120^\circ} \circ e = e \circ R_{120^\circ}$, $R_{240^\circ} \circ e = e \circ R_{120^\circ}$.

Outro movimento que pode-se fazer com o modelo de modo a sobrepô-lo ao desenho do triângulo equilátero é chamado reflexão. A reflexão consiste em girar o modelo em π radianos em torno da reta e_1 que passa pelo ponto A e o baricentro do triângulo como apresentado na Figura 7.

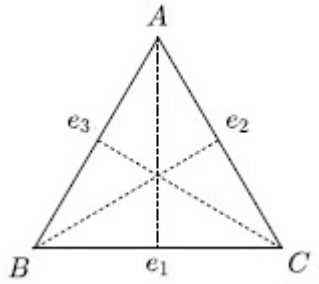
Figura 7: Triângulo Refletido em torno do eixo e_1.



Fonte: elaborada pelo autor.

Existem ainda mais dois eixos em torno dos quais o triângulo pode ser refletido de modo a se sobrepor ao desenho feito no papel. Esses eixos são e_2 e e_3 mostrados na Figura 8.

Figura 8: Triângulo com os eixos e_1, e_2 e e_3.



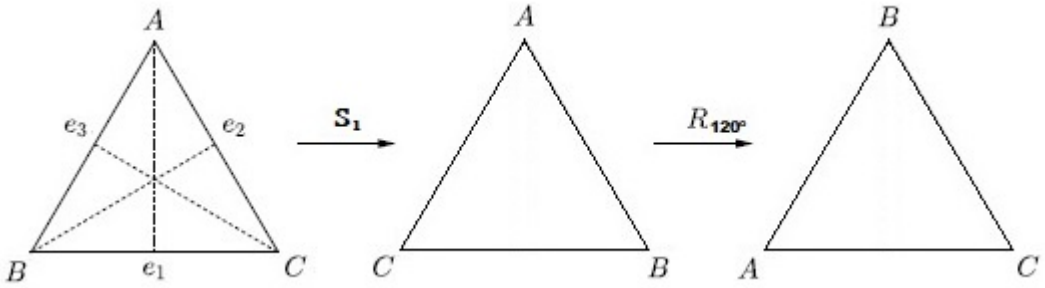
Fonte: elaborada pelo autor.

Existe três reflexões do triângulo equilátero. A seguir será listado quais são as reflexões e uma comparação entre a posição inicial e final do triângulo.

- Reflexão em torno de e_1; sendo denotada por S_1. Aqui, após a reflexão, o vértice A é levado em si mesmo; o vértice B é levado no vértice C; e o vértice C é levado no vértice B;
- Reflexão em torno de e_2; sendo denotada por S_2. Neste caso, após a reflexão, o vértice A é levado no vértice C; o vértice B é levado no vértice B; e o vértice C é levado no vértice A;
- Reflexão em torno de e_3; sendo denotada por S_3. Agora, após aplicar a reflexão, o vértice A é levado no vértice B; o vértice B é levado no vértice A; e o vértice C é levado em si mesmo.

É possível efetuar a composição de rotações com reflexões. Ao efetuar a composição $R_{120^\circ} \circ S_1$. Primeiro efetua-se a reflexão S_1, para só então aplicar a rotação R_{120°. Observe na Figura 9 como fica a composição dos dois movimentos.

Figura 9: Ilustração da composição $R_{120^\circ} \circ S_1$.



Fonte: elaborada pelo autor.

O conjunto $D_3 = \{e,\ R_{120^\circ},\ R_{240^\circ},\ S_1,\ S_2,\ S_3\}$ formado por todas as rotações e reflexões de um triângulo equilátero é um grupo denotado por grupo diedral $(D_3, \circ)$.

De fato, pode-se verificar que e é o elemento neutro do grupo. É válida a associatividade, por se tratar de composição de transformações. E as inversas de e, R_{120°, R_{240°, S_1, S_2 e S_3

são respectivamente e, R_{240°, R_{120°, S_1, S_2, S_3. Portanto efetivamente se trata de um grupo. A tábua de operações deste grupo é dada por:

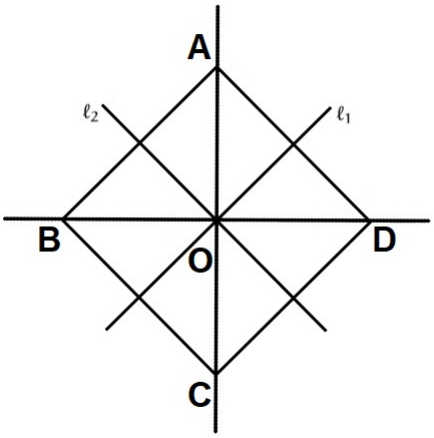
Tabela 6: Tábua de operações do grupo diedral D_3 do triângulo equilátero

$\circ$	e	R_{120°	R_{240°	S_1	S_2	S_3
e	e	R_{120°	R_{240°	S_1	S_2	S_3
R_{120°	R_{120°	R_{240°	e	S_3	S_1	S_2
R_{240°	R_{240°	e	R_{120°	S_2	S_3	S_1
S_1	S_1	S_2	S_3	e	R_{120°	R_{240°
S_2	S_2	S_3	S_1	R_{240°	e	R_{120°
S_3	S_3	S_1	S_2	R_{120°	R_{240°	e

Observe que é possível descrever essas seis bijeções do grupo $(D_3, \circ)$ a partir de $r = R_{120^\circ}$ e $s = S_1$, pois $e = s^2$, $R_{120^\circ} = r$, $R_{240^\circ} = r^2$, $S_1 = s$, $S_2 = s \circ r$ e $S_3 = s \circ r^2 = r \circ s$.

Ao analisar as rotações e reflexões de um quadrado de vértices A, B, C, D, observa-se que as rotações ocorrem a partir do centro O do quadrado, ou seja, no encontro das diagonais $\overleftrightarrow{AC}$ e $\overleftrightarrow{BD}$ do quadrado, no sentido anti-horário, girando por ângulos de 90°. E as reflexões ocorrem em relações às duas diagonais $\overleftrightarrow{AC}$ e $\overleftrightarrow{BD}$ e às retas l_1 formada pela perpendicular do lado $\overline{AD}$ passando pelo ponto médio de $\overline{BC}$ e à l_2 formada pela perpendicular do lado $\overline{AB}$ passando pelo ponto médio de $\overline{CD}$. Conforme figura 10.

Figura 10: Quadrado de centro O

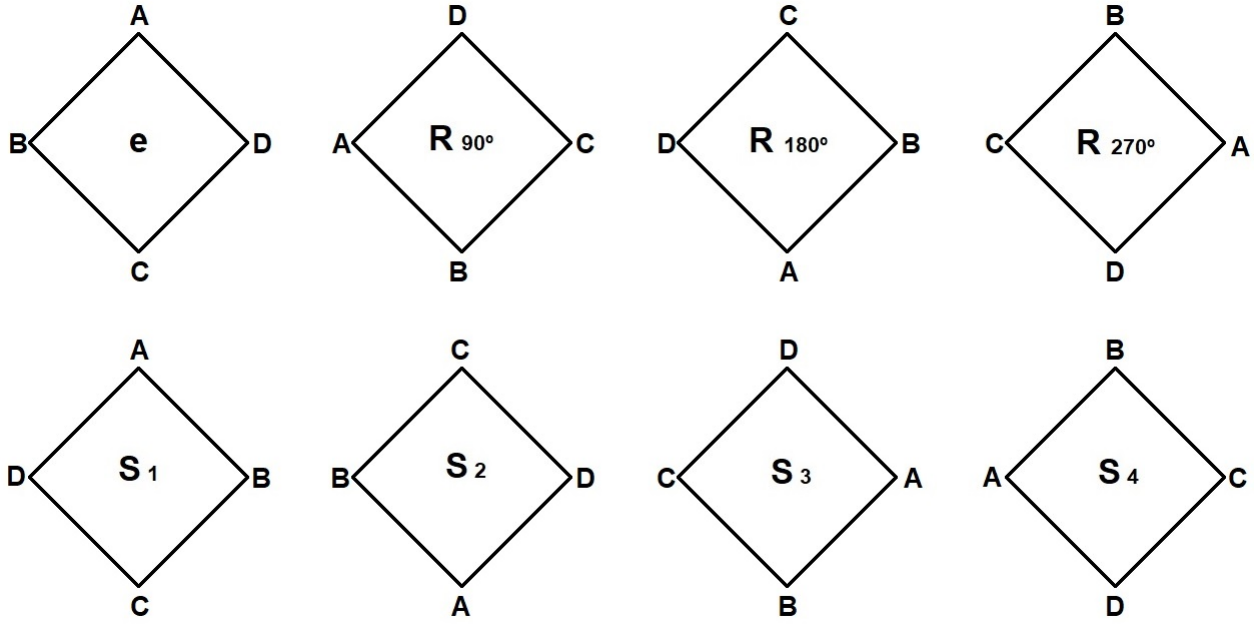


Fonte: elaborada pelo autor.

Existem quatro rotações do plano em torno do ponto O, no sentido anti-horário, que deixam o quadrado invariante, isto é, e é o elemento neutro formado pela rotação de 360°, o elemento R_{90° é a rotação de 90°, o elemento R_{180° é a rotação de 180° e o elemento R_{270° é a rotação de 270°. Além disso, existem quatro reflexões S_1 é a reflexão através da diagonal $\overleftrightarrow{AC}$, S_2 é a reflexão através da diagonal $\overleftrightarrow{BD}$, S_3 é a reflexão através da reta l_1 e S_4 é a

reflexão através da reta l_2. O conjunto D_4 é formado por oito bijeções a saber, $D_4 = \{e,$ R_{90°, R_{180°, R_{270°, S_1, S_2, S_3, $S_4\}$ que são todas as rotações e reflexões do quadrado. A Figura 11 representa essas transformações de forma geométrica.

Figura 11: Conjunto D_4



Fonte: elaborada pelo autor.

A tábua de operações de D_4 é dada por:

Tabela 7: Tábua de operações de D_4.

$\circ$	e	R_{90°	R_{180°	R_{270°	S_1	S_2	S_3	S_4
e	e	R_{90°	R_{180°	R_{270°	S_1	S_2	S_3	S_4
R_{90°	R_{90°	R_{180°	R_{270°	e	S_3	S_4	S_2	S_1
R_{180°	R_{180°	R_{270°	e	R_{90°	S_2	S_1	S_4	S_3
R_{270°	R_{270°	e	R_{90°	R_{180°	S_4	S_3	S_1	S_2
S_1	S_1	S_4	S_2	S_3	e	R_{180°	R_{270°	R_{90°
S_2	S_2	S_3	S_1	S_4	R_{180°	e	R_{90°	R_{270°
S_3	S_3	S_1	S_4	S_2	R_{90°	R_{270°	e	R_{180°
S_4	S_4	S_2	S_3	S_1	R_{270°	R_{90°	R_{180°	e

A partir da tábua de operações é possível ver que a composição de simetrias é uma operação em D_4. A composição de aplicações é associativa, portanto vale a associatividade em D_4. O elemento neutro é dado por e como pode ser visto na tábua de operações. E as inversas dos seus elementos são $e' = e$, ${R_{90^\circ}}' = R_{270^\circ}$, ${R_{180^\circ}}' = R_{180^\circ}$, ${R_{270^\circ}}' = R_{90^\circ}$, ${S_1}' = S_1$, ${S_2}' = S_2$, ${S_3}' = S_3$ e ${S_4}' = S_4$. Portanto, D_4 é um grupo.

Observe que o conjunto D_4 pode ser descrito utilizando $r = R_{90^\circ}$ e $s = S_1$, de fato $e = s^2$, $R_{90^\circ} = r$, $R_{180^\circ} = r^2$, $R_{270^\circ} = r^3$, $S_1 = s$, $S_2 = s \circ r^2$, $S_3 = s \circ r$ e $S_4 = r \circ s$.

Teorema 4.1 *O conjunto D_n das simetrias de um polígono regular de n lados é grupo com a operação composição de aplicações. O grupo $(D_n, \circ)$, também é conhecido como Grupo Diedral de ordem $2n$ e, constituí-se por n rotações de $k\frac{2\pi}{n}$ em torno do centro de gravidade, para $k = \{0, 1, ..., n-1\}$, e por n reflexões em torno dos eixos de simetria do polígono.*

Teorema 4.2 *O conjunto D_n é grupo.*

Demonstração: A operação de composição está bem definida, ou seja,
$R_i \circ S^u \circ R_j \circ S^v \in D_n$.
Sejam $(R_i \circ S^u; \circ R_j \circ S^v) \in D_n \times D_n$, com i, $j \in \{0, 1, \cdots, n-1\}$ e u, $v \in \{0, 1\}$.
Para isso, observar-se os seguintes casos:
(1) Para $u = 0$ segue que $R_i \circ S^0 \circ R_j \circ S^v = R_i \circ e \circ R_j \circ S^v = R_i \circ R_j \circ S^v = R_{i+j} \circ S^v \in D_n$.
(2) Para $u = 1$ segue que $R_i \circ S \circ R_j \circ S^v = R_i \circ R_{n-j} \circ S \circ S^v = R_{n+i-j} \circ s^{v+1} \in D_n$.
Note que $S^2 = S \circ S = e$ ou $S^3 = S \circ S \circ S = e \circ S = S$ e, portanto, podem-se reduzir as potências de S a e ou S.
Vale a associatividade em D_n, pois é decorrente da operação composição.
D_n possui um elemento neutro, em que $S^0 = e$.
Existe um elemento inverso:
Agora resta provar que $R_i \circ S^u \in D_n$ possui um inverso. Basta observar os casos a seguir:
(1) Para $u = 0$: Se $R_i \circ S^0 = R_i$, então R_{n-i} é o inverso de $R_i \circ S^0$. Basta verificar que $R_i \circ R_{n-i} = e$.
(2) Para $u = 1$: Como $R_i \circ S \circ R_i \circ S = R_i \circ R_{n-i} \circ S \circ S = R_n \circ S^2 = e \circ e = e$.
Portanto, o inverso de $R_i \circ S$ é ele mesmo.
Mostrando assim que D_n é grupo. □

5 Teorema de Cayley

Nesta seção exibimos o homomorfismo, isomorfismo e Teorema de Cayley, usando como referências [7, 11, 13, 14].

Correspondências entre grupos são tratadas através de homomorfismos e isomorfismos. O teorema de Cayley fará uso dessas definições.

As funções entre grupos que preservam as operações destes grupos são chamadas de homomorfismos de grupos.

Definição 5.1 *Sejam $(G, \triangle)$ e $(H, *)$ grupos. Um homomorfismo de G em H é uma função $f : G \longrightarrow H$ que satisfaz*

$$f(a \triangle b) = f(a) * f(b), \ \forall\, a, b \in G.$$

Exemplo 5.1 *Considere os grupos* $(\mathbb{C}^*, .)$ *e* $(\mathbb{R}^*, .)$*. A função*

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

é um homomorfismo de grupos.

De fato, pois

$$\varphi(z, w) = |z.w| = |z|.|w| \Pi(z).\varpi(w),$$

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

Definição 5.2 *Sejam dois grupos* $(G, .)$ *e* $(G', *)$*. A função* $\varpi : G \longrightarrow G'$ *é um isomorfismo de grupos, se e somente se,* ϖ *é um homomorfismo de grupos bijetor.*

A seguinte notação é utilizada para grupos isomorfos: $G \simeq G'$.

Observação 5.1 *Grupos isomorfos possuem a mesma quantidade de elementos, seus elementos são correspondentes e possuem a mesma tábua de operação.*

Exemplo 5.2 *O grupo* S_3 *é isomorfo ao grupo* D_3*.*

De fato, considere o conjunto S_3 formado pelas permutações dos elementos $\{1, 2, 3\}$. A representação do conjunto é dado por $S_3 = \{e_s, P_1, P_2, P_3, P_4, P_5\}$ onde:

$$e_s = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} ; P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} ; P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix};$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} ; P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ e } P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

e o grupo $D_3 = \{e, R_{120^\circ}, R_{240^\circ}, S_1, S_2, S_3\}$ como já visto anteriormente.

O grupo S_3 possui as mesmas características do grupo diedral D_3. De fato, os elementos do conjunto $S_3 = \{e_s, P_1, P_2, P_3, P_4, P_5\}$ correspondem respectivamente aos elementos $\{e, R_{120^\circ}, R_{240^\circ}, S_1, S_2, S_3\}$ do conjunto D_3 e S_3 e D_3 possuem a mesma tábua de operações. Portanto os grupos são isomorfos.

Existem algumas maneiras interessantes de relacionar um grupo G com um outro grupo H, como os homomorfismos e os isomorfismos. Um dos casos mais notáveis destas relações está no exemplo anterior em que é mostrado que o grupo diedral D_3 é isomorfo ao grupo de permutações S_3.

A natureza dos grupos variam amplamente por exemplo, há grupos de números, grupos de permutações, grupos de matrizes, grupos diedrais, entre outros. O objetivo do Teorema de Cayley é mostrar que há um certo elo entre todos os tipos de grupos. Ao longo da história da matemática, a maioria dos grupos finitos surgiu como grupos de permutações. Ocorre que todo grupo é isomorfo a um subgrupo de um grupo de permutações. O teorema de Cayley garante esse fato e tem a vantagem de dar um certo caráter de concretude ao grupo de estudo por mais abstrato que ele seja. O Teorema de Cayley enuncia-se como abaixo.

Teorema 5.1 *Se G é um grupo, a aplicação $T : G \to B_ij(G)$ que associa a cada elemento g a translação T_g isto é, $T_g(x) = gx$ é isomorfismo de grupo.*

Demonstração: Seja G um grupo e considere o grupo de permutações $B_{ij}(G)$. Defina

$$\begin{array}{c} T : G \longrightarrow B_{ij}(G) \\ g \mapsto T_g, \end{array}$$

onde

$$\begin{array}{c} T_g : G \longrightarrow G \\ x \mapsto gx. \end{array}$$

Note que se $g = h$, então $T_g = T_h$, pois $T_g(x) = gx = hx = T_h(x)$, $\forall x \in G$. Além disso, T_g é claramente bijetora. Logo, T está bem definida.
T é homomorfismo de grupos. De fato, dados $g_1, g_2 \in G$:
$T_{g_1g_2}(x) = g_1g_2x = g_1(g_2x) = T_{g_1}(T_{g_2}(x)) = (T_{g_1} \circ T_{g_2})(x)$, $\forall x \in G$.
Isso mostra que
$T_{g_1g_2} = T_{g_1} \circ T_{g_2}$, então $T(g_1g_2) = T(g_1) \circ T(g_2)$.
Portanto, T é homomorfismo de grupos.
Observe que T é injetora, mostrando que $N(T) = e$.
Seja $g \in G$, então:

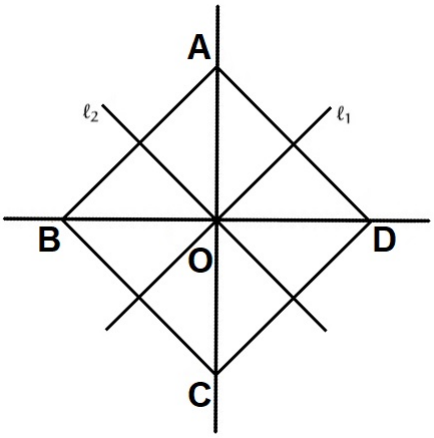
$$\begin{array}{c} g \in N(T) \Leftrightarrow T(g) = Id \Leftrightarrow T_g = Id \\ T_g(x) = Id(x), \forall x \in G \\ \Leftrightarrow gx = x, \forall x \in G \\ \Leftrightarrow g = e. \end{array}$$

Logo, $N(T) = \{e\}$ e T é injetora. Segue que $G \simeq T(G) \leq B_{ij}(G)$.
Portanto, G é isomorfo a um subgrupo do grupo de permutações $B_{ij}(G)$. □

Exemplo 5.3 *O grupo D_4 é isomorfo a um subgrupo grupo S_4.*

De fato, seja um quadrado de vértices ABCD. Sejam AC e BD as diagonais, l_1 e l_2 as mediatrizes do quadrado e O o baricentro da figura. Considere o conjunto das transformações que preservam o quadrado, com a operação de composição.

Figura 12: Quadrado de centro O



Fonte: elaborada pelo autor.

Essas transformações consistem em $e, R_{90^\circ}, R_{180^\circ}, R_{270^\circ}$, as rotações centradas em O, no sentido anti-horário, de ângulos zero, $90^\circ, 180^\circ$ e 270° respectivamente, e S_1, S_2, S_3, S_4, as reflexões em torno das retas AC, BD, l_1 e l_2 respectivamente. Portanto $D_4 = \{e, R_{90^\circ}, R_{180^\circ}, R_{270^\circ}, S_1, S_2, S_3, S_4\}$.

D_4 munido da operação de composição de funções é um grupo, conforme abordado na seção grupos diedrais.

Ao analisar a tabela 7 dada na seção grupos diedrais, note que para cada um dos elementos de D_4, observando a posição dos quatro vértices iniciando pelo vértice superior podemos definir as seguintes funções:

$$\varphi(e) = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix} \text{ que pode ser identificada com a permutação } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix};$$

$$\varphi(R_{90^\circ}) = \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix} \text{ que pode ser identificada com a permutação } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix};$$

$$\varphi(R_{180^\circ}) = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} \text{ que pode ser identificada com a permutação } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix};$$

$$\varphi(R_{270^\circ}) = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix} \text{ que pode ser identificada com a permutação } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix};$$

$$\varphi(S_1) = \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} \text{ que pode ser identificada com a permutação } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix};$$

$$\varphi(S_2) = \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix} \text{ que pode ser identificada com a permutação } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix};$$

$$\varphi(S_3) = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} \text{ que pode ser identificada com a permutação } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix};$$

$$\varphi(S_4) = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} \text{ que pode ser identificada com a permutação } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Portanto, pelo teorema de Cayley o conjunto

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

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

Exemplo 5.4 *Sejam* $G = \{2^m 3^n \,/\, m,\, n \in \mathbb{Z}\}$ *e* $J = \left\{ \begin{bmatrix} m & n \\ -n & m \end{bmatrix} / \, m,\, n \in \mathbb{Z} \right\}$. *O grupo* $(G, .)$ *é isomorfo ao subgrupo* $(J, +)$.

Primeiro deve-se mostrar que $(G, .)$ é subgrupo de $(\mathbb{R}_+^*, .)$. Escolhendo $m = n = 1$, obtêm-se $6 = 2^1.3^1 \in G$ o que implica que G não é um conjunto vazio. Sejam $x, y \in G$. Existem m, n, r, $s \in \mathbb{Z}$ tais que $x = 2^m 3^n$ e $y = 2^r 3^s$ implica que $x.y^{-1} = 2^m 3^n 2^{-r} 3^{-s} = 2^{m-r} 3^{n-s}$.

Como $m - r \in \mathbb{Z}$ e $n - s \in \mathbb{Z}$, segue que $x.y^{-1} \in G$ de onde concluí-se que G é um subgrupo de $(\mathbb{R}_+^*, .)$.

Agora, deve-se mostrar que $(J, +)$ é subgrupo de $(M_2(\mathbb{R}), +)$. Para isso atribuindo um valor qualquer a m e n, por exemplo, escolhendo $m = 2e n = 0$ obtêm-se $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in J$ segue que $J \neq 0$. Sejam $X, Y \in J$. Existem m, n, r, $s \in \mathbb{Z}$ tais que $X = \begin{bmatrix} m & n \\ -n & m \end{bmatrix}$ e $Y = \begin{bmatrix} r & s \\ -s & r \end{bmatrix}$. Então, $X + (-Y) = \begin{bmatrix} m & n \\ -n & m \end{bmatrix} - \begin{bmatrix} r & s \\ -s & r \end{bmatrix} = \begin{bmatrix} m-r & n-s \\ -n+s & m-r \end{bmatrix}$. Como $m - r \in \mathbb{Z}$, $n - s \in \mathbb{Z}$ e $-n + s = -(n - s)$ segue que $X - Y \in J$. Logo, J é um subgrupo de $(M_2((R), +)$.

Para mostrar que existe isomorfismo entre G e J, deve-se encontrar uma função $f : G \longrightarrow J$ que seja bijetora e homomorfismo de grupos.

Seja $f : G \longrightarrow J$ definida por $f(2^m 3^n) = \begin{bmatrix} m & n \\ -n & m \end{bmatrix}$.

Sejam m, n, r, $s \in \mathbb{Z}$ tais que $f(2^m 3^n) = f(2^r 3^s)$. Daí,

$$\begin{bmatrix} m & n \\ -n & m \end{bmatrix} = \begin{bmatrix} r & s \\ -s & r \end{bmatrix}$$

Então, $m = r$ e $n = s \Rightarrow 2^m 3^n = 2^r 3^s$. Isso mostra que f é uma função injetora.

Dado um elemento genérico $Y \in J$, tem-se que Y é da forma $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, onde $a, b \in \mathbb{Z}$. Escolhendo $x = 2^a 3^b \in G$ tem-se que $f(x) = f(2^a 3^b) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = Y$. Logo, f é uma função sobrejetora.

6 Aplicação

De acordo com a Base Nacional Comum Curricular [5], o conceito de simetria aparece no primeiro ciclo, onde o aluno deve ser capaz de observar se as formas geométricas presentes em elementos naturais e nos objetos criados pelo homem são simétricos ou não, e a partir do segundo ciclo sendo utilizado para identificar características das figuras geométricas, percebendo semelhanças e diferenças entre elas. Também no segundo ciclo é introduzido aos alunos os movimentos de reflexão e rotação, utilizando o plano cartesiano.

O uso de rotações de poliedros pode fazer com que o aluno experimente e entenda intuitivamente conceitos como a composição de funções, comutatividade e não comutatividade

de operações, representação algébrica e mesmo a simplificação dessas operações a partir da identificação de suas propriedades.

A composição de funções é feita aplicando uma função e sobre o resultado aplicando a outra, ou seja, os alunos aplicaram uma transformação de rotação ou reflexão e ao resultado dessa transformação aplicará outra transformação de rotação ou reflexão através de duas transformações seguidas.

É possível observar a comutatividade ou não comutatividade do conjunto de transformações, quando existe comutatividade das operações e em quais momentos isso acontece com os poliedros. Existem algumas operações de transformação que são comutativas e outras não. Em geral, os alunos pensam que a comutatividade é sempre garantida e nas operações de transformações é possível mostrar que nem sempre isso acontece, algumas operações são comutativas outras não.

A representação algébrica do conjunto é a apresentação do conjunto utilizando letras, números, símbolos, etc. para que se possa manipulá-las e aplicar operações de transformação a este conjunto.

Ao analisar um grupo, pode-se identificar propriedades que permitam a simplificação de operações, por exemplo aplicar duas transformações de reflexão sobre o mesmo eixo, equivale a identidade. Então ao combinar uma certa sequência de rotações e reflexões para obter determinado resultado é possível fazer isso utilizando menos operações do que as realizadas anteriormente.

Aplicando-se transformações isométricas básicas nos poliedros, percebe-se que há correspondência de cada operação com um elemento do grupo de permutações correspondente. O Teorema de Cayley dá a importância dos grupos de permutação para teoria dos grupos, pois permite representar qualquer grupo com um subgrupo conveniente do grupo de permutações. Em outras palavras, grupos de permutação são um modelo universal para todos os grupos possíveis. O teorema de Cayley é um exemplo do que é conhecido como um teorema de representação, onde cada grupo pode ser representado como a algo razoavelmente concreto.

Objetivo da Aplicação é relacionar grupos diedrais através do teorema de Cayley com os grupos de permutações. Além disso, mostrar como se pode representar as operações dos grupos algebricamente. É possível apresentar os poliedros aos alunos de forma concreta, de modo que ele possa manipulá-los e auxiliar no desenvolvimento da atividade na visualização das operações de transformação.

Deve se restringir a regra de operações sobre o poliedro construído de forma que ela represente somente as transformações básicas, que são rotação no sentido anti-horário e a simetria de reflexão em torno de um único eixo.

A correspondência dos grupos diedrais com subgrupos dos grupos de permutação pode ser apresentada ao aluno na forma de decodificação e transmissão de códigos. No exemplo a ser mostrado no presente trabalho, é utilizado os grupos D_3 e D_4, cujos isomorfismos são descritos a seguir.

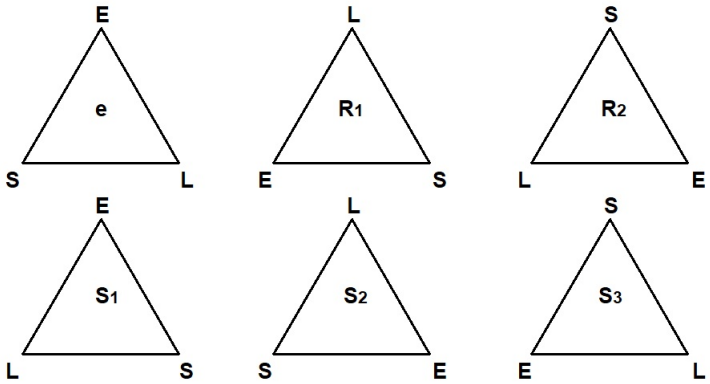
No grupo D_3, considere a posição inicial do triângulo quando a bissetriz do triângulo estiver na vertical, sendo denotada por e, que pode ser vista na Figura 13. As operações que podem ser feitas com o modelo são movimentos de rotação por ângulos de 120°, girando o palito que está no centro da figura no sentido anti-horário e a reflexão virando a figura em torno da bissetriz do vértice que está apontado para cima. É possível usar letras, símbolos,

cores, várias formas podem ser usadas para identificar os vértices dos poliedros e o movimento de rotação e reflexão. Neste trabalho é considerado os vértices do triângulo como sol, estrela e lua e o movimento de rotação denotado por r e a reflexão por s e para a composição de operações pode-se utilizar um símbolo, o mais utilizado pelos matemáticos é $\circ$.

Um exemplo de como fazer a correspondência entre o grupo D_3 e o subconjunto das permutações é considerar os vértices do triângulo de tal forma que possa formar um grupo de permutações utilizando a mesma identificação do conjunto. Se os vértices são estrela, sol e lua, para facilitar a codificação pode-se simplificar a escrita destes vértices utilizando letras do alfabeto para representá-los. No caso a estrela, sol e lua corresponde as letras E, S e L.

São obtidos seis resultados diferentes para as simetrias do triângulo, denotados por $e, R_1, R_2, S_1, S_2, S_3$, que pode ser visto na Figura 13.

Figura 13: Simetrias do triângulo.



Fonte: elaborada pelo autor.

Pode-se propor ao aluno que ele faça várias operações de composição, como por exemplo, $r \circ s \circ r^2$.

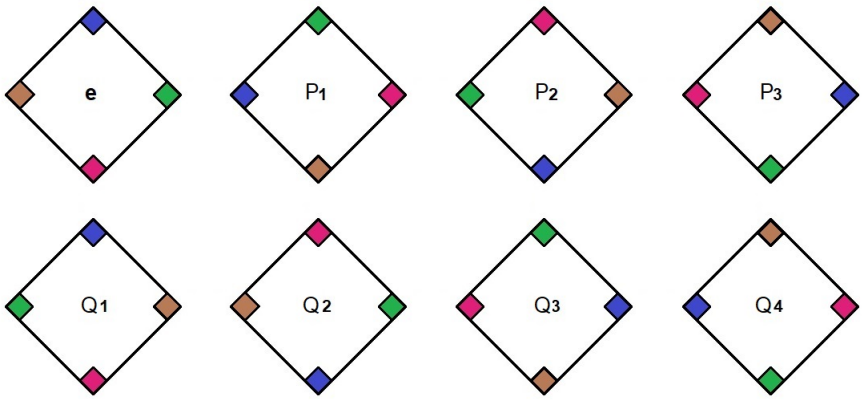
Os alunos devem ser capazes de observar que o resultado das operações, por exemplo, que a composição de transformação $r \circ s$ é diferente da composição de transformação feita invertendo a ordem da composição, ou seja, $r \circ s \neq s \circ r$, verificando assim a não comutatividade das operações. Porém para alguns elementos existe a comutatividade das operações.

O discente, após fazer várias operações, poderá perceber intuitivamente o fechamento do grupo quando consideradas as operações de e, s e r. Para formar a álgebra de interesse, devem considerar uma sequência de uma mesma operação incluindo um índice sobre-escrito, em notação semelhante à de potências. Nessa notação, r^{-1} representa uma rotação no sentido horário e a reflexão 'inversa' s^{-1}, feita como uma rotação no eixo de um vértice também no sentido contrário. A não comutatividade dessas operações deve ser um dos aspectos fundamentais a serem explorados. A partir dessa convenção é possível que o aluno identifique relações simples, realize simplificações e agrupamentos onde forem permitidos.

De maneira análoga, é possível estabelecer uma notação para as operações de simetria sobre um quadrado, que formam o grupo D_4. O conjunto é gerado pelos elementos: p, representando uma rotação de 90 graus em torno do centro do quadrado, girando no sentido anti-horário e q, uma reflexão em torno de um eixo vertical ligando dois vértices. O conjunto gerado por D_4 possui oito resultados diferentes denotados por $e = q^2$, $P_1 = p$, $P_2 = p \circ p = p^2$,

$P_3 = p \circ p \circ p = p^3$ $Q_1 = q$, $Q_2 = q \circ p \circ p = q \circ p^2$, $Q_3 = q\circ$ p e $Q_4 = p \circ q$. Os elementos $e, P_1, P_2, P_3, Q_1, Q_2, Q_3$, podem ser vistos na Figura 14.

Figura 14: Simetrias do quadrado com vértices coloridos.



Fonte: elaborada pelo autor.

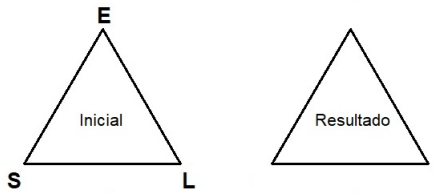
6.1 Primeira Etapa: Leitura e Escrita das Representações Algébricas

É possível apresentar um exercício ao aluno onde ele possa, inicialmente, fazer operações mais básicas. O objetivo desse exercício é que o aluno seja capaz de ler uma representação algébrica e efetuar uma sequência de operações usando letras para representar as operações no poliedro.

Embora essa primeira parte seja mais básica, alguns conceitos já estão sendo elaborados e serão mais tarde tratados, como a comutatividade ou não comutatividade de um conjunto e também a aplicação de compostas de funções.

Exemplo 6.1 *A partir do elemento neutro e indicado como posição inicial mostrada na Figura 15, execute as operações listadas e escreva a posição dos vértices na figura ao lado. Denotando por r a rotação no sentido anti-horário por ângulos de* 120° *e s a reflexão virando a figura em torno da bissetriz vertical do triângulo. a)* $r \circ s$*; b)* $r \circ s \circ r \circ s$*.*

Figura 15: Posição inicial dos vértices de um triângulo e resultado.

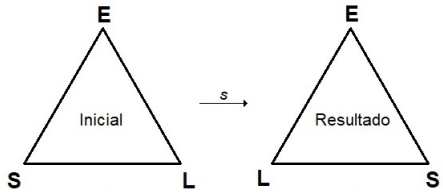


Fonte: elaborada pelo autor.

A composição de funções é executada da direita para a esquerda, portanto aplica-se a reflexão e ao resultado aplica-se a operação de rotação para encontrar o resultado do item a).

A operação s pode ser vista na Figura 16.

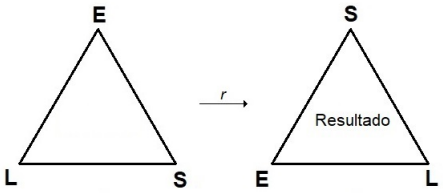
Figura 16: Operação s.



Fonte: elaborada pelo autor.

E ao resultado visto na Figura 16, efetua-se a operação r. Veja Figura 17.

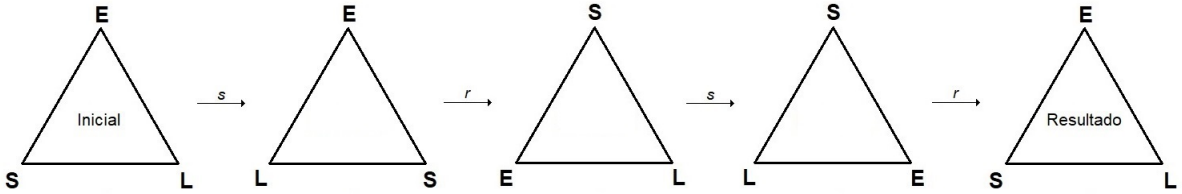
Figura 17: Operação r.



Fonte: elaborada pelo autor.

Para fazer as operações descritas em b utiliza-se novamente o triângulo inicial. O resultado da operação $r \circ s \circ r \circ s$ pode ser visto na Figura 18.

Figura 18: Operação $r \circ s \circ r \circ s$.



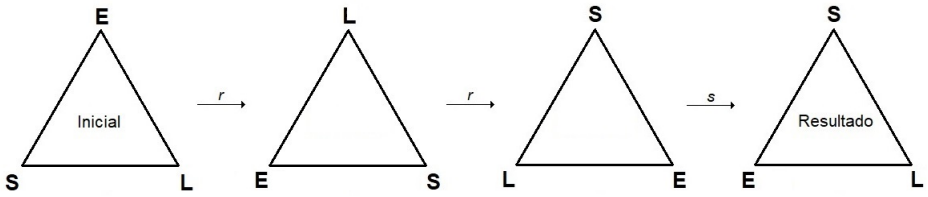
Fonte: elaborada pelo autor.

Essa parte é a mais elementar do processo de aplicação de transformações, onde é possível verificar se o aluno é capaz de absorver uma linguagem de símbolos que na verdade é a representação algébrica do conjunto que ele irá aplicar daqui em diante.

Exemplo 6.2 *Dada as operações a seguir escreva transformações alternativas que levam ao mesmo resultado. a)* $s \circ r \circ r$*; b)* $r \circ s \circ r \circ s$*.*

Primeiro é preciso descobrir o resultado da operação que pode ser vista na Figura 19.

Figura 19: Operação $s \circ r \circ r$.

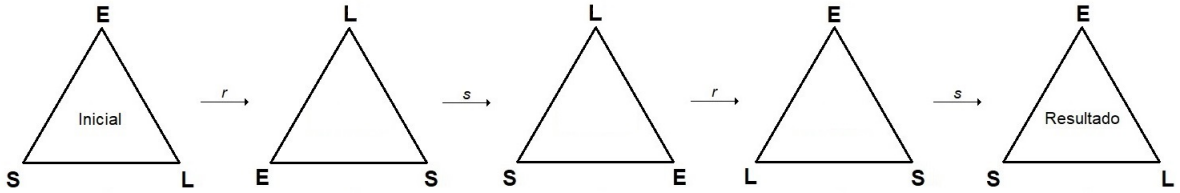


Fonte: elaborada pelo autor.

Uma sugestão é tentar apresentar uma composição de transformações mais simples que a dada, ou seja, onde se faça menos operações para obter o mesmo resultado. No exemplo 6.1, no item a), foi apresentado uma operação cujo resultado também era mesmo dado pela operação $r \circ s$.

O resultado da operação $s \circ r \circ s \circ r$ do item b) pode ser observado na Figura 20.

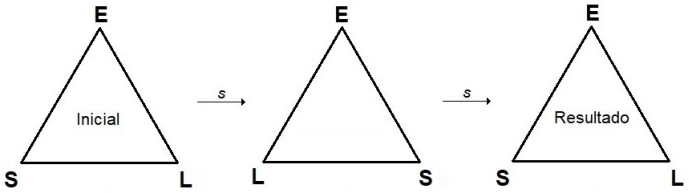
Figura 20: Operação $r \circ s \circ r \circ s$.



Fonte: elaborada pelo autor.

Uma operação em que é encontrado o mesmo resultado da operação $s \circ r \circ s \circ r$ é dada pela operação $s \circ s$ que pode ser vista na Figura 21.

Figura 21: Operação $s \circ s$.



Fonte: elaborada pelo autor.

6.2 Segunda Etapa: Simplificação de uma Representação Algébrica

A partir desse ponto, pode ser interessante que o professor ou a professora coordenando a atividade apresente algumas relações de simplificação básicas para que os alunos possam se apropriar das regras de manipulação algébrica, como por exemplo, no triângulo $s^{-1} = s$, $r \circ r = r^2 = r^{-1}$.

Nesta etapa além de obter expressões mais simples, o aluno efetua a simplificação de uma representação algébrica através da propriedade associativa da composição de transformações no poliedro. Veja o exemplo 6.3.

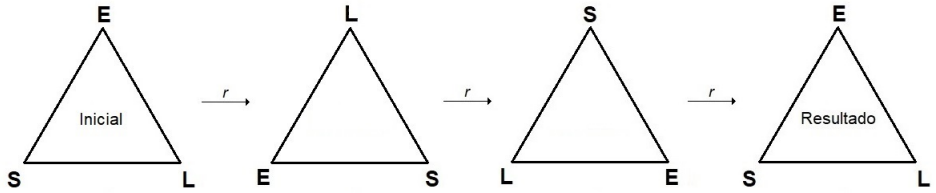
Exemplo 6.3 *Dada as composições de transformações simplifique o máximo possível as operações. a)* $s \circ s \circ r \circ s$*; b)* $s \circ r \circ r \circ r \circ s$ *c)* $s \circ r \circ r$*.*

No exemplo 6.2, item b) a operação $s \circ s$ é igual ao elemento neutro e descrito na primeira etapa como triângulo inicial. Ao operar com e significa não fazer nenhum movimento. Portanto, é possível simplificar a operação apresentada no item a) da seguinte forma:

$$s \circ s \circ r \circ s = e \circ r \circ s = r \circ s.$$

Ao analisar o item b) deve-se efetuar a operação de rotação por 3 vezes. Ao fazer esta operação obtêm-se o elemento neutro e como pode ser visto na Figura 22.

Figura 22: Operação $r \circ r \circ r$



Então é possível simplificar as operações do item b) da seguinte forma: $s \circ r \circ r \circ r \circ s = s \circ e \circ s$. Como operar com e não se faz nenhum movimento, então $s \circ e \circ s = s \circ s = e$.

No item c) como já foi mencionado $r \circ r = r^2 = r^{-1}$, então pode-se simplificar as operações da seguinte forma: $s \circ r \circ r = s \circ r^2 = s \circ r^{-1}$.

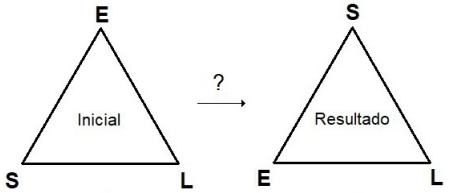
6.3 Terceira Etapa: Escrita de operações de transformações

Nessa etapa será feito o inverso da primeira etapa, ou seja, dado uma figura, quais operações podem ser feitas para se chegar ao resultado apresentado?

O objetivo dessa etapa é desenvolver a habilidade do aluno, a partir do que se já viu, de se expressar através da linguagem matemática, através de operações de transformações. Esta etapa, necessariamente deve vir após ter se cumprido todos os objetivos da primeira e segunda etapas, devido o nível de dificuldade que existe em aprender a escrever operações de transformações.

Exemplo 6.4 *Escreva uma transformação que corresponda ao elemento apresentado na Figura 23.*

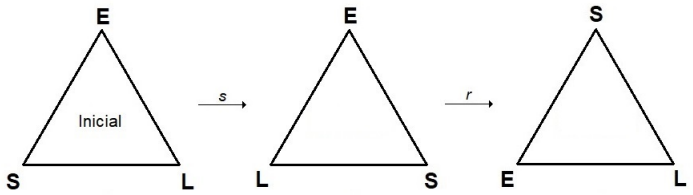
Figura 23: Resultado



Fonte: elaborada pelo autor.

Uma transformação que leva ao resultado apresentado é dada por $r \circ s$, sendo apresentada na Figura 24.

Figura 24: Operação $r \circ s$



Fonte: elaborada pelo autor.

6.4 Quarta Etapa: Propriedades das operações de transformações

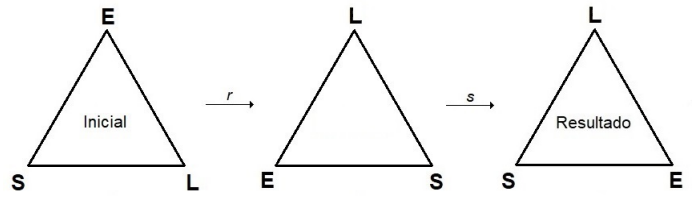
É possível trabalhar algumas propriedades das operações de transformações, como a comutatividade. O objetivo dessa etapa é que o aluno seja capaz de perceber que nem todas as operações de transformações são comutativas e também entender em quais situações a propriedade comutativa acontece.

Exemplo 6.5 *Aplique as seguintes transformações e compare os resultados obtidos.*
a) $r \circ s$ *e* $s \circ r$*; b)*$r \circ s \circ r^2$ *e* $r^2 \circ s \circ r$ *c)* $r \circ r^2$ *e* $r^2 \circ r$*.*

Observe que o exemplo quer que seja aplicado as transformações da direita para a esquerda e da esquerda para a direita e compare seus resultados.

No item a) a transformação $r \circ s$ é dada na Figura 24 apresentada no exemplo 6.4. E a transformação $s \circ r$ é dada na Figura 25.

Figura 25: Operação $s \circ r$

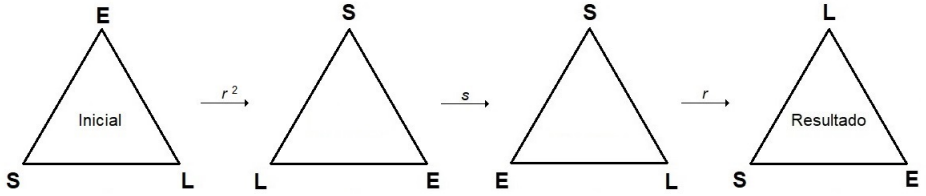


Fonte: elaborada pelo autor.

Ao comparar os resultados das transformações observa-se que $r \circ s \neq s \circ r$ mostrando que esta operação de transformação não é comutativa.

A transformação $r \circ s \circ r^2$ é dada na Figura 26.

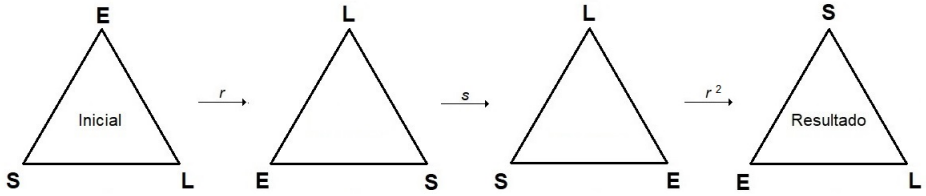
Figura 26: Operação $r \circ s \circ r^2$



Fonte: elaborada pelo autor.

E a transformação $r^2 \circ s \circ r$ pode ser vista da Figura 27.

Figura 27: Operação $r^2 \circ s \circ r$



Fonte: elaborada pelo autor.

Comparando os resultados das duas transformações verificamos que $r \circ s \circ r^2 \neq r^2 \circ s \circ r$.

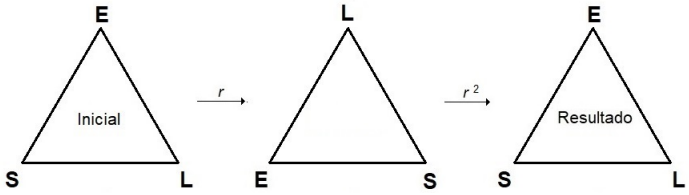
O último item c) a transformação $r \circ r^2$ é dado pela Figura 28.

Figura 28: Operação $r \circ r^2$

Fonte: elaborada pelo autor.

E a transformação $r^2 \circ r$ pode ser observada na Figura 29.

Figura 29: Operação $r \circ r^2$



Fonte: elaborada pelo autor.

Ao comparar os resultados verifica-se que $r \circ r^2 = r^2 \circ r$. Com isso pode ser observado que as operações de rotação são comutativas.

6.5 Códigos

Nesta subseção, será abordada de forma introdutória os Códigos, usando como referência [9].

Os códigos se apresentam de formas tão simples no cotidiano que, às vezes, nos permite ignorar seu funcionamento e usufruir de seus resultados. Um código é um sistema de palavras ou outros símbolos usados para representar um dado conjunto de palavras ou outros símbolos. É de conhecimento que esse conceito é comum aos sistemas de criptografia, muito vistos em filmes de espionagem e livros, mas ele é aplicado a códigos mais comuns ao cotidiano, tais como códigos binários e hexadecimais, os diferentes tipos de alfabetos (o grego e o cirílico russo moderno), a LIBRAS (linguagem brasileira de sinais), o Braile (alfabeto usado para leitura por deficientes visuais).

Um código é a representação de uma determinada palavra ou símbolo por uma outra palavra ou símbolo.

Dados dois conjuntos A e B finitos e $f : A \longrightarrow B$ uma bijeção. Assuma φ como:
$\varphi : \quad A^n \longrightarrow B^n$
$(x_1, x_2, ..., x_n) \longmapsto (f(x1), f(x2), ..., f(xn))$.

Essa função é bijetora, uma vez que cada coordenada é levada à uma imagem de uma função bijetora, caracterizando essa função como uma isometria. A partir de um código $C \subset A^n$, com m elementos e distância mínima d, ao aplicar a função $\varphi(C) = C' \subset B^n$, tem-se que a imagem é um código sobre o alfabeto B com parâmetros iguais à C. Dessa forma, é possível mudar o alfabeto de qualquer código para um alfabeto sobre um conjunto finito através de uma função bijetora $f : A \longrightarrow B$.

A vantagem desse método é poder realizar os estudos de códigos sempre sobre conjuntos finitos, uma vez que sempre é possível construir uma bijeção que leve esse alfabeto ao desejado.

Mostrar aos alunos que eles podem construir uma tabela de códigos para o alfabeto, vogais acentuadas, sinais de pontuação e demais caracteres necessários para escrever um texto utilizando os elementos de D_3 e D_4.

Observe que é possível identificar os elementos de D_3 através de dois dos seus vértices, uma opção é usar o vértices localizados na base do triângulo. Assim é conjunto D_3 pode ser representado por $e = SL$, $R_1 = ES$, $R_2 = LE$, $S_1 = LS$, $S_2 = SE$ e $S_3 = EL$; No

D_4 também podemos identificar seus elementos através de dois vértices adjacentes. Então os elementos de D_4 podem ser representados por $e = AM$, $P_1 = VA$, $P_2 = RV$, $R_3 = MR$, $S_1 = AV$, $S_2 = RM$, $S_3 = VR$ e $S_4 = MA$.

Um exemplo de tabela de códigos utilizando os elementos de D_3 e D_4 pode ser vista na tabela 8.

Tabela 8: Tábua de códigos.

	AM	VA	RV	MR	AV	RM	VR	MA
SL	A	G	M	S	Y	Ú	Ç	;
ES	B	H	N	T	Z	Â	(	!
LE	C	I	O	U	Á	Ê	)	?
LS	D	J	P	V	É	Ô	,	”
SE	E	K	Q	W	Í	Ã	.	-
EL	F	L	R	X	Ó	Õ	!	$

E para gerar cada código combinamos um elemento de D_3 com um elemento de D_4.

Exemplo 6.6 *Codifique a palavra amor usando os códigos da tabela anterior.*

Para gerar o código basta fazer a correspondência de cada letra com a tabela. Então A = SLAM, M = SLRV, O = LERV, R = ELRV. Gerando o código SLAMSLRVLERVELRV, para a palavra amor.

Para descobrir um código é necessário conhecer a tabela codificadora. E a partir dela, localizar cada letra e decodificar um texto.

Exemplo 6.7 *Descubra a frase gerada pelo código: LSAMLERM LEAMLERVELRVSE-AMSLMR SLAM LSMRLEVALSAMSLAMSEVR.*

Para descobrir o código basta analisar a tabela 8. A cada quatro letras, as duas primeiras correspondem a algum elemento da primeira coluna da tabela e as duas seguintes a algum elemento da primeira linha da tabela, a interseção desses dois elementos nos fornece a letra decifrada. Portanto fazendo as correspondências das letras com a tabela encontramos a frase DÊ CORES A VIDA.

A partir daí, pode-se mostrar o aluno que ele pode construir uma tabela de códigos da forma que desejar e assim poder conversar de forma codificada para que seu texto não possa ser lido facilmente por qualquer pessoa.

7 Considerações Finais

Acredita-se que este trabalho possa despertar o interesse em alunos e professores para um caráter mais contemplativo da Matemática, já que, de modo geral, o raciocínio abstrato tem

sido deixado de lado em detrimento de um treinamento que estimulam ideias meramente calcadas no pragmatismo. Para finalizar, abordou-se atividades que pudessem ser desenvolvidas com alunos do ensino fundamental, pois em sala de aula os professores são frequentemente questionados pelos alunos sobre aplicações do assunto estudado e como podem usá-lo em seu dia a dia, e muitas vezes o docente não conhece uma aplicação próxima da realidade do aluno que poderia chamar sua atenção e servir como elemento motivacional para o estudo.
Assim, as atividades propostas tinham como objetivo contextualizar o assunto que estava sendo estudado afim de tornar as aulas menos abstratas, mostrando de forma lúdica que os movimentos estudados (reflexão e rotação) estão presentes no nosso cotidiano, que o Teorema de Cayley pode ser aplicado em uma atividade para alunos do ensino fundamental e de forma que a aprendizagem fosse mais prazerosa com aulas diferenciadas facilitando o processo de ensino-aprendizagem, despertando a curiosidade e o interesse do aluno.

Comentário e agradecimento final

Agradeço primeiramente à Deus, que me deu o dom da vida e me abençoa todos os dias. E a Nossa Senhora por sua intercessão.

A minha mãe pela paciência e apoio ao longo dessa caminhada.

Aos amigos do Profmat, pela ajuda em vários momentos de dificuldades.

Aos professores, em especial meu orientador Maurício Reis e Silva Junior, pela disponibilidade, paciência, ensinamentos e persistência que contribuíram para a conclusão deste trabalho, também minha co-orientadora Amanda Gonçalves Saraiva, que me incentivou a terminar este trabalho.

À CAPES pelo apoio financeiro.

Referências

[1] ALLENBY, R. B. J. & SLOMSON, A. *How to Count an Introduction to Combinatorics*, 2ª edição, UK, (2011).

[2] BALLENTINE, L. E. *Quantum Mechanics: A Modern Development World Scientific*, Singapura, (1998).

[3] BASSALO, J. M. F. & CATTANI, M. S. D. *Teoria de Grupos*, Editora Livraria da Física, São Paulo, (2008).

[4] BAUMGART, J. K; trad: DOMINGUES, H. H.. *Tópicos de História da Matemática para uso em Sala de Aula*, Atual Editora, São Paulo, (1992).

[5] BNCC. *Base Nacional Comum Curricular* (2019). Disponível em: https://drive.google.com/drive/folders/1AtalHFmOsbpcsKzr8gt8j31ZJySGR4jZ?usp=sharin. Acessado em 10 de dezembro de 2019.

[6] CHAQUIAN, M. & de SÁ, P. F. *Algebra*, UEPA, Pará, (2011).

[7] DOMINGUES, H. H. & IEZZI, G.*Álgebra Moderna*, Atual Editora, 4ª edição reformulada, São Paulo, (2003).

[8] GALDINO, A. L. *Álgebra I: Grupos, Subgrupos e Homomorfismos de Grupos*

[9] HEFEZ, A & VILELA M. L. T. *Códigos corretores de Erros*, IMPA, Rio de Janeiro

[10] INFORSATO, A. P. *Grupos de friso*, Rio Claro, (2018).

[11] JANESH; O. R. *Álgebra II*, UFSC/EAD/CED/CFM, Florianópolis, (2008).

[12] SAKURAI, J. J. & TUAN, S. F. (editor). *Modern Quantum Mechanics*, Editora Addison Wesley, (1994).

[13] VILELA, M. L. T., Grupos, (2008).

[14] YARTEY, J. N. A. *Álgebra II*, UFBA: Instituo de Matemática e Estatística, Salvador, (2017).