Universidade Federal de Santa Catarina
Curso de Pós-Graduação em Matemática

Uma Breve Introdução à Teoria de Grupos

Rodrigo Luiz de Souza

Orientador: Prof. Dr. Fernando de Lacerda Mortari

Florianópolis, Fevereiro de 2014.

Universidade Federal de Santa Catarina

Uma Breve Introdução à Teoria de Grupos

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática, do Centro de Ciências Físicas e Matemáticas da Universidade Federal de Santa Catarina, para obtenção do grau de Mestre em Matemática com Área de Concentração PROFMAT-UFSC associado ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT).

Rodrigo Luiz de Souza

Florianópolis, Fevereiro de 2014.

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Souza, Rodrigo Luiz de Souza
Uma Breve Introdução à Teoria de Grupos / Rodrigo Luiz de Souza Souza ; orientador, Fernando de Lacerda Mortari - Florianópolis, SC, 2014.
73 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro de Ciências Físicas e Matemáticas. Programa de Pós-Graduação em Matemática.

Inclui referências

1. Matemática. 2. Permutações. 3. Teoria de Grupos. 4. Ensino Médio. I. Lacerda Mortari, Fernando de . II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Matemática. III. Título.

Uma Breve Introdução à Teoria de Grupos

por

Rodrigo Luiz de Souza

Esta dissertação foi julgada aprovada para a obtenção do Título de Mestre em Matemática e aprovada em sua forma final pelo Programa de Pós-Graduação em Matemática.

Prof. Dr. Celso Melchiades Doria
Coordenador do Curso

Banca Examinadora

Prof. Dr. Fernando de Lacerda Mortari
Universidade Federal de Santa Catarina -
Orientador

Prof. Dr. Danilo Royer
Universidade Federal de Santa Catarina

Prof. Dr. Gilles Gonçalves de Castro
Universidade Federal de Santa Catarina

Prof. Dr. Márcio Rostirolla Adames
Universidade Tecnológica Federal do Paraná

Florianópolis, 26 de fevereiro de 2014.

Este trabalho é dedicado à pessoa que acreditou em mim quando até eu mesmo já havia desistido: Thiane.

AGRADECIMENTOS

Antes de qualquer outra pessoa, gostaria de agradecer a minha esposa Thiane Pereira que tem me apoiado em todas as empreitadas ao longo dos últimos anos, sobretudo nos anos em que cursei o PROFMAT. Além dela agradeço aos meus pais Marcio Luiz de Souza e Adelair Sardá que estão sempre dispostos a ajudar mesmo quando estão nas condições mais adversas; à minha tia Maristela de Souza Goulart pelas estadias nos finais de semana; aos professores pelo conhecimento compartilhado e pelas proveitosas discussões ao longo desses dois anos, sobretudo ao professor Fernando de Lacerda Mortari pela orientação das atividades deste trabalho e aos membros da banca; ao meu colega Felipe Lamberg pelas caronas de todos os sábados; ao meu decano amigo Deividi Ricardo Pansera pelos ajustes finos feitos na etapa final da escrita deste trabalho; aos diretores Karina Ribas, Erimá Ribeiro, Alôncio da Silva e Marília Bianchini de Souza pela compreensão com minha agenda apertadíssima ao longo desses anos. A todos que de alguma maneira fizeram possível a realização desse trabalho, sobretudo à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pelo apoio financeiro ao longo do curso.

“Janelas do meu quarto,
Do meu quarto de um dos milhões do mundo que ninguém sabe quem é
(E se soubessem quem é, o que saberiam?)”
Fernando Pessoa

RESUMO

Este trabalho tem como objetivo ser uma breve introdução à Álgebra. Na parte inicial foi introduzido o conceito de permutação e sua definição como funções bijetivas de um conjunto em si mesmo. Na sequência, foi introduzido o conceito de grupo e subgrupo e apresentadas algumas das propriedades básicas de tais estruturas. No terceiro capítulo foram expostos e discutidos os conceitos de homomorfismo e de isomorfismo de modo a pavimentar o caminho para a demonstração do Teorema de Cayley que foi abordado no capítulo seguinte. Encerrando o trabalho foi apresentado um plano de aula de modo a sugerir uma aplicação do conteúdo abordado para uma turma de Ensino Médio.

Palavras-chave: Permutações. Teoria de Grupos. Ensino Médio.

ABSTRACT

The main goal of this coursework is to be a brief introduction to Algebra. In the very first part the concept of permutation was introduced and defined as a bijective function from a group in itself. After that, the concept of group and subgroup were exhibited and discussed, as well as their basic properties. In the third part of this work the concepts of homomorphism and isomorphism were exposed and discussed in order to pave the way for the demonstration of Cayley's Theorem, which was studied in the last chapter. To finish the work it was presented an application of the content covered here in a high school class.

Keywords: Permutations. Group Theory. High School.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O principal objetivo deste trabalho foi criar um material que pudesse ser utilizado por estudantes de Ensino Médio e alunos de graduação que desejem ter um primeiro contato com a Álgebra, mais especificamente com a Teoria de Grupos. Por esse motivo, ao longo do trabalho buscamos escrever um texto com o máximo possível de exemplos que sejam, se não familiares, de fácil compreensão por parte desse público. Um leitor que já tenha um contato prévio com assuntos tratados aqui, pode julgar o conteúdo um tanto elementar. Mesmo para este público, buscamos uma abordagem menos convencional, partindo do conceito de permutação para motivar o estudo de grupos. Optamos por tal abordagem em virtude do público-alvo a que destinamos nossos escritos.

No primeiro capítulo, tratamos das permutações. Nosso interesse não foi fazer grande aprofundamento teórico, mas criar uma motivação para o estudo a partir da qual seja natural compreendê-las como funções bijetivas de um conjunto em si mesmo. Isso porque, o contato com permutações durante o curso do Ensino Médio é essencialmente de quantificá-las, no sentido de contar quantas são as permutações dos elementos de um determinado conjunto finito. Como as funções bijetivas de um conjunto em si próprio tem algumas propriedades como a invertibilidade, a composição associativa e a existência da função identidade, podemos estender essas propriedades às permutações e elas nos direcionam para o estudo da Teoria de Grupos.

No segundo capítulo, novamente a partir de exemplos, motivamos o estudo dos grupos. Apresentamos a definição de grupo e alguns resultados teóricos sobre essas estruturas algébricas. Tratamos também dos subgrupos e apresentamos critérios para decidir se um determinado subconjunto não vazio de um grupo constitui um subgrupo além de exibir algumas de suas propriedades intrínsecas. Ainda nesse capítulo reservamos um espaço para o estudo dos grupos de simetria do triângulo e do quadrado, uma vez que as simetrias de tais polígonos que são um excelente recurso para se estudar grupos de permutações.

O terceiro capítulo trata basicamente do estudo dos homomorfismos e dos isomorfismos, tendo sempre em vista buscar exemplos da Matemática estudada no Ensino Médio de forma a tornar as ideias tão acessíveis quanto possível. Nessa parte do trabalho incluímos alguns resultados teóricos, de forma a alicerçar o assunto do último capítulo: o Teorema de Cayley.

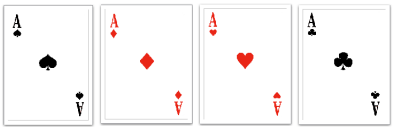
Dando prosseguimento à abordagem, chegamos ao Teorema de Cayley. Exibimos algumas situações que permitam ao leitor a aplicação do resultado demonstrado em exemplos explorados ao longo do trabalho e alguns outros exemplos correlacionados. O Teorema de Cayley também dá ao leitor um vislumbre das generalizações 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, apresentamos um plano de aula sugerindo uma aplicação do conteúdo em uma turma de Ensino Médio.

2 PERMUTAÇÕES

Consideremos um conjunto formado pelos quatro ases de um baralho comum dispostos em uma determinada ordem. Como na figura a seguir.

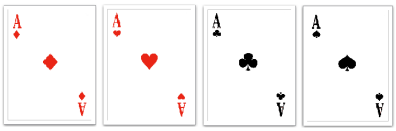
Figura 1: Uma sequência de ases.



Fonte: elaborada pelo autor.

Parece natural supor que a ordem estabelecida para se dispor estas cartas seja de natureza totalmente arbitrária e que, além disso, a sequência dada na Figura 1 não é a única iniciada pelo ás de espadas. De modo que caso o leitor desejasse começar a sequência pelo ás de ouros ao invés de iniciar pelo ás de espadas, bastaria posicionar a carta citada na primeira posição e dispor as demais em uma ordem qualquer.

Figura 2: Uma outra sequência de ases.



Fonte: elaborada pelo autor.

É evidente, pelo que foi exposto nos parágrafos anteriores, que dispor as cartas em qualquer uma das sequências citadas, mesmo aquelas iniciadas pelo naipe de ouros, é um processo totalmente aleatório, já que, para montar uma determinada sequência, é suficiente que se escolha a posição que se queira para cada carta. Observe, porém, que se quiséssemos obter a sequência que aparece na Figura 2 *a partir* da que foi dada na Figura 1, seria necessário fazermos um certo *embaralhamento*. No caso do exemplo que citamos, o embaralhamento foi obtido colocando o ás de espadas na quarta posição; o ás de ouros na primeira; o ás de copas na segunda; e o ás de paus na terceira. Desse modo, se quisermos obter uma certa sequência dos quatro ases a partir de uma sequência previamente estipulada, já não poderemos arbitrar a ordem em que colocaremos cada carta, uma vez que, a partir da sequência inicial, cada embaralhamento corresponderá a uma determinada ordem das cartas.

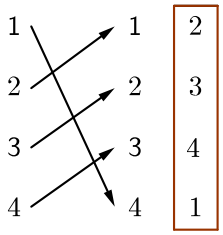
Consideremos agora uma segunda situação. Tomemos o conjunto $A = \{1,2,3,4\}$. Uma sequência possível para seus elementos é $(1,2,3,4)$. A partir daí, podemos reordenar os números da sequência como $(2,3,4,1)$. Denotaremos, de agora em diante, este embaralhamento de $(1,2,3,4)$ pela matriz

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \tag{2.1}$$

onde a primeira linha representa a sequência dada e a segunda linha exprime o embaralhamento feito com tal sequência. Em outros termos, na matriz acima, o elemento a_{2i} indica em que posição o elemento a_{1i}, $1 \leq i \leq 4$, foi alocado após o embaralhamento no seguinte sentido: os elementos da primeira coluna significa que, após o embaralhamento, o 1 ocupará a posição

que originalmente era do número 4; os elementos da segunda coluna dizem que o número 2 será mandado para a posição que era do número 1; a terceira indica que o número 3 ficará na posição que era originalmente ocupada pelo número 2; e a quarta coluna significa que o número 4 será mandado para a posição que, originalmente, era do número 3. Estas informações podem ser resumidas como no diagrama a seguir, que é uma forma mais prática de se obter a sequência permutada. A ordem resultante é aquela destacada pelo retângulo na Figura 3.

Figura 3: Esquema para o embaralhamento em (2.1).



Fonte: elaborada pelo autor.

Assim como fixamos o ás de copas na primeira posição no exemplo anterior e vimos que a partir daí podemos obter outras sequências, aqui, de modo totalmente análogo, poderíamos fixar o número 1 na quarta posição e obter outras sequências, como por exemplo

$$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix} \text{ e } \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}.$$

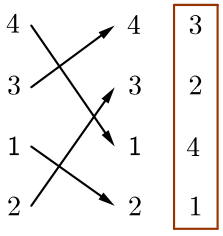
As matrizes acima correspondem, respectivamente, às sequências $(2,4,3,1)$, $(2,3,4,1)$, $(4,3,2,1)$, $(3,2,4,1)$ e $(4,2,3,1)$.

Note que o fato de termos estipulado a sequência inicial $(1,2,3,4)$ é totalmente arbitrário. Poderíamos, por exemplo, ter começado com a sequência $(4,3,1,2)$ e um embaralhamento obtido a partir dessa sequência, pelo que foi estabelecido anteriormente, seria denotado por

$$\begin{pmatrix}4&3&1&2\\1&4&2&3\end{pmatrix} \tag{2.2}$$

que corresponde ao embaralhamento $(3,2,4,1)$. Observe na Figura 4 o significado deste embaralhamento e a sequência resultante da permutação dada pela matriz acima.

Figura 4: Diagrama para o embaralhamento em (2.2).



Fonte: elaborada pelo autor.

Contudo, note que obter a sequência $(3,2,4,1)$ a partir de $(1,2,3,4)$ requer um certo em-

baralhamento, enquanto que para obter a mesma sequência a partir de $(2,3,1,4)$ devemos fazer um embaralhamento diferente. De modo que, estabelecida a sequência inicial, cada sequência é gerada a partir de uma troca de posições bem definida. Sendo assim, podemos associar a cada sequência uma determinado embaralhamento e, é claro, cada embaralhamento corresponde a uma sequência. Vamos analisar o exemplo acima por um uma perspectiva diferente. Seja $S = \{x_1, x_2, x_3, x_4\}$ e considere seus elementos organizados segundo a ordem crescente de seus índices. Poderíamos representar um embaralhamento desses elementos como em (2.1) da seguinte maneira

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_4 & x_2 & x_1 \end{pmatrix}.$$

A matriz acima nos diz que após o embaralhamento, o elemento x_1 ocupará a posição ocupada orginalmente pelo elemento x_3; o elemento x_2 a do elemento x_4; o elemento x_3 a do elemento x_2; e o elemento x_4 a do elemento x_1. Isso significa que a nova sequência para os elementos de S será (x_4, x_3, x_1, x_2). Observe que esta mesma sequência poderia ser obtida por um embaralhamento diferente se os elementos de S fossem tomados na ordem $S = \{x_1, x_3, x_2, x_4\}$ do seguinte modo:

$$\begin{pmatrix} x_1 & x_3 & x_2 & x_4 \\ x_2 & x_3 & x_4 & x_1 \end{pmatrix}.$$

Note que tomando os elementos de S ordenados de uma determinada forma e fazendo um embaralhamento, estamos estabelecendo uma relação ϕ entre os elementos de S onde $\phi(x_i) = x_j$, $1 \leq i, j \leq 4$ indica que a posição do elemento x_i após o embaralhamento será aquela ocupada originalmente pelo elemento x_j. Esta relação dá origem a uma função de S em S. Além disso, observe dois elementos x_i e x_j não podem, após o embaralhamento, ocupar uma mesma posição de um outro elemento x_k. O que significa que a função ϕ é injetiva.

Um segundo fato sobre ϕ é que todo elemento de S é imagem por ϕ de algum elemento de S. Suponha que exista, em S, um elemento tal que $\phi(x_i) \neq x_j$ para cada $1 \leq i, j \leq 4$. Ora, mas assim, teríamos uma ordenação dos elementos de S com menos de 4 elementos ou um mesmo elemento ocupando mais de uma posição. O que é absurdo. Logo, cada elemento de S, necessariamente é imagem de algum elemento de S pela função ϕ.

Gostaríamos de exprimir ϕ de uma maneira mais precisa. Uma tentativa seria exibir individualmente a imagem de cada um dos elementos $x_i \in S$. A seguir, exibimos um exemplo para $n = 4$.

$$\begin{aligned} \phi(x_1) &= x_2 \\ \phi(x_2) &= x_4 \\ \phi(x_3) &= x_1 \\ \phi(x_4) &= x_3 \end{aligned}$$

Sendo assim, a sequência resultante seria $(\phi(x_1), \phi(x_2), \phi(x_3), \phi(x_4)) = (x_2, x_4, x_1, x_3)$, ou seja, a posição de x_1 após a aplicação de ϕ é aquela ocupada por x_2; a de x_2 é a posição que era ocupada por x_4; x_3 ocupará a posição originalmente ocupada por x_1; e a de x_4 será aquela em que figurava o elemento x_4. Explicitamente, essa sequência se escreve como (x_3, x_1, x_4, x_2).

Observe, contudo, que isso acaba tornando-se inviável em algumas situações, sobretudo para valores grandes de n. Uma maneira um pouco mais econômica de se escrever ϕ é a notação exibida em (2.1). Genericamente, uma ordenação qualquer dos elementos de $(x_1, x_2 \ldots, x_n)$

obtida a partir da função ϕ pode ser representada por

$$\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_{i_1} & x_{i_2} & x_{i_3} & \cdots & x_{i_n} \end{pmatrix}, \tag{2.3}$$

onde i_k, $1 \leq k \leq n$ é a imagem do elemento x_i por ϕ.

Note que o símbolo x ainda é supérfluo em (2.3). De modo que podemos representar a imagem de $(x_1, x_2 \cdots, x_n)$ por ϕ simplesmente como

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}. \tag{2.4}$$

Onde os termos x_i da sequência s foram substituidos simplesmente pelo número da posição em que se encontram. Voltando ao caso $n = 4$ teríamos, por exemplo

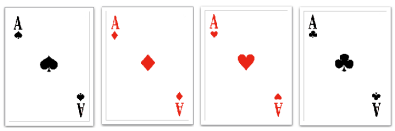
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Desse modo, se $S = \{x_1, x_2, \ldots, x_n\}$ e $\phi : S \to S$ é uma função bijetiva, então ϕ é chamada de *permutação dos elementos de S*. Como vimos logo acima, podemos nos referir a uma permutação de $(x_1, x_2, \ldots, x_n)$ como indicado em (2.4), isto é, levando em consideração apenas a posição do elemento e não sua natureza.

2.1 COMPOSIÇÃO DE PERMUTAÇÕES

Na seção anterior, vimos que uma permutação pode ser expressa por uma função. E dado o arcabouço teórico existente sobre as funções, podemos nos perguntar se podemos usar linguagem usual de funções para estudarmos as permutações. Para isso, retomemos o exemplo dado no início do capítulo envolvendo os ases de um baralho e façamos algumas considerações. Inicialmente, tínhamos sequência de cartas como na Figura 5.

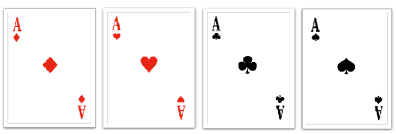
Figura 5: A mesma sequência de ases.



Fonte: elaborada pelo autor.

Considere agora a permutação ϕ cuja aplicação sobre o conjunto de ases dado na Figura 5 gera a configuração da Figura 6.

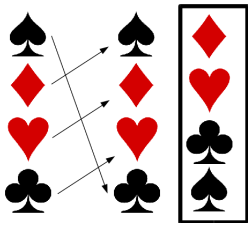
Figura 6: Configuração obtida a partir da sequência original.



Fonte: elaborada pelo autor.

O diagrama da Figura 7 mostra como obter a configuração de cartas exibida na Figura 6.

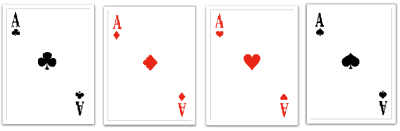
Figura 7: Diagrama que mostra como ϕ atua sobre cada uma das cartas.



Fonte: elaborada pelo autor.

Agora, considere uma nova configuração dos ases, mostrada na Figura 8 e feita a partir daquela exibida na Figura 6, por meio da permutação τ.

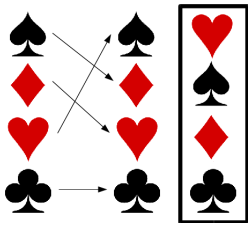
Figura 8: Permutação obtida a partir da sequência permutada.



Fonte: elaborada pelo autor.

O diagrama da Figura 9 mostra como τ atua sobre uma sequência de ases.

Figura 9: Como τ atua sobre as cartas.



Fonte: elaborada pelo autor.

Observação 2.1.1. Os símbolos dos naipes nas funções ϕ e τ referem-se à sequência original. Por exemplo, para a função τ temos que: a carta que ocupa a posição que originalmente era do ás de espadas será alocada na posição que originalmente era do ás de ouros; a carta que está na posição que era originalmente ocupada pelo ás de ouros deve ser posta na posição que originalmente era do ás de copas; a carta que está na posição que originalmente era do ás de copas será colocada na posição que originalmente era do ás de espadas; e a carta que ocupa posição que originalmente era a posição ás de paus fica inalterada.

É claro que, do ponto de vista prático, o passo intermediário poderia ser ignorado e poderíamos obter a sequência de ases da Fig. 8 aplicando uma única permutação como indicado a seguir:

$$\begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \clubsuit & \diamondsuit & \heartsuit & \spadesuit \end{pmatrix}, \tag{2.5}$$

ou seja, trocando as posições das cartas de espadas e de paus. Contudo, se analisarmos mais cuidadosamente do ponto de vista teórico a opeação realizada aqui, vemos que de algum modo, estamos efetuando uma operação com permutações. Sob a ótica do que foi apresentado na seção anterior, a operação efetuada aqui é a composição de duas funções, já que estamos aplicando uma permutação em uma configuração obtida previamente de uma outra permutação. Para a primeira permutação a imagem de cada um dos naipes dos ases é dada por

$$\phi = \begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \clubsuit & \spadesuit & \diamondsuit & \heartsuit \end{pmatrix}.$$

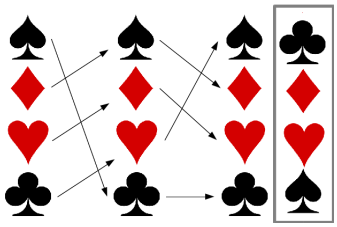
Analogamente, podemos representar a segunda permutação, função τ, cuja imagem de cada naipe pode ser escrita como

$$\tau = \begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \diamondsuit & \heartsuit & \spadesuit & \clubsuit \end{pmatrix}.$$

Para um recurso visual mais explícito da composição de τ com ϕ, nesta ordem, veja a Figura 10. Nesse diagrama, está representada a composição e a sequência resultante é aquela destacada pelo retângulo.

É importante salientar que a composição $\tau\phi$ de duas funções $\phi : A \to B$ e $\tau : B \to C$ sempre será efetuada da direita para a esquerda, isto é, dado $x \in A$, primeiro computamos $\phi(x)$, para só então aplicarmos τ sobre a imagem de x por ϕ. Assim, $\tau\phi(x) = \tau(\phi(x))$. Para efeitos de notação, temos que $\tau\phi(x) = \tau(\phi(x)) = (\tau \circ \phi)(x)$.

Figura 10: Diagrama da composição $\tau\phi$.



Fonte: elaborada pelo autor.

De modo que se efetuarmos $\tau \circ \phi$ teremos o que foi obtido em (2.5). Isso significa que podemos trocar a composição de τ com ϕ por uma única permutação. Essa operação pode ser representada como a seguir

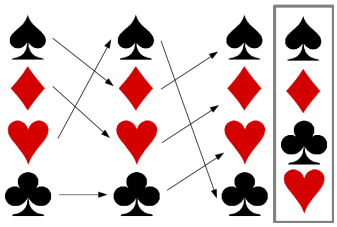
$$\tau \circ \phi = \begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \diamondsuit & \heartsuit & \spadesuit & \clubsuit \end{pmatrix} \circ \begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \clubsuit & \spadesuit & \diamondsuit & \heartsuit \end{pmatrix} = \begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \clubsuit & \diamondsuit & \heartsuit & \spadesuit \end{pmatrix}$$

Observação 2.1.2. Para efeitos de simplicidade de notação, sempre que quisermos nos referir a composição das permutações ϕ e τ, denotaremos essa operação por $\phi \cdot \tau$ ou tão somente $\phi\tau$.

Continuando nosso estudo, poderíamos nos perguntar ainda, se a ordem em que efetuamos uma composição altera a permutação obtida como resultado final. Observe no esquema a seguir como fica a composição $\phi\tau$.

Verificamos, então, que a composição de permutações *não é comutativa*, uma vez que, $\tau\phi \neq \phi\tau$. Vamos agora realizar a operação de composição $\phi\tau$ usando a notação de permutação.

Figura 11: Diagrama da composição $\phi\tau$.



Fonte: elaborada pelo autor.

$$\phi \cdot \tau = \begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \clubsuit & \spadesuit & \diamondsuit & \heartsuit \end{pmatrix} \cdot \begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \diamondsuit & \heartsuit & \spadesuit & \clubsuit \end{pmatrix} = \begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \spadesuit & \diamondsuit & \spadesuit & \heartsuit \end{pmatrix},$$

o que mostra que a operação não é comutativa.

Ainda fazendo um paralelo entre funções e permutações, podemos verificar facilmente que toda permutação pode ser invertida. Isso se deve ao fato demonstrado anteriormente que uma permutação de um conjunto finito S é uma função bijetiva de S em si mesmo. Do ponto de vista prático, isso significa que dada uma permutação de um conjunto S, sempre poderemos colocar seus elementos na posição em que eles foram dados originalmente. Isso nos obriga a considerar a própria sequência original como uma permutação dos elementos de S. Esta permutação é chamada permutação identidade. Analisando novamente o exemplo das cartas, se tomarmos a sequência original e deixarmos elas nas posições em que se encontram, este pode ser considerado um embaralhamento dos quatro ases! Analisando do ponto de vista teórico, podemos mostrar que dado um conjunto finito S com n elementos tomados em uma ordem pré estabelecida, existe uma permutação que não altera a ordem dos elementos de S. Basta que para isso, tomemos a seguinte permutação

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

Uma dúvida ainda permanece: será que existe uma segunda permutação que não altera a ordem estabelecida previamente dos elementos de um conjunto S? Essa conjectura é facilmente refutada pois, se e_1 e e_2 são duas permutações distintas que não alteram a ordem dos elementos de S. Temos que

$$\begin{aligned} e_1 e_2 &= e_1 \\ e_1 e_2 &= e_2 \end{aligned}$$

A primeira das igualdades acima é válida pois, a permutação e_2 é uma permutação identidade e portanto, ao aplicarmos tal permutação sobre e_1 obteremos a própria permutação e_1. De forma análoga, a segunda igualdade é verdadeira. As igualdades que acabamos de discutir mostram que só pode existir uma única permutação identidade. Em última instância, poderíamos nos perguntar se dadas três permutações, ϕ, τ e μ de S em S, S um conjunto finito, se a operação é associativa, isto é, poderíamos questionar a validade da igualdade

$$(\phi\tau)\mu = \phi(\tau\mu). \tag{2.6}$$

E, mais uma vez, o fato de termos definido permutação como uma função nos será útil, uma vez

que, sendo a composição de funções associativa, também o será a composição de permutações.

A natureza das operações que viemos realizando até aqui guardam certas características intrínsecas que não dependem dos objetos que usamos para efetuá-las. No nosso caso, tais objetos são as permutações, mas a esta altura o leitor já deve ter percebido que as propriedades estudadas não são de exclusividade das permutações. Na Matemática, não é difícil exemplificar operações que atuam sobre os elementos de um determinado conjunto e que tenham as propriedades listadas anteriormente. A discussão que fizemos até aqui pode ser generalizada pela *Teoria de Grupos* que será nossso objeto de estudo no próximo capítulo.

3 TEORIA BÁSICA DE GRUPOS

3.1 NOÇÕES PRELIMINARES

Neste capítulo vamos generalizar alguns dos conceitos vistos no capítulo anterior e passaremos a estudar uma das partes fundamentais da Álgebra Abstrata, a *Teoria de Grupos*. Contudo, antes de começarmos a descrever formalmente o que são grupos, vamos considerar um exemplo bastante ingênuo.

Exemplo 3.1.1. Considere o conjunto $\mathbb{Z}$ dos números inteiros, com a operação usual de adição. Usaremos aqui a notação usual desta operação, ou seja, $a+b$, onde $a,b \in \mathbb{Z}$. Sabemos de antemão algumas propriedades desse conjunto com a operação considerada. Por exemplo, sabemos que $a+b \in \mathbb{Z}$, ou seja, $\mathbb{Z}$ é fechado com relação à soma. Além disso, dados $a,b,c \in \mathbb{Z}$ é sabido que a operação de adição é associativa. Simbolicamente, isso significa que $(a+b)+c = a+(b+c)$. Temos ainda um elemento $e \in \mathbb{Z}$ para o qual $a+e = e+a = a$ para cada $a \in \mathbb{Z}$. Nesse caso, temos que $e = 0$. E, finalmente, sabemos que para cada $a \in \mathbb{Z}$, existe um outro elemento b, também em $\mathbb{Z}$, tal que $a+b = b+a = e$. Como $e = 0$, concluímos que $b = -a$.

No exemplo anterior consideramos um conjunto com uma operação e infinitos elementos, porém, nada nos impede de criar um conjunto finito com a mesma estrutura descrita anteriormente.

Exemplo 3.1.2. Observe que o conjunto $G = \{1,-1\}$, com a operação de multiplicação usual de números reais, guarda as mesmas propriedades descritas no Exemplo 3.1.1. De fato, se multiplicarmos dois elementos de G, o produto ainda permanece em G. A operação de multiplicação é trivialmente associativa. Sabemos ainda que existe $e \in G$ tal que $e \cdot a = a \cdot e = a$ para cada $a \in G$. A saber, tal elemento é o número 1. E, por fim, observe que para cada elemento de G, existe um elemento b tal que $a \cdot b = b \cdot a = e$. Lembre-se de que $e = 1$. Observe que para para $a = 1$, temos que $b = 1$; e para $a = -1$, ocorre que $b = -1$.

O leitor deve lembrar-se de que ao discutirmos as operações de permutação e composição de permutação no capítulo anterior, elas tinham as mesmas propriedades apresentadas nos exemplos 3.1.1 e 3.1.2. Naquele contexto,verificamos que a composição de permutações ainda é uma permutação; que a composição de permutações é associativa; a existência (e unicidade) do elemento neutro, que chamamos de permutação identidade; e que toda permutação possui inversa, isto é, se ϕ é uma permutação de um conjunto finito de elementos então existe ϕ^{-1} tal que $\phi \cdot \phi^{-1} = \phi^{-1} \cdot \phi = e$, onde e é a permutação identidade.

De modo geral, podemos estabelecer uma definição:

Definição 3.1.1. Um *grupo* consiste de um conjunto não vazio G, munido de uma operação indicada por $\cdot$ (isto é, uma regra que a cada par ordenado de elementos (a,b) de G associa um terceiro elemento de G que denotaremos por $a \cdot b$) satisfazendo as seguintes propriedades:

(i) $a,b,c \in G$ implica que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, ou seja, a operação é *associativa*.

(ii) Existe um elemento $e \in G$ tal que para todo $a \in G$ vale $a \cdot e = e \cdot a = a$ para todo $a \in G$. O elemento e é denominado *elemento neutro de G com relação à operação* $\cdot$.

(iii) Para todo $a \in G$ existe um elemento $a^{-1} \in G$ tal que $a \cdot a^{-1} = a \cdot a^{-1} = e$. O elemento a^{-1} é denominado *inverso de a pela operação* $\cdot$.

Tendo em vista o que foi definido acima, podemos afirmar que os conjuntos dos exemplos 3.1.1 e 3.1.2 com as suas respectivas operações formam grupos. No exemplo 3.1.1, temos que a^{-1} é o inverso de a pela operação de soma, portanto $a^{-1} = -a$. Já no exemplo 3.1.2, temos que a^{-1} é o inverso do elemento a pela operação de multiplicação. Sendo assim, para $a = 1$, temos que $a^{-1} = 1$ e para $a = -1$, $a^{-1} = -1$.

Exemplo 3.1.3. O conjunto dos números reais positivos sem o zero, denotado por $\mathbb{R}_+^*$ com a operação de multiplicação é um grupo. De fato, temos que a operação de multiplicação é associativa e possui um elemento neutro, a saber: o número 1. Além disso, sabemos que para cada $x \in \mathbb{R}$, existe um número real y tal que $xy = yx = 1$, a saber, este número é o inverso multiplicativo de x e é denotado por $\frac{1}{x}$ ou x^{-1}. Portanto, como todas as propriedades da Definição 3.1.1 foram satisfeitas, segue que este é um grupo.

Exemplo 3.1.4. O conjunto dos múltiplos inteiros de um número inteiro fixado com a operação usual de adição é um grupo. Antes de verficar as propriedades de grupo, note que o grupo é fechado com relação à soma, isto é, se tomarmos nx e ny dois múltiplos distintos de n, onde n é um número inteiro, temos que $n \cdot x + n \cdot y = n \cdot (x+y)$ que ainda é um múltiplo de n. Verifiquemos agora as propriedades, sabemos que a adição tem a propriedade associativa. Sabemos que $0 = n \cdot 0$, ou seja, 0 está no conjunto de múltiplos de n e, além disso, $0 + n \cdot x = n \cdot x + 0 = n \cdot x$ para todo mútiplo de n, portanto 0 é o elemento neutro da operação. Por fim, temos que para todo número da forma $n \cdot x$ existe um número k tal que $n \cdot x + k = 0$. Para determinar que número é k basta observar que

$$n \cdot x + k = 0 \Rightarrow k = -n \cdot x.$$

Mostrando que este é de fato um grupo.

Note que se uma das propriedades da Definição 3.1.1 não se verificar para um determinado conjunto munido com uma operação não teremos um grupo. Observe os dois próximos exemplos.

Exemplo 3.1.5. Consideremos o conjunto dos números inteiros com a operação de subtração. Este não é um grupo, pois não vale a propriedade de associatividade da operação exigida na Definição 3. De fato, temos que por um lado $(1-2)-7 = -1-7 = -8$ e, por outro, que $1-(2-7) = 1-(-5) = 1+5 = 6$. O que mostra que este não é um grupo.

Exemplo 3.1.6. O conjunto de todas as matrizes de ordem 2, denotado aqui por $\mathbb{M}_2$ com a multiplicação usual de matrizes não é um grupo. Sabemos que a multiplicação usual de matrizes é associativa. Sabemos também que existe um elemento neutro que é a matriz identidade $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Contudo, nem todas as matrizes de $\mathbb{M}_2$ são invertíveis. Considere, por exemplo, a matriz $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Se A for invertível, existe uma matriz $B \in \mathbb{M}_2$ tal que $AB = BA = I_2$. Seja $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, onde $a, b, c, d \in \mathbb{R}$. Então,

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

Como B supostamente é a inversa de A temos que

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

O que é impossível independente dos valores de a, b, c e d.

Observe, contudo, que se nos restringirmos às matrizes de $\mathbb{M}_2$ que são invertíveis, todas as condições da Definição 3.1.1 serão satisfeitas. O grupo das matrizes invertíveis de ordem 2 é chamado de *grupo linear geral de grau 2* e denotado por $GL(2)$. É importante notar que neste exemplo fica bastante evidente que a operação desse grupo não é comutativa, já que, em geral, dadas as matrizes $A, B \in \mathbb{M}_2$, temos que $AB \neq BA$.

Um grupo onde ocorre a comutatividade é chamado de *grupo abeliano* e não constitui papel fundamental no desenvolvimento deste trabalho. Para maiores detalhes sobre grupos abelianos consulte (Hernstein,1970) ou (Garcia;Lequain, 2012).

Observação 3.1.1. Para efeitos de notação, em qualquer grupo G e para qualquer elemento $a \in G$, definiremos de agora em diante que

$$\begin{aligned} a^0 &= e \\ a^1 &= a \\ a^2 &= a \cdot a \\ a^3 &= a \cdot a^2 \\ \vdots &= \vdots \\ a^k &= a \cdot a^{k-1} \end{aligned}$$

e também definiremos que

$$\begin{aligned} a^{-2} &= (a^{-1})^2 \\ a^{-3} &= (a^{-1})^3 \\ \vdots &= \vdots \\ a^{-n} &= (a^{-1})^n \end{aligned}$$

e assim por diante. Não é difícil verificar que as regras usuais de expoentes continuam válidas. A saber, para dois inteiros quaisquer m e n valem as igualdades

$$a^m \cdot a^n = a^{m+n} \tag{3.1}$$

$$(a^m)^n = a^{m \cdot n}. \tag{3.2}$$

Usando a notação introduzida na Definição 3.1.1, vamos analisar novamente o Exemplo 3.1.1. Nesse caso, o elemento neutro do grupo é o número zero pois $a+0 = 0+a = a$ para cada $a \in \mathbb{Z}$. Temos que o elemento inverso a^{-1} de um elemento $a \in \mathbb{Z}$ pela soma é denotado por $-a$, já que $a + (-a) = 0$. Além disso, note que, neste grupo,

$$a^n = \underbrace{a + a + a + \cdots a}_{n \text{ parcelas}} = na.$$

Já com relação às propriedades de potência citadas anteriormente, temos que

$$a^n + a^m = na + ma = (n+m)a = a^{n+m}$$

e que

$$(a^m)^n = a^m + a^m + \cdots a^m = na^m = nma = mna.$$

Observe, contudo, que para o Exemplo 3.1.2 a mesma notação terá um sentido distinto

daquele que acabamos de discutir. Neste caso, o elemento inverso a^{-1} é o inverso multiplicativo usual que é comumente denotado por $\frac{1}{a}$. Uma particularidade neste grupo é que cada elemento é inverso de si próprio. Ainda com relação ao Exemplo 3.1.2, temos que o elemento neutro é o número 1, já que estamos tratando da operação usual de multiplicação; a potência a^n também tem o significado ao qual já estamos acostumados, isto é, $a^n = a \cdot a \cdot a \cdot \ldots \cdot a$.

Um outro fato a se observar é que para grupos finitos, isto é, grupos com uma quantidade finita de elementos, uma propriedade importante do grupo é a quantidade de seus elementos que chamaremos de *ordem* de G e indicaremos por $o(G)$

A natureza dos elementos dos grupos discutidos nos dois primeiros exemplos é essencialmente numérica. Contudo, isso não é imperativo para que tenhamos um grupo. Um caso bastante peculiar é o que discutiremos a seguir.

Exemplo 3.1.7. Seja X um conjunto não vazio qualquer. Considere o conjunto $A(X) = \{\phi : X \to X : \phi \text{ é uma bijeção}\}$. Vamos mostrar que $A(X)$ com a operação de composição de funções é um grupo. Primeiro, devemos mostrar que se fizermos a composição de dois elementos de $A(S)$ ainda obteremos um elemento desse conjunto, ou seja, que a composição de duas bijeções ainda resulta em uma bijeção. Sejam ϕ_1, $\phi_2 \in A(X)$. Queremos mostrar que $\phi_2 \circ \phi_1 \in A(X)$. Vejamos que $\phi_2 \circ \phi_1$ é injetiva. Para tanto, tome $x, y \in X$, e suponhamos que $(\phi_2 \circ \phi_1)(x) = (\phi_2 \circ \phi_1)(y)$, ou seja, $\phi_2(\phi_1(x)) = \phi_2(\phi_1(y))$. Ora, mas tanto ϕ_2 quanto ϕ_1 são invertíveis. Sendo assim, temos que

$$\begin{aligned} \phi_2(\phi_1(x)) &= \phi_2(\phi_1(y)) \\ \phi_2^{-1}(\phi_2(\phi_1(x))) &= \phi_2^{-1}(\phi_2(\phi_1(y))) \\ \phi_1(x) &= \phi_1(y) \\ \phi_2^{-1}(\phi_2(x)) &= \phi_2^{-1}(\phi_2(y)) \\ x &= y, \end{aligned}$$

o que mostra que a função é injetiva. Para mostrar a sobrejetividade devemos mostrar que todo elemento de X é imagem de algum elemento de X por $\phi_2 \circ \phi_1$. Como ϕ_1 é uma bijeção, então, em particular ϕ_1 é sobrejetiva. Então todo y elemento de X se escreve como $\phi_1(x)$ para algum $x \in X$. Analogamente conlui-se que $\phi_2(y) = z$ para $z \in X$. Ora, mas assim, temos que $z = \phi_2(y) = \phi_2(\phi_1(x)) = (\phi_2 \circ \phi_1)(x)$ para z em X, mostrando que a composição ainda é uma função sobrejetiva. E, portanto, a composição de funções de $A(X)$ resulta uma função ainda em $A(X)$.

Verifiquemos agora as propriedades de grupo. Como a operação é a composição de funções e esta é uma operação associativa, verificamos a primeira das propriedades da definição 3.1.1. Além disso, como todas as funções em $A(X)$ são bijetivas, segue que também são invertíveis. Sendo assim, cada elemento ϕ de $A(X)$ possui um inverso que denotamos por ϕ^{-1}. Observe ainda que a função $I(x) = x$, a função identidade, está em $A(X)$ e que $(I \circ \phi)(x) = (\phi \circ I)(x) = \phi(x)$, para cada $\phi \in A(X)$. Dado um conjunto X, não vazio, o conjunto $A(X)$ das bijeções de X em si mesmo, com a operação de composição de funções, é chamado de grupo das permutações do conjunto X e é denotado por S_X.

Nas últimas páginas analisamos alguns exemplos à luz do que foi estabelecido na Definição 3.1.1, contudo um leitor mais atento poderia conjecturar alguns fatos sobre o que acabamos de discutir. Vimos, por exemplo, que todo elemento de um grupo G tem inverso, mas poderíamos nos perguntar se tal elemento é de fato único como afirmamos na definição de grupo, ou ainda, se existe um único elemento neutro no grupo. E, mais ainda, qual é o significado de $(a^{-1})^{-1}$,

onde a é um elemento do grupo. Reuniremos todas essas afirmações na seguinte proposição.

Proposição 3.1.1. *Se G é um grupo, então*

(i) o elemento neutro de G é único;

(ii) todo elemento $a \in G$ tem um único inverso em G;

(iii) para cada $a \in G$, $(a^{-1})^{-1} = a$;

(iv) para todos $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Demonstração. Começaremos a demonstração pela parte (i). Aqui, devemos mostrar que se existirem dois elementos distintos, e_1 e e_2 em G, tais que $a \cdot e_1 = e_1 \cdot a = a$ e que $a \cdot e_2 = e_2 \cdot a = a$, para cada elemento $a \in G$, então $e_1 = e_2$. De fato, se e_1 e e_2 forem dois elementos neutros distintos de G, temos que

$$e_2 = e_1 \cdot e_2 = e_2 \cdot e_1 = e_1,$$

mostrando que $e_1 = e_2$.

Para mostrar a parte (ii) devemos mostrar que se $x \cdot a = a \cdot x = e$ e $y \cdot a = a \cdot y = e$, onde $a, x, y \in G$ então $x = y$. Suponhamos então que $a \cdot x = e$ e $a \cdot y = e$, então, obviamente, $a \cdot x = a \cdot y$. Sabemos, ainda, que existe um elemento $b \in G$ tal que $b \cdot a = a \cdot b = e$, nada sabemos sobre a unicidade deste elemento b. Desse modo, temos que $b \cdot (a \cdot x) = b \cdot (a \cdot y)$, usando a propriedade associativa da operação $\cdot$ em G, temos que

$$x = e \cdot x = (b \cdot a) \cdot x = b \cdot (a \cdot x) = b \cdot (a \cdot y) = (b \cdot a) \cdot y = e \cdot y = y.$$

Note que a demonstração que fizemos para a parte (ii) é um resultado muito mais geral do que a unicidade do inverso de a pela operação $\cdot$, já que mostramos que $a \cdot x = a \cdot y$ implica que $x = y$. De forma totalmente análoga, podemos mostrar que $x \cdot a = y \cdot a$ implica no fato de que $x = y$. Pelo que acabamos de demonstrar, vale a lei do cancelamento *pelo mesmo lado* para a resolução de equações em G. Note, porém, que não temos como afirmar nada sobre x e y se tivermos que $a \cdot x = y \cdot a$, pois não temos nenhum resultado que garanta a comutatividade da operação em G.

Para a parte (iii), observe que, pela definição de elemento inverso, que $(a^{-1})^{-1}$ é um elemento que quando multiplicado por a^{-1} resulta em e, mas sabemos que a é um tal elemento, já que a^{-1} é inverso de a, e pela parte (ii) garante a unicidade do inverso. Portanto, $(a^{-1})^{-1} = a$.

Para demonstrar a parte (iv) temos que mostrar que

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

De fato, pela propriedade associativa da operação em G temos que

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

Analogamente, temos que

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

De modo que $e = (a \cdot b) \cdot (b^{-1} \cdot a^{-1})$ e $e = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b)$. Portanto, $b^{-1} \cdot a^{-1}$ é o inverso de $a \cdot b$ e a parte (ii) desta proposição garante a sua unicidade. □

Um resultado imediato da Proposição 3.1.1 é o seguinte.

Corolário 3.1.1. *Seja G um grupo. Dados $a,b \in G$, então as equações $a \cdot x = b$ e $y \cdot a = b$, têm soluções únicas para x e y em G.*

Demonstração. Demonstraremos a unicidade da solução da equação $a \cdot x = b$. Como $a \cdot x = b$, temos então que

$$a \cdot x = b \Rightarrow a^{-1} \cdot a \cdot x = a^{-1} \cdot b \Rightarrow e \cdot x = a^{-1} \cdot b \Rightarrow x = a^{-1} \cdot b.$$

Como o inverso de a é único a solução da equação também o é.

O outro caso é totalmente análogo. □

Observação 3.1.2. De agora em diante, para nos referirmos à operação entre dois elementos a e b do grupo G escreveremos apenas ab para denotar $a \cdot b$.

Exemplo 3.1.8. Considere o conjunto $V = \{e,a,b,c\}$ com uma operação $\cdot$ que tenha a propriedade de que cada elemento é seu próprio inverso. Vamos construir uma tábua de multiplicação – uma espécie de tabuada – para este grupo. Na verdade, devemos completar a tabela abaixo.

$\cdot$	e	a	b	c
e				
a				
b				
c				

Observação 3.1.3. Para efetuarmos $x \cdot y$ tomamos o primeiro dos fatores, no caso x, nos elementos da primeira coluna e y na primera linha. Note que esta ordem é importante, pois não temos nada que garanta a comutatividade da operação até aqui. O resultado obtido será colocado na célula da tabela que fica determinada pelo encontro da linha correspondente ao elemento x com a coluna correspondente ao elemento y.

Sabemos que cada elemento é inverso de si mesmo e que todo elemento multiplicado pelo elemento neutro resulta nele mesmo. Então, já sabemos como preencher a segunda linha, a segunda coluna e uma das diagonais da tabela como a seguir.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

Agora, observe que $a \cdot b = b \cdot a = c$, pois se $a \cdot b = a$ ou $b \cdot a = a$, pela lei do cancelamento que demonstramos na parte (ii) da Proposição 3.1.1, teríamos que

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

ou seja, significaria que b é o elemento neutro de G. Vejamos o caso $b \cdot a$:

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

De modo análogo, conclui-se que, $a \cdot b = b$ ou $b \cdot a = b$ nos diria que a é o elemento neutro de G e sabemos que isso não é verdade, portanto, só podemos ter $a \cdot b = c$. O leitor poderia ainda suspeitar que $a \cdot b = b \cdot a = e$, mas isso significaria que $a^{-1} = b$ e sabemos que isso não é verdade, já que a é o seu próprio inverso e o inverso de um elemento em um grupo é unico.

Para os demais pares, por meio de conclusões análogas, podemos completar a tábua.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Portanto, em um grupo de quatro elementos onde seja imposta a condição de que cada elemento é inverso de si próprio, *necessariamente* a operação será comutativa. Outra maneira de perceber que a operação de um grupo é comutativa é observar se a tabela de multiplicação forma uma matriz simétrica. Observe que a tabela acima é simétrica com relação à sua diagonal, portanto a operação é comutativa.

O grupo que acabamos discutir é chamado de Grupo de Klein, em homenagem ao matemático alemão Christian Felix Klein[1].

3.2 SUBGRUPOS

Em alguns casos, o estudo de determinados subconjuntos de um dado grupo pode ser mais interessante do que o do próprio grupo em si. No entanto, não estaremos interessados em subconjuntos de natureza arbitrária, mas, sim, naqueles que guardam uma estrutura algébrica que seja de nosso interesse. Por exemplo, retomemos o exemplo 3.1.1, onde consideramos o conjunto dos números inteiros com a operação de adição e considere a restrição feita no exemplo a seguir.

Exemplo 3.2.1. Seja G o grupo dos números inteiros com a operação de adição. Considere H o conjunto dos números inteiros pares. Podemos verificar facilmente que H, com a operação de adição, também é um grupo. Note que se somarmos dois números pares, o resultado ainda é par. De fato, sejam $2n$ e $2m$, $m,n \in \mathbb{Z}$ dois elementos de H, temos que $2n+2m = 2(n+m)$, que é par e, portanto, está em H. Além disso, todo elemento a de H possui um inverso aditivo que é o mesmo inverso que a admitia em G, a saber, devemos encontrar $x \in H$ tal que $a+x=0$. Logo $x=-a$ e, como a é par, também o é $-a$. Por fim, a propriedade associativa é trivialmente válida, de modo que H tem uma estrutura de grupo. De um modo totalmente análogo, poderíamos definir um grupo H_n dos múltiplos de um inteiro n que tem a mesma estrutura mostrada anteriormente (como fizemos no exemplo 3.1.4). Observe que se n e m forem inteiros distintos, então $H_n \cap H_m$ é o grupo dos múltiplos comuns de n e m.

Exemplo 3.2.2. Seja X um conjunto não vazio e S_X o grupo das permutações de dos elementos de X, como no exemplo 3.1.7. Dado $x_0 \in X$ fixado arbitrariamente. Seja $H(x_0) = \{\phi \in S_X : \phi(x_0) = x_0\}$, ou seja, $H(x_0)$ é o subconjunto de S_X formado pelas permutações de X que mantém fixo o elemento x_0. Vejamos, agora, se $H(x_0)$ com a operação de composição de funções é subgrupo de S_X. Sejam ϕ e τ duas funções em $H(x_0)$. Para mostrar que $H(x_0)$ é um grupo, devemos primeiro verificar se ao compormos duas funções de $H(x_0)$ a função resultante ainda está no conjunto. De fato, temo temos que $\phi(x_0) = x_0$ e $\tau(x_0) = x_0$. Sendo assim, temos que

$$(\phi \circ \tau)(x) = \phi(\tau(x_0)) = \phi(x_0) = x_0,$$

mostrando que $H(x_0)$ é fechado com relação à operação de composição de funções. Como toda função ϕ em $H(x_0)$ é bijetiva, segue que ϕ é invertível. Temos ainda que a função identidade,

[1] Christian Felix Klein(1849-1925), matemático alemão cujos trabalhos abrangem as áreas de Geometria Não-Euclidiana e nas interligações entre a Teoria dos Grupos e a Geometria.

isto é, a função I tal que $I(x) = x$ para cada $x \in S$, obviamente, cumpre a condição particular de que $I(x_0) = x_0$. Finalmente, como a composição de funções é associativa é claro que a operação estabelecida em $H(x_0)$ é associativa. Portanto, $H(x_0)$ tem estrutura de grupo.

Observe que nos dois exemplos citados acima sempre exibimos um subconjunto H de um grupo G em que a estrutura algébrica de G se mantém. De modo geral, os subconjuntos de G que consideraremos de agora em diante terão suas propriedades algébricas herdadas de G. Os subconjuntos mais naturais deste tipo são os *subgrupos*.

Definição 3.2.1. Um subconjunto H de um grupo G é chamado de *subgrupo* de G se, com relação à operação de G, o próprio H forma um grupo.

Observação 3.2.1. Uma inferência imediata que se pode tirar da Definição 3.2.1 é a de que se H é um subgrupo de G e K é um subgrupo de H, então K é um subgrupo de G. Para um exemplo dessa situação, o leitor pode observar que se tomarmos o grupo H_n, como definido no exemplo 3.2.1 e o grupo $H_n \cap H_m$ também definido naquele contexto, veremos que $H_n \cap H_m$ é subgrupo de H_n e H_n é subgrupo do grupo G dos números inteiros com a operação de adição. Sem muito esforço, o leitor pode verificar que o próprio $H_n \cap H_m$ é subgrupo de G. Um outro exercício interessante é encontrar um subgrupo de $H(x_0)$ como definido no exemplo 3.2.2.

Uma nota de precaução se faz necessária aqui. No Exemplo 3.2.1 verificamos que o elemento neutro do subgrupo H era o mesmo do grupo G. Além disso, vimos que dado um elemento de $x \in H$, seu inverso em G e em H coincidem. Vimos que isso também ocorreu no Exemplo 3.2.2. Muito embora isto pareça ser uma coisa bastante natural, deve-se observar que, mesmo sendo H subgrupo de G, tratam-se de grupos diferentes, o que torna os conceitos de elemento inverso e de elemento neutro relativos. Sendo assim, não há nada na definição que nos garanta que $e_G = e_H$, onde e_G é o elemento neutro de G e e_H o elemento neutro de H, ou que, dado $x \in H$, $x_G^{-1} = x_H^{-1}$, onde x_G^{-1} denota o inverso de x no grupo G e x_H^{-1} o inverso de x em H. Mostraremos na proposição a seguir que, dados o grupo G e um subgrupo H de G, de fato ocorre $e_G = e_H$ e se $x \in H$, então $x_G^{-1} = x_H^{-1}$.

Proposição 3.2.1. *Sejam G um grupo e H um subgrupo de G e $x \in H$. O inverso de x em H é o mesmo inverso de $x \in G$ e o elemento neutro de H é o mesmo elemento neutro de G.*

Demonstração. Seja $x \in H$ e denote por x_H^{-1} o inverso de x em H; por x_G^{-1} o inverso de x em G; por e_H o elemento neutro de H; e por e_G o elemento neutro de G. Queremos mostrar que $x_H^{-1} = x_G^{-1}$ e que $e_H = e_G$. Temos que $xx_H^{-1} = e_H$ e como $e_H \in G$, segue que $e_H = e_H e_G$. Juntando essas informações, temos que

$$xx_H^{-1} = e_H = e_H e_G = e_H(xx_G^{-1}) = (e_H x)x_G^{-1} = xx_G^{-1}$$

Da cadeia de igualdades acima concluímos que $xx_H^{-1} = xx_G^{-1}$. Portanto, podemos afirmar que

$$x_G^{-1}xx_H^{-1} = x_G^{-1}xx_G^{-1} \Rightarrow e_G x_H^{-1} = e_G x_G^{-1} \Rightarrow x_H^{-1} = x_G^{-1}.$$

Vamos mostrar que são iguais também os elementos neutros em H e em G. Para isso nos será útil o fato de que $x_H^{-1} = x_G^{-1}$, pois podemos escrever

$$e_H = xx_H^{-1} = xx_G^{-1} = e_G.$$

O que conclui a demonstração. □

Note que nos exemplos 3.2.1 e 3.2.2 para decidir se o subconjunto do grupo considerado era um subgrupo, tivemos que checar se o subconjunto verificava todas as condições da definição de grupo. Convenhamos que esta é uma tarefa bastante maçante e seria útil estabelecermos um critério que nos poupasse de tamanho esforço. Esse critério é fornecido pelo seguinte resultado.

Proposição 3.2.2. *Um subconjunto não vazio H do grupo G é um subgrupo de G se, e somente se,*

(i) $a, b \in H$ *implica que* $ab \in H$.

(ii) $a \in H$ *implica que* $a^{-1} \in H$.

Demonstração. Suponha H um subgrupo de G. Então, pela própria definição de grupo as condições (i) e (ii) são satisfeitas.

Reciprocamente, suponha válidas (i) e (ii), vamos mostrar que H é um subgrupo de G. Para tanto, devemos mostrar que $e \in H$ e que vale a propriedade associativa para as elementos de H. Mostraremos primeiro que $e \in H$. De fato, seja $a \in H$, então, de (ii), temos que $a^{-1} \in H$. Agora, por (i), podemos inferir que $aa^{-1} \in H$. Como $aa^{-1} = e$, segue que $e \in H$. Devemos ainda mostrar que é válida a propriedade associativa da operação de G em H. Ora, mas já sabemos que H é fechado com relação a operação de G e que, em G, vale a propriedade associativa. Sendo assim, é claro que a lei associativa vale em H, o que completa a demonstração. □

Uma outra maneira de se caracterizar um subgrupo H de um grupo G é a seguinte:

Proposição 3.2.3. *Sejam G um grupo e H um subconjunto não vazio de G. H é subgrupo de G se, e somente se, para quaisquer $x, y \in H$, tem-se que $xy^{-1} \in H$.*

Demonstração. Suponhamos que H é subgrupo de um grupo G. Então, pela Proposição 3.2.2, temos que dados $b \in H$, seu inverso b^{-1} também está em H. Tome um segundo elemento a em H. Como H é subgrupo de G, o resultado de ab^{-1} está em H.

Reciprocamente, suponha que, dados $a, b \in H$, $ab^{-1} \in H$, onde H é um subconjunto de H. Vamos mostrar que H é sugrupo de G. Primeiramente, note que dado $a \in H$ temos que $aa^{-1} = e \in H$, em que e é o elemento neutro de G. Portanto, H contém o elemento neutro de G. Sejam agora $a, b \in H$. Como sabemos que $e \in H$, podemos escrever que $eb^{-1} = b^{-1}$ o que mostra que b^{-1} está em H. Além disso, por hipótese, temos que $a(b^{-1})^{-1} \in H$, ou seja, $ab \in H$, mostrando que H é fechado com respeito à operação de G. Falta agora mostrar que H tem estrutura de grupo. Para isso, vamos verificar as condições de 3. Observe que já mostramos que H tem um elemento neutro e que dado $a \in H$ ocorre que $a^{-1} \in H$. Portanto, só nos resta mostrar que a operação é associativa em H. Ora, mas sabemos que a operação em H é a mesma de G que sabemos ser associativa, além disso, H é fechado com relação a esta operação. Portanto a associatividade vale também em H. □

De modo geral, se H for um subgrupo finito podemos até mesmo ignorar a condição (ii) da Proposição 3.2.2. Vejamos isso na seguinte proposição.

Proposição 3.2.4. *Se H é um subconjunto finito não vazio de um grupo G e H é fechado com relação à operação de G, então H é subgrupo de G.*

Demonstração. Pelo que vimos na Proposição 3.2.2, é suficiente mostrarmos que $a^{-1} \in H$ para cada $a \in H$. Suponhamos $a \in H$; assim $a^2 = aa \in H$, $a^3 = a^2a \in H$, $a^4 = a^3a \in H$, ..., $a^m \in H$, ... pois H é fechado com relação à operação induzida de G. De modo que $a, a^2, a^3, \ldots, a^m, \ldots$

estão todos em H, que é um subconjunto finito de G. Assim, concluímos que há repetições nesta coleção de elementos, isto é, para certos inteiros r e s com $r > s > 0$, $a^r = a^s$. Pelo cancelamento em G, temos que

$$a^r = a^s \Rightarrow a^r a^{-s} = a^s a^{-s} \Rightarrow a^{r-s} = e.$$

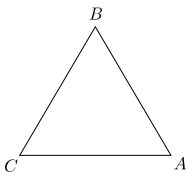
Além disso, como estamos supondo $r > s$, segue que $r - s \geq 1$. Agora, como $r - s > 0$ e $a^{r-s} = e$, segue que e está em H e, por isso, em particular, temos que $a^0 = e$ está em H. Isto significa que a^k é elemento de H para todo k inteiro e maior ou igual que zero. Como $r - s \geq 1$, temos que $r - s - 1 \geq 0$. O que nos permite afirmar que a^{r-s-1} está em H e que, além disso, a^{r-s-1} é o inverso de a. De fato, temos que $a^{r-s-1}a = a^{r-s} = e$. Portanto, temos que $a^{r-s-1} \in H$ e que $a^{r-s-1} = a^{-1}$, ou seja, mostramos que $a^{-1} \in H$ e isso conclui a demonstração. □

A proposição 3.2.4 nos diz, então, que para verificarmos que um subconjunto finito de um grupo G é um subgrupo, basta ver se ele é fechado ou não com relação à operação de G. Neste ponto, o leitor já deve ter concluído que G é sempre subgrupo de si mesmo e que o conjunto constituído somente pelo elemento e é um subgrupo de G. Esses grupos são chamados de *subgrupos triviais* e, embora tenham sua importância em Teoria de Grupos, nenhum deles tem interesse especial do ponto de vista do que estudaremos sobre subgrupos neste trabalho.

3.3 GRUPOS DE SIMETRIA E PERMUTAÇÕES

Considere a seguinte situação: suponha que tenhamos desenhado em uma folha um triângulo equilátero como o da figura 12 e que, separadamente, tenhamos um modelo de triângulo equilátero com os vértices identificados da mesma forma que no desenho. Assuma, ainda, que o modelo

Figura 12: Triângulo que estamos supondo desenhado em uma folha de papel.



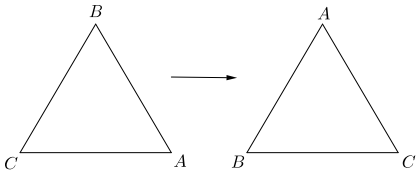
Fonte: elaborada pelo autor.

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. Um questionamento natural que podemos fazer é: quais movimentos podemos fazer, sem deformar o modelo, de modo que, ao final do movimento, ele se sobreponha ao desenho da folha de papel? Um desses movimentos, que inclusive já deve ter ocorrido ao leitor é a rotação pelo arco de $\frac{2\pi}{3}$ em torno do baricentro do triângulo, como na Figura 13. Por conveniência, sempre que nos referirmos a uma rotação, ela será feita no sentido anti-horário e em torno do baricentro do triângulo.

Observe que o mesmo resultado poderia ser obtido se fizéssemos uma rotação de $\frac{8\pi}{3} = 2\pi + \frac{2\pi}{3}$. Contudo, o que é do nosso interesse aqui é a comparação entre as posições inicial e final do modelo. De modo que dizemos que é equivalente fazer uma rotação de $\frac{8\pi}{3}$ ou uma rotação de $\frac{2\pi}{3}$.

O leitor já deve ter percebido que outras duas rotações fazem ainda que o modelo se

Figura 13: Um triângulo equilátero rotacionado em $\frac{2\pi}{3}$.

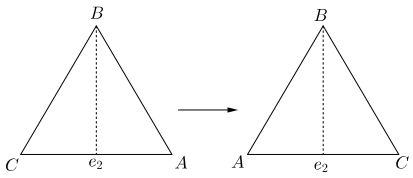


Fonte: elaborada pelo autor.

sobreponha ao desenho. A saber, tais rotações pelos arcos de $\frac{4\pi}{3}$ e 2π. Observe, contudo, que a rotação de 2π gera o mesmo resultado que não fazer rotação nenhuma e indicaremos esta rotação por e.

Um movimento de natureza distinta da rotação que podemos fazer com o modelo de modo a sobrepô-lo ao desenho do triângulo equilátero é uma reflexão como na Figura 14.

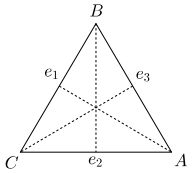
Figura 14: Um triângulo refletido em torno do eixo e_2.



Fonte: elaborada pelo autor.

Aqui, novamente, o que nos interessa é a comparação entre os estados inicial e final do triângulo. Não estamos nos importando com o processo que faz a reflexão e sim em como ela atua sobre o modelo. Existem ainda mais dois eixos em torno dos quais podemos refletir o modelo de modo que ele se sobreponha ao desenho feito no papel. Esses eixos são os eixos e_1 e e_3 mostrados na Figura 15.

Figura 15: Triângulo com os eixos e_1, e_2 e e_3.



Fonte: elaborada pelo autor.

Todos os movimentos que comentamos logo acima são chamados de *simetrias* do triângulo. Deve ficar bem claro que ao efetuar as rotações e as reflexões estamos apenas movendo o modelo. Não estamos deformando-o, no sentido de que não estamos ampliando-o, cortando-o ou esticando-o, por exemplo. Em resumo, então, encontramos seis simetrias do triângulo. Listamos a seguir quais são e uma comparação da posição inicial e final do triângulo em cada caso. Quando dizemos que "o vértice A é levado no vértice B", isto significa que a posição do vértice A após a movimentação é aquela que originalmente era do vértice B.

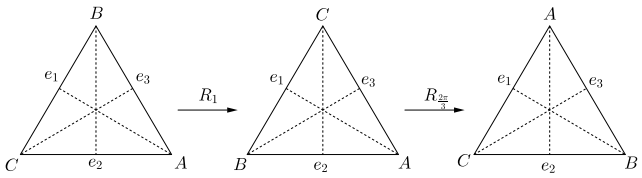
- Reflexão em torno de e_1; que denotaremos por R_1. Aqui, temos que, após reflexão, o

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; que denotaremos por R_2. Neste caso, temos que, 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; que denotaremos por R_3. Agora, temos que, após aplicarmos 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.
- Rotação de 2π rad ou de 0 rad; que denotaremos por e. Aqui temos que 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 $\frac{2\pi}{3}$ rad; que denotaremos por $R_{\frac{2\pi}{3}}$. Agora temos que, 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 mostrado na Figura 13.
- Rotação de $\frac{4\pi}{3}$ rad; que denotaremos por $R_{\frac{4\pi}{3}}$. Neste caso, temos que, 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.

Feita essa análise, é natural que se pergunte se ao efetuarmos a composição de simetrias, isto é, ao fazermos um movimento após o outro, ainda obteremos uma das simetrias listadas. Vejamos o exemplo da composição $R_{\frac{2\pi}{3}}R_1$. Sempre efetuaremos as composições da direita para a esquerda, como já fizemos com as permutações. Portanto, nesse caso, primeiro fazemos a reflexão em torno de e_1, para só então aplicarmos a rotação $R_{\frac{2\pi}{3}}$. Observe na Figura 16 como fica a composição dos dois movimentos.

Figura 16: Ilustração da composição $R_{\frac{2\pi}{3}}R_1 = R_3$.

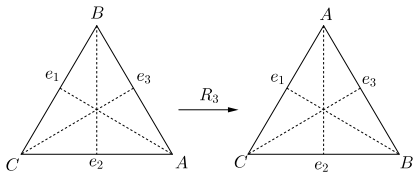


Fonte: elaborada pelo autor.

Sendo assim, ao efetuarmos $R_{\frac{2\pi}{3}}R_1$ obtemos R_3 que também é uma simetria do triângulo conforme já havíamos pontuado.

Compare a Figura 16, com a figura 17, onde aplicamos sobre o triângulo somente a movimentação R_3, que gera o mesmo resultado que a composição $R_{\frac{2\pi}{3}}R_1$.

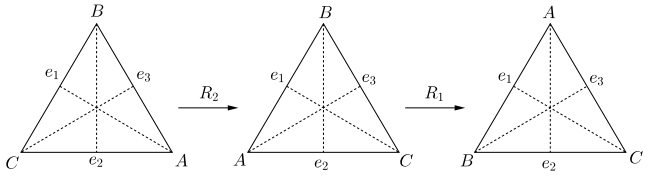
Figura 17: Ilustração da movimentação R_3.



Fonte: elaborada pelo autor.

Como um segundo exemplo vejamos a composição R_1R_2 resulta em $R_{\frac{2\pi}{3}}$. Acompanhe esta composição na Figura 18. Comparando o resultado da composição mostrado na Figura 18

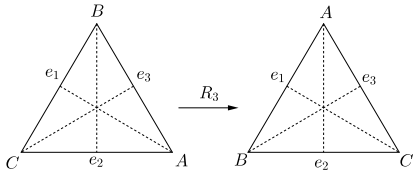
Figura 18: Ilustração da composição $R_1R_2 = R_{\frac{2\pi}{3}}$



Fonte: elaborada pelo autor.

com o da Figura 19, vemos que a aplicação do movimento $R_{\frac{2\pi}{3}}$ sobre o triângulo gera o mesmo resultado que a composição R_1R_2

Figura 19: Ilustração aplicação do movimento $R_{\frac{2\pi}{3}}$.



Fonte: elaborada pelo autor.

Nos dois exemplos que vimos, ambas as composições de simetrias resultaram em uma simetria do triângulo equilátero. Isso, de fato, sempre acontece, como podemos comprovar na tabela de multiplicação a seguir.

$\cdot$	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
e	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e	R_3	R_1	R_2
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e	$R_{\frac{2\pi}{3}}$	R_2	R_3	R_1
R_1	R_1	R_2	R_3	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$
R_2	R_2	R_3	R_1	$R_{\frac{4\pi}{3}}$	e	$R_{\frac{2\pi}{3}}$
R_3	R_3	R_1	R_2	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e

Na verdade, com a tabela feita, podemos facilmente verificar que o conjunto S_Δ das simetrias de um triângulo equilátero, isto é, $S_\Delta = \left\{e, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\right\}$, munido da operação de composição de funções é um grupo. De fato, temos que o conjunto é fechado pela operação que definimos; ademais, a composição de funções é associativa; além disso, observe que existe um elemento neutro, que é a rotação por 0 rad; e, ainda, cada elemento possui um inverso. A saber: cada uma das reflexões R_1, R_2, R_3 é a inversa de si própria, já que $R_1R_1 = e$, $R_2R_2 = e$ e $R_3R_3 = e$ e, ainda, $ee = e$ (óbvio), $R_{\frac{2\pi}{3}}R_{\frac{4\pi}{3}} = R_{\frac{4\pi}{3}}R_{\frac{2\pi}{3}} = R_{\frac{6\pi}{3}} = R_{2\pi} = e$.

Quando listamos as simetrias do triângulo e comparamos as posições inicial e final após a aplicação de cada um dos movimentos correpondentes, o leitor deve ter suspeitado de estar lendo algo familiar. Se analisarmos mais detidamente o que ocorre com os vértices do triângulo, podemos ver que é muito similar às permutações que já estudamos anteriormente e isso é, de fato, verdade. Podemos usar a notação de permutação para associar a cada um dos elementos de S_Δ uma permutação dos vértices do triângulo equilátero. Levando em conta que, na posição inicial, a sequência dos vértices no sentido anti-horário seja ABC, tal qual na Figura 12 temos que e pode ser associado à permutação $\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$, onde e representa a rotação de de 0 rad em torno do baricentro do triângulo ABC. De modo que as rotações descritas anteriormente podem ser identificadas naturalmente por permutações como a seguir:

- A rotação por 0 rad, que denotamos por e está associada à permutação identidade, como acabamos de mencionar;
- A rotação $R_{\frac{2\pi}{3}}$ pode ser identificada como $\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$;
- A rotação de $R_{\frac{4\pi}{3}}$ pode ser identificada com a permutação $\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$.

De modo similar, podemos identificar as reflexões em torno de cada um dos eixos e_1, e_2 e e_3 com uma permutação da seguinte forma:

- A reflexão R_1, pode ser associada à permutação $\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$;
- A reflexão R_2, em torno do eixo e_2, pode ser identificada com a permutação $\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$;
- A reflexão R_3 pode ser associada à permutação $\begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$.

Portanto, de acordo com o que foi exposto acima, vemos que o grupo de simetrias do triângulo equilátero tem uma relação muito estreita com o grupo de permutação de um conjunto de três elementos. Vamos agora reinterpretar as composições $R_{\frac{2\pi}{3}}R_1$ e R_1R_2 que fizemos anteriormente usando a notação de permutação. Pelo que foi listado acima temos que a composição $R_{\frac{2\pi}{3}}R_1$ pode ser entedida como a composição das permutações $\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$ e $\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$, como a seguir:

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}. \tag{3.3}$$

Note que a permutação que obtivemos é aquela associada à simetria R_3 e sabemos que $R_{\frac{2\pi}{3}}R_1 = R_3$.

Já a composição R_1R_2 do ponto de vista das permutações dos vértices do triângulo, corresponde à composição mostrada em 3.4.

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}. \tag{3.4}$$

Observe que obtemos como resultado a permutação correspondente à simetria $R_{\frac{2\pi}{3}}$. Comprovando que analisar as simetrias do ponto de vista de permutações é realmente eficaz.

Podemos ainda escrever o grupo de simetrias de um triângulo de um outro modo que nos permite fazer algumas generalizações mais facilmente. Para isso, vamos tomar $a = R_{\frac{2\pi}{3}}$ e $b = R_1$ e usaremos e como o elemento neutro, como já viemos fazendo ao longo do texto. Assim, temos que

$$\begin{aligned} a^2 &= R_{\frac{4\pi}{3}}, \\ a^3 &= e, \\ ba &= R_2, \\ ab &= R_3, \\ b^2 &= e. \end{aligned}$$

As igualdades acima mostram que para obter cada um dos elementos de S_Δ é suficiente que se faça composições adequadas da rotação $R_{\frac{2\pi}{3}}$ e da reflexão R_1 entre si e consigo mesmas. Além disso, essas mesmas igualdades mostram que, levando em conta a relação vista anteriormente entre as simetrias de um triângulo equilátero e o grupo S_X, grupo das permutações de um conjunto $X = \{A,B,C\}$, todos os elementos de S_X podem ser obtidas por meio de composições adequadas de $\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$ e $\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$, já que estas permutações foram identificadas com as simetrias $R_{\frac{2\pi}{3}}$ e R_1, respectivamente. A nova notação permite ainda que confirmemos a estreita relação existente entre os dois grupos sobre os quais estamos discursando nos últimos parágrafos. Nesta nova notação, a tabela de composição das simetrias do triângulo e das permutações dos elementos do conjunto T são iguais! A nova tabela fica como a seguir.

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

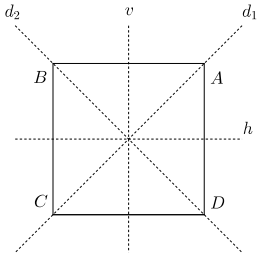
Observação 3.3.1. Atente para o fato de que a operação neste grupo não é comutativa isto é se x e y são elementos de S_Δ, em geral, $xy \neq yx$. Para constatar isso, observe a tábua de multiplicação acima e observe que, por exemplo, $ab \neq ba$.

Note que a cada simetria do triângulo corresponde uma permutação do conjunto S_X, em que $X = \{A,B,C\}$. Sendo assim, uma função que a cada simetria do triângulo associa uma permutação em S_X é uma função injetiva, já que cada simetria é levada na única permutação

que determina. Sabemos da Análise Combinatória que S_X tem 6 elementos e a função é injetora. Portanto, existem, no máximo, seis simetrias do triângulo e exibimos seis delas. Vemos, assim, que o grupo de simetrias do triângulo tem exatamente seis elementos, ou seja, é um grupo de ordem 6. Esse grupo também é conhecido como grupo diedral de ordem 6 e é chamado de D_6.

Vamos agora analisar o grupo de simetrias de um quadrado com a operação de composição de funções – que será denotado por $S_\square$ – e traçar um paralelo com o que acabamos de ver sobre o grupo de simetrias do triângulo equilátero. Para o que segue, vamos tomar por base a Figura 20.

Figura 20: Um quadrado e seus eixos de simetria.



Fonte: elaborada pelo autor.

Observe que o quadrado possui algumas simetrias, a seguir listaremos cada uma delas já identificando cada uma delas como uma permutação dos vértices, a exemplo do que foi feito com as simetrias do triângulo.

- Reflexão em torno da reta d_1; que denotaremos por R_1. Em termos de permutação, essa simetria age do seguinte modo sobre os vértices do quadrado:

$$\begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix};$$

- Reflexão em torno da reta d_2; que denotaremos por R_2. Em termos de permutação, essa simetria tem o seguinte efeito sobre os vértices do quadrado:

$$\begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix};$$

- Reflexão em torno da reta h; que denotaremos por R_h. Em termos de permutação, essa simetria altera as posições dos vértices como segue:

$$\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix};$$

- Reflexão em torno da reta v; que denotaremos por R_v. Em termos de permutação, essa simetria altera as posições dos vértices do quadrado do seguinte modo:

$$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix};$$

- Rotação de $\frac{\pi}{2}$ rad em torno do centro do quadrado no sentido anti-horário; que denotaremos por $R_{\frac{\pi}{2}}$. Em termos de permutação, essa simetria age do seguinte modo sobre as posições dos vértices:

$$\begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix};$$

- Rotação de π rad em torno do centro do quadrado no sentido anti-horário; que denotaremos por R_{π}. Em termos de permutação, essa simetria altera as posições dos vértices como segue:

$$\begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix};$$

- Rotação de $\frac{3\pi}{2}$ rad em torno do centro do quadrado no sentido anti-horário; que denotaremos por $R_{\frac{3\pi}{2}}$. Em termos de permutação, essa simetria altera as posições dos vértices da seguinte maneira:

$$\begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix};$$

- Rotação de 2π rad ou 0 rad em torno do centro do quadrado no sentido anti-horário; que denotaremos por e. Esta simetria não altera as posições dos vértices. De modo que, em termos de permutação ficamos com:

$$\begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}.$$

Sabemos que existem 24 permutações possíveis para os elementos do conjunto $V = \{A,B,C,D\}$. Note, porém, que relacionamos apenas oito delas com as simetrias do quadrado. Por exemplo a permutação $\begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$ não representa uma simetria do quadrado $ABCD$, pois ela, altera a posição relativa entre os vértices do polígono. Para entender melhor, observe que em nenhuma das permutações que fizemos correponder uma simetria o vértice D aparece entre os vértices A e B, o que ocorre na permutação que acabamos de citar. Vamos mostrar agora que as únicas permutações do conjunto V que representam simetrias de um quadrado são as oito que citamos anteriormente. Para isso, vamos dividir a análise em casos.

Caso 1: Se uma simetria do quadrado fixa um dos vértices, então, necessariamente tem que fixar o vértice oposto. Isso não ocorre nos seguintes casos: $\begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ A & D & B & C \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ D & B & A & C \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ C & B & D & A \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ B & D & C & A \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ D & A & C & B \end{pmatrix}$ $\begin{pmatrix} A & B & C & D \\ B & C & A & D \end{pmatrix}$ e $\begin{pmatrix} A & B & C & D \\ C & A & B & D \end{pmatrix}$.

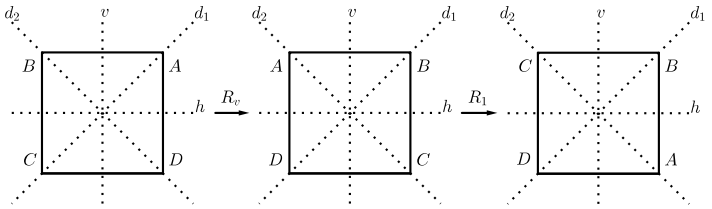
Caso 2: Se uma simetria do quadrado fixa dois vértices não colineares com o centro do quadrado, então, necessariamente teria que ser a identidade. Isso não ocorre nos seguintes casos $\begin{pmatrix} A & B & C & D \\ A & B & D & C \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ A & C & B & D \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ B & A & C & D \end{pmatrix}$ e $\begin{pmatrix} A & B & C & D \\ D & B & C & A \end{pmatrix}$.

Observe que em ambos os casos discutidos anteriormente, a posição relativa entre os vértices do quadrado não se preserva na mesma ordem exibida na Figura 20. Por exemplo, observe a primeira permutação exibida no Caso 1 que é $\begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix}$ e que corresponde à sequência (A,D,B,C). Note, porém, que é impossível que os vértices apareçam nessa ordem pois aqui A e B são vértices opostos, mas isso *nunca* ocorre em uma simetria do quadrado, já que A e B são vértices adjacentes. Note que a primeira permutação exibida no Caso 2 corresponde à sequência (A,B,D,C) que exibe B e D como vértices adjacentes e sabemos que eles sempre serão opostos em qualquer que seja a posição do quadrado. O leitor pode verificar que todas as permutações que exibimos nos casos 1 e 2 exibem ordenações dos vértices cujas posições relativas são diferentes daquelas exibidas na Figura 20. Note que as quatro permutações que faltam, que são $\begin{pmatrix} A & B & C & D \\ B & D & A & C \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ C & A & D & B \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ C & D & B & A \end{pmatrix}$ e $\begin{pmatrix} A & B & C & D \\ D & C & A & B \end{pmatrix}$, enquadram-se nessa situação, pois exibem B e D como vértices adjacentes. E em todas as simetrias do quadrado tais vértices são opostos.

De modo totalmente análogo ao que fizemos para as simetrias do triângulo equilátero, podemos mostrar que o conjunto $S_{\square} = \left\{ e, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}, R_1, R_2, R_h, R_v \right\}$ com seus elementos definidos como fizemos anteriormente com a operação de composição de funções é um grupo. Esse grupo é também conhecido como grupo diedral de ordem 8 e é denotado por D_8.

Vamos exemplificar algumas operações com elementos do grupo de simetria do quadrado. Por exemplo, podemos verificar que $R_1 R_v = R_{\frac{3\pi}{2}}$. Podemos fazer isso usando um recurso geométrico como na Figura 21.

Figura 21: Ilustração da composição $R_1 R_v = R_{\frac{3\pi}{2}}$



Fonte: elaborada pelo autor.

ou então via permutações como a seguir. Lembre-se de que a composição é sempre feita da direita para a esquerda, isto é, primeiro efetuamos R_v e aplicamos R_1 ao resultado obtido. Desse modo, teremos que

$$\begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix}. \tag{3.5}$$

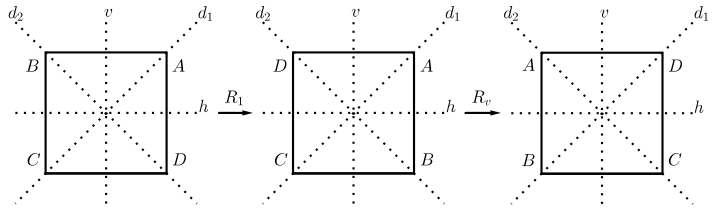
Vamos determinar também a composição $R_v R_1$, por meio de permutações.

$$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}, \tag{3.6}$$

o que nos diz que $R_v R_1 = R_{\frac{\pi}{2}}$. Se utilizarmos um recurso geométrico, teremos o que mostra a Figura 22.

Na tabela a seguir estão todas as possíveis composições das simetrias de um quadrado.

Figura 22: Ilustração da composição $R_v R_1 = R_{\frac{\pi}{2}}$



Fonte: elaborada pelo autor.

$\cdot$	e	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	R_1	R_h	R_2	R_v
e	e	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	R_1	R_h	R_2	R_v
$R_{\frac{\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	e	R_h	R_2	R_v	R_1
R_π	R_π	$R_{\frac{3\pi}{2}}$	e	$R_{\frac{\pi}{2}}$	R_2	R_v	R_1	R_h
$R_{\frac{3\pi}{2}}$	$R_{\frac{3\pi}{2}}$	e	$R_{\frac{\pi}{2}}$	R_π	R_h	R_1	R_v	R_2
R_1	R_1	R_v	R_2	R_h	e	$R_{\frac{3\pi}{2}}$	R_π	$R_{\frac{\pi}{2}}$
R_h	R_h	R_1	R_v	R_2	$R_{\frac{\pi}{2}}$	e	$R_{\frac{3\pi}{2}}$	R_π
R_2	R_2	R_h	R_1	R_v	R_π	$R_{\frac{\pi}{2}}$	e	$R_{\frac{3\pi}{2}}$
R_v	R_v	R_2	R_h	R_1	$R_{\frac{3\pi}{2}}$	R_π	$R_{\frac{\pi}{2}}$	e

A exemplo do que foi feito com o grupo de simetrias do triângulo equilátero, existe uma outra forma de representar o grupo de simetrias do quadrado que permite uma maior facilidade para deduzir certas generalizações. Para isso, vamos fazer $a = R_{\frac{\pi}{2}}$ e $b = R_1$ e indicaremos o elemento neutro por e, como já é costume. O leitor pode verificar facilmente que por meio de composições adequadas de $R_{\frac{\pi}{2}}$ e R_1 pode-se obter qualquer um dos elementos de $S_\square$, como vemos nas igualdades abaixo.

$$\begin{aligned} a^2 &= R_\pi \\ a^3 &= R_{\frac{3\pi}{2}} \\ a^4 &= e \\ b^2 &= e \\ ab &= R_h \\ a^2 b &= R_2 \\ a^3 b &= R_v \\ ba &= R_v = a^3 b \end{aligned}$$

Nessa nova notação, a tabela de composições fica como mostrado a seguir.

$\cdot$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Toda a discussão que fizemos nesta seção pode ser reinterpretada do seguinte modo: seja S_X tal qual definimos anteriormente. Note que o conjunto S_X é constituído por todas as permutações dos elementos do conjunto $X = \{A,B,C\}$. Além disso, S_X, munido da operação de composição de funções, constitui um grupo como vimos anteriormente. Seja ainda $\phi : S_\Delta \to S_X$. Assim, se tomarmos a e b elementos de S_Δ, temos que $\phi(ab) = \phi(a)\phi(b)$, desde que definamos $\phi(R_1) = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$ e $\phi\left(R_{\frac{2\pi}{3}}\right) = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$. Vamos revisitar as igualdades em (3.3) e (3.4) tendo em vista a função ϕ que acabamos de definir. Assim, temos de (3.3)

$$\phi\left(R_{\frac{2\pi}{3}}R_1\right) = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = \phi\left(R_{\frac{2\pi}{3}}\right)\phi(R_1).$$

Já da igualdade (3.4) podemos inferir que

$$\phi(R_1R_2) = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = \phi(R_1)\phi(R_2).$$

Analogamente ao que fizemos acima podemos também reinterpretar as equações (3.5) e (3.6). Para tanto, tome $\tau : S_\square \to Q$, onde

$$Q = \left\{ \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix} \right\}.$$

Note que em Q não estão todos os elementos do conjunto S_V, onde $V = \{A,B,C,D\}$. Contudo, as permutações que estão em Q constituem um subgrupo do conjunto de todas as permutações dos elementos de V. Agora, definamos $\tau(R_1) = \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}$ e $\tau(R_{\frac{\pi}{2}}) = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$.

De modo que a equação (3.5) pode ser entendida como

$$\tau(R_1R_v) = \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} = \tau(R_1)\tau(R_2).$$

Já da equação (3.6) deduzimos que

$$\tau(R_vR_1) = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} = \tau(R_v)\tau(R_1).$$

Funções com uma peculiaridade tão interessante como as funções que definimos logo acima não devem ser uma feliz coincidência. Na verdade, as funções com a propriedade de que $\phi(ab) = \phi(a)\phi(b)$ serão melhor estudadas no capítulo 3, onde falaremos sobre homomorfismos.

Tanto do grupo de simetrias do triângulo como do grupo de simetrias do quadrado, podemos extrair um subgrupo particularmente interessante que é um grupo de rotação. De modo mais geral, podemos extrair um grupo de rotação do grupo de simetrias de qualquer polígono. Vejamos no seguinte exemplo.

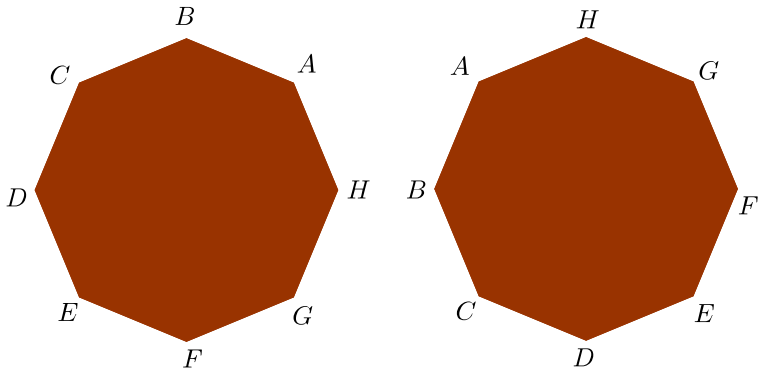
Exemplo 3.3.1. Vamos mostrar que o conjunto $R_n$das rotações de um polígono regular em torno do seu centro munido com a operação de composição de funções é um grupo. Denotaremos a rotação pelo arco de $\frac{2\pi i}{n}$ rad, $0 \leq i \leq n$, no sentido anti-horário, por $R_{\frac{2\pi i}{n}}$. Pelo que vimos anteriormente, uma rotação é um movimento rígido e como a rotacionaremos sempre em arcos múltiplos de $\frac{2\pi}{n}$ ao aplicarmos uma tal rotação (mesmo que repetidas vezes), faremos com que o polígono sobreponha a si próprio. Isso significa que cada vértice ocupará a posição que era originalmente ocupada por um outro vértice do polígono e que a posição relativa entre os vértices não se alterará após a rotação.

Vejamos um caso particular para $n = 8$. Para o octógono, o conjunto R_8 das rotações é

$$R_8 = \left\{ e, R_{\frac{2\pi}{8}}, R_{\frac{4\pi}{8}}, R_{\frac{6\pi}{8}}, R_{\frac{8\pi}{8}}, R_{\frac{10\pi}{8}}, R_{\frac{12\pi}{8}}, R_{\frac{14\pi}{8}} \right\}.$$

Veremos agora, por que o conjunto R_8 com a operação de composição de funções é um grupo. Primeiro, observe que cada composição de rotações ainda é uma rotação. Como a operação em questão é a composição de funções, sabemos que esta operação é associativa. É claro que existe um elemento neutro que é a rotação 2π rad ou 0 rad. Além disso, cada elemento tem um inverso. A saber, a rotação $R_{\frac{2\pi}{n}}$ ter por inverso a rotação por seu arco replementar. Portanto, o inverso de $R_{\frac{2\pi}{n}}$ por inverso a rotação $R_{2\pi-\frac{2\pi}{n}}$.

Figura 23: Um octógono rotacionado em $2\frac{2\pi}{8} = \frac{\pi}{2}$ no sentido anti-horário.



Fonte: elaborada pelo autor.

No caso exibido na Figura 23, temos que $R_{\frac{2\pi}{8}}R_{\frac{2\pi}{8}} = R_{\frac{\pi}{2}}$. Observe que ao aplicarmos a rotação de $\frac{2\pi}{8} = \frac{\pi}{4}$ duas vezes, ou seja, rotacionarmos o polígono em $\frac{\pi}{2}$, cada um dos vértices

ocupou o lugar previamente ocupado por outro vértice do octógono. Note também que a posição relativa entre os vértices é a mesma antes e depois da rotação.

Observação 3.3.2. Atente para o fato de que o conjunto de reflexões do polígono munido da operação de composição de funções *não é um grupo* pois não é fechado com respeito a esta operação, isto é, caso fosse um grupo, ao compormos duas reflexões deveríamos ter uma terceira reflexão (não necessariamente distinta das duas primeiras), mas basta olhar o exemplo da Figura 21 para perceber que a composição de duas reflexões pode resultar em uma rotação.

4 HOMOMORFISMOS

4.1 HOMOMORFISMOS

A discussão conduzida na seção anterior nos mostrou que há algumas funções com uma propriedade bastante interessante e que definimos como a seguir.

Definição 4.1.1. Sejam G e G' grupos. Uma função ϕ de G em G' é dita um homomorfismo se para todos $a,b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Observação 4.1.1. Note que na igualdade da Definição 4.1.1 no termo $\phi(ab)$, ab é calculado com a operação de G, já em $\phi(a)\phi(b)$ a operação em questão é a operação de G'.

Um exemplo imediato de homomorfismo é o seguinte.

Exemplo 4.1.1. Sejam G e G' grupos e ϕ uma função de um grupo G em um grupo G' tal que $\phi(x) = e$ para cada $x \in G$. Este é obviamente um homomorfismo, já que temos que

$$\phi(xy) = e = ee = \phi(x)\phi(y),$$

para todos $x,y \in G$, o que mostra que ϕ é um homomorfismo. Usando este mesmo raciocínio, o leitor pode verificar que a função τ de G em G, definida por $\tau(x) = x$ para todo $x \in G$, é um homomorfismo.

Embora o conceito de homomorfismo seja um dos conceitos centrais da álgebra, ele aparece em contextos muito mais elementares do que este em que estamos. Já no primeiro ano do Ensino Médio o estudante se depara com a função logarítmica que é um homomorfismo do conjunto $\mathbb{R}_+^*$ dos números reais positivos com a operação de multiplicação no conjunto dos números reais com a operação de adição.

Exemplo 4.1.2. Vejamos o porquê de a função logaritmo ser um homomorfismo tal qual descrevemos no parágrafo acima. Definamos a função $\phi : \mathbb{R}_+^* \to \mathbb{R}$ tal que $\phi(x) = \log_b x$, onde b é um número real fixo positivo e diferente de 1. Uma das primeiras propriedades estudadas desta função é a de que

$$\log_b(xy) = \log_b x + \log_b y,$$

onde b é a base do logaritmo. Ora, mas essa propriedade mostra exatamente o que queríamos, já que devíamos mostrar que

$$\phi(xy) = \phi(x) + \phi(y). \tag{4.1}$$

Observe a afirmação feita na Observação 4.1.1 fica ainda mais explícita na equação 4.1, isto é, no termo $\phi(xy)$ a operação é a multiplicação e é efetuada no domínio de ϕ, enquanto que no membro direito da equação, a operação é aquela definida no contradomínio de ϕ, ou seja, a adição.

Um segundo exemplo de homomorfismo que aparece em matemática elementar é a multiplicação por um número fixado. No exemplo a seguir consideramos o caso particular em esse número é o número 2.

Exemplo 4.1.3. Seja G o grupo dos inteiros com a operação de adição e G' o conjunto dos números inteiros pares com a operação de soma. Defina a função $\phi : G \to G'$ onde $\phi(x) = 2x$. Temos então que

$$\phi(x+y) = 2(x+y) = 2x+2y = \phi(x) + \phi(y).$$

Isso mostra que ϕ é um homomorfismo.

Observação 4.1.2. Observe que nem sempre a multiplicação por um número fixo será um homomorfismo. Isso depende do grupo que estamos considerando. Sendo assim, se considerarmos $G = G'$ o grupo dos números reais positivos sem o zero com a operação de multiplicação e $\phi : G \to G'$ definida como no exemplo 4.1.3, ou seja $\phi(x) = 3x$ para cada $x \in G$, temos por um lado que $\phi(xy) = 3xy$ e por outro que $\phi(x)\phi(y) = 3x3y = 9xy$. Logo, $\phi(xy) \neq \phi(x)\phi(y)$, mostrando que ϕ não é um homomorfismo.

Um outro exemplo que podemos citar das funções estudada no Ensino Médio e que não é um homomorfismo é a função quadrática. Vejamos no exemplo a seguir.

Exemplo 4.1.4. Sejam G o grupo dos números reais não nulos com a operação de multiplicação; G' o grupo dos números reais com a operação de adição e $\phi : G \to G'$, ta que $\phi(x) = x^2$. Este, claramente, não é um homomorfismo já que $\phi(xy) = (xy)^2 = x^2y^2$ e que $\phi(x) + \phi(y) = x^2 + y^2$ e, de modo geral, sabemos que $x^2y^2 \neq x^2 + y^2$.

Um segundo contraexemplo de homomorfismo é o seguinte.

Exemplo 4.1.5. Sejam $G = G' = \mathbb{R}$; G e G' munidos com a operação usual de adição; e $\phi : G \to G'$ tal que $\phi(x) = |x|$. Este não é um homomorfismo, pois $\phi(x+y) = |x+y|$ e $\phi(x) + \phi(y) = |x| + |y|$ e sabemos que, em geral, $|x+y| \leq |x| + |y|$.

Voltemos agora aos exemplos de homomorfismos.

Exemplo 4.1.6. Seja G o grupo dos números reais não nulos com a operação de multiplicação e $G' = \{1, -1\}$, onde definiremos que $1 \cdot 1 = 1$, $(-1)(-1) = 1$, $1(-1) = -1$ e $(-1)1 = -1$. Seja a função $\phi : G \to G'$ definida como

$$\phi(x) = \begin{cases} 1 & \text{, se } x \text{ positivo.} \\ -1 & \text{, se } x \text{ negativo.} \end{cases}$$

Observe que G' com a operação definida acima é um grupo, já que é fechado em relação à operação de multiplicação; a operação é trivialmente associativa; existe um elemento neutro para a operação (que é o número 1); e cada elemento é inverso de si mesmo. Vejamos que ϕ é um homomorfismo. Sejam x e y números reais não nulos. Então $\phi(xy) = 1$ se, e somente se, x e y têm o mesmo sinal. De modo que se x e y são ambos positivos, temos que

$$\phi(xy) = 1 = 1 \cdot 1 = \phi(x)\phi(y).$$

Caso x e y sejam ambos negativos, ocorre que

$$\phi(xy) = 1 = (-1)(-1) = \phi(x)\phi(y).$$

Além disso, sabemos que $\phi(xy) = -1$ se, e somente se, x e y têm sinais distintos. Assim, temos que

$$\phi(xy) = -1 = 1(-1) = \phi(x)\phi(y),$$

quando x é positivo e y negativo. Contudo, se tivermos que x negativo e y positivo, obteremos

$$\phi(xy) = -1 = (-1)1 = \phi(x)\phi(y).$$

O que mostra que ϕ é um homomorfismo entre G e G'. O fato de ϕ ser um homomorfismo é equivalente ao adágio da matemática que diz que: positivo vezes positivo resulta positivo,

positivo vezes negativo resulta negativo, negativo vezes positivo resulta negativo e negativo vezes negativo resulta positivo.

Ainda em se tratando de exemplos da Matemática Elementar, podemos nos valer do Teorema de Binet[1] para dar mais um exemplo de homomorfismo. O Teorema de Binet afirma que se duas matrizes são quadradas e de mesma ordem, então $\det(AB) = \det(A)\det(B)$. Para garantirmos a estrutura de grupo, faremos como no exemplo 3.1.6 e nos restringiremos ao espaço das matrizes quadradas de mesma ordem invertíveis.

Exemplo 4.1.7. Sejam G o conjunto das matrizes quadradas invertíveis de ordem n (note que n é fixo) com a operação usual de multiplicação de matrizes, G' o conjunto dos números reais não nulos com a operação usual de multiplicação de números reais e $\phi : G \to G'$, uma função que toma uma matriz em G e calcula o seu determinante. Queremos mostrar que a função determinante é um homomorfismo de G e G', ou seja, que $\phi(AB) = \phi(A)\phi(B)$. Ora, mas isso é exatamente o que afirma o Teorema de Binet, o que já mostra que a função ϕ é um homomorfismo de G em G'.

Exemplo 4.1.8. Seja G o grupo dos números reais com a operação de adição e seja G' o grupo dos números reais não nulos com o produto usual. Defina $\phi : G \to G'$ por $\phi(x) = 2^x$. A fim de verificar que este é um homomorfismo devemos verificar que $2^{a+b} = 2^a 2^b$, o que de fato é verdade.

Antes de prosseguirmos, atente para o fato de que, para todos os exemplos de homomorfismos que fornecemos, sempre teremos que $\phi(e) = e'$, onde e é o elemento neutro do domínio de ϕ e e' é o elemento neutro do contradomínio de ϕ. O leitor pode verificar que este fato é válido para qualquer exemplo de homomorfismo que seja capaz de criar, porém, como é usual em Matemática pouparemos tamanho esforço generalizando tal fato no seguinte resultado.

Proposição 4.1.1. *Seja ϕ um homomorfismo de G em G', então:*

(i) $\phi(e) = e'$, *com e' elemento neutro da operação em G'.*

(ii) $\phi(x^{-1}) = \phi(x)^{-1}$

Demonstração. Começaremos demonstrando a parte (i). Observe que

$$\phi(x)e' = \phi(x) = \phi(xe) = \phi(x)\phi(e).$$

Concluímos, então, que $\phi(x)e' = \phi(x)\phi(e)$. Assim, pela lei do cancelamento em G', ocorre que $e' = \phi(e)$, provando o que queríamos.

Mostraremos agora a parte (ii), que depende, basicamente, do que acabamos de mostrar em (i). De fato, temos que

$$e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}).$$

De modo que a Proposição 3.1.1 nos garante que $\phi(x)^{-1} = \phi(x^{-1})$. □

A proposição 4.1.1 nos diz que se $\phi : G \to G'$ é um homomorfismo de G em G', a imagem de e por ϕ é justamente e', onde e e e', são os elementos neutros de G e de G', respectivamente. Contudo, poderíamos nos perguntar se $\phi(x) = e'$ somente para $x = e$. O que foi exposto no exemplo 4.1.7 pode ser usado para refutar esta hipótese. Queremos exibir uma matriz diferente da matriz identidade em $GL(2)$ e cujo determinante seja igual a 1. Por exemplo, a

[1] Jacques Philippe Marie Binet(1786-1856), matemático, físico e astrônomo francês que fez contribuições importantes em Teoria de Números e Álgebra de Matrizes.

matriz $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ nos basta para um contra-exemplo. Mas poderíamos ainda citar $\begin{pmatrix} 3 & -7 \\ 1 & -2 \end{pmatrix}$, $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -1 & 1 \end{pmatrix}$, ou ainda $\begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix}$, onde $\theta \in \mathbb{R}$. Na verdade, há infinitos exemplos de matrizes de ordem 2 que têm determinante 1.

Para que tenhamos um segundo exemplo nesse sentido considere o seguinte.

Exemplo 4.1.9. Seja $G = \mathbb{R}^2$, com a operação usual de soma de vetores e $G' = \mathbb{R}$ com a operação usual de adição. Considere a função $\phi : G \to G'$ tal que $\phi(x,y) = x+y$. Temos que o elemento neutro de G, neste caso é o par $(0,0)$ e o de G' é o número zero. É claro que $\phi(0,0) = 0$, contudo, observe que há uma infinidade de outros pares tais que $\phi(x,y) = 0$. De fato, temos que

$$\phi(x,y) = 0 \Rightarrow x+y = 0 \Rightarrow x = -y.$$

Portanto, para que tenhamos $\phi(x,y) = 0$, é suficiente que se tome $x = -y$.

Revisitando o exemplo 4.1.6, vemos que $\phi(x) = 1$ sempre que $x > 0$. Portanto, neste caso, há também uma infinidade de elementos do domínio de ϕ cuja imagem é 1, o elemento neutro do contradomínio da função

De posse do resultado que demonstramos na parte (i) da Proposição 4.1.1, temos uma outra maneira de decidir se função pode ou não ser um homomorfismo.

Exemplo 4.1.10. Sejam $G = G' = \mathbb{R}$; G e G' munidos com a operação usual de adição; e $\phi : G \to G'$ tal que $\phi(x) = x+1$. A função ϕ não é um homomorfismo pois, $\phi(x+y) = x+y+1$ e $\phi(x)+\phi(y) = x+1+y+1 = x+y+2$. Como $x+y+1 \neq x+y+2$, segue que $\phi(x+y) \neq \phi(x)+\phi(y)$.

Uma outra maneira de perceber que ϕ não é um homomorfismo é usar a Proposição 4.1.1. Para isso, observe que o elementos neutros de G e de G' são ambos iguais a zero. Temos que $\phi(0) = 1$. Aqui, para que ϕ seja um homomorfismo é necessário (mas não suficiente) que $\phi(0) = 0$.

Proposição 4.1.2. *Se $\phi : G \to G'$ é um homomorfismo e se H é um subgrupo de G, então $\phi(H)$ é um subgrupo de G'. Onde $\phi(H) = \{\phi(h) : h \in H\}$*

Demonstração. Sabemos que $e_G \in H$ pois H é subgrupo de G, então $\phi(e_G) = e_{G'} \in \phi(H)$ e, portanto, $\phi(H)$ não é vazio. Sejam $x,y \in \phi(H)$, então existem $a,b \in H$, tais que $\phi(a) = x$ e $\phi(b) = y$. Assim,

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

Como $ab^{-1} \in H$ temos que $\phi(ab^{-1}) \in \phi(H)$. Sendo assim, xy^{-1} é um elemento de $\phi(H)$ e pela proposição 3.2.3 temos que $\phi(H)$ é subgrupo de G'. □

O leitor poderia se perguntar se a composição de homomorfismos ainda é um homomorfismo. Esse resultado está demonstrado na proposição seguinte.

Proposição 4.1.3. *Sejam G, G' e G'' grupos. Se $\phi : G' \to G''$ e $\tau : G \to G'$ são homomorfismos, então a composição $\phi \circ \tau$ é um homomorfismo de G em G''.*

Demonstração. Para demonstrar este resultado, é suficiente que se verifique a igualdade $(\phi \circ \tau)(xy) = (\phi \circ \tau)(x)(\phi \circ \tau)(y)$ para todos $x,y \in G$. Como ϕ e τ são homomorfismos, temos que, dados $x,y \in G$,

$$[\phi \circ \tau](x)[\phi \circ \tau](y) = \phi(\tau(x))(\phi\tau(y)) = \phi(\tau(x)\tau(y)) = \phi(\tau(xy)) = (\phi\tau)(xy) = [\phi \circ \tau](xy),$$

o que conclui a demonstração. □

Ao estudarmos funções é interessante analisarmos suas características quanto a injetividade ou sobrejetividade. Relembremos as definições de tais termos.

Definição 4.1.2. Uma função $\phi : A \to B$ é injetiva se sempre que $x_1 \neq x_2$, tivermos $\phi(x_1) \neq \phi(x_2)$.

Definição 4.1.3. Uma função $\phi : A \to B$ é sobrejetiva se para todo $b \in B$, $b = \phi(a)$, para algum $a \in A$.

De posse dessas definições, podemos classificar as funções que demos como exemplos de homomorfismos anteriormente. No o exemplo 4.1.1, note que nem o domínio nem o contradomínio foram explicitados. Para que a função seja sobrejetiva, devemos ter $G' = \{e\}$, por consequência, para que seja injetiva, o domínio tem que ser necessariamente $G = \{e\}$.

Passemos a analisar o exemplo 4.1.3. A função que definimos em tal exemplo é $\phi : G \to G'$, onde G é o conjunto dos números inteiros e G' é o conjunto dos inteiros pares; e a função é tal que $\phi(x) = 2x$. Esta função é claramente injetiva pois, se x_1 e x_2 são elementos de G, então $2x_1 = 2x_2$ implica que $x_1 = x_2$. Além disso, ϕ é sobrejetiva, uma vez que todo número par é escrito como $2x$, onde x é um número inteiro.

Com relação à função do exemplo 4.1.6, vemos claramente que ela é sobrejetiva já que todos os elementos de G' são imagem dos elementos de G. Note contudo, que a função ϕ não é injetiva, pois, por exemplo, $\phi(x) = 1$ para $x > 0$.

Note, contudo, que o homomorfismo entre as matrizes invertíveis de $\mathbb{M}_n$ e o conjunto dos números reais com a operação de multiplicação no exemplo 4.1.7 não é injetor pois um número real x_0 qualquer existem várias matrizes invertíves em $\mathbb{M}_n$ que o têm como determinante, mas é sobrejetor pois qualquer que seja o número real, sempre podemos criar uma matriz que o tenha como determinante. Digamos que queiramos uma matriz quadrada de ordem n cujo determinante seja x_0. Então tomamos uma matriz diagonal com $n-1$ entradas iguais a 1 em sua diagonal principal e com um elemento igual a x_0 em sua diagonal principal. Esta matriz terá determinante x_0. Este é o determinante da matriz M_n a seguir

$$M_n = \begin{pmatrix} x_0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Observe que o exemplo 4.1.9 exibe um homomorfismo que não é injetor, pois dado um número real existem infinitas maneiras de expressá-lo como soma de outros dois números reais, mas é sobrejetor já que dado um número real sempre poderemos expressá-lo como soma de dois outros números reais.

Considere agora o exemplo 4.1.8. Observe que a função $\phi : G \to G'$, onde G é o grupo dos números reais com a operação de soma e G' é o grupo dos reais não nulos com a operação de multiplicação, definida por $\phi(x) = 2^x$ não é sobrejetiva pois $2^x > 0$ para qualquer valor de x. Como ϕ é estritamente crescente, podemos concluir que $x_1 < x_2$, implica em $\phi(x_1) < \phi(x_2)$, o que mostra que a função é injetiva.

Vejamos agora, a função dada no exemplo 4.1.2. A função que devemos analisar é $\phi : \mathbb{R}^*_+ \to \mathbb{R}$, tal que $\phi(x) = \log_b x$. Como a função logaritmo é estritamente crescente quand $b > 1$,

segue que $x_1 < x_2$ implica em $\log_b x_1 < \log_b x_2$. Caso, $0 < b < 1$ temos que $x_1 < x_2$ resulta $\log_b x_1 > \log_b x_2$. Então, em ambos os casos, ocorre que $x_1 \neq x_2$ implica em $\phi(x_1) \neq \phi(x_2)$, ou seja, a função logaritmo é injetiva. Além disso, a função logaritmo é sobrejetiva, pois dado $y \in \mathbb{R}$, *sempre* existe um $x_0 \in \mathbb{R}_+$ tal que $\log_b x_0 = y$, independentemente da base b. Para mostrar tal fato, temos que demonstrar que y pode assumir qualquer valor no conjunto dos números reais para qualquer valor de x na equação $\log_b x = y$. Isso é verdade, pois

$$\log_b x = y \Rightarrow b^y = x,$$

onde $x > 0$. Tendo em vista que $b > 0$ e $b \neq 1$, isso se verifica para qualquer $x > 0$, segue que a pode assumir qualquer valor em $\mathbb{R}$.

Os exemplos que acabamos de exibir nos motivam as seguintes definições:

Definição 4.1.4. Um homomorfismo ϕ de G em G' é chamado de *monomorfismo* quando ϕ é injetiva.

Definição 4.1.5. Um homomorfismo ϕ de G em G' é chamado de *isomorfismo* quando ϕ é bijetiva. Nesse caso, escrevemos $G \approx G'$ e dizemos que G e G' são isomorfos.

No sentido da definição 4.1.4, temos que são monomorfismos as funções dos exemplos 4.1.2, 4.1.3 e 4.1.8. Dos exemplos que citamos nesta seção tratam-se de isomorfismos os exemplos 4.1.2 e 4.1.3.

Proposição 4.1.4. *Sejam G e G' grupos. Se ϕ é um isomorfismo de G em G', então ϕ^{-1} (a inversa de ϕ) é um isomorfismo de G' em G.*

Demonstração. Como ϕ é um isomorfismo, segue que ϕ é uma função bijetiva e, portanto, invertível. Além disso, ϕ^{-1}, a inversa de ϕ, também é bijetiva e invertível. Se mostrarmos que ϕ^{-1} é um homomorfismo de G' em G, teremos demonstrado o resultado. Como ϕ é sobrejetiva, temos que todo elemento de G' é da forma $\phi(w)$ para $w \in G$. Sejam $u = \phi(x)$ e $v = \phi(y)$ elementos de G'. Então, temos, por um lado, que

$$\phi^{-1}(u)\phi^{-1}(v) = \phi^{-1}(\phi(x))\phi^{-1}(\phi(y)) = xy$$

e, por outro, que

$$\phi^{-1}(uv) = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}(\phi(xy)) = xy.$$

Mostramos, então, que $\phi^{-1}(u)\phi^{-1}(v) = \phi^{-1}(uv)$, ou seja, que ϕ^{-1} é um homomorfismo. □

Algumas consequências imediatas da definição 4.1.5 são as que estão enunciadas a seguir.

Proposição 4.1.5. *Dados os grupos G, G' e G'' são verdadeiras as seguintes afirmações:*

(i) $G \approx G$.

(ii) *Se* $G \approx G'$, *então* $G' \approx G$.

(iii) *Se* $G \approx G'$ *e* $G' \approx G''$, *então* $G \approx G''$.

Demonstração. (i) Precisamos mostrar que existe um isomorfismo de G em G. Para tanto, tome a função $\phi : G \to G$ tal que $\phi(x) = x$, para cada $x \in G$. Este é um monomorfismo pois se $\phi(x_1) = \phi(x_2)$, então $x_1 = x_2$. E é sobrejetiva pois $\phi(x) = x$ para cada $x \in G$.

(ii) Sabemos existir um isomorfismo de G em G'. Isso significa que existe uma função bijetiva $\phi : G \to G'$. Como ϕ é bijetiva, é, também, invertível. Portanto, existe uma função

inversa de ϕ que denotaremos por ϕ^{-1} de G' em G, tal que $\phi^{-1}(\phi(x)) = \phi(\phi^{-1}(x)) = x$. Como ϕ^{-1} é a inversa de ϕ, segue que ϕ^{-1} é bijetiva. Logo $\phi^{-1} : G' \to G$ é um isomorfismo de G' em G.

(iii) Antes de começarmos a demonstração, vamos ver o que devemos demonstrar. Queremos mostrar que existe um isomorfismo de G em G'', isto é, devemos exibir uma função de G em G'' que seja, simultaneamente, injetiva e sobrejetiva. Uma forte candidata é a composição de $\tau : G' \to G''$ com $\phi : G \to G'$, onde τ e ϕ são os isomorfismos aos quais o enunciado se refere. Sejam, então, $x_1 \neq x_2$, tais que $\tau(\phi(x_1)) = \tau(\phi(x_2))$. Como τ é um isomorfismo de G' em G'', segue que é invertível, portanto

$$\tau(\phi(x_1)) = \tau(\phi(x_2)) \Rightarrow \tau^{-1}(\tau(\phi(x_1))) = \tau^{-1}(\tau(\phi(x_2))) \Rightarrow \phi(x_1) = \phi(x_2).$$

Sabemos que ϕ também é um isomorfismo e, portanto, é invertível. Logo,

$$\phi(x_1) = \phi(x_2) \Rightarrow \phi^{-1}(\phi(x_1)) = \phi^{-1}(\phi(x_2)) \Rightarrow x_1 = x_2,$$

Ora, mas havíamos suposto $x_1 \neq x_2$. Chegamos, então, a um absurdo, o que significa que nossa suposição é impossível, dentro das condições da proposição. Concluímos então que $\tau(\phi(x_1)) = \tau(\phi(x_2))$, implica, necessariamente, que $x_1 = x_2$, ou seja, a função $\tau\phi$ é injetiva.

Para mostrar que $\tau\phi$ é sobrejetiva, basta notar que $z = \tau(y)$ para cada $z \in G''$ e algum $y \in G'$, pelo fato de τ ser um isomorfismo. Do mesmo modo, como ϕ é um isomorfismo de G em G', segue que para cada $y \in G'$, $y = \phi(x)$ para algum $x \in G$. Sendo assim, $z = \tau(\phi(x))$ para cada $z \in G''$, o que mostra que a função é sobrejetiva.

□

No capítulo anterior exibimos uma função bijetiva de S_Δ em S_X, em que $X = \{A, B, C\}$. Se mostrarmos que esta função é um homomorfismo, teremos demonstrado que ambos os grupos são isomorfos. Primeiro, a função $\phi : S_\Delta \to S_X$ tal que

$$\begin{aligned}
\phi(e) &= \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \\
\phi\left(R_{\frac{2\pi}{3}}\right) &= \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \\
\phi\left(R_{\frac{4\pi}{3}}\right) &= \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \\
\phi\left(R_1\right) &= \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \\
\phi\left(R_2\right) &= \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \\
\phi\left(R_3\right) &= \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}
\end{aligned}$$

Vamos mostrar que esta função é um isomorfismo. Ao construirmos a tábua de multiplicação de S_Δ, obtivemos o seguinte:

$\cdot$	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
e	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e	R_3	R_1	R_2
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e	$R_{\frac{2\pi}{3}}$	R_2	R_3	R_1
R_1	R_1	R_2	R_3	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$
R_2	R_2	R_3	R_1	$R_{\frac{4\pi}{3}}$	e	$R_{\frac{2\pi}{3}}$
R_3	R_3	R_1	R_2	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e

Vamos agora construir uma tabela de multiplicação para o grupo S_X e tentar identificar algumas similaridades com a tábua acima. Antes, porém, por simplicidade de notação, faremos:

$$\begin{aligned}\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} &= a \\ \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} &= b\end{aligned}$$

Nessa notação temos que são verdadeiras as seguintes igualdades:

$$\begin{aligned} a^2 &= \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}, \\ a^3 &= \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, \\ ba &= \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}, \\ ab &= \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}, \\ b^2 &= \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}. \end{aligned}$$

Sendo assim, a tabela de multiplicações fica como a seguir

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Note que esta tábua é exatamente igual àquela que exibimos para as simetrias do conjunto S_Δ, após termos feito as identificações, $a = R_{\frac{2\pi}{3}}$ e $b = R_1$. Isso significa que ambos os grupos, em suma, são iguais! Em outras palavras eles são isomorfos já que têm a mesma quantidade de elementos e a mesma tábua de multiplicação. De agora em diante, estaremos mais interessados em estudar funções que são isomorfismos.

Quando dois grupos são isomorfos, então, a menos de notação, eles são iguais. Isso significa que se temos um isomorfismo ϕ de G em G' e conhecemos uma computação entre os

elementos de G. Esse isomorfismo nos diz como podemos "converter" os elementos de G para a notação dos elementos de G' e fazer a computação análoga em G'. Contudo, saber que dois grupos são isomorfos pode ser insuficiente em muitos casos, muitas vezes o objeto de interesse pode ser justamente o isomorfismo. Antes de continuarmos a discussão sobre isomorfismos, vamos exemplificar alguns grupos *que não são isomorfos*.

Exemplo 4.1.11. Dois grupos cujas ordens são diferentes não são isomorfos. De fato, suponha $\phi : G \to G'$, onde G tem m elementos e G' tem n elementos, com $m \neq n$. Vamos mostrar que ϕ não pode ser bijetiva. Primeiro o caso em que $m < n$. Suponha $m < n$ e ϕ sobrejetiva, mas isso é impossível pois se ϕ sobrejetiva, necessariamente teremos pelo menos um elemento de G relacionado com mais de um dos elementos de G'. Agora, se $m > n$ e ϕ não pode ser injetiva pois a imagem de ϕ deveria ter pelo menos m elementos o que é impossível.

Exemplo 4.1.12. Não podem ser isomorfos um grupo G onde a operação é comutativa – um grupo abeliano conforme a observação 3.3.1 – e um grupo G' cuja operação não comuta, uma vez que, necessariamente, suas tabelas de multiplicação serão diferentes.

Exemplo 4.1.13. Não são isomorfos $\mathbb{Q}$ com a operação de soma e $\mathbb{Q}_+$ com a operação de multiplicação. De fato, se $\phi : \mathbb{Q} \to \mathbb{Q}_+$ fosse um isomorfismo, teríamos que $\phi(x) = \phi\left(\frac{x}{2} + \frac{x}{2}\right) = \phi\left(\frac{x}{2}\right)\phi\left(\frac{x}{2}\right)$. E sabemos que para todo $x \in \mathbb{Q}$, a equação $\phi\left(\frac{x}{2}\right)\phi\left(\frac{x}{2}\right) = \left[\phi\left(\frac{x}{2}\right)\right]^2 = 2$ não tem solução. Logo $2 \notin \phi(\mathbb{Q})$.

5 O TEOREMA DE CAYLEY

No capítulo anterior vimos que existem algumas maneiras interessantes de se relacionar um um grupo G com um outro grupo H, como os homomorfismos e os isomorfismos. Um dos casos mais notáveis destas relações apareceu quando discutimos o grupo de simetrias de um triângulo que é isomorfo ao grupo de permutações S_X, onde $X = \{A,B,C\}$ e o grupo de simetrias do quadrado é isomorfo a um subgrupo do grupo de permutações S_V, em que $V = \{A,B,C,D\}$. Na realidade, ao longo da História da Matemática, a maioria dos grupos finitos surgiu como grupos de permutações. Arthur Cayley(1821-1895) foi um matemático britânico que fez grandes contribuições em sua área. Foi o primeiro a definir o conceito moderno de grupo, mas suas contribuições não se restringem à Teoria de Grupos, abrangendo também a Álgebra Linear – onde definiu o conceito de multiplicação de matrizes, a Teoria de Grafos e Análise Combinatória. Antes da contribuição de Cayley o conceito de grupo era entendido somente no sentido de grupos de permutação. Cayley foi o primeiro a observar que todo grupo é isomorfo a um subgrupo de S_X – o conjunto das funções bijetoras de um conjunto X em si mesmo, tornado grupo com a operação de composição de funções. O Teorema de Cayley enuncia-se como abaixo.

Teorema 5.0.1. *Todo grupo é isomorfo a um subgrupo de algum grupo de permutações.*

Demonstração. A prova que daremos aqui é construtiva no sentido que ela dá um algoritmo para converter um grupo dado em um grupo de permutação. Seja G um grupo e S_G o grupo das permutações dos elementos de G. Fixe $g \in G$ e considere a função $\tau_g : G \to G$ definida por $\tau_g(x) = gx$ para cada $x \in G$. Observe que τ_g tal como foi definida é bijetiva. De fato, se $\tau_g(x) = \tau_g(y)$, temos que $gx = gy$ e, portanto, pela propriedade do cancelamento pela esquerda, ocorre que $x = y$, garantindo a injetividade. Agora, seja $y \in G$, temos que

$$y = gg^{-1}y = g(g^{-1}y) = \tau_g(g^{-1}y),$$

mostrando que τ_g é sobrejetiva. Portanto, τ_g é permutação dos elementos de G.

Definamos, agora, a função $\psi : G \to S_G$, tal que $\psi(g) = \tau_g$. Vamos mostrar que ψ é um homomorfismo de grupos. De fato, temos que

$$[\psi(g)\psi(h)](x) = \tau_g\tau_h(x) = \tau_g(\tau_h(x)) = \tau_g(hx) = g(hx) = (gh)x = \tau_{gh}(x) = [\psi(gh)](x),$$

o que mostra que ψ é um homomorfismo. Se mostrarmos que ψ é uma função injetiva, o resultado terá sido demonstrado. Com efeito, suponha $\psi(g) = \psi(h)$. Então, temos que $\tau_g = \tau_h$ e, em particular, temos que $\tau_g(e) = \tau_h(e)$

$$\begin{aligned} \tau_g(e) &= \tau_h(e) \\ ge &= he \\ g &= h \end{aligned}$$

□

Para entender melhor o que acabamos de afirmar no parágrafo anterior considere o seguinte exemplo.

Exemplo 5.0.14. Considere o grupo do exemplo 3.1.8, isto é, o conjunto $V = \{e,a,b,c\}$ com

uma operação $\cdot$ que tenha a propriedade de que cada elemento é seu próprio inverso. Construímos a tabela com todas as operações possíveis neste grupo e que exibimos a seguir.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Note que para cada um dos elementos de G podemos definir as seguintes funções:

- $\tau_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}$ que pode ser identificada com a permutação $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$;
- $\tau_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix}$ que pode ser identificada como a permutação $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$;
- $\tau_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}$ que pode ser identificada pela permutação $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$;
- $\tau_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}$ que pode ser interpretada como $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

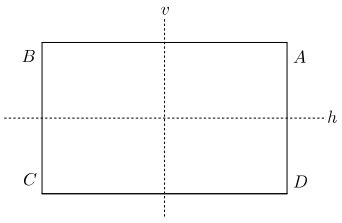
Portanto, pelo Teorema 5.0.1, o conjunto

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

com a operação de composição de funções é um grupo isomorfo ao grupo G.

Exemplo 5.0.15. Um exemplo similar ao grupo de simetrias do quadrado que estudamos na seção 3.3 é o grupo de simetrias do retângulo. Observe na Figura 24 que o retângulo tem somente dois eixos de simetria o eixo h e o eixo v. As reflexões em torno de h e de v, serão denotadas por R_h e R_v, respectivamente. Além disso, existem somente duas rotações do retângulo que levam vértice em vértice que são as rotações de 0 rad e π rad que serão denotados por e e R_π, respectivamente.

Figura 24: Um retângulo e seus eixos de simetria.



Fonte: elaborada pelo autor.

Vamos denotar por $S_{ret} = \{e, R_\pi, Rv, R_h\}$ o conjunto de simetrias do retângulo. Esse conjunto com a operação de composição de funções forma um grupo. Note que $R_h R_h = R_v R_v = R_\pi = ee = e$, ou seja, cada um dos elementos é inverso de si próprio. Além disso, observe que $R_h R_v = R_v R_h = R_\pi$, $R_h R_\pi = R_\pi R_h = R_v$ e $R_v R_\pi = R_\pi R_v = R_h$. Vamos escrever a tabela de multiplicação desse grupo.

$\cdot$	e	R_π	R_v	R_h
e	e	R_π	R_v	R_h
R_π	R_π	e	R_h	R_v
R_v	R_v	R_h	e	R_π
R_h	R_h	R_v	R_π	e

Observe que para cada um dos elementos de S_{ret} podemos atribuir uma permutação dos elementos de S_{ret} que pode ser identificada com um elemento do grupo S_4 como a seguir.

- $\tau_e = \begin{pmatrix} e & R_\pi & R_v & R_h \\ e & R_\pi & R_v & R_h \end{pmatrix}$ que pode ser identificada com $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$;
- $\tau_{R_\pi} = \begin{pmatrix} e & R_\pi & R_v & R_h \\ R_\pi & e & R_h & R_v \end{pmatrix}$ que pode ser identificada com $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$;
- $\tau_{R_v} = \begin{pmatrix} e & R_\pi & R_v & R_h \\ R_v & R_h & e & R_\pi \end{pmatrix}$ que pode ser identificada com a permutação $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$;
- $\tau_{R_h} = \begin{pmatrix} e & R_\pi & R_v & R_h \\ R_h & R_v & R_\pi & e \end{pmatrix}$ que pode ser associada à permutação. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

Portanto, pelo Teorema 5.0.1 temos que o grupo de simetrias do retângulo é isomorfo a um subgrupo de S_4.

Observe que o grupo S_{ret} do exemplo 24 é isomorfo a um determinado grupo H de S_4 que por sua vez é isomorfo ao grupo de simetrias do retângulo. Então, pela proposição 4.1.5 temos que são isomorfos os grupos S_{ret} e o grupo de Klein.

Não por acaso, o exemplo acima deve ter lembrado o leitor da situação que analisamos na Seção 3.3. Naquele contexto, analisamos os grupos de simetrias do triângulo e o grupo de simetrias do quadrado e constatamos que eles têm uma relação muito estreita com alguns grupos de permutação. Vimos por exemplo que existe uma bijeção do grupo de simetrias do triângulo no grupo S_3, o que mostra que estes grupos são isomorfos como afirma o Teorema 5.0.1. Já com relação ao grupo de simetrias do quadrado, vimos que este é isomorfo ao conjunto Q munido da operação de composição de funções, uma vez que estabelecemos uma bijeção entre $S_\square$ e

$$Q = \left\{ \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix} \right\}.$$

6 APLICAÇÃO NO ENSINO MÉDIO

Neste capítulo, apresentamos um plano de aula que trata-se de uma sugestão de aplicação dos grupos de simetria do triângulo e do quadrado vistos neste trabalho. O principal objetivo é fazer com que os alunos percebam a relação entre as de simetria desses polígonos com as permutações dos elementos que identificam seus vértices de modo a motivar a definição de grupo.

6.1 GRUPOS DE SIMETRIA NO ENSINO MÉDIO

1. Objetivos:
   - Apresentar os grupos de simetrias do triângulo equilátero e do quadrado;
   - Fazer com que o aluno perceba as relações entre os grupos de simetria e os de permutação.
2. Recursos:
   - Folhas de papel com um desenho de um triângulo equilátero com os vértices identificados;
   - Modelos de cartolina de um triângulo idêntico àquele desenhado no papel com os vértices identificados em frente e verso;
   - Folhas com um desenho de um quadrado com os vértices identificados;
   - Modelos de cartolina de um quadrado idêntico àquele desenhado no papel com os vértices identificados em frente e verso;
   - Um modelo de cartolina de um triângulo equilátero com seus vértices identificados em frente e verso em tamanho grande;
   - Um modelo de cartolina de um quadrado com seus vértices identificados em frente e verso em tamanho grande;
   - Quadro negro e giz.
3. Duração:
   - Quatro a seis aulas;
4. Metodologia:
   - Primeiro momento:
     - Solicitar aos alunos que listem todas as permutações do conjunto $X = \{A, B, C\}$;
     - Pedir aos alunos que posicionem o modelo de cartolina sobre a folha com o desenho do triângulo de modo a fazer corresponder os mesmos vértices do triângulo da folha com os do modelo de cartolina;
     - Solicitar que façam movimentos com o modelo de cartolina do triângulo de modo a sobrepô-lo ao triângulo desenhado na folha e que comparem a posição original com a posição obtida a cada movimento. Deve-se voltar à posição original após cada movimento. O professor pode auxiliar nesse passo utilizando o modelo em tamanho grande;

  - Pedir que associem cada permutação do conjunto X com um dos movimentos feitos no passo anterior;
  - Comparar a quantidade simetrias encontradas com a de permutações dos elementos de X;
  - Explicar que a associação feita foi uma função do conjunto do grupo de simetrias do triângulo no conjunto de permutações do conjunto X;
  - Solicitar que classifiquem esta função quanto à injetividade e quanto à sobrejetividade. Caso não consigam, fazê-lo;
  - Fazer o aluno perceber que toda simetria foi associada a uma permutação de X.
- Segundo momento:
  - Perguntar aos alunos se os movimentos feitos com o triângulo podem ser desfeitos de modo a retornar o triângulo à sua posição original;
  - Perguntar aos alunos se algum dos movimentos deixa as posições dos vértices do triângulo inalterada;
  - Solicitar aos alunos que componham alguns movimentos se o resultado obtido pode ser obtido por apenas um movimento;
  - Escolher três das simetrias do triângulo e fazer com que os alunos percebam que esta a operação de composição de simetrias é associativa;
  - Perguntar aos alunos se conhecem outros conjuntos que têm essas mesmas propriedades. Caso não conheçam exemplificar alguns;
- Terceiro momento:
  - Solicitar aos alunos que listem todas as permutações do conjunto $Y = \{A, B, C, D\}$
  - Pedir aos alunos que posicionem o modelo de cartolina sobre a folha com o desenho do quadrado de modo a fazer corresponder os mesmos vértices do quadrado da folha com os do modelo de cartolina;
  - Solicitar que façam movimentos com o modelo de cartolina do quadrado de modo a sobrepô-lo ao quadrado desenhado na folha e que comparem a posição original com a posição obtida a cada movimento. Deve-se voltar à posição original após a cada movimento. O professor pode auxiliar nesse passo utilizando o modelo em tamanho grande;
  - Listadas as permutações, solicitar que usando o modelo façam movimentos com o modelo de cartolina do quadrado de modo a sobrepô-lo ao quadrado desenhado na folha e que comparem as posições dos vértices antes e depois dos movimentos aplicados e que registrem cada um deles;
  - Pedir que associem cada permutação do conjunto Y com um dos movimentos feitos no passo anterior;
  - Comparar a quantidade de simetrais encontradas com a quantidade de permutações dos elementos de Y;
  - Explicar que a associação feita foi uma função do conjunto do grupo de simetrias do triângulo no conjunto de permutações do conjunto Y;
  - Solicitar que classifiquem esta função quanto à injetividade e quanto à sobrejetividade;
  - Perguntar aos alunos o porquê de algumas permutações do conjunto Y não estão associadas a nenhum dos movimentos feitos. Caso não percebam, explicar o motivo.

- Quarto momento:
  - Perguntar aos alunos se os movimentos feitos com o quadrado podem ser desfeitos de modo a retornar o triângulo à sua posição original;
  - Perguntar aos alunos se algum dos movimentos deixa as posições iniciais dos vértices do quadrado inalterada com relação à posição originial;
  - Solicitar aos alunos que componham alguns movimentos e verifiquem se o resultado obtido pode ser obtido por apenas um movimento;
  - Deixar que os alunos escolham três das simetrias do quadrado e fazer com que os alunos percebam que esta operação de composição de simetrias é associativa;
  - Perguntar aos alunos se conhecem outros conjuntos que têm essas mesmas propriedades. Caso não conheçam exemplificar alguns;

7 CONCLUSÃO

Acreditamos que a abordagem que fizemos nestre trabalho possa despertar alunos e professores para um caráter mais contemplativo da Matemática, já que, de modo geral, o racicínio abstrato tem sido deixado de lado em detrimento de um treinamento que estimulam ideias meramente calcadas no pragmatismo. A abstração de idéias que o método matemático proporciona pode ser uma via de passagem para aqueles que desejam entender como a formulação de hipóteses sobre situações aparentemente corriqueiras, como o embaralhamento de quatro cartas de um baralho, podem desencadear a conjectura de resultados muito mais profundos e gerais.

Uma das principais características da Matemática é seu poder de abstração e generalização; e esse poder manifesta-se muito claramente na Álgebra. Nesse trabalho, tal poder é evidenciado, sobretudo, pelo resultado do Teorema de Cayley. Acreditamos que este pequeno vislumbre sobre a Matemática desperte o interesse em um maior aprofundamento teórico por parte dos estudantes que tomem conhecimento desse trabalho, principalmente em concluintes do Ensino Médio.

Temos plena consciência de que uma abordagem tal qual foi feita ao longo destas páginas seja inviável para uma aplicação direta em sala de aula. Contudo, com pequenas adaptações, estes temas podem ser incluídos em debates sobre os temas curriculares no Ensino Médio ou mesmo em um curso extra-classe de curta duração.

Projetos futuros incluem o aprofundamento no estudo de Álgebra e possivelmente a publicação de um artigo relacionado à Teoria de Grupos em uma revista destinada ao público docente/discente como a Revista do Professor de Matemática ou a Revista da Olimpíada Regional de Matemática. Acreditamos que um meio de divulgação desse porte possa potencializar a mensagem que tentamos transmitir com este trabalho.

REFERÊNCIAS

ARMSTRONG, M. A.. **Groups and Symetry**. New York: Springer-Verlag, 1998.

LIMA, E. L. et al. **A Matemática do Ensino Médio**. 9. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006. (Coleção do Professor de Matemática).

FLORENCIO, M. P.. **Transformações no Plano e Grupos de Simetria**. 2011. 46 f. TCC (Graduação) - Curso de Matemática, Univerdade Federal de São Carlos, São Carlos, 2011.

GARCIA, A.; LEQUAIN, Y.. **Elementos de Álgebra**. 6. ed. Rio de Janeiro: Impa, 2012. (Projeto Euclides).

HERNSTEIN, I. N.. **Tópicos de Álgebra**. São Paulo: Polígono, 1970.

SILVA, R. M. da. **Uma Introdução às Álgebras com Identidades Polinomiais**. 2013. 96 f. TCC (Graduação) - Curso de Matemática, Universidade Federal de Santa Catarina, Florianópolis, 2013.