



Ciência e Natura

ISSN: 0100-8307

cienciaenaturarevista@gmail.com

Universidade Federal de Santa Maria

Brasil

de Souza, Rodrigo Luiz
Permutações, Grupos e Simetrias
Ciência e Natura, vol. 37, núm. 3, 2015, pp. 289-307
Universidade Federal de Santa Maria
Santa Maria, Brasil

Disponível em: <http://www.redalyc.org/articulo.oa?id=467547643024>

- Como citar este artigo
- Número completo
- Mais artigos
- Home da revista no Redalyc

redalyc.org

Sistema de Informação Científica

Rede de Revistas Científicas da América Latina, Caribe, Espanha e Portugal

Projeto acadêmico sem fins lucrativos desenvolvido no âmbito da iniciativa Acesso Aberto

Permutações, Grupos e Simetrias

Permutations, Groups and Symmetries

Rodrigo Luiz de Souza *¹

1 Mestre em Matemática - Professor substituto da Universidade do Estado de Santa Catarina, SC, Brasil

Resumo

Este artigo tem por objetivo ser uma breve introdução à Teoria de Grupos. Iniciando a abordagem foi introduzindo o conceito de permutação e sua definição como funções bijetivas de um grupo em si mesmo. Na sequência, a partir do que foi exposto sobre permutações, foram apresentados os conceitos de grupo e subgrupo, bem como algumas das propriedades básicas de tais estruturas. Dando prosseguimento à discussão, foram apresentados os grupos de simetria do triângulo e do quadrado com o intuito de fazer um paralelo entre o que foi estudado sobre permutações e as simetrias de tais figuras planas. No fechamento do trabalho foi sugerido um pequeno plano de aula de modo a abordar alguns temas expostos aqui em uma aula de uma turma de Ensino Médio.

Palavras-chave: *Álgebra, permutações, Teoria de Grupos, Grupos de Simetria, Ensino Médio.*

Abstract

The main goal this paper is to be a brief introduction to the Group Theory. To begin the study, the concept of permutation was introduced and defined as a bijective function from a group on itself. After that, the concepts of group and subgroup were exhibited and discussed, as well as their basic properties. Using the concepts discussed so far, the symmetry groups for the equilateral triangle and for the square were presented in order to compare this particular groups with the permutation groups. In the last section of this paper, we suggest a guide to apply the concept discussed here on a High School class.

Keywords: *Algebra, permutations, Group Theory, Symmetry Groups, High School.*

1 Introdução

Este artigo tem por objetivo fazer uma breve exposição sobre alguns temas da Álgebra, em particular sobre a Teoria de Grupos, para alunos de Ensino Médio e estudantes de graduação que desejem ter um primeiro contato com tal área da Matemática. Buscamos, sempre que possível a abordagem de exemplos que, se não familiares, são de fácil compreensão por parte desse público.

Na primeira parte tratamos das permutações. Nosso objetivo não foi o de fazer grande aprofundamento teórico, mas criar uma motivação para o estudo a partir da qual seja natural compreendê-las como funções de um conjunto em si mesmo. A partir das propriedades das funções bijetivas e estendendo tais propriedades às permutações, direcionamos nosso estudo às ideias básicas da Teoria de Grupo.

Na sequência após alguns resultados sobre grupos e subgrupos, reservamos um espaço para o estudo dos grupos de simetrias do triângulo equilátero e do quadrado, uma vez que as simetrias de tais polígonos são um excelente recurso para estudar grupos de permutações.

Finalizando o trabalho, deixamos como sugestão de abordagem dos temas tratados neste artigo em um pequeno plano de aula para 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.

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.

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 arbitrário, já que, para montar uma determinada sequência, é suficiente



Figura 2: Uma outra sequência de ases.

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 do embaralhamento 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. Tome-mos 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

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad (2.1)$$

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 significam 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 da Figura 3, que é uma forma mais prática de se obter a sequência permutada. A ordem resultante é aquela destacada pelo retângulo.

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

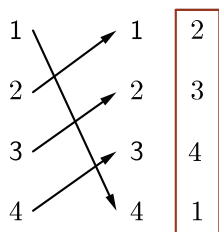


Figura 3: Esquema para o embaralhamento em (2.1).

ção 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

$$\begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 4 & 2 & 3 \end{pmatrix} \quad (2.2)$$

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.

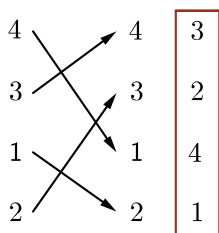


Figura 4: Diagrama para o embaralhamento em (2.2).

Contudo, note que obter a sequência $(3,2,4,1)$ a partir de $(1,2,3,4)$ requer um certo embaralhamento, 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 um 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 originalmente 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 a seguinte $(\phi(x_1), \phi(x_2), \phi(x_3), \phi(x_4)) = (x_2, x_4, x_1, x_3)$, 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, \dots, x_n) obtida a partir da função ϕ pode ser representada por

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

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 a imagem de (x_1, x_2, \dots, x_n) por ϕ pode ser representada simplesmente por

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

Onde os termos x_i da sequência s foram substituídos 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 $S = \{x_1, x_2, \dots, x_n\}$ e $\phi : S \rightarrow S$ 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, \dots, 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 a linguagem usual de funções para estudarmos as permutações. Para isso, retomemos o exemplo dado no início da seção anterior 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.

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.

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

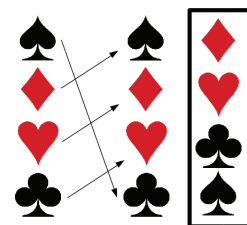


Figura 7: Diagrama que mostra como ϕ atua sobre cada uma das cartas.

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: Disposição obtida a partir da sequência permutada.

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

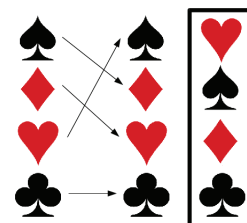


Figura 9: Como τ atua sobre as cartas.

Observação 2.1. 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 Figura 8 aplicando uma única permutação como indicado a seguir:

$$\begin{pmatrix} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \clubsuit & \diamondsuit & \heartsuit & \spadesuit \end{pmatrix}, \quad (2.5)$$

ou seja, trocando as posições das cartas de espadas e de paus. Contudo, se analisarmos mais cuidadosamente do ponto de vista teórico a operação 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 $\phi : A \rightarrow B$ e $\tau : B \rightarrow C$ 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 $\tau\phi(x) = \tau(\phi(x)) = (\tau \circ \phi)(x)$.

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. A operação $\tau \circ \phi$ na notação de 2.4 será representada como a seguir

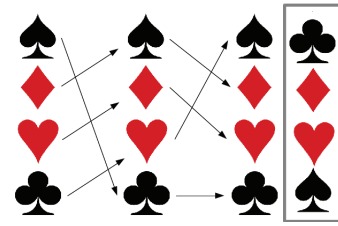


Figura 10: Diagrama da composição $\tau\phi$.

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

Continuando nosso estudo, poderíamos nos perguntar ainda, se a ordem em que efetuamos uma composição altera a permutação obtida como resultado final. Observe como fica a composição $\phi\tau$ na Figura 11.

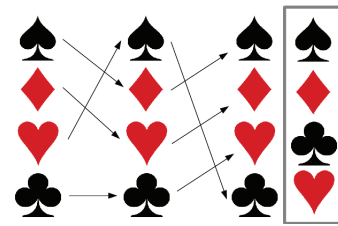


Figura 11: Diagrama da composição $\phi\tau$.

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 como em 2.4 temos que a composição $\phi\tau$ é escrita como segue.

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

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! 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

$$(\phi\tau)\mu = \phi(\tau\mu). \quad (2.6)$$

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 efetuar-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 abordaremos mais detalhadamente na próxima seção.

3 Noções Básicas sobre Grupos

3.1 Conceitos Preliminares

Nesta seção vamos generalizar alguns dos conceitos vistos na seção anterior e discutiremos uma das partes fun-

damentais 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. Considere o conjunto \mathbb{Z} dos números inteiros, com a operação usual de adição. 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 3.2. 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. 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 $a = 1$, temos que $b = 1$; e para $a = -1$, ocorre que $b = -1$.

Quando tratamos das operações de permutação e composição de permutações na seção anterior vimos que as mesmas propriedades que são válidas nos Exemplos 3.1 e 3.2. De modo geral, podemos estabelecer uma definição:

Definição 3.1. 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 $a \cdot a^{-1} = a^{-1} \cdot a = e$. 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 e 3.2 com as suas respectivas operações formam grupos. No Exemplo 3.1, temos que a^{-1} é o inverso de a pela operação de soma, portanto $a^{-1} = -a$. Já no Exemplo 3.2, 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 $a = -1$, $a^{-1} = -1$. Além disso, o conjunto das permutações de um determinado conjunto com a operação de composição de permutações também é um grupo (verifique).

Exemplo 3.3. O conjunto dos números reais positivos sem o zero, denotado por \mathbb{R}_+^* com a operação de multiplicação é um grupo. Primeiro observe que quando multiplicarmos dos elementos desse conjunto o produto permanece em \mathbb{R}_+^* . 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 foram satisfeitas, segue que este é um grupo.

Exemplo 3.4. O conjunto dos múltiplos inteiros de um número inteiro fixado com a operação usual de adição é um grupo. Antes de verificar 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 múltiplo 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 não se verificar para um determinado conjunto munido com uma operação não teremos um grupo. Observe os dois próximos exemplos.

Exemplo 3.5. 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 3.1. 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 3.6. 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 independentemente dos valores de a, b, c e d .

Observe, porém, que se nos restringirmos às matrizes de \mathbb{M}_2 que são invertíveis, todas as condições da Definição 3.1 serão satisfeitas. 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 $AB \neq BA$.

Observação 3.1. Para efeitos de notação, em qualquer grupo G e para qualquer elemento $a \in G$, definiremos de agora em diante que

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

e também definiremos que

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

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

$$\begin{aligned}a^m \cdot a^n &= a^{m+n} \\ (a^m)^n &= a^{m \cdot n}.\end{aligned}$$

Usando a notação introduzida na Definição 3.1, vamos analisar novamente o Exemplo 3.1. 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 3.2 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 3.2, 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, $a^n = a \cdot a \cdot a \cdot \dots \cdot a$.

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 seguinte.

Exemplo 3.7. Seja X um conjunto não vazio qualquer. Considere o conjunto $A(X)$ tal que $A(X) = \{\phi : X \rightarrow X : \phi \text{ é uma bijeção}\}$. 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 $A(X)$ ainda obteremos um elemento desse conjunto, ou seja, que a composição de duas bijeções ainda resulta em uma bijeção. Sejam $\phi_1, \phi_2 \in A(X)$. 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

$$\phi_2(\phi_1(x)) = \phi_2(\phi_1(y))$$

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

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 conclui-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. 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 .

Até aqui analisamos alguns exemplos à luz do que foi estabelecido na Definição 3.1, 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 único, 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. 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

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

De fato, pela propriedade associativa da operação em G temos que $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a (b \cdot b^{-1}) a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$. Analogamente, temos que $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot e \cdot b = b^{-1} \cdot b = e$. 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. \square

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, onde consideramos o conjunto dos números inteiros com a operação de adição e considere a restrição feita no exemplo a seguir.

Exemplo 3.8. 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 3.4). 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 3.9. Seja X um conjunto não vazio e S_X o grupo das permutações dos elementos de X , como no Exemplo 3.7. 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, 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, 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. 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. Uma inferência imediata que se pode tirar da Definição 3.2 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 3.8 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 3.9.

Uma nota de precaução se faz necessária aqui. No Exemplo 3.8 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 3.9. 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. A seguinte proposição mostra que essa conjectura é verdadeira

Proposição 3.2. *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. \square

Note que nos Exemplos 3.8 e 3.9 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 3.3. *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. \square

De modo geral, se H for um subgrupo finito podemos até mesmo ignorar a condição (ii) da Proposição 3.3. Vejamos isso na seguinte proposição.

Proposição 3.4. *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 3.3, é suficiente mostrarmos que $a^{-1} \in H$ para cada $a \in H$. Suponhamos $a \in H$; assim $a^2 = aa \in H$, $a^3 = a^2 a \in H$, $a^4 = a^3 a \in H$, ..., $a^m \in H$, ... pois H é fechado com relação à operação induzida de G . De modo que $a, a^2, a^3, \dots, a^m, \dots$ 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. \square

A proposição 3.4 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 Simetrias 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,

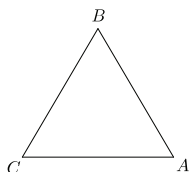


Figura 12: Triângulo que estamos supondo desenhado em uma folha de papel.

que o modelo sobreponha-se exatamente ao triângulo desenhado no papel e que em sua posição inicial os vértices A , B e C do modelo estejam respectivamente sobre os vértices A , B e C do desenho. 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.

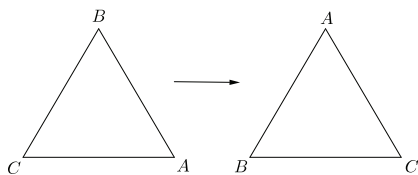


Figura 13: Um triângulo equilátero rotacionado em $\frac{2\pi}{3}$.

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 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 sobrepor-lo ao desenho do triângulo equilátero é uma reflexão como na Figura 14.

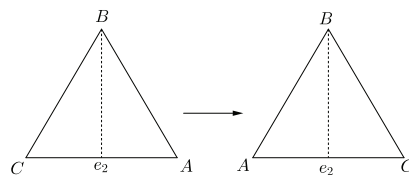


Figura 14: Um triângulo refletido em torno do eixo e_2 .

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.

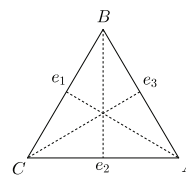


Figura 15: Triângulo com os eixos e_1 , e_2 e e_3 .

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.

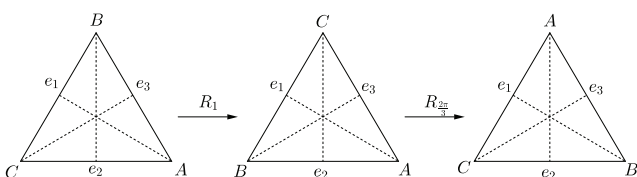


Figura 16: Ilustração da composição $R_{\frac{2\pi}{3}}R_1 = R_3$.

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 $R_{\frac{2\pi}{3}}R_1$.

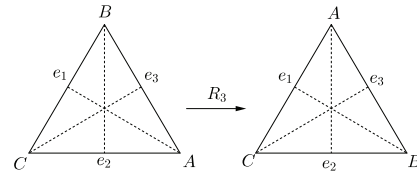


Figura 17: Ilustração da movimentação R_3 .

Tabela 1: Tabela de Multiplicação do Grupo S_Δ .

\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

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

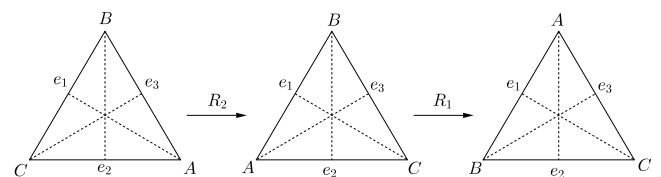


Figura 18: Ilustração da composição $R_1R_2 = R_{\frac{2\pi}{3}}$.

mostrado na Figura 18 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 .

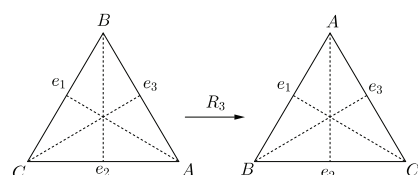


Figura 19: Ilustração aplicação do movimento $R_{\frac{2\pi}{3}}$.

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 ¹ a seguir.

Na verdade, com a tabela feita, podemos facilmente verificar que o conjunto S_Δ das simetrias de um triângulo equilátero, isto é, $S_\Delta = \{e, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}$, 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

¹Uma tabela de multiplicação consiste em uma espécie de tabuada de uma determinada operação efetuada com os elementos de um certo conjunto.

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 $R_1 R_1 = e$, $R_2 R_2 = e$ e $R_3 R_3 = e$ 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 correspondentes, 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 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 $R_{\frac{2\pi}{3}}$ em torno do baricentro do triângulo 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 $R_1 R_2$ 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 entendida 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:

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}. \quad (3.1)$$

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 $R_1 R_2$ do ponto de vista das permutações dos vértices do triângulo, corresponde à composição mostrada em 3.2.

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}. \quad (3.2)$$

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

¹Uma tabela de multiplicação consiste em uma espécie de tabuada de uma determinada operação efetuada com os elementos de um certo conjunto.

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

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 , como mostra a Tabela 2, são iguais!

Tabela 2: Tábua de multiplicação de S_Δ em nova notação.

\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. 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. 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.

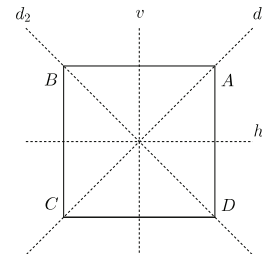


Figura 20: Um quadrado e seus eixos de simetria.

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. A permutação $\begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$, por exemplo, 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 corresponder uma simetria o vértice D aparece entre os vértices A e B , o que ocorre na permutação que acabamos de citar. Deixamos a cargo do leitor encontrar as outras 15 permutações que não representam uma simetria do quadrado.

De modo totalmente análogo ao que fizemos para as simetrias do triângulo equilátero, podemos mostrar que o conjunto $S_{\square} = \{e, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}, R_1, R_2, R_h, R_v\}$ 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.

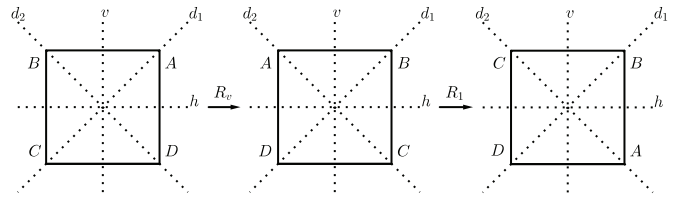


Figura 21: Ilustração da composição $R_1 R_v = R_{\frac{3\pi}{2}}$

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

$$\begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix}. \quad (3.3)$$

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

$$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}, \quad (3.4)$$

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.

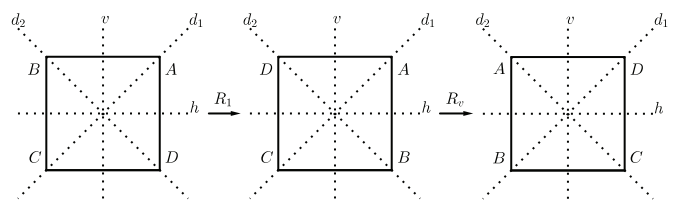


Figura 22: Ilustração da composição $R_v R_1 = R_{\frac{\pi}{2}}$

Na Tabela 3 a seguir estão todas as possíveis composições das simetrias de um quadrado.

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 com-

posições adequadas de $R_{\frac{\pi}{2}}$ e R_1 pode-se obter qualquer um dos elementos de S_{\square} , como vemos nas igualdades abaixo.

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

Nessa nova notação, a tabela de composições fica como mostrado na Tabela 4.

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 $\phi: S_{\Delta} \rightarrow S_X$. Assim, se tomarmos a e b elementos de S_{Δ} , teremos que se verifica a igualdade $\phi(ab) = \phi(a)\phi(b)$, desde que definamos $\phi(R_1) = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$ e $\phi(R_{\frac{2\pi}{3}}) = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$. Vamos revisitar as igualdades em (3.1) e (3.2) tendo em vista a função ϕ que acabamos de definir. Assim, temos de (3.1)

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

e

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

Mostrando que

$$\phi(R_{\frac{2\pi}{3}}R_1) = \phi(R_{\frac{2\pi}{3}})\phi(R_1)$$

Já da igualdade (3.2) podemos inferir que

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

e, também,

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

Mostrando que

$$\phi(R_1R_2) = \phi(R_1)\phi(R_2)$$

Analogamente ao que fizemos acima, podemos também reinterpretar as equações (3.3) e (3.4) do quadrado. Para tanto, tome $\tau: S_{\square} \rightarrow Q$, onde

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

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 da a equação (3.3) temos

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

Podemos concluir, então, que $\tau(R_1R_v) = \tau(R_1)\tau(R_v)$.

Já da equação (3.4) deduzimos que

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

ou seja, temos que $\tau(R_vR_1) = \tau(R_v)\tau(R_1)$. Funções com uma peculiaridade tão interessante como as funções que definimos logo acima não são uma feliz coincidência. As funções com a propriedade de que $\phi(ab) = \phi(a)\phi(b)$ são chamadas de *homomorfismos* e não serão abordadas aqui além de sua definição.

Definição 3.3. 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 3.4. Se a função ϕ da Definição 3.3 for bi-jetiva, dizemos que ϕ é um *isomorfismo* de G em G' e dizemos que G e G' são isomorfos.

Uma das maneiras de ver que dois grupos são iso-

Tabela 3: Tabela de Multiplicação de S_{\square} .

\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

Tabela 4: Tabela de Multiplicação de S_{\square} em nova notação.

\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

morfos é verificar que suas tábuas de multiplicação são iguais. Assim como fizemos anteriormente para os grupos de simetria do triângulo e para o grupo de permutações de $\{A,B,C\}$ e para o grupo de simetrias do quadrado e do conjunto $\{A,B,C,D\}$.

4 Aplicação no Ensino Médio

Nesta seção, 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, nos valendo dos conceitos de isomorfismo de grupos. O principal objetivo é fazer com que os alunos percebam a relação entre as simetrias desses polígonos com

as permutações dos elementos que identificam seus vértices de modo a motivar a definição de grupo e permitir que eles criem, a partir de sua experiência escolar, seus próprios exemplos de grupos.

4.1 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 simetrias 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 original;
 - 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;

5 Conclusões

Acreditamos que a abordagem que fizemos neste trabalho possa despertar alunos e professores para um caráter mais contemplativo da Matemática, já que, de modo geral, o raciocínio abstrato tem sido deixado de lado em detrimento de um treinamento que estimulam ideias meramente calcadas no pragmatismo. 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. 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. E acreditamos que a sugestão de aplicação em sala de aula pode servir como um pequeno passo na direção de instigar os alunos a fazerem suas próprias generalizações.

Referências

- [1] ARMSTRONG, M. A.. **Groups and Symetry**. New York: Springer-Verlag, 1998.
- [2] GARCIA, A.; LEQUAIN, Y.. **Elementos de álgebra**. 6. ed. Rio de Janeiro: Impa, 2012. (Projeto Euclides).
- [3] HERNSTEIN, I. N.. **Tópicos de álgebra**. São Paulo: Polígono, 1970.
- [4] 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).