Universidade Estadual Paulista “Júlio de Mesquita Filho”
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

# Cubo Mágico: Propriedades e Resoluções envolvendo Álgebra e Teoria de Grupos

**Luis Gustavo Hauff Martins Grimm**

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional – PROFMAT como requisito parcial para a obtenção do grau de Mestre

Orientadora
**Profa. Dra. Carina Alves**

**2016**

512 Grimm, Luis Gustavo Hauff Martins
G864c Cubo mágico : propriedades e resoluções envolvendo álgebra e Teoria de Grupos / Luis Gustavo Hauff Martins Grimm. - Rio Claro, 2016
82 f. : il., figs., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas
Orientadora: Carina Alves

1. Álgebra. 2. Cubo de Rubik. 3. Grupos de permutação. 4. Comutadores e conjugados. 5. Proposta didática. I. Título.

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

## TERMO DE APROVAÇÃO

Luis Gustavo Hauff Martins Grimm

Cubo Mágico: Propriedades e Resoluções envolvendo Álgebra e Teoria de Grupos

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática Universitária do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Carina Alves
Orientadora

Prof. Dr. Cristiane Alexandra Lázaro
UNESP - Faculdade de Ciências - Bauru

Prof. Dr. Agnaldo José Ferrari
UNESP - Faculdade de Ciências - Bauru

**Rio Claro, 30 de agosto de 2016.**

*À minha família*

Agradecimentos

À minha esposa pelo apoio, incentivo, companhia nos estudos e pelo auxílio com o LaTeX.

À professora Carina Alves pela competência e paciência durante a orientação deste trabalho.

A todos os professores do Mestrado Profissional em Matemática em Rede Nacional da UNESP de Rio Claro pela contribuição nesse processo de formação continuada de profissionais que atuam na educação básica.

Aos funcionários da secretaria de pós-graduação da UNESP de Rio Claro pela atenção e empenho em ajudar prontamente.

À Sociedade Brasileira de Matemática (SBM) por implementar o PROFMAT no Brasil, ao Departamento de Matemática da UNESP de Rio Claro pela apoio acadêmico e à Capes pelo apoio financeiro.

*Se você for curioso, encontrará quebra-cabeças em torno de você. Se você estiver determinado, irá resolvê-los.*

Ernö Rubik

# Resumo

O cubo mágico é um dos quebra-cabeças mais famosos do mundo, e em geral atrai a atenção de muita gente, em especial a dos matemáticos. O desafio, as formas, simetrias e movimentos induzem a ideia de estarmos diante de um objeto matemático. E podemos ir além. As ações e movimentos no cubo mágico são elementos que atendem a todas as condições da estrutura de um grupo, assim como também se relacionam com um grupo de permutações. À luz da Teoria de Grupos e dos Grupos de Permutações, iremos analisar algumas sequências de movimentos como os comutadores e conjugados. Existem vários algoritmos que resolvem o cubo mágico e que são fáceis de serem obtidos, por exemplo, na internet. O objetivo desta dissertação, além de trazer uma proposta de resolução, é o de proporcionar um caminho para além da simples memorização de um algoritmo, no sentido de compreendê-lo. Consequentemente, a justificativa para a possibilidade de se resolver um cubo mágico é de ordem matemática e não empírica.

**Palavras-chave:** Cubo de Rubik, Teoria de grupos, Grupos de permutação, Comutadores e conjugados, Proposta didática.

# Abstract

The Rubik's Cube is one of the most famous puzzle of the world, and generally attracts the attention of many people, especially mathematicians. The challenge, shapes, symmetries and movements induce the idea of being in front of a mathematical object. And we can go further. The actions and movements in the magic cube are elements that meet all the conditions of the structure of a group, as well as relate to a group of permutations. In light of the Group Theory and Permutations groups we will examine some sequences of movements such as commutators and conjugates. There are several algorithms that solve the magic cube and which are easy to obtain, for example, at the Internet. The aim of this dissertation, beyond to show a resolution, is to provide a path beyond simple memorization of an algorithm in order to understand it. Consequently, the justification for the possibility of solving a Rubik's Cube is math and not empirical.

**Keywords:** Rubik's cube, Group theory, Permutation group, Commutators and conjugates, Didatic proposal.

# Lista de Figuras

# Lista de Tabelas

# Sumário

# 1 Introdução

Durante décadas o desafio da resolução do cubo mágico, também chamado de cubo de Rubik, em homenagem ao seu inventor, intrigou muita gente. Ernö Rubik nasceu em 13 de julho de 1944 em Budapeste, Hungria e na década de 70 dava aulas de arquitetura na School for Commercial Artists. Em 1974 teve a ideia de construir um cubo capaz de rotacionar suas faces para que então pudesse ilustrar melhor para seus alunos o conceito tridimensional. O primeiro exemplar era de madeira e cada uma das seis faces do cubo era pintada de uma cor diferente. Cada face é dividida em 9 cubinhos menores totalizando 26 cubos visíveis e um virtual que se existisse estaria localizado no interior do cubo. Este 27º cubinho virtual é justamente o mecanismo que prende as 6 faces. No mesmo ano da criação, o cubo de Rubik ganhou o prêmio alemão de jogo do ano. Ernö Rubik não tinha exatamente a intenção de criar um quebra–cabeça cuja solução consiste em deixar cada uma das faces somente com uma cor. O próprio criador do cubo demorou cerca de um mês para remontá-lo à sua configuração inicial. Em 1980 o cubo começou a ser produzido de forma industrial e estima–se que desde então já tenham sido vendidos mais de 350 milhões de unidades em todo o mundo.

Inicialmente, no Capítulo 2, iremos trazer noções sobre seu mecanismo de funcionamento e quais movimentos são permitidos efetuar. Esta primeira apresentação é necessária para entendermos o que é e como funciona um cubo mágico. E, além disso, os movimentos das faces, bem como dos cubinhos, são o objetivo alvo deste trabalho, pois são estes os elementos que iremos estudar mais adiante.

No Capítulo 3 iremos abordar alguns conceitos básicos sobre a Teoria de Grupos e Grupos de Permutações. A partir deles identificaremos o cubo mágico como um objeto matemático, assim como as ações e os movimentos no cubo serão identificados como operações que atendem às definições que serão vistas.

No Capítulo 4 iremos aplicar os conceitos abordados, no intuito de entendermos alguns movimentos, estados e algoritmos que resolvem o cubo mágico. Além disso, calcularemos o número total de configurações que o cubo mágico pode assumir, juntamente com a justificativa de que algumas configurações são impossíveis de serem atingidas.

Finalmente, nos dois últimos capítulos poderemos nos aprofundar nos algoritmos de resolução. No Capítulo 5 iremos apresentar e detalhar três formas diferentes de resolução: com menos movimentos, em menor tempo e com menor memorização. Neste último iremos apresentar um método de resolução baseado nos conceitos que foram abordados nos capítulos anteriores. Tal método exige um certo conhecimento e familiaridade com o cubo mágico. Já no Capítulo 6 mostraremos outro método que é recomendado a iniciantes. Por este motivo, nos basearemos neste método para sugerir uma proposta didática. Neste capítulo será detalhado todas os estados e sequências necessários à resolução do cubo mágico, sem nos preocuparmos com qualquer demonstração, e sim apenas como um método memorizável.

# 2 O Cubo Mágico

O entendimento e familiaridade com o cubo mágico dependem de conhecermos certos conceitos que o cercam, como sua estrutura, código dos elementos (cubinhos, faces e movimentos) e até mesmo sua manipulação. Veremos que o modo como o seguramos é crucial para chegarmos à sua resolução. Ao longo deste capítulo faremos a descrição de todos os conceitos necessários para iniciarmos nosso estudo sobre o cubo de Rubik.

## 2.1 Elementos de um cubo mágico e seu mecanismo

Primeiramente vamos descrever e classificar todos os 26 cubinhos que compõem o cubo mágico. Nem todas as faces dos cubinhos são visíveis, dependendo de sua posição no cubo eles apresentam 1, 2 ou 3 faces visíveis. Podemos quantificar e classificar os cubinhos de 3 maneiras:

- 6 cubinhos chamados de centrais por estarem no centro das faces do cubo, onde só uma face é visível;
- 12 cubinhos chamados de aresta, ou de meio, e que compõem a aresta do cubo, onde duas faces são visíveis;
- 8 cubinhos chamados de canto, ou de quina, e que são os vértices do cubo, onde três de suas faces são visíveis.

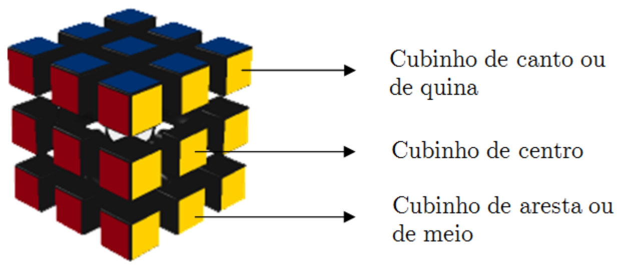


Figura 2.1: Visão explodida de um cubo mágico $3 \times 3 \times 3$.

A figura 2.1 mostra um cubo mágico $3 \times 3 \times 3$ de modo a visualizarmos sua montagem.

Os cubinhos centrais são os que determinam qual será a cor da face do cubo e o único movimento que eles realizam é o de rotação em torno do eixo que os prende ao mecanismo central. Dizemos que estes cubinhos são fixos. A Figura 2.2 ilustra o mecanismo interno onde podemos observar que o cubinho central é fixo e seu único movimento permitido é o de rotação em torno do eixo que o prende.

Figura 2.2: Mecanismo interno de um cubo mágico $3 \times 3 \times 3$.

## 2.2 Formatos e variações do cubo de Rubik

Existem dezenas de tipos, formatos e tamanhos de cubo mágico. O próprio Rubik quando idealizou o cubo pensou em um cubo $2 \times 2 \times 2$, entretanto a ideia de construir a configuração, que se tornou a mais famosa, surgiu do fato de que ele queria manter os centros fixos. O conceito do quebra cabeça se expandiu e muitos deixaram de ter o formato cúbico, sendo utilizadas outras formas geométricas como um tetraedro ou então um dodecaedro. Existem também aqueles com formas irregulares. A Figura 2.3 traz, dentre as dezenas, 60 tipos e formatos derivados do cubo de Rubik.

O formato mais comum é o cubo $3 \times 3 \times 3$ de 5,7 cm de aresta e de faces pintadas nas cores branca, amarela, azul, verde, vermelho e laranja. A Figura 2.4 ilustra esta configuração.

A compreensão dos movimentos e até da solução do cubo mágico dependem do modo como realizamos as rotações das faces. Mas para isso precisamos estabelecer uma referência que geralmente é a face que fica voltada para frente de quem manipula o cubo. O nome das faces é dado em função de sua posição quando olhamos para o cubo de frente. O padrão mais comum é baseado nos termos em inglês, de forma abreviada, estabelecendo um código. A Tabela 2.1 mostra o nome das faces, em ambos os idiomas e com seus respectivos códigos.

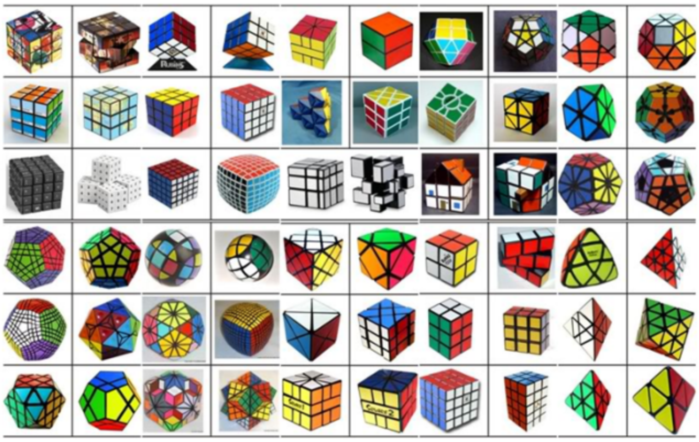

Figura 2.3: Tipos e formatos derivados do cubo de Rubik.

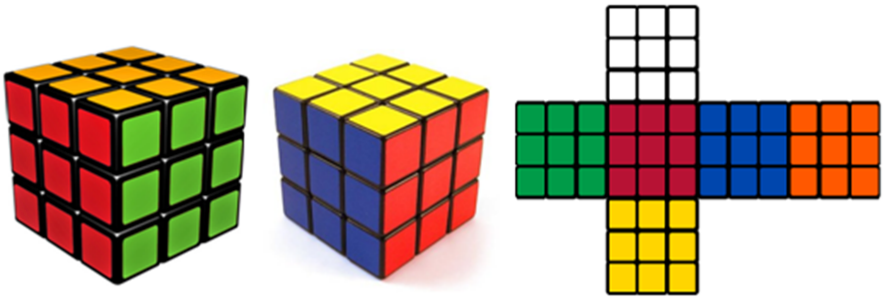

Figura 2.4: Faces do cubo $3 \times 3 \times 3$ e sua planificação.

Tabela 2.1: Nomes e códigos das faces

| Português | Inglês | Código |
|---|---|---|
| Frente | Front | $F$ |
| Trás | Back | $B$ |
| Direita | Right | $R$ |
| Esquerda | Left | $L$ |
| Cima | Up | $U$ |
| Baixo | Down | $D$ |

Para facilitar a visualização dos movimentos dos cubinhos vamos estabelecer uma nomenclatura para cada um deles utilizando a mesma referência citada na seção anterior, isto é, a face da frente. A nomenclatura é baseada na intersecção das faces em que o cubinho se encontra. Por exemplo, o cubinho de aresta que estiver na interseção da face da frente ($F$) com a face de cima ($U$) será chamado de $FU$ e o cubinho de canto que estiver na intersecção da face de trás ($B$), com a face da direita ($R$) e com a face de cima ($U$) será chamado de $BRU$. A figura abaixo ilustra a nomenclatura de todos os cubinhos do cubo mágico.

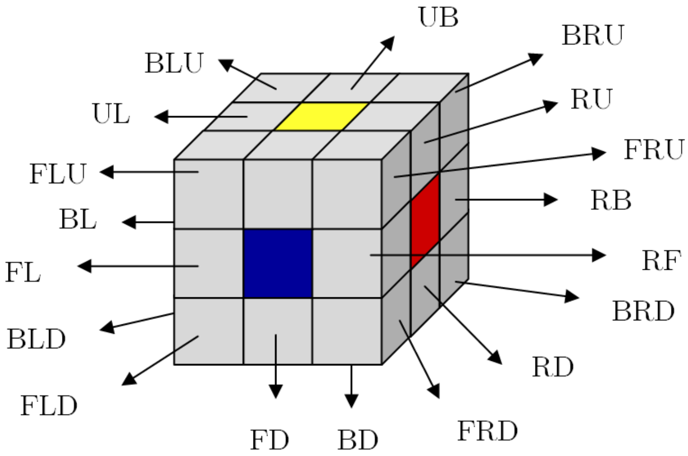


Figura 2.5: Nomenclatura dos cubinhos.

**Observação 2.1.** Não há distinção entre as ordens com que a notação é escrita, ou seja, $FRD = FDR = RFD = RDF = FRD = FDR$.

## 2.3 Movimentos das faces

O mecanismo interno permite que cada face tenha a liberdade de rotação de 0° a 360° em torno do eixo que fixa o cubinho central ao mecanismo interno, tanto no sentido horário quanto anti-horário tomando como referência sempre a face que fica à frente de quem manipula o cubo.

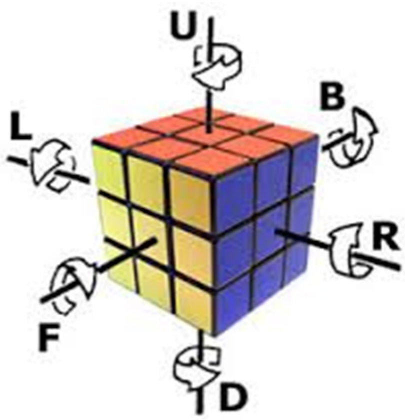


Figura 2.6: Eixos de rotação.

O movimento será completo (vide Figura 2.6) quando a face for rotacionada de 90°, em qualquer um dos dois sentidos. É fácil observar que se aplicarmos, em uma determinada face, quatro vezes repetida o movimento completo o cubo não é alterado, ou seja, é uma operação neutra.

Nos métodos mais tradicionais de resolução do cubo utilizam-se códigos para identificar cada movimento de rotação das faces. Estes códigos seguem a mesma lógica da nomenclatura das faces, isto é, a primeira letra maiúscula do nome do lado, em inglês. Para distinguir a rotação no sentido horário ou anti-horário, geralmente são utilizados dois símbolos: uma apóstrofe sobrescrita na letra ou a letra seguida de um $i$ minúsculo. Por exemplo, se quisermos realizar um movimento da face direita uma vez no sentido anti-horário escrevemos[1] $R'$ ou $Ri$.

Cada cubinho do cubo mágico possui uma posição e uma orientação.

- Definimos como posição, o local correto em que o cubinho deve se encontrar em relação aos cubinhos de centro.
- Definimos como orientação a configuração correta que as cores de um determinado cubinho deve se encontrar em relação aos cubinhos de centro.

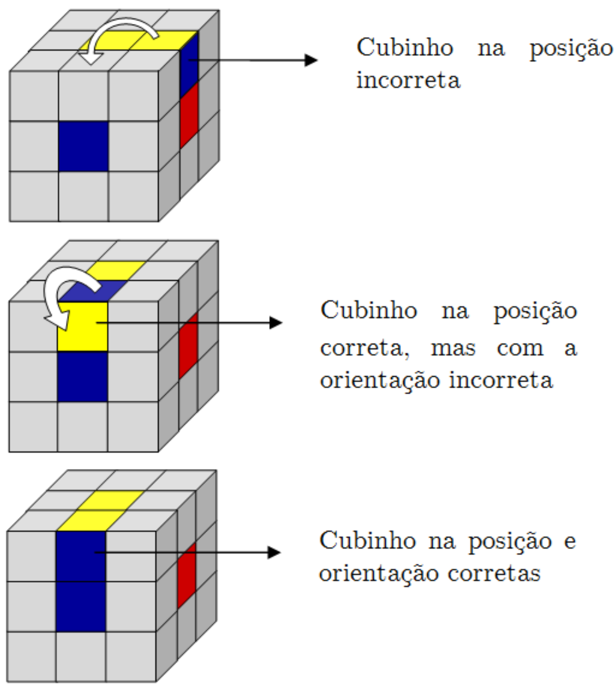


Figura 2.7: Exemplos de posição e orientação.

Um cubinho de aresta pode estar na sua posição correta, porém com sua orientação invertida. O mesmo pode ocorrer com um cubinho de quina. Note por estas duas

[1] O código mais comum utilizado é a letra com a apóstrofe sobrescrita.

razões um cubinho de aresta possui 12 posições diferentes para assumir, 1 correta e 11 erradas, assim como suas cores podem assumir 2 orientações diferentes, 1 correta e 1 errada. Analogamente um cubinho de quina possui 8 posições diferentes para assumir, 1 correta e 7 erradas, assim como suas cores podem assumir 3 orientações diferentes, 1 correta e 2 erradas. Vejamos alguns exemplos tanto de posição e orientação corretos e incorretos na figura 2.7.

## 2.4 Macro ou sequências de movimentos

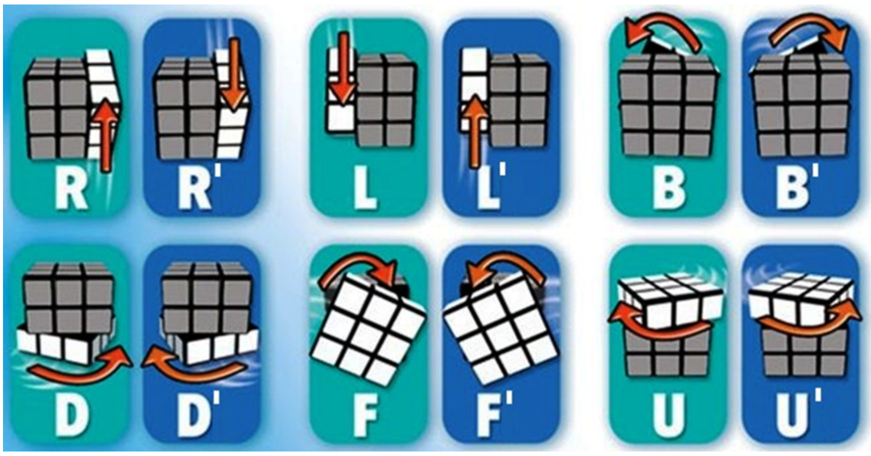


Figura 2.8: Códigos das rotações das faces.

Uma sequência de movimentos é descrita pela sequência de códigos das rotações que se deseja efetuar, escrita da esquerda para a direita na mesma ordem em que as operações devem ser realizadas e tomando como referência a face que está à frente de quem o manuseia. A esta sequência daremos o nome de macro. Quando uma sequência ou uma macro for aplicada no cubo uma importante regra deve ser seguida: uma vez iniciada a sequência a face frontal de referência não pode ser alterada até que ela seja concluída. Qualquer rotação do próprio cubo em qualquer direção e sentido irá interferir na sequência. Por esta razão, quando uma sequência de movimentos é efetuada, as únicas rotações que devem ser aplicadas serão somente nas faces respectivas ao código. A Figura 2.8 ilustra os códigos mais utilizados nos algoritmos de solução do cubo.

Agora vamos supor que queremos efetuar quatro movimentos seguidos na seguinte ordem: uma rotação da face superior no sentido horário, uma rotação da face direita no sentido horário, uma rotação da face superior no sentido anti-horário e uma rotação da face direita no sentido anti-horário. O código para esta macro S será:

$$S = URU'R'.$$

Caso se queira aplicar um mesmo movimento $X$ mais de uma vez, utiliza-se a seguinte notação: $S = XX = X^2$, $T = XXX = X^3$, etc. Por exemplo, para se efetuar duas rotações consecutivas da face superior no sentido horário escreve-se: $S = U^2$.

Como é possível perceber, a codificação dos movimentos é essencial, a fim de tornar tanto a leitura quanto a própria execução das macros mais simples e ágil[2]. No Capítulo 5 voltaremos a tratar dos códigos e sequências que compõem os algoritmos que levam à solução do cubo.

[2]A criação de códigos na Matemática é algo crucial para o seu próprio desenvolvimento e entendimento, e no cubo a ideia não é diferente.

# 3 Álgebra no Cubo Mágico

Neste capítulo vamos abordar conceitos básicos de Álgebra, que podem ser encontrados nas referências [1], [2], [3] e [4] como, por exemplo, a teoria de grupos e grupos de permutação, com o objetivo de relacionar movimentos específicos do cubo mágico com tais conceitos. A ideia é utilizar estas duas teorias para auxiliar a obtenção de macros que possibilitem, uma vez que o cubo esteja embaralhado, retorná–lo à posição original, isto é, as 6 faces estarem todas com suas respectivas cores.

## 3.1 Teoria Básica de Grupos

**Definição 3.1.** *Um conjunto $G$ não vazio, com uma determinada operação $(*)$ tal que*

$$G \times G \to G$$

$$(a, b) \mapsto a * b$$

*será chamado de grupo e denotamos por $(G, *)$ se as três seguintes condições para tal operação forem satisfeitas:*

1. *Associatividade:*
$$a * (b * c) = (a * b) * c, \quad \forall a, b, c \in G.$$

2. *Elemento neutro:*
$$\exists\, e \in G \text{ tal que } e * a = a * e = a, \quad \forall a \in G.$$

3. *Elemento simétrico:*
$$\forall a \in G,\ \exists\, a' \in G \text{ tal que } a * a' = a' * a = e.$$

Um grupo é chamado de *abeliano* ou *comutativo* se apresenta também a seguinte condição:

4. *Comutatividade:*
$$a * b = b * a, \quad \forall a, b \in G.$$

**Exemplo 3.1.** Grupos:

1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ são grupos aditivos e $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$ e $(\mathbb{C}\setminus\{0\},\cdot)$ são grupos multiplicativos. Note que todos eles são grupos abelianos, pois em todos eles a propriedade comutativa é válida.

2. Para aplicar propriedades da Álgebra no cubo mágico, vejamos um exemplo geométrico, onde escreveremos o grupo $G_Q$ referente às simetrias espaciais de um quadrado.
   Seja $Q_1Q_2Q_3Q_4$ um quadrado cujo centro está na origem $O$ dos eixos cartesianos. Chamaremos as retas que passam pelas diagonais do quadrado e por suas mediatrizes de $d_1$, $d_2$, $r$ e $s$, respectivamente, conforme a Figura 3.1.

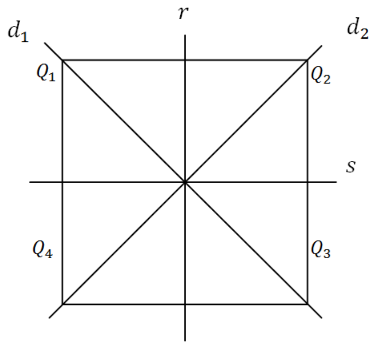


Figura 3.1: Quadrado representativo do grupo $G_Q$.

As transformações espaciais (simetrias) que preservam a forma do quadrado podem ocorrer tanto no plano quanto no espaço:

- Transformações planas:
  Denotaremos por $id$, $R_{\frac{\pi}{2}}$, $R_\pi$ e $R_{\frac{3\pi}{2}}$ as rotações em torno da origem $O$ do quadrado, de ângulos 0, $\frac{\pi}{2}$, $\pi$ e $\frac{3\pi}{2}$, no sentido anti–horário, respectivamente.

- Transformações espaciais:
  Denotaremos por $R_1$, $R_2$, $R_r$ e $R_s$ as rotações de ângulo $\pi$ em relação aos eixos $d_1$, $d_2$, $r$ e $s$, respectivamente.

Assim $G_Q = \left\{id, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}, R_1, R_2, R_r, R_s\right\}$ e com a operação de composição de funções é um grupo.

Note que o grupo $G_Q$ não é abeliano, pois a propriedade comutativa não é verificada. De fato, vamos verificar que as composições $R_r \circ R_1$ e $R_1 \circ R_r$ não são iguais.

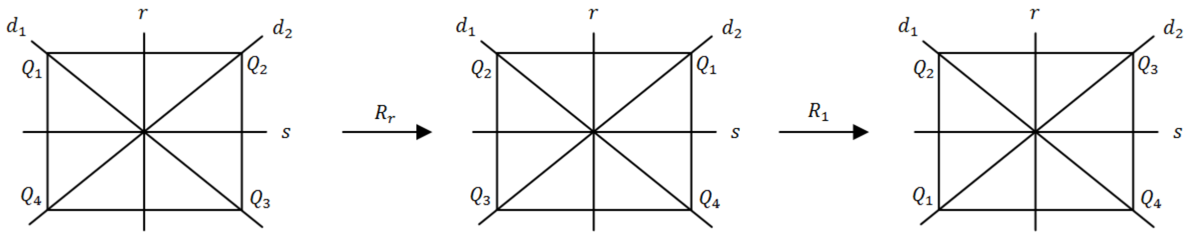


Figura 3.2: Composição $R_r \circ R_1$.

Logo $R_r \circ R_1 = R_{\frac{\pi}{2}}$.

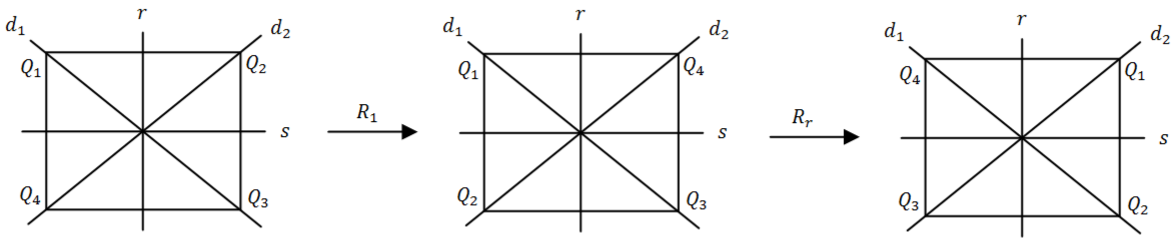


Figura 3.3: Composição $R_1 \circ R_r$.

Logo $R_1 \circ R_r = R_{\frac{3\pi}{2}}$.

Veremos mais adiante que o Grupo de Rubik não é abeliano. Em particular este é um dos motivos pelo qual o Cubo de Rubik apresenta alto nível de dificuldade em ser resolvido.

## 3.2 Grupos aditivos e multiplicativos de classes de restos

O conjunto das classes de resto módulo $m$, é o conjunto quociente de $\mathbb{Z}$ pela relação de congruência, módulo $m$. Isto é

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}, \forall m > 1; m \in \mathbb{Z}.$$

Sendo assim $\overline{0}$ é formado por todos os inteiros côngruos a 0, módulo $m$, $\overline{1}$ por todos os inteiros côngruos a 1, módulo $m$, e assim sucessivamente.

Agora seja a operação $(+)$ de adição módulo $m$ sobre $\mathbb{Z}_m$, a qual vale a associatividade e a comutatividade e que é definida definida por

$$\overline{a} + \overline{b} = \overline{a+b}, \text{ onde } \overline{a}, \overline{b} \in \mathbb{Z}_m.$$

Em relação à esta operação existe um elemento neutro e um oposto:

$$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}.$$

Portanto, $\overline{0}$ é o elemento neutro.

$$\overline{a} + \overline{m - a} = \overline{a + (m - a)} = \overline{m} = \overline{0}, \text{ já que } m \equiv 0 \pmod{m}$$

Portanto, $-\overline{a} = \overline{m - a}$ é o elemento oposto.

Assim, $(\mathbb{Z}_m, +)$ é um grupo abeliano, para todo inteiro $m > 1$, que é chamado de *grupo aditivo de classes de resto módulo m*. Note que a ordem deste grupo é $m$.

Agora seja também a operação $(\cdot)$ de multiplicação módulo $m$ em $\mathbb{Z}_m$ onde também são válidas a associatividade e a comutatividade e que é definida por:

$$\overline{a} \cdot \overline{b} = \overline{ab}, \text{ onde } \overline{a}, \overline{b} \in \mathbb{Z}_m.$$

Em relação à esta operação existe um elemento neutro:

$$\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}.$$

Portanto $\overline{1}$ é o elemento neutro.

Agora é preciso notar que o elemento $\overline{0}$ não está definido no conjunto $\mathbb{Z}_m$ com a operação $(\cdot)$, pois ele não apresenta um inverso na multiplicação módulo $m$, logo devemos considerar apenas o conjunto $\mathbb{Z}_m - \{\overline{0}\}$. Entretanto, mesmo observada esta restrição, não há garantias de que o conjunto restante será um grupo multiplicativo. Com efeito, temos que a restrição para a multiplicação módulo 4 aos elementos de $\mathbb{Z}_4 - \{\overline{0}\}$, nem sequer é uma operação sobre este conjunto, uma vez que $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$.
Neste sentido, provaremos que a multiplicação módulo $m$ aplicada aos elementos de $\mathbb{Z}_m^* = \mathbb{Z}_m - \{\overline{0}\}$ é uma operação sobre este conjunto se, e somente se, $m$ é um número primo.

Primeiramente vamos supor, por absurdo, que $m$ não é primo. Como $m > 1$, podemos obter dois inteiros $a, b > 1$ tais que $ab = m$. Logo $\overline{ab} = \overline{m}$. E neste caso, como $\overline{ab} = \overline{a} \cdot \overline{b}$ e $\overline{m} = \overline{0}$, então teríamos que $\overline{a} \cdot \overline{b} = \overline{0}$, o que é absurdo pela hipótese.

Por outro lado, vamos supor, por absurdo, que $\overline{ab} = \overline{0}$ para algum $\overline{a}, \overline{b} \in \mathbb{Z}_m^*$. Consequentemente temos que $ab \equiv 0 \pmod{m}$. Logo, $m \mid ab$, e como por hipótese $m$ é primo, então $m \mid a$ ou $m \mid b$. Sem perda de generalidade vamos supor o primeiro caso, o que implica que $a = mq$, para algum inteiro $q$, e portanto temos:

$$\overline{a} = \overline{mq} = \overline{m} \cdot \overline{q} = \overline{0} \cdot \overline{q} = \overline{0}$$

o que é absurdo, já que por hipótese $\overline{a} \in \mathbb{Z}_m^*$.

Por fim, vamos mostrar que, se $m$ é primo, a multiplicação módulo $m$, quando restrita aos elementos de $\mathbb{Z}_m^*$, faz desse conjunto um grupo. Para isto, basta mostrar que $\forall\ \overline{a} \in \mathbb{Z}_m^*$, pode-se encontrar $\overline{b} \in \mathbb{Z}_m^*$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Com efeito, se $\overline{a} \in \mathbb{Z}_m^*$, então $a$ não é múltiplo de $m$, e como $m$ é primo, então $mdc(m, a) = 1$. Logo, podemos escrever $mx_0 + ay_0 = 1$, para convenientes inteiros $x_0$ e $y_0$ (identidade de Bezout). Reduzindo-se essa igualdade módulo $m$ temos:

$$\overline{mx_0 + ay_0 = 1} = \overline{m} \cdot \overline{x_0} + \overline{a} \cdot \overline{y_0} = \overline{a} \cdot \overline{y_0} = \overline{1}$$

onde obtemos que $\overline{y_0}$, que pertence a $\mathbb{Z}_m^*$, é o inverso de $\overline{a}$.

Assim, $(\mathbb{Z}_m^*, \cdot)$ é um grupo, se e somente se, $m$ é um número primo. Vejamos um exemplo:

**Exemplo 3.2.** Usando o raciocínio utilizado na demosntração acima, vamos determinar o inverso de $\overline{4}$ em $\mathbb{Z}_5^*$. Logo, uma possível solução para a equação Diofantina $5x_0 + 4y_0 = 1$ pode ser o par $(x_0, y_0) = (1, -1)$, ou seja, $y_0 = -1$. Portanto o inverso de $\overline{4}$ é $\overline{-1} = \overline{4}$, pois $4 \equiv -1 \pmod 5$.

## 3.3 Classes Laterais

Seja $G$ um grupo e seja $H$ um subgrupo de $G$. À respeito de $G$, definimos a relação de equivalência $\underset{E}{\sim}$ da seguinte maneira:

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

Por definição, a classe de equivalência que contém o elemento $x$ é o conjunto $\left\{y \in g \mid y \underset{E}{\sim} x\right\} = \{xh \mid h \in H\}$; denotaremos este conjunto por $xH$ e o chamaremos de *classe lateral à esquerda* de $H$ em $G$ que contém $x$. Caso não haja confusão, simplesmente a chamaremos de classe lateral de $x$ à esquerda. Em particular, $H$ é a classe lateral do elemento neutro $e$ à esquerda. Observe que $y \in xH \Leftrightarrow yH = xH$.
De maneira análoga, podemos ainda definir a seguinte relação de equivalência:

$$y \underset{D}{\sim} x \Leftrightarrow \exists h \in H \text{ tal que } y = hx.$$

Desta forma obtemos as *classes laterais à direita* de $H$ em $G$. Portanto a classe lateral de $x$ à direita é $Hx = \{hx \mid h \in H\}$.

**Definição 3.2.** *A cardinalidade do conjunto das classes laterais à esquerda é o índíce de $H$ em $G$. Denotaremos ele por $(G : H)$.*

**Observação 3.1.** O índice de $H$ em $G$ também é a cardinalidade do conjunto das classes laterais à direita de $H$ em $G$, pois a aplicação $\varphi$ abaixo é uma bijeção:

$$\varphi : \{\text{classes laterais à esquerda}\} \to \{\text{classes laterais à direita}\}$$
$$xH \to Hx^{-1}$$

**Definição 3.3.** *Dada uma partição de um conjunto, um sistema de representantes é um conjunto $\{x_\alpha\}_{\alpha\in\Gamma}$ que tem exatamente um elemento em cada subconjunto da partição. Em particular, a cardinalidade de qualquer sistema de presentantes das classes laterais à esquerda de $H$ em $G$ é igual a $(G : H)$.*

**Proposição 3.1.** *Todas as classes laterais de $H$ em $G$ têm a mesma cardinalidade, igual à cardinalidade de $H$.*

*Demonstração.* A função

$$H \to xH$$
$$h \mapsto xh$$

é claramente uma bijeção. □

**Teorema 3.1.** *(Teorema de Lagrange) Sejam $G$ um grupo finito e $H$ um subgrupo de $G$. Então teremos $|G| = |H|(G : H)$. Em particular, a ordem e o índice de $H$ dividem a ordem de $G$.*

*Demonstração.* Vamos considerar a relação de equivalência à esquerda $\underset{E}{\sim}$ em $G$. Desta forma iremos obter uma partição de $G$ em classes de equivalência. A proposição anterior mostra que em cada uma dessas classes temos $|H|$ elementos. Como, por definição, o número de classes é $(G : H)$, temos a igualdade $|G| = |H|(G : H)$ □

**Corolário 3.1.** *Seja $G$ um grupo finito e seja $\alpha \in G$. Então a ordem de $\alpha$ divide a ordem de $G$.*

*Demonstração.* Por definição, $\mathcal{O}(\alpha) = |\langle\alpha\rangle|$. Por fim aplicamos o Teorema de Lagrange ao subgrupo $\langle\alpha\rangle$. Note que, equivalentemente, este corolário mostra que $\alpha^{|G|} = e$ □

**Corolário 3.2.** *Seja $G$ um grupo de ordem prima. Então $G$ é cíclico.*

*Demonstração.* Seja $\alpha \in G \setminus \{e\}$ e considere $\langle\alpha\rangle$ o subgrupo gerado por $\alpha$. Pelo Teorema de Lagrange, $|\langle\alpha\rangle|$ divide $|G|$ e portanto $|\langle\alpha\rangle| = |G|$, pois $|G|$ é primo. Logo $G = \langle G\rangle$. □

## 3.4 Grupo de Rubik

Conforme visto no Capítulo 2, chamamos de $R$, $L$, $F$, $B$, $U$ e $D$, os movimentos no sentido horário das faces direita, esquerda, frente, trás, cima e baixo, respectivamente. O conjunto de todos os movimentos permitidos no cubo, por exemplo, ao embaralhá-lo, chamaremos de Grupo $\mathcal{R}$ de Rubik. Vamos verificar a existência das três condições que satisfazem a definição de grupo para o cubo de Rubik:

1. Associatividade:
   Ao realizarmos uma sequência qualquer, por exemplo, de 3 movimentos genéricos $X$, $Y$, $Z$, verificamos que: $X(YZ) = (XY)Z$.
   Ao manipular o cubo a prova desta condição é evidente e a consideraremos como trivial.

2. Elemento neutro:
   A existência do elemento neutro é verificada pelo movimento "não fazer nada" em qualquer das 6 faces. Com isso garantimos a identidade $I$ de qualquer uma das seis faces do cubo ou de qualquer sequência de movimentos.

3. Elemento inverso:
   O elemento inverso no Grupo $\mathcal{R}$ de Rubik significa desfazer a sequência, de um ou mais movimentos, realizada. E aqui há duas importantes considerações a serem feitas: se o movimento foi de apenas uma face ou de uma macro. Seja um movimento genérico $X$, uma rotação de uma das 6 faces de 90° no sentido horário, então seu elemento inverso será o movimento, também de 90°, desta mesma face, porém no sentido anti-horário. Denotaremos este elemento inverso de $X$ como sendo $X^{-1}$ ou simplesmente $X'$. Caso seja feito uma sequência de movimentos, então o elemento inverso será a realização dos inversos dos movimentos, porém na ordem inversa, como no exemplo a seguir.

**Exemplo 3.3.** Seja uma macro $S = FR'U$, então seu inverso será $S^{-1} = U'RF'$.

**Observação 3.2.** O elemento inverso em um grupo é único, por isso que no caso do cubo mágico é necessário que ele esteja bem definido para que se evite duplicidade quando se deseja obter o elemento inverso de um movimento ou o de uma combinação de movimentos. Por este motivo, devemos ter claro que realizar apenas um movimento é um caso particular de se realizar uma sequência de movimentos, e com isso garantimos a unicidade do elemento neutro dentro do Grupo $\mathcal{R}$ de Rubik.

Apesar de valer a propriedade comutativa entre movimentos em faces opostas, a mesma não é verificada entre movimentos em faces adjacentes. Os movimentos $FR$ e $RF$ não são iguais, conforme a Figura 3.4.

Alguns exemplos de movimentos comutativos são:

$$FB = BF, RL = LR \text{ e } UD = DU$$

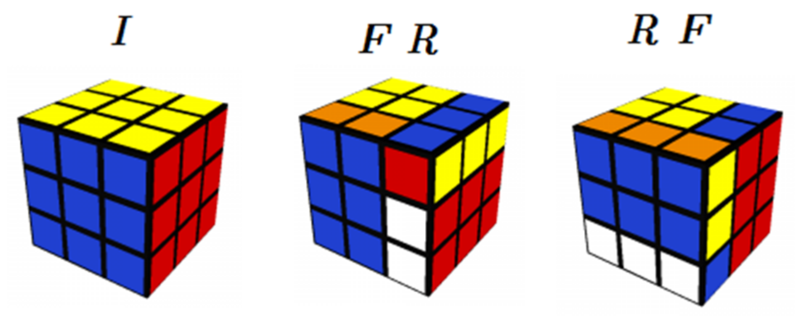


Figura 3.4: Macros $FR$ e $RF$.

Portanto, concluímos que o Grupo $\mathcal{R}$ de Rubik não é abeliano. Este fato torna o cubo, em particular, um quebra-cabeças difícil de ser resolvido.

## 3.5 Subgrupos

**Definição 3.4.** *Seja $(G, *)$ um grupo, chamaremos de subgrupo de $G$, um subconjunto $H$ de $G$ não vazio (denotaremos por $H < G$) quando com a operação de $G$, este subconjunto $H$ é um grupo com as seguintes condições satisfeitas para cada elemento $h$ de $H$:*

1. *Fechamento:*
$$h_1 * h_2 \in H, \quad \forall h_1, h_2 \in H.$$

2. *Associatividade:*
$$h_1 * (h_2 * h_3) = (h_1 * h_2) * h_3, \quad \forall h_1, h_2, h_3 \in H.$$

3. *Elemento neutro:*
$$\exists e_h \in H \text{ tal que } e_h * h = h * e_h = h, \quad \forall h \in H.$$

4. *Elemento simétrico:*
$$\forall h \in H, \quad \exists h' \in H \text{ tal que } h * h' = h' * h = e_h.$$

**Observação 3.3.** A condição 2 é sempre satisfeita, pois a igualdade $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$, é válida para todos os elementos de $G$.

**Observação 3.4.** O elemento neutro $e_h$ de $H$ é necessariamente igual ao elemento neutro $e$ de $G$. De fato, sejam $e$ e $e_h$, respectivamente os elementos neutros de $G$ e $H$. Como

$$e_h * e_h = e_h = e_h * e$$

e para todo elemento do grupo é válido em relação à operação $*$, então $e = e_h$.

**Observação 3.5.** Dado $h \in H$, o inverso de $h$ em $H$ é necessariamente igual ao inverso de $h$ em $G$. De fato, seja um elemento $b \in H$ e indiquemos por $b^{`}$ e $b^{`}_h$ seus simétricos em $G$ e $H$, respectivamente. Como, porém,

$$b^{`}_h * b = e_h = e = b^{`} * b$$

então $b^{`}_h = b^{`}$.

Na prática, para verificar que um subconjunto $H$ é um subgrupo de um grupo $G$, basta usarmos a seguinte proposição:

**Proposição 3.2.** *Seja $(G, *)$ um grupo. Para que um conjunto, não vazio, $H \subset G$ seja um subgrupo de $G$, é necessário e suficiente que $a * b^{`}$ seja um elemento de $H$ sempre que $a$ e $b$ pertencerem a este conjunto.*

*Demonstração.* ($\Rightarrow$) Se $a, b \in H$, então $a * b^{`}_h \in H$ já que, por hipótese, $(H, *)$ é um grupo. Mas pela observação 3.4 temos que $b^{`}_h = b^{`}$ e, portanto, $a * b^{`} \in H$.

($\Leftarrow$) Como, por hipótese, H é não vazio, então é possível considerarmos um elemento qualquer $x_0 \in H$. Por este fato, e pela hipótese temos que $x_0 * x^{`}_0 = e \in H$. Considerando agora um elemento $b \in H$, da hipótese e da conclusão anterior segue que:

$$e * b^{`} = b^{`} \in H.$$

Agora vamos mostrar que $H$ é fechado em relação à operação $*$. Com efeito, se $a, b \in H$, então pela conclusão anterior, $a, b^{`} \in H$. De onde, usando novamente a hipótese, temos que:

$$a * (b^{`})^{`} = a * b \in H.$$

A associatividade em $H$ é imediata, pois se $a, b, c \in H$, então $a, b, c \in G$ e, portanto $a * (b * c) = (a * b) * c$ (uma vez que essa propriedade é válida em G).

□

Vejamos alguns exemplos:

**Exemplo 3.4.** Se $G$ é um grupo, então $\{e\}$ e $G$ são subgrupos de $G$, chamados de subgrupos triviais de $G$.

**Exemplo 3.5.** $(2\mathbb{Z},+)$ é um subgrupo de $(\mathbb{Z},+)$. De maneira mais geral, se $n$ é um inteiro qualquer, $(n\mathbb{Z},+)$ é um subgrupo de $(\mathbb{Z},+)$.

**Exemplo 3.6.** $\{id, R_\pi\}$ e $\left\{id, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}\right\}$ são subgrupos de $G_Q$.

### 3.5.1 Subgrupo gerado por um subconjunto

Usaremos aqui a notação multiplicativa, por ser mais simples e de uso mais frequente em Teoria dos Grupos.

Sejam $G$ um grupo e $S$ um subconjunto não vazio de $G$. Utilizaremos a seguinte notação:

$$< S >= \{a_1 \cdot a_2 \cdot ... \cdot a_n; n \in \mathbb{N}, a_i \in S \text{ } ou \text{ } a_i^{-1} \in S\}$$

Quando S é finito da forma $S = \{a_1, a_2, ..., a_m\}$ é comum denotarmos simplesmente por:

$$\langle S\rangle = \langle a_1 \cdot a_2 \cdot ... \cdot a_m\rangle \text{ no lugar de } \langle S\rangle = \langle\{a_1, a_2, ..., a_m\}\rangle$$

Note que se $g \in G$ então

$$\langle g\rangle = \{..., (g^{-1})^2, g^{-1}, e, g, g^2, ...\}$$

E ainda, se usarmos a notação $g^{-r}$ para $(g^{-1})^r, r \in \mathbb{N}$ teremos:

$$\langle g\rangle = \{g^t; t \in \mathbb{Z}\}$$

**Proposição 3.3.** *Seja $S$ um subconjunto do grupo $G$, então o conjunto $\langle S\rangle$ é um subgrupo de $G$.*

*Demonstração.* Sejam $x, y \in \langle S\rangle$ temos:

$$x = a_1 \cdot a_2 \cdot ... \cdot a_n \text{ com } a_i \in S \text{ ou } a_i^{-1} \in S$$

$$y = b_1 \cdot b_2 \cdot ... \cdot b_m \text{ com } b_i \in S \text{ ou } b_i^{-1} \in S$$

Logo, $x \cdot y = a_1 \cdot a_2 \cdot ... \cdot a_n \cdot b_1 \cdot b_2 \cdot ... \cdot b_m$ e $x^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdot ... \cdot a_2^{-1} \cdot a_1^{-1}$ também estão em $\langle S\rangle$. □

**Definição 3.5.** *Se $S$ é um subconjunto não vazio do grupo $G$, então $\langle S\rangle$ é chamado subgrupo gerado por $S$.*

*Em particular, para todo elemento $g$ do grupo $G$, o subgrupo gerado por $g$ é $\langle g\rangle = \{g^t; t \in \mathbb{Z}\}$.*

**Definição 3.6.** *Um grupo multiplicativo $G$ é dito cíclico quando ele pode ser gerado por um de seus elementos, isto é, quando $G = \langle g \rangle$, para algum $g \in G$.*

**Exemplo 3.7.** Os grupos $\mathbb{Z} = \langle 1 \rangle$ e $\mathbb{Z}_n = \langle \overline{1} \rangle$ são exemplos de grupos cíclicos.

**Definição 3.7.** *Seja $G$ um grupo. O subgrupo $\langle \{xyx^{-1}y^{-1} | x, y \in G\} \rangle$ chama-se subgrupo dos comutadores de $G$ e é denotado por $G^{‘}$.*

**Definição 3.8.** *Seja $G$ um grupo. O subgrupo $\{x \in G; xg = gx, \forall g \in G\}$ chama-se centro de $G$, e é denotado por $Z(G)$.*

**Definição 3.9.** *Seja $G$ um grupo e $x, y \in G$. Diremos que $x$ e $y$ são conjugados em $G$, se existe $g \in G$ tal que $y = gxg^{-1}$.*

No Capítulo 4 veremos a utilidade destas duas operações $XYX^{-1}Y^{-1}$ e $XYX^{-1}$ chamados de comutador e conjugados, respectivamente, para a resolução do cubo mágico.

**Definição 3.10.** *A ordem de um grupo $G$ é o número de elementos em $G$. Ela será denotada por $|G|$. Se $\alpha$ é um elemento do grupo $G$, a ordem de $\alpha$ é a ordem do subgrupo gerado por $\alpha$, e ela será denotada por $\mathcal{O}(\alpha)$.*

**Exemplo 3.8.** $|\mathbb{Z}| = \infty$ e $|\mathbb{Z}_n| = n$.

## 3.6 Subgrupos Normais e Grupos Quocientes

Seja $G$ um grupo e seja $H$ um subgrupo de $G$. Iremos agora observar se a operação de $G$ induz de maneira natural uma operação sobre o conjunto das classes laterais à esquerda de $H$ em $G$, isto é, se a operação

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

é bem definida, no sentido de não depender da escolha dos elementos $x$ e $y$. Se tomarmos $x, y \in G$ e $h, k \in H$ arbitrários, então $x$ e $xh$ são representantes da mesma classe $xH$ e, $y$ e $yk$ são representantes da mesma classe $yH$. Desta forma, a operação induzida sobre as classes laterais à esquerda é bem definida, se e somente se,

$$xyH = xhykH, \quad \forall x, y \in G, \quad \forall h, k \in H$$

logo,

$$y^{-1}x^{-1}xyH = y^{-1}x^{-1}xhyk,$$

ou seja,

$$H = y^{-1}hyH, \quad \forall y \in G, \quad \forall h \in H,$$

e portanto,

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

**Proposição 3.4.** *Seja $H$ um subgrupo de um grupo $G$. As afirmações a seguir são equivalentes:*

1. *A operação induzida sobre as classes laterais à esquerda de $H$ em $G$ é bem definida.*
2. $gHg^{-1} \subseteq H, \quad \forall g \in G.$
3. $gHg^{-1} = H, \quad \forall g \in G.$
4. $gH = Hg, \quad \forall g \in G.$

*Demonstração.* $1 \Leftrightarrow 2$ já foi feito.
$3 \Leftrightarrow 4$ é óbvio.
$3 \Rightarrow 2$ é óbvio.
$2 \Rightarrow 3$ Suponhamos que $gHg^{-1} \subseteq H$, $\forall g \in G$; precisamos provar que $H \subseteq gHg^{-1}$, $\forall g \in G$. Sejam então $h \in H$ e $g \in G$; temos

$$h = g(g^{-1}hg)g^{-1} \in g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}.$$

□

**Definição 3.11.** *Um subgrupo $H$ é um subgrupo normal de $G$, denotado por $H \triangleleft G$, se ele satisfaz qualquer uma das quatro afirmações anteriores. Neste caso, as classes laterais à esquerda de $H$ são iguais às classes laterais à direita de $H$; chamaremos simplesmente de classes laterais de $H$.*

**Exemplo 3.9.** $\{e\}, G$ são subgrupos normais de $G$.

**Exemplo 3.10.** $G' = \langle \{xyx^{-1}y^{-1} | x, y \in G\} \rangle$ é um subgrupo normal de $G$.

*Demonstração.* Primeiro, vamos observar que se chamamos de $S$ o conjunto $\{xyx^{-1}y^{-1} \mid x, y \in G\}$ e se $\alpha \in S$, então $\alpha^{-1} \in S$; consequentemente, se $\xi$ é um elemento qualquer de $G' = \langle S \rangle$, então $\xi$ se escreve da forma $\xi = \alpha_1 \dots \alpha_n$ com $\alpha_1, \dots, \alpha_n \in S$. Segundo, se $g \in G$, temos

$$g\xi g^{-1} = g(\alpha_1 \dots \alpha_n)g^{-1} = (g\alpha_1 g^{-1})(g\alpha_2 g^{-1}) \dots (g\alpha_n g^{-1})$$

e consequentemente, para ver que $g\xi g^{-1} \in G'$, basta ver que $g\alpha g^{-1} \in S$ quando $\alpha \in S$. Seja então $\alpha = xyx^{-1}y^{-1}$ um elemento de $S$; temos

$$\begin{aligned} g\alpha g^{-1} &= g(xyx^{-1}y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) \\ &= (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} \in S. \end{aligned}$$

□

**Teorema 3.2.** *Sejam $G$ um grupo e $H$ um subgrupo normal de $G$. Então o conjunto das classes laterais, com a operação induzida de $G$, é um grupo.*

Esta demonstração pode ser encontrada em [2]; O elemento neutro de $G/H$ é a classe lateral $H$;o elemento inverso da classe $gH$ é a classe $g^{-1}H$.

**Definição 3.12.** *Sejam $G$ um grupo e $H$ um subgrupo normal de $G$. O grupo de suas classes laterais com a operação induzida de $G$ é o grupo quociente de $G$ por $H$; ele será denotado por $G/H$ ou por $\frac{G}{H}$.*

**Subgrupos gerados pela união de dois subgrupos**

Sejam $H$ e $K$ dois subgrupos de um grupo $G$. Temos

$$\langle H \cup K \rangle \supseteq HK := \{hk \mid h \in H \text{ e } k \in K\} \supseteq H \cup K.$$

Portanto é claro que

$$\langle H \cup K \rangle = HK \Leftrightarrow HK \text{ é um subgrupo de } G$$

Vejamos agora as condições para que $HK$ seja um grupo.

**Proposição 3.5.** *Sejam $H, K$ dois subgrupos de $G$. Então:*

$$HK \textit{ é um subgrupo de } G \Leftrightarrow HK = KH.$$

*Demonstração.* ($\Rightarrow$) Seja $\alpha \in KH$. Então existem $k \in K$ e $h \in H$ tais que $\alpha = kh$. Temos $\alpha^{-1} = h^{-1}k^{-1} \in HK$. Como $HK$ é por hipótese um subgrupo de $G$ e $\alpha^{-1} \in HK$, então $\alpha \in HK$; assim provamos que $KH \subseteq HK$. Para provar a inclusão contrária, tome $\gamma \in HK$. Como $HK$ é um subgrupo, temos $\gamma^{-1} \in HK$; logo $\gamma^{-1} = h_2k_2$ com $h_2 \in H$, $k_2 \in K$. Tomando inversos, obtemos $\gamma = k_2^{-1}h_2^{-1} \in KH$. Portanto temos $HK = KH$.

($\Leftarrow$) Suponhamos que $HK = KH$. Para provarmos que $HK$ é subgrupo basta provarmos o seguinte:
1) $xy \in HK$, $\forall x, y \in HK$
2) $x^{-1} \in HK$, $\forall x \in HK$.

Sejam $x, y \in HK$; se escrevermos $x = h_1k_1$ e $y = h_2k_2$ com $h_1, h_2 \in H$, $k_1, k_2 \in K$ teremos

$$xy = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2.$$

Como $k_1h_2 \in KH$ e por hipótese $KH = HK$, existem $h_3 \in H$ e $k_3 \in K$ tais que $k_1h_2 = h_3k_3$; substituindo na expressão para $xy$, obteremos

$$xy = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2) \in HK$$

Agora, teremos também

$$x = h_1k_1 \Rightarrow x^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$$

□

**Corolário 3.3.** *Sejam $H$ e $K$ dois subgrupos de $G$. Se $H$ ou $K$ for normal em $G$, então $HK$ é um subgrupo de $G$.*

*Demonstração.* Faremos a prova no caso em que $H \triangleleft G$ e $K$ é um subgrupo qualquer; o outro caso é totalmente análogo. Vamos mostrar que $HK = KH$. Seja $\alpha = hk \in HK$. Temos $\alpha = hk = kk^{-1}hk = k\beta$ com $\beta := k^{-1}hk \in H$ pois $H \triangleleft G$; portanto $\alpha = k\beta \in KH$. Provamos então que $HK \subseteq KH$. Para provar a inclusão contrária, seja $\gamma = kh \in KH$. Temos $\gamma = kh = khk^{-1}k = \delta k$ com $\delta := khk^{-1} \in H$ pois $H \triangleleft G$; portanto $\gamma = \delta k \in HK$. □

## 3.7 Homomorfismos de Grupos

**Definição 3.13.** *Sejam $(G, \cdot)$ e $(\mathcal{G}, \times)$ dois grupos. Chamamos de homomorfismo uma função $f : G \to \mathcal{G}$, que seja compatível com as estruturas de ambos os grupos, ou seja, se*

$$f(a \cdot b) = f(a) \times f(b), \quad \forall a, b \in G.$$

**Exemplo 3.11.** Sejam $(\mathbb{R}, +)$ e $(\mathbb{R}^*, \cdot)$ temos que $f : \mathbb{R} \to \mathbb{R}^*$, onde $f(x) = 2^x$ é um homomorfismo. Para provarmos, basta tomarmos dois elementos $x, y \in \mathbb{R}$. Assim temos que $f(x) = 2^x$, $f(y) = 2^y$ e $f(x+y) = 2^{x+y}$. Utilizando as propriedades de potência podemos escrever $2^{x+y} = 2^x \cdot 2^y$. Finalmente temos que $f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$.

**Propriedades Elementares**

Seja $f : (G, \cdot) \to (\mathcal{G}, \times)$ um homomorfismo de grupos. Então são válidas as seguintes propriedades:

1. $f(e_G) = e_{\mathcal{G}}$.
   Com efeito, $e_{\mathcal{G}} \cdot f(e_G) = f(e_G) = f(e_G \cdot e_G) = f(e_G) \times f(e_G) \Rightarrow e_{\mathcal{G}} = f(e_G)$

2. $f(x^{-1}) = f(x)^{-1}$. Com efeito, $e_{\mathcal{G}} = f(e_G) = f(x \cdot x^{-1}) = f(x) \times f(x^{-1})$.

3. $Ker\ f := \{x \in G | f(x) = e_{\mathcal{G}}\}$ é um subgrupo normal de $G$ chamado núcleo do homomorfismo $f$.

   *Demonstração.* Vejamos primeiramente que $ker\ f < G$. Dados $x, y \in ker f$, temos:

$$f(x \cdot y) = f(x) \times f(y) = e_{\mathcal{G}} \times e_{\mathcal{G}} = e_{\mathcal{G}}$$

$$f(x^{-1}) = f(x)^{-1} = e_{\mathcal{G}}^{-1} = e_{\mathcal{G}}$$

   portanto $ker\ f < G$. Para provar que $ker\ f \triangleleft G$ iremos mostrar que:

$$gxg^{-1} \in ker\ f, \ \ \forall g \in G \ \text{ e } \ \forall x \in ker\ f.$$

   E de fato, temos

$$\begin{aligned} f(gxg^{-1}) &= f(g) \times f(x) \times f(g^{-1}) = f(g) \times e_{\mathcal{G}} \times f(g)^{-1} \\ &= f(g) \times f(g)^{-1} = e_{\mathcal{G}}. \end{aligned}$$

   □

**Definição 3.14.** *Um homomorfismo $f : G \to \mathcal{G}$ é chamado de isomorfismo se existe um homomorfismo $g : \mathcal{G} \to G$ tal que $f \circ g = id_{\mathcal{G}}$ e $g \circ f = id_G$. Quando existe um isomorfismo entre dois grupos $G$ e $\mathcal{G}$ dizemos que $G$ e $\mathcal{G}$ são isomorfos e denotamos por $G \simeq \mathcal{G}$.*

Temos a seguinte proposição:

**Proposição 3.6.** *Seja $f : (G, \cdot) \to (G, \times)$ um homomorfismo de grupos. então, $f$ é um isomorfismo se, e somente se, $f$ for uma bijeção.*

*Demonstração.* ($\Rightarrow$) trivial
($\Leftarrow$) Precisamos mostrar que se $f$ é um homomorfismo bijetivo, então $f^{-1}$ é um homomorfismo, ou seja,

$$f^{-1}(\alpha \times \beta) = f^{-1}(\alpha) \cdot f^{-1}(\beta), \quad \forall \alpha, \beta \in \mathcal{G}.$$

Agora sejam $\alpha, \beta \in \mathcal{G}$, e também sejam $a = f^{-1}(\alpha)$ e $b = f^{-1}(\beta)$ então temos que

$$f^{-1}(\alpha \times \beta) = f^{-1}(f(a) \times f(b)) = f^{-1}(f(a \cdot b)) = a \cdot b = f^{-1}(\alpha) \cdot f^{-1}(\beta).$$

□

Com a noção de Grupos de Permutação que veremos a seguir é possível estabelecer isomorfismos entre Grupos Simétricos e Subgrupos de Rubik. E é desta forma que se dá a combinação destes dois conceitos para que sejam analisadas e criadas sequências de movimentos ou macros para resolver o Cubo Mágico.

## 3.8 Permutações

Permutação é o termo usado para designar uma bijeção de um conjunto nele mesmo. Se $E$ indica um conjunto não vazio, e $S(E)$ o conjunto das permutações dos elementos de E, a composição de aplicações, é uma operação sobre $S(E)$. De fato, se $f$ e $g$ são permutações de $E$, isto é,

$$f : E \to E \qquad \text{e} \qquad g : E \to E$$

são bijeções, então a composta $g \circ f : E \to E$ também é uma bijeção.
Pode-se provar que $(S(E), \circ)$ é um grupo, chamado de grupos das permutações sobre $E$.

Quando $E = \{1, 2, \ldots, n\}, n \geq 1$, usa-se a notação $S_n$ para indicar o conjunto das permutações sobre $E$. O grupo $(S_n, \circ)$ é chamado de grupo simétrico de grau $n$ e tem ordem $n!$.

**Definição 3.15.** *Uma permutação $\sigma \in S_n$ é chamada de $r$-ciclo se existem elementos distintos $a_1, \ldots, a_r \in \{1, \ldots, n\}$ tais que $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, \ldots, \sigma(a_{r-1}) = a_r$, $\sigma(a_r) = a_1$, e tais que $\sigma(a_j) = a_j, \forall j \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_r\}$. A notação para este $r$-ciclo será $(a_1 \ldots a_r)$. O número $r$ significa o comprimento do ciclo. Os 2-ciclos também são chamados de transposições.*

Há outras formas de representar um ciclo de elementos distintos $a_1, \ldots, a_r \in \{1, \ldots, n\}$:

1. Sucessivas transições de um elemento para outro até retornar ao elemento inicial.

   $$a_1 \to a_2 \to a_3 \to \ldots \to a_{r-1} \to a_r \to a_1$$

   e assim fecha o ciclo.

2. A forma matricial, onde cada coluna da matriz representa a transição de um elemento em outro:

   $$\begin{pmatrix} a_1 & a_2 & \ldots & a_{r-1} & a_r \\ a_2 & a_3 & \ldots & a_r & a_1 \end{pmatrix}.$$

Em geral a notação $\begin{pmatrix} 1 & 2 & 3 & \dots \\ a & b & c & \dots \end{pmatrix}$ representa a função definida por $f(1) = a$, $f(2) = b$, $f(3) = c$, e assim por diante.

Vejamos alguns exemplos em $S_5$:

**Exemplo 3.12.** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ é um 5-ciclo, denotado por (1 2 3 4 5). Outras possibilidades de notação seriam: (2 3 4 5 1), ou (3 4 5 1 2), ou (4 5 1 2 3), ou (5 1 2 3 4).

**Exemplo 3.13.** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$ é um 3-ciclo, e pode ser denotado por (1 4 3), ou também por (4 3 1), ou ainda por (3 1 4). Note que as transições de 2 em 2 e 5 em 5, ficam omitidas na notação, já que seus elementos não são permutados, isto é, permanecem inalterados.

**Exemplo 3.14.** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$ é uma transposição denotada por (1 3), ou então (3 1).

**Exemplo 3.15.** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ não é um $r$-ciclo, qualquer que seja r.

**Exemplo 3.16.** O único 1-ciclo é a identidade, que denotamos por (1) ou por $(\alpha)$ com $\alpha \in \{1, 2, 3, \dots, n\}$.

**Exemplo 3.17.** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$ é um 3-ciclo, pois $\sigma(1) = 4$, $\sigma(4) = 2$ e $\sigma(2) = 1$, $\sigma(3) = 3$ e $\sigma(5) = 5$ .

Em geral podemos pensar que efetuar uma permutação é a ação de reorganizar ou reordenar um conjunto de elementos ou objetos. No caso do cubo mágico este pensamento é aplicada aos cubinhos e também às suas cores. De acordo com a Figura 2.1, os cubinhos de quina possuem 3 cores e os cubinhos de aresta possuem 2 cores. Um fato importante, que decorre da teoria de grupos de permutação aplicada ao cubo de Rubik que veremos mais adiante, é a impossibilidade de permutar, por exemplo, 2 cores de apenas um cubinho de aresta e manter todo o restante do cubo inalterado.

**Definição 3.16.** *Seja $\sigma \in S_n$ um $r$-ciclo e seja $\tau \in S_n$ um $s$-ciclo, diremos que as permutações $\sigma$ e $\tau$ são disjuntas se nenhum elemento de $\{1, 2, \ldots, n\}$ é movido por ambas, isto é, $\forall a \in \{1, 2, \ldots, n\}$, temos $\sigma(a) = a$ ou $\tau(a) = a$.*

Vejamos alguns exemplos em $S_5$:

**Exemplo 3.18.** Os ciclos (1 3 5) e (2 4) são disjuntos.

**Exemplo 3.19.** Os ciclos (1 2 3) e (3 5) não são disjuntos, pois o elemento 3 é movido por ambas as permutações.

### 3.8.1 Produto de Ciclos

Seja o conjunto $\{1, 2, 3, 4, 5\}$ e $\sigma, \tau \in S_5$ duas permutações tais que $\sigma = (1\ 2\ 4)(3\ 5)$ e $\tau = (1\ 3\ 5)(2\ 4)$. Queremos obter uma permutação $\varphi = \sigma \circ \tau$. Para isto basta seguirmos a transição de cada elemento do conjunto, de uma permutação para outra.

Iniciamos em $\sigma$ que leva o $1 \to 2$, mas em $\tau$ temos que $2 \to 4$. Portanto em $\varphi$ temos o $1 \to 4$. Continuando em $\sigma$ temos que $4 \to 1$, mas em $\tau$ temos que $1 \to 3$. Portanto em $\varphi$ o $4 \to 3$. Seguindo em $\sigma$ o $3 \to 5$, e em $\varphi$ o $5 \to 1$. Portanto em $\varphi$ temos que o $3 \to 1$. Com isso fechamos o ciclo. Note que em $\sigma$ o $2 \to 4$ e em $\varphi$ o $4 \to 2$, logo o 2 não se move. O mesmo ocorre com o 5, logo ele também não se move. Com isto chegamos ao resultado do produto $\varphi = \sigma \circ \tau = (1\ 2\ 4)(3\ 5) \circ (1\ 3\ 5)(2\ 4) \Rightarrow \varphi = (1\ 4\ 3)$.

**Observação 3.6.** Escrever o produto $(1\ 2\ 4)(3\ 5) \circ (1\ 3\ 5)(2\ 4)$ é o mesmo que escrever $(1\ 2\ 4)(3\ 5)(1\ 3\ 5)(2\ 4)$.

**Proposição 3.7.** *Sejam $\sigma, \tau \in S_n$ dois ciclos disjuntos, então temos que $\sigma\tau = \tau\sigma$.*

*Demonstração.* Sejam $\sigma$ e $\tau$ ciclos de $S_n$ disjuntos com relação aos conjuntos $A$ e $B$, respectivamente. Se $x$ é um elemento do conjunto $I_n = \{1, 2, \ldots, n\}, n \geq 2$, então há três hipóteses possíveis

- $x \in A$.
  Então, $\sigma \circ \tau(x) = \sigma(\tau(x)) = \sigma(x)$, ao passo que $(\tau \circ \sigma)(x) = \tau(\sigma(x)) = \sigma(x)$. Portanto, $\sigma \circ \tau$ e $\tau \circ \sigma$ coincidem em A.

- $x \in B$ (é análogo ao anterior).
- $x \notin A$ e $x \notin B$.
  Neste caso, $(\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(x) = x$, ao passo que $(\tau \circ \sigma)(x) = \tau(\sigma(x)) = \sigma(x) = x$. Portanto, $\sigma \circ \tau$ e $\tau \circ \sigma$ também coincidem fora de $A$ e $B$.

□

**Proposição 3.8.** *Seja a permutação $\sigma \in S_n$, $\sigma \neq id$, então podemos escrevê-la como um produto de ciclos disjuntos de comprimentos $\geq 2$. Esta fatoração é única a menos da ordem dos fatores.*

*Demonstração.* Como $\alpha$ é $id$, existe $i_1$ tal que $\alpha(i_1) \neq i_1$. Considere a sequência $i_1, \alpha(i_1), \alpha^2(i_1), \ldots$; claramente, existe $r_1$, $2 \leq r_1 \leq n$, tal que $i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)$ são todos distintos e $\alpha^{r_1}(i_1) \in \{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)\}$; é imediato verificar que $\alpha^{r_1}(i_1) = i_1$. Portanto a restrição de $\alpha$ ao conjunto $\{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)\}$ é tal que

$$\alpha \mid_{\{i_1, \alpha(i_1), \ldots \alpha^{r_1-1}(i_1)\}} = (i_1 \alpha(i_1) \ldots \alpha^{r_1-1}(i_1)).$$

Denotaremos este $r_1$-ciclo $(i_1 \alpha(i_1) \ldots \alpha^{r_1-1}(i_1))$ por $\sigma_1$.

Se a restrição de $\alpha$ ao complementar de $\{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)\}$ é a identidade, acabou: $\alpha = \sigma_1$. Senão, tomamos um elemento $i_2 \in \{1, 2, \ldots, n\} \setminus \{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)\}$ tal que $\alpha(i_2) \neq i_2$; de maneira similar à etapa precedente, vai existir um inteiro $r_2 \geq 2$ tal que

$$\alpha \mid_{\{i_2, \alpha(i_2), \ldots \alpha^{r_2-1}(i_2)\}} = (i_2 \alpha(i_2) \ldots \alpha^{r_2-1}(i_2)).$$

Denotaremos este $r_2$-ciclo $(i_2 \alpha(i_2) \ldots \alpha^{r_2-1}(i_2))$ por $\sigma_2$. Observe que $\sigma_1$ e $\sigma_2$ são disjuntos. Se a restrição de $\alpha$ ao complementar do conjunto $\{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1), i_2, \alpha(i_2), \ldots \alpha^{r_2-1}(i_2)\}$ é a identidade, acabou: $\alpha = \sigma_1\sigma_2 = \sigma_2\sigma_1$. Senão, tomamos $i_3 \in \{1, 2, \ldots, n\} \setminus \{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1), i_2, \alpha(i_2), \ldots, \alpha^{r_2-1}(i_2)\}$ tal que $\alpha(i_3) \neq i_3$ e continuamos o processo. Claramente este processo vai ter que parar após um número finito de etapas, e assim obteremos que $\alpha = \sigma_1\sigma_2 \ldots \sigma_t$, onde $\sigma_1, \sigma_2, \ldots, \sigma_t$ são ciclos disjuntos de comprimentos $\geq 2$.

Agora, para provar a unicidade, suponha que temos também $\alpha = \tau_1\tau_2 \ldots \tau_u$ com $\tau_1, \tau_2, \ldots, \tau_u$ ciclos disjuntos, cada um deles de comprimento $\geq 2$. Como $\tau_1, \ldots \tau_u(i_1) = \alpha(i_1) \neq i_1$ e como os $\tau_i$'s são ciclos disjuntos, existe um único $\tau_j$ tal que $\tau_j(i_1) = \alpha(i_1)$. Como os $\tau_i$'s comutam entre si, podemos supor que $j = 1$ e então $\tau_1(i_1) = \alpha(i_1)$. Vamos mostrar que $\tau_1 = \sigma_1$. O ciclo $\tau_1$ não pode deixar $\alpha(i_1)$ fixo, isto é, $\tau_1$ não pode mandar $\alpha(i_1)$ sobre $\alpha(i_1)$, pois $\tau_1$ já manda $i_1$ sobre $\alpha(i_1)$; como os $\tau_i$'s são ciclos disjuntos, então, $\forall j \geq 2$, $\tau_j$ deixa $\alpha(i_1)$ fixo e portanto $\alpha(\alpha(i_1)) = \tau_1(\alpha(i_1))$; assim $\tau_1(\alpha(i_1)) = \alpha^2(i_1)$. De maneira similar obtemos que $\tau_1(\alpha^{k-1}(i_1) = \alpha^k(i_1), \forall k \geq 0$, e portanto que $\tau_1 = \sigma_1$. Similarmente, trabalhando com $i_2$ no lugar de $i_1$, iremos obter que $\tau_2 = \sigma_2$; continuando assim, obteremos que $u = t$ e que a menos da ordem $\sigma_j = \tau_j$, para cada $j = 1, \ldots, t$. □

A unicidade do produto de ciclos disjuntos é de grande auxílio ao se realizar operações no grupo $S_n$.

**Exemplo 3.20.** A permutação $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 2 & 7 & 4 \end{pmatrix}$ pode ser escrita como o produto $(1\ 3)(2\ 5)(4\ 6\ 7)$, ou seja, dois 2-ciclo e um 3-ciclo.

**Exemplo 3.21.** A permutação de $S_8$

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

pode ser escrita em ciclos disjuntos da seguinte maneira:

Como $\sigma(1) = 1$, vamos começar o processo descrito na demonstração com o elemento 2:

$$2, \sigma(2) = 6, \sigma^2(2) = \sigma(\sigma(2)) = \sigma(6) = 5, \sigma(5) = 7, \sigma(7) = 2.$$

Portanto

$$\sigma_1 = (2\ 6\ 5\ 7).$$

Repetindo-se o processo a partir do 3 obteremos:

$$3, \sigma(3) = 8, \sigma(8) = 4, \sigma(4) = 3.$$

Então

$$\sigma_2 = (3\ 8\ 4).$$

Portanto:

$$\sigma = (2\ 6\ 5\ 7) \circ (3\ 8\ 4).$$

**Proposição 3.9.** *Todo elemento de $S_n$ é um produto de transposições, isto é, $S_n = \langle\{transposições\}\rangle$.*

*Demonstração.* Temos $id = (1\ 2)(1\ 2) \in \langle\{\text{transposição}\}\rangle$. Utilizando a proposição 3.8, basta mostrarmos que todo ciclo $(a_1 \dots a_r)$ é um produto de transposições, e de fato, temos

$$(a_1\ a_2 \dots a_r) = (a_1\ a_r)(a_1\ a_{r-1}) \dots (a_1\ a_3)(a_1\ a_2).$$

$\square$

**Exemplo 3.22.** Vejamos como decompor, em transposições, a seguinte permutação em $S_8$:

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

Como visto no exemplo 3.21: $\sigma = (2\ 6\ 5\ 7) \circ (3\ 8\ 4)$. Mas devido à identidade exibida na proposição:

$$\sigma = (2\,6\,5\,7) = (2\,7) \circ (2\,5) \circ (2\,6) \text{ e } (3\,8\,4) = (3\,4) \circ (3\,8).$$

Portanto

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

**Observação 3.7.** A decomposição de um elemento $\alpha \in S_n$ como produto de transposições não é única, mesmo ao se estabelecer um número mínimo de transposições, como é o que acontence em $(1\,2\,3) = (1\,3)(1\,2) = (2\,3)(1\,3)$. Entretanto, mais a frente veremos que a paridade do número de transposições é bem definida.

### 3.8.2 Repetição de ciclos e ordem

Vejamos agora como se comporta a repetição de um ciclo, isto é, aplicar o produto de um $n$-ciclo a ele mesmo sucessivas vezes. Por exemplo, vamos considerar o 3-ciclo $\sigma = (1\,2\,3)$, e verificar o comportamento de $\sigma^1$, $\sigma^2$ e $\sigma^3$.

1. $\sigma^1 = (1\,2\,3) = id$
2. $\sigma^2 = (1\,2\,3)(1\,2\,3) = (1\,3\,2)$
3. $\sigma^3 = (1\,2\,3)(1\,2\,3)(1\,2\,3) = (1\,2\,3) = id$

É possível notar que ao aplicar o 3–ciclo a ele mesmo 3 vezes, o resultado é ele próprio, isto é, a identidade.

**Definição 3.17.** *Seja $\sigma \in S_n$ um $r$-ciclo. O número mínimo de aplicações, a ele mesmo, necessário para que o ciclo retorne à sua posição original, isto é, a identidade (id) será chamado de ordem de $\sigma$ ($\mathcal{O}(\sigma)$), que é igual a $r$.*

**Proposição 3.10.** *Se $\sigma = (a_1\ a_2\ a_r) \in S_n$ é um ciclo de comprimento $r > 1$, então $\mathcal{O}(\sigma) = r$ e, portanto, se $\varepsilon$ indicar a permutação idêntica de $S_n$, $[\sigma] = \{\varepsilon, \sigma, \sigma^2, \ldots, \sigma^{r-1}\}$.*

*Demonstração.* Da definição de ciclo decorre diretamente que $\sigma^{i-1}(a_1) = a_1$, $(i = 1, 2, \ldots, r)$ e $\sigma^r(a_1) = a_1$. então $\sigma^i \neq \varepsilon$ sempre que $1 \leq i < r$, e, portanto, $r \leq \mathcal{O}(\sigma)$. Por outro lado, se $i$ é um índice tal que $1 \leq i \leq r$, então $\sigma^r(a_i) = \sigma^r(\sigma^{i-1}(a_1)) = \sigma^{i-1}(\sigma^r(a_1)) = \sigma^{i-1}(a_1) = a_i$. Considerando-se que $\sigma(x) = x$ sempre que $x \neq a_i$, $(i = 1, 2, \ldots, r)$, então $\sigma^r = \varepsilon$ e, por conseguinte, $\mathcal{O}(\sigma) \leq r$. De onde, $\mathcal{O}(\sigma) = r$. □

**Proposição 3.11.** *Sejam $\sigma_1, \ldots, \sigma_t \in S_n$ ciclos disjuntos de comprimentos $r_1, \ldots, r_t$ respectivamente. A ordem do produto $\sigma_t \ldots \sigma_1$ tem ordem igual ao m.m.c.$(r_1, \ldots, r_t)$, onde m.m.c. é a abreviação de mínimo múltiplo comum.*

Maiores detalhes podem ser encontrados em [2].

**Exemplo 3.23.** Seja $\sigma = (1\ 2)(3\ 4\ 5)$ o produto disjunto entre um 2-ciclo e um 3-ciclo. Como a ordem de $(1\ 2)$ é igual a 2 e a ordem de $(3\ 4\ 5)$ é igual a 3, segue que $\mathcal{O}(\sigma) = m.m.c.(2, 3) \Rightarrow \mathcal{O}(\sigma) = 6$.

No caso do cubo mágico, temos o seguinte exemplo: Seja a macro $S = F^4$. Ao aplicarmos 4 vezes o movimento $F$ retornamos à identidade, conforme a Figura 3.5.


Figura 3.5: Macro $F^4$.

Portanto a ordem de $S$ é igual 4, isto é, $\mathcal{O}(S) = 4$. Todos os 8 movimentos $(UU'DD'RR'LL'FF'BB')$ das faces tanto no sentido horário quanto no sentido anti-horário são de ordem 4. Já as macros $T = URU'R'$ e $V = RU$, possuem ordens $\mathcal{O}(T) = 6$ e $\mathcal{O}(V) = 105$, respectivamente.

Utilizando o cubo mágico é fácil verificar a ordem de uma macro. Por exemplo, a partir da posição inicial do cubo, isto é, com ele resolvido, basta repetir sucessivas vezes a mesma macro e contar o número de repetições até que se retorne, pela primeira vez, à posição inicial. Mais adiante no Capítulo 4 veremos que é possível calcular tais ordens.

## 3.9 Assinatura de uma Permutação

Conforme visto na seção anterior, é possível realizarmos a decomposição de um ciclo em um produto de transposições, porém ela não é única. De fato, como $(a\ b) \circ (b\ a)$ é a aplicação idêntica de $I_n$, que é o elemento neutro de $S_n$, então num produto de transposições podemos inserir tantas expressões deste tipo quanto desejarmos, o que não afetará o resultado. Por exemplo, em $S_7$:

$$(2\,6\,5\,7) = (2\,7) \circ (2\,5) \circ (2\,6) = (1\,2) \circ (2\,1) \circ (2\,7) \circ (2\,5) \circ (2\,6)$$

Entretanto é possível demonstrarmos que todas as decomposições de um mesmo ciclo, em transposições, têm em comum a paridade. Isto é, se em uma delas o número de transposições é par (ímpar), então o mesmo acontecerá em todas as outras. Contudo, para provarmos este resultado, é necessário que antes introduzamos o conceito de *assinatura* de uma permutação.

**Definição 3.18.** *A assinatura de uma permutação* $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ *é o número real, aqui denotado por* $sgn(\sigma)$*, e definido por:*

$$sgn(\sigma) = \prod \frac{a_i - a_j}{b_i - b_j}$$

*em que o produto é estendido a todos os pares* $(i, j)$ *de índices tais que* $i > j$*.*

Da definição, decorre diretamente que a assinatura da permutação idêntica é igual a 1.

Devemos observar que o produto que define $sgn(\sigma)$ independe da ordem das colunas na expressão de $\sigma$ e que cada quociente $\dfrac{a_i - a_j}{b_i - b_j}$ é uma função do par $(i, j)$.

**Exemplo 3.24.** A assinatura da permutação $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ é:

$$sgn(\sigma) = \frac{2-1}{3-2} \cdot \frac{3-1}{1-2} \cdot \frac{3-2}{1-3} = (1)(-2)(-1/2) = 1.$$

**Proposição 3.12.** *A assinatura de uma transposição é -1.*

*Demonstração.* Seja $\tau \in S_n$ uma transposição. Podemos representá-la da seguinte maneira:

$$\tau = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a-2 & a_1 & a_3 & \dots & b_n \end{pmatrix}.$$

Se $(r, s)$ é um par de índices da primeira linha da transposição $\tau$ e $1 \leqslant r < s \leqslant n$, então podemos ter as seguintes situações possíveis:

(a) $(r, s) = (1, 2)$ cujo fator correspondente em $sgn(\tau)$ é $\dfrac{a_2 - a_1}{a_1 - a_2} = -1$.

(b) $r = 1$ e $s > 2$, caso em que o fator correspondente de $(r, s)$ em $sgn(\tau)$ é $\dfrac{a_s - a_1}{a_s - a_2}$.

(c) $r = 2$ e $s > 2$, caso em que o fator correspondente de $(r, s)$ em $sgn(\tau)$ é $\dfrac{a_s - a_2}{a_s - a_1}$.

(d) $r > 2$ e neste caso, o fator correspondente de $(r, s)$ em $sgn(\tau)$ é $\dfrac{a_s - a_r}{a_s - a_r} = 1$.

Como os fatores de (b) e (c) aparecem em pares cujo produto é 1, então:

$$sgn(\tau) = \frac{a_2 - a_1}{a_1 - a_2} = -1$$

□

**Proposição 3.13.** *Para quaisquer permutações $\sigma, \varphi \in S_n$, $sgn(\varphi \circ \sigma) = (sgn(\varphi))(sgn(\sigma))$.*

*Demonstração.* Permutando convenientemente as colunas de $\varphi$, podemos escrever:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \text{ e } \tau = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

Portanto:

$$(sgn(\varphi))(sgn(\sigma)) = (sgn(\sigma))(sgn(\varphi)) = \prod \frac{a_i - a_j}{b_i - b_j} \prod \frac{b_i - b_j}{c_i - c_j} = \prod \frac{a_i - a_j}{c_i - c_j} = sgn(\varphi \circ \sigma)$$

□

**Corolário 3.4.** *Se $\sigma \in S_n$, então $sgn(\sigma) = \pm 1$.*

*Demonstração.* Como toda permutação pode ser escrita como um produto de transposições, então:

$$\sigma = \tau_1 \circ \tau_2 \circ \dots \tau_r.$$

para convenientes transposições $\tau_1, \tau_2, \dots \tau_r \in S_n$. Então, se usarmos a generalização da proposicão anterior para $r$ fatores e sabendo que a assinatura de uma transposição é igual a -1:

$$\begin{aligned} sgn(\sigma) = sgn(\tau_1 \circ \tau_2 \circ \dots \tau_r) &= (sgn(\tau_1))(sgn(\tau_2)) \dots (sgn(\tau_r)) = \\ &= (-1)(-1) \dots (-1) = (-1)^r = \pm 1. \end{aligned}$$

□

### 3.9.1 Paridade de Ciclos

**Definição 3.19.** *Seja $\sigma \in S_n$. Diremos que $\sigma$ é uma permutação par quando $\sigma$ se escreve como um produto de um número par de transposições. E diremos que $\sigma$ é uma permutação ímpar quando $\sigma$ se escreve como um produto de um número ímpar de transposições.*

**Exemplo 3.25.** Seja a permutação $\sigma = (1\ 2\ 4)(3\ 5) = (1\ 2)(1\ 4)(3\ 5)$, portanto $\sigma$ é ímpar. Seja a permutação $\tau = (1\ 4\ 3) = (1\ 4)(1\ 3)$, portanto $\tau$ é par. O elemento neutro $(1) \in S_n$ é par, pois $(1) = (1\ 2)(1\ 2)$.

Podemos ainda definir:

**Definição 3.20.** *Seja um elemento $\sigma \in S_n$ escrito como o seguinte produto:*

$$\prod_{1 \leqslant i < j \leqslant n} (x_j - x_i) = (x_2 - x_1)(x_3 - x_1)\dots(x_n - x_1)(x_3 - x_2)\dots(x_n - x_{n-1})$$

*Diremos que a permutação é par, se o produto for positivo e diremos que a permutação é ímpar se o produto for negativo.*

**Exemplo 3.26.** Seja o ciclo $(1\ 3\ 2) = (1\ 3)(1\ 2)$. Então $x_1 = 3$, $x_2 = 1$ e $x_3 = 2$.

Logo teremos $(x_2 - x_1)(x_3 - x_1)(x_3 - x_2) = (1-3)(2-3)(2-1) = 2 > 0$. Então o ciclo $(1\ 3\ 2)$ é par.

**Proposição 3.14.** *Seja $\sigma \in S_n$ uma dada permutação e consideremos duas composições de $\sigma$ em transposições:*

$$\sigma = \tau_1 * \tau_2 * ... * \tau_r \text{ e } \sigma = \rho_1 * \rho_2 * ... * \rho_s$$

*então os inteiros $r$ e $s$ têm a mesma paridade.*

*Demonstração.* Devido ao corolário 3.4, $sgn(\sigma) = (-1)^r = (-1)^s$. Se $r$ for par, então $(-1)^r = 1$; daí $(-1)^s = 1$ e, portanto, $s$ também é par. O raciocínio é análogo no caso em que $r$ é ímpar. □

**Proposição 3.15.** *Seja $A_n = \{\alpha \in S_n | \alpha$ é uma permutação par$\}$ . Então $A_n$ é um subgrupo das permutações pares de $S_n$ e é chamado de grupo alternado.*

**Observação 3.8.** Note que a outra metade das permutações ímpares não é um subgrupo já que não contém o elemento neutro (1).

Veremos no próximo capítulo como o conceito de paridade nos auxilia não só na análise do cubo mágico, bem como na sua resolução. É também através deste conceito que se justifica a impossibilidade de se obter certas permutações entre os cubinhos como, por exemplo, permutar as 2 cores de um cubinho de aresta sem alterar todos os outros.

# 4 Aplicações da Teoria de Grupos e Grupos de Permutação no Cubo Mágico

Neste capítulo utilizaremos os conceitos abordados no capítulo anterior com o objetivo de calcular o número de configurações possíveis que o cubo mágico pode assumir, além de compreender o funcionamento das macros em especial os comutadores e conjugados. Com isto provaremos a impossibilidade de permutar posições e orientações específicas dos cubinhos e de suas cores. Mas acima de tudo é através deste capítulo que mostraremos que a justificativa da possibilidade da resolução do cubo mágico é matemática e não empírica. As principais referências utilizadas para o desenvolvimento deste capítulo foram [3], [4], [5] e [6].

## 4.1 Calculando a ordem de uma macro

Seja a macro $S = URU'R'$. No exemplo 3.23 vimos que $\mathcal{O}(S) = 6$.

De fato, para chegarmos neste valor precisamos primeiro observar, utilizando o próprio cubo mágico, quais cubinhos são afetados por esta macro. A figura 4.1 mostra quais deles são permutados.

Ao realizar esta macro uma ou mais vezes percebemos que todos os cubinhos que se movem ocupam apenas algumas posições, isto é, durante a permutação eles não são todos permutados entre si. Na verdade percebemos que estas permutações ocorrem em grupos formando um ciclo, onde somente os cubinhos pertencentes a um mesmo ciclo permutam entre si. Com efeito, notamos que os cubinho $UB$, $UR$ e $FR$ permutam entre si, da mesma forma que os cubinhos $LUB$ e $RUB$ permutam entre si e finalmente os cubinhos $RUF$ e $RDF$ permutam entre si. Logo podemos escrever, em notação de ciclo, a macro $S$ que provoca as seguintes permutações: $S = (UB\ UR\ FR)(LUB\ RUB)(RUF\ RDF)$, isto é, composta de 1 3-ciclo e 2 2-ciclo.

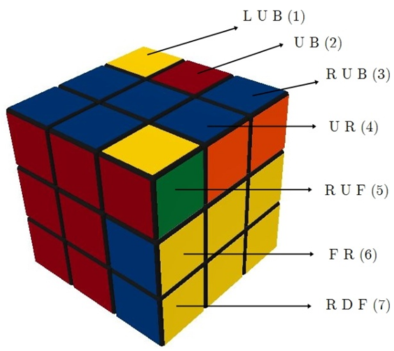


Figura 4.1: Cubinhos afetados pela macro $S$.

Podemos ainda fazer uma associação com números da seguinte forma:

$$\begin{array}{ccccccc} UB & UR & FR & LUB & RUB & RUF & RDF \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 6 & 1 & 3 & 5 & 7 \end{array}$$

Portanto podemos escrever a permutação $S$ da seguinte maneira:

$$S = (2\ 4\ 6)(1\ 3)(5\ 7)$$

Os comprimentos dos ciclos $(UB\ UR\ FR)$, $(LUB\ RUB)$ e $(RUF\ RDF)$, são respectivamente 3, 2, 2. Logo a ordem de $S$ é dada pelo mínimo múltiplo comum (m.m.c.) entre 3,2,2. Portanto $\mathcal{O}(S) = m.m.c.(3, 2, 2) = 6$. Concluímos também que a permutação gerada por $S$ é par, afinal $S$ pode ser escrita como um produto de um número par de transposições, por exemplo: $S = (2\ 4)(2\ 6)(1\ 3)(5\ 7)$.

## 4.2 Paridade dos movimentos das faces

Vimos no capítulo 2 que uma macro nada mais é do que uma sequência de dois ou mais movimentos de qualquer uma das 6 faces do cubo, tanto no sentido horário quanto no sentido anti-horário, logo podemos associá-la com um produto de ciclos. Se analisarmos a paridade de apenas um movimento de uma face, por exemplo, o movimento $F$ (girar em 90° a face da frente no sentido horário), podemos estender esta paridade a qualquer macro. Ao efetuarmos o movimento $F$ os cubinhos afetados são: $FU, FUR, FR, FDR, FD, FDL, FL, FUL$. A figura 4.2 ilustra este movimento.

Em notação de ciclos temos: $F = (FU\ FR\ FD\ FL)(FUL\ FUR\ FDR\ FDL)$ ou ainda associando números $F = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$. Se escrevermos $F$ como produto de ciclos disjuntos teremos:

$$F = (1\ 3)(1\ 5)(1\ 7)(2\ 4)(2\ 6)(2\ 8).$$

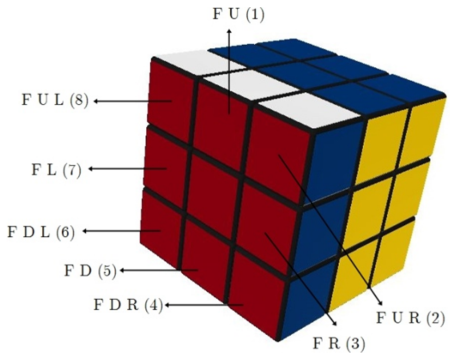


Figura 4.2: Cubinhos afetados pelo movimento $F$

Portanto o movimento $F$ tem paridade par. Sem perda de generalidade o mesmo ocorre para o movimento das outras 5 faces. Como uma macro é composta de dois ou mais movimentos é, portanto deste fato que decorre a impossibilidade de, com um ou mais movimentos, permutarmos apenas um par de cubinhos sem alterar todo o resto do cubo. Para isto o movimento da face necessitaria ter paridade ímpar. De maneira análoga não existe uma sequência que permute apenas 2 cores de um cubinho de aresta sem alterar todo o resto. Esta impossibilidade é outro motivo que torna a resolução do cubo bastante desafiadora. É deste fato também que ao permutarmos as 3 cores de um cubinho de canto em um sentido, invariavelmente será permutado no sentido contrário as 3 cores de um cubinho de canto adjacente, se quisermos que mais nenhum outro cubinho saia de sua posição. Mais a frente veremos como isto é possível.

Seja a macro $S = F^2R^2$. Ela move 13 cubinhos, portanto temos os seguintes ciclos:

$$S = (UF\ DF)(DR\ UR)(FL\ FR\ BR)(UFL\ DFR\ UBR)(DFL\ UFR\ DBR)$$

A macro $S$ possui paridade par e ordem $\mathcal{O}(S) = 6$. Se aplicarmos $S$ por três vezes, isto é, $S^3$, veremos que os cubinhos do 3-ciclo voltaram ao seu lugar e os cubinhos dos 2-ciclos permaneceram permutados. Afinal a ordem dos 3-ciclos é 3 e, portanto ao aplicarmos a macro 3 vezes eles retornaram às suas posições originais, enquanto que o 2-ciclo, que tem paridade par, foi executado um número ímpar de vezes não retornando ao seu estado inicial. Mais a frente veremos macros que permutam ciclicamente 3 cubinhos de mesmo tipo, deixando todo o resto do cubo inalterado. Tais macros evidentemente são permutações pares. É através dos conceitos de paridade e ordem que os métodos que resolvem o cubo em poucos movimentos são embasados, pois organizam os movimentos pelas suas ordens.

## 4.3 Calculando o número de posições do cubo mágico

Para contarmos o número ($N$) de posições, de acordo com [5], que o cubo mágico pode assumir, precisamos recordar que há 12 cubinhos de arestas, cada um contendo 2 cores diferentes e 8 cubinhos de canto, cada um contendo 3 cores diferentes. Portanto, teoricamente deveríamos ter para os cubinhos de aresta $12! \cdot 2^{12}$ possibilidades e para os cubinhos de canto $8! \cdot 3^8$ possibilidades, gerando um total de $12! \cdot 2^{12} \cdot 8! \cdot 3^8$. Entretanto, vimos anteriormente que há algumas impossibilidades de posições devido à paridade do cubo. Não existe a possibilidade de alterarmos apenas um cubinho de aresta, logo somente 11 dos 12 cubinhos é que podem sofrer permutação, em nossa contagem. O mesmo ocorre com os cubinhos de canto, isto é, não podemos alterar apenas um cubinho de canto, logo somente 7 dos 8 cubinhos de canto é que sofrem permutação. Devido à paridade vimos também que metade delas são pares e ímpares, onde estas últimas não podem ser alcançadas devido à paridade dos movimentos das faces serem pares. Logo, teremos o seguinte cálculo:

$$N = \frac{(12! \cdot 2^{11}) \cdot (8! \cdot 3^7)}{2} = 43\ 252\ 003\ 274\ 489\ 856\ 000 \cong 4,0 \times 10^{19} \text{ possibilidades.}$$

Diante de um número de tão grandes proporções, podemos concluir que é praticamente impossível alguém, movendo o cubo aleatoriamente, resolvê-lo em algum momento sem utilizar qualquer método mais estratégico. Afinal somente 1 destas posições é a que o cubo se encontra montado, isto é, aquela em que apresenta todas as suas faces com suas respectivas cores.

## 4.4 Comutadores e conjugados

Na seção 3.5.1 vimos a existência de subgrupos chamados de comutadores, cuja forma é $XYX^{-1}Y^{-1}$ e conjugados, cuja forma é $GHG^{-1}$. Podemos ainda denotar um comutador da seguinte forma $[X,Y] = XYX^{-1}Y^{-1}$, e um conjugado da seguinte forma $H\hat{}G = GHG^{-1}$.

Através deles podemos pensar em sequências que permutem, por exemplo, apenas alguns cubinhos que se queira, sem alterar todo o resto do cubo. Para isso associamos $X$ e $Y$, no caso dos comutadores, aos movimentos das faces, sejam eles simples ou sequências de movimento. Ao aplicarmos, tanto os comutadores quanto os conjugados, em um cubo mágico notamos que o efeito provocado é o que se pode dizer de "destruir e reconstruir". E ainda com uma familiaridade maior com o cubo, tais movimentos tornam-se intuitivos no sentido de se compreender o que está acontecendo durante a execução. É nítido, por exemplo, observar um determinado cubinho saindo de sua posição, indo para outra que se queira, e dando lugar a outro cubinho que também se queria posicionar no lugar do primeiro, enquanto que os restantes dos cubinhos, que não se queria alterar, mudam de lugar durante a execução, porém ao final retornam a suas posições em que estavam inicialmente. Vejamos agora alguns exemplos de comutadores e conjugados:

**Exemplo 4.1.** Permutar 2 cubinhos de aresta que estão na face frontal. Sejam as macros $S = UFU'F'$ e $T = U'F'UF$. A ação gerada por $S$ leva o cubinho $FU$ em $FL$ e a ação gerada por $T$ leva o cubinhos $FU$ em $FR$. Ao final a orientação da cor do cubinho foi preservada. A figura 4.3 mostra o efeito das macros $S$ e $T$:


Figura 4.3: Efeito gerado pelas macros $S$ e $T$.

Analisando temos:

$$S = UFU'F' \text{ onde} \begin{cases} X = U & Y = F \\ X^{-1} = U' & Y^{-1} = F' \end{cases}$$

$$T = U'F'UF \text{ onde} \begin{cases} X = U' & Y = F' \\ X^{-1} = U & Y^{-1} = F \end{cases}$$

Note que ao aplicar $S$, o primeiro movimento é $U$, isto é, girar a face superior em 90° no sentido horário. Isto faz com que o cubinho em $FU$ seja levado para a face da esquerda, terminando em $FL$. De modo análogo, ao aplicar $T$, o primeiro movimento é $U'$, isto é, girar a face superior em 90° no sentido anti-horário. Isto faz com o cubinho em $FU$ seja levado para a face da direita, terminando em $FR$.

Ambas as macros afetam outros cubinhos além daqueles que se desejam alterar. No caso da macro $S$, os cubinhos afetados formam os seguintes ciclos:

$$S = (FL\ FU\ UR)(FLD\ FLU)(LUF\ LUB)$$

Onde o que nos interessa é o 3-ciclo. Note que se aplicarmos $S^3$, os cubinhos deste ciclo retornam às suas posições originais, deixando os demais permutados, afinal $\mathcal{O}(S) = 6$.

Se chamarmos de $M = UF$ e $N = U'F'$, temos que $S = MN$ e $T = NM$. Tal fato, em particular, faz com que as macros $S$ e $T$ produzam um efeito simétrico em relação à face frontal.

**Exemplo 4.2.** Permutar 3 cubinhos de canto que estão na face superior, alterando suas orientações.

Sejam as macros $S = R'(ULU')R(UL'U')$ e $S^{-1} = (ULU')R'(UL'U')R$. A ação gerada por ambas permutam os cubinhos $UFL$, $UFR$ e $UBR$ no sentido anti-horário e no sentido horário, respectivamente. Ao final além das posições as cores destes cubinhos também são reorientadas. A figura 4.4 mostra o efeito das macros $S$ e $S^{-1}$:


Figura 4.4: Permutação de 3 cubinhos de canto com alteração de suas orientações.

Diferentemente do exemplo anterior, em que os elementos são movimentos simples das faces, neste caso um dos elementos do comutador é uma sequência de movimentos.

Analisando temos:

$$S = R'(ULU')R(UL'U') \text{ onde} \begin{cases} X = R' & Y = ULU' \\ X^{-1} = R & Y^{-1} = UL'U' \end{cases}$$

$$S^{-1} = (ULU')R'(UL'U')R \text{ onde} \begin{cases} X = ULU' & Y = R' \\ X^{-1} = UL'U' & Y^{-1} = R \end{cases}$$

As macros $ULU'$ e $UL'U'$ são inversas, pois se realizarmos uma em ordem inversa, invertendo individualmente cada movimento, temos a outra. Por este fato, em $S$, o que é $X = R'$ e $Y = ULU'$, em $S^{-1}$ é o inverso, isto é, $X = ULU'$ e $Y = R'$. E ainda se realizarmos uma macro em ordem inversa, invertendo individualmente cada movimento temos outra. Portanto, temos que o efeito provocado por ambas as macros permutam os mesmos cubinhos, porém em sentido contrário.

Note que apenas os cubinhos do 3-ciclo, isto é, $(UFL\ UFR\ UBR)$ é que foram permutados deixando todo o resto do cubo intacto, embora tenha sido permutado além de suas posições, também suas cores.

**Exemplo 4.3.** Permutar 3 cubinhos de canto que estão na face superior, sem alterar suas orientações.

Sejam as macros $G = LD$ e $G^{-1} = D'L'$ e os comutadores $H = (R'D'R)U(R'DR)U'$ e $H^{-1} = U(R'D'R)U'(R'DR)$. Agora vamos compor os seguintes conjugados: $W = H\hat{}G = GHG^{-1}$ e $W^{-1} = H^{-1}\hat{}G = GH^{-1}G^{-1}$. Em notação do cubo mágico teremos:

$$W = GHG^{-1} = LD[(R'D'R)U(R'DR)U']D'L'$$

$$W^{-1} = GH^{-1}G^{-1} = LD[U(R'D'R)U'(R'DR)]D'L'$$

A ação gerada por ambas permutam os cubinhos $UFL$, $UFR$ e $UBR$ no sentido anti-horário e no sentido horário, respectivamente, sem alterar suas orientações. A figura 4.5 mostra o efeito das macros $W$ e $W^{-1}$:


Figura 4.5: Permutação de 3 cubinhos de canto sem alteração de suas orientações.

Ao contrário do exemplo anterior esta macro conservou as orientações, já que no exemplo da figura os 3 cubinhos permutados permaneceram com suas faces azuis voltadas para cima.

Por este exemplo, fica evidente que é impossível permutar apenas 2 cantos, conservando suas orientações, sem alterar o restante do cubo, afinal a paridade de um 3-ciclo é par.

Até agora vimos exemplos de permutações entre cubinhos, em que pode ocorrer ou não a reorientação das cores. Entretanto podemos realizar macros que gerem, ao final da execução, somente a permutação das cores dos cubinhos sem movê-los de lugar. Sabemos da seção 4.2 que é impossível permutar apenas as cores de um cubinho de aresta sem alterar todo o restante do cubo. Porém é possível permutar as 3 cores de dois cubinhos de canto adjacentes, afinal são 2 3-ciclo, cuja paridade é par. É o que veremos no próximo exemplo.

**Exemplo 4.4.** Permutar as 3 cores de 2 cubinhos de canto da face frontal.

Sejam as macros $M = LD^2L'F'D^2FeN = U$. Vamos compor os seguintes comutadores $S = MNM^{-1}N^{-1}$ e $S^{-1} = NMN^{-1}M^{-1}$, cujas formas são $XYX^{-1}Y^{-1}$:

$$S = (LD^2L'F'D^2F)U(F'D^2FLD^2L')U'$$

$$S^{-1} = U(LD^2L'F'D^2F)U'(F'D^2FLD^2L')$$

A ação gerada por ambas as macros permutam as cores dos cubinhos $UFL$ e $UFR$. A permutação ocorre em sentidos contrários simultaneamente, isto é, enquanto para um cubinho as cores são permutadas no sentido horário, as cores do outro cubinho são permutadas no sentido anti-horário e vice-versa. A figura 4.6 mostra o efeito das macros $S$ e $S^{-1}$.


Figura 4.6: Rotação dos cubinhos de canto.

Como neste exemplo, ao invés das posições, as cores é que são permutadas, poderíamos associar para cada cor de cada cubinho um número e escrever os seguintes 3-ciclo: (1 2 3) e (4 5 6), respectivamente para os cubinhos $UFL$ e $UFR$.

# 5 Resolvendo o Cubo Mágico

Este capítulo é dedicado às diversas abordagens de se resolver o Cubo Mágico de Rubik. Para efeito de organização, vamos classificar tais abordagens em três categorias que se distinguem quanto à otimização: uma com relação ao menor número de movimentos, outra com relação ao menor tempo de resolução e outra com relação à menor memorização de algoritmos. O método que mostraremos ao final deste capítulo privilegia esta última. A razão da escolha feita se justifica por dois motivos, pois ela utiliza os resultados obtidos pela combinação das duas teorias abordadas nesta dissertação, a Teoria de Grupos e a Teoria dos Grupos de Permutação e também por ser relativamente simples para quem já possui familiaridade com o cubo mágico. As poucas macros que são adotadas neste método utilizam comutadores e conjugados, os mesmos apresentados no Capítulo 4. Já no Capítulo 6, o método que será apresentado privilegia resolver o cubo no menor tempo possível, entretanto é necessária a memorização de um número maior de macros.

Ao detalhar as 3 categorias veremos que é muito difícil conciliar os 3 quesitos em um único método, isto é, elaborar um método que resolva o cubo mágico com o menor número de movimentos, no menor tempo e utilizando poucas macros memorizadas. Na verdade, o que se observa é: quanto mais um quesito é privilegiado, menos os outros dois são.

Para os aficionados pelo Cubo Mágico são realizadas competições nacionais e mundiais[1]. Existem várias modalidades que vão desde resolver o cubo com os pés ou com os olhos vendados até outras que utilizam configurações diferentes do cubo ou até mesmo outros formatos que não são cúbicos. Entre elas podemos destacar duas: resolução no menor tempo e resolução no menor número de movimentos. A título de curiosidade atualmente (05/2016) os recordes mundiais são:

- Modalidade resolução no menor tempo:
  Lucas Etter (Estadunidense) – Campeonato realizado em Clarksville, Maryland, USA em 21 de novembro de 2015. Melhor resultado: 4,90 segundos.

[1]WCA – World Cube Association www.worldcubeassociation.org

- Modalidade resolução no menor número de movimentos:
  Marcel Peters (Alemão) – Campeonato realizado em Colônia, Alemanha em 9/10 de janeiro de 2016. Melhor resultado: 19 movimentos.

Para o desenvolvimento deste capítulo as principais referências foram [6] e [7].

## 5.1 Resolvendo o Cubo Mágico com o menor número de movimentos

Entre as 3 categorias, esta sem dúvidas é a mais complexa de todas e exige um conhecimento sobre o Cubo Mágico bastante aprofundado, assim como toda álgebra envolvida nele. Veremos que, para este método, há dois tipos de algoritmos: um realizado por computadores e outro realizável por humanos que seria uma adaptação do método efetuado por computadores, já que este é extremamente complexo e impossível de ser memorizado.

### 5.1.1 Método realizado por computador

É conhecido como Algoritmo de Deus (God's Algorithm) o algoritmo que resolve o Cubo Mágico com o menor número de movimentos possível. Demonstra–se que qualquer que seja a posição que o cubo está embaralhado, por pior que esteja, é possível resolvê–lo em um determinado número de movimentos ou menos. A este número é dado o nome de Número de Deus (God's Number), e atualmente seu valor é 20. Em geral este tipo de algoritmo só é possível de ser executado por um computador, pois sua memorização é extremamente complexa.

Conforme vimos no Capítulo 2, ele foi construído por Ernö Rubik em 1974. Sete anos depois, em julho de 1981, o inglês Morwen Thistlethwaite, então professor no Polytechnic of the South Bank, em Londres, foi o primeiro a elaborar um algoritmo capaz de resolver o cubo mágico em poucos movimentos, na verdade em não mais que 52 movimentos. Depois deste, outros métodos foram elaborados até chegarmos no número 20.

A maioria dos algoritmos conhecidos para resolver o cubo mágico seguem basicamente dois padrões:

- Resolver por camadas, uma a uma, primeiro a camada de baixo, depois a do meio e então a camada de cima;

- Ou então resolver primeiro todos os cubinhos de aresta para então resolver os cubinhos de canto.

Um dos motivos que torna o algoritmo de Thistlethwaite impressionante é o fato de ele não seguir nenhum destes dois padrões. Seu método consiste em resolver todos os cubinhos simultaneamente até que haja somente um movimento possível, que é justamente aquele que retorna o cubo à sua posição original, isto é, com todas as cores orientadas. Não faremos a demonstração deste método, entretanto vamos detalhar o princípio do algoritmo de Thistlethwaite.

A primeira ideia em que este método se baseia é nas inúmeras simetrias que o cubo de Rubik pode assumir. Ao manusear o cubo fica claro que podemos ter situações semelhantes que se diferem apenas pelas cores, por exemplo, com a face branca para cima, ter os cubinhos de arestas todos rotacionados apenas uma única vez, é o mesmo que ter esta mesma situação, porém com a face azul para cima. Neste caso, a sequência de movimentos que resolve uma situação é idêntica à sequência de movimentos que resolve a outra. Portanto, Thistlethwaite separou todas as simetrias em subgrupos. Para aplicar este método com o intuito de resolver o cubo mágico que se encontre embaralhado, tais simetrias somente poderiam ser observadas e identificadas a qual grupo pertencem, utilizando–se um computador, já que memorizá–las seria algo impossível. O método consiste de quatro estágios, cada qual possui um determinado grupo de simetrias. A cada grupo é somente permitida uma classe de movimentos de modo que com eles se atinja o próximo estágio. E assim, uma vez identificado em qual subgrupo o cubo mágico encontra–se, a ele é aplicado os movimentos necessários com o objetivo de passar de um estágio para o outro, até atingir o último estágio e retornar o cubo à identidade. Vejamos como são estes grupos:

Sejam os grupos

- $G_0 = \langle L, R, F, B, U, D \rangle$,
- $G_1 = \langle L, R, F, B, U^2, D^2 \rangle$,
- $G_2 = \langle L, R, F^2, B^2, U^2, D^2 \rangle$ e
- $G_3 = \langle L^2, R^2, F^2, B^2, U^2, D^2 \rangle$.

O objetivo é seguir a cadeia $G = G_0 \to G_1 \to G_2 \to G_3 \to I$. Esta sequência de $G_i$ até $G_{i+1}$ é feita utilizando apenas movimentos em $G_i$ que é o subgrupo onde o cubo se encontra. Em cada estágio a restrição de movimentos tem como consequência fixar determinadas condições dos cubinhos, como por exemplo, orientar todos os cubinhos de arestas apenas. Devido a este fato e às simetrias, podemos organizar em uma tabela, para cada estágio seus respectivos grupos, movimentos permitidos, números de elementos possíveis, isto é, todas as possíveis combinações que o cubo pode assumir para aquele grupo e um fator, que é definido pelo número de repetições que cada estágio gera, isto é, a ordem do grupo. Vejamos a tabela 5.1 que representa estas condições.

Tabela 5.1: Grupos do algoritmo de Thistlethwaite

| Grupo | Movimentos | Número de posições | Fator |
|---|---|---|---|
| $G_0$ | $L, R, F, B, U, D$ | $4,33 \cdot 10^{19}$ | $2^{11} = 2048$ |
| $G_1$ | $L, R, F, B, U^2, D^2$ | $2,11 \cdot 10^{16}$ | $3^7 \cdot \binom{12}{4} = 1082565$ |
| $G_2$ | $L, R, F^2, B^2, U^2, D^2$ | $1,95 \cdot 10^{10}$ | $2 \cdot 3 \cdot \binom{8}{4}^2 = 29400$ |
| $G_3$ | $L^2, R^2, F^2, B^2, U^2, D^2$ | $6,63 \cdot 10^5$ | $\frac{4!^5}{12} = 663552$ |

Por exemplo, no grupo $G_0$ o número de posições são todas as possibilidades possíveis que o cubo pode assumir e que foi demonstrada no Capítulo 4. Neste caso, o fator é obtido considerando que os cubinhos de aresta serão todos orientados corretamente e, portanto somente estes é que serão permutados. Como cada um deles possui 2 cores e pela paridade somente 11 dos 12 cubinhos poderão ter suas 2 cores alternadas, logo chegamos ao valor $2^{11}$, que seria o pior caso onde todos os cubinhos precisariam ser orientados corretamente. Para os demais grupos o raciocínio é análogo, exceto pelas restrições de movimentos particulares de cada um deles. Cada estágio do algoritmo é baseado em tabelas[2] que mostram a sequência de permutação de cada elemento do subgrupo em que o cubo mágico se encontra.

### 5.1.2 Método realizável por humanos

Em 2003 um australiano chamado Ryan Heise conseguiu construir um método de resolução que tornou o algoritmo de Thistlethwaite adaptado a nós humanos. De todos os métodos conhecidos, este sem dúvidas é o mais eficiente, porém o mais complexo. Seu princípio está baseado em um profundo conhecimento do cubo mágico, o que o torna um método intuitivo e com poucas memorizações. O resultado é que com poucos movimentos se chega à resolução do cubo mágico. Este método também se baseia em 4 etapas. Na primeira os cubinhos são montados de forma a se ter 4 quadrados[3]. Na

[2] Vide referência [7]

[3] Aqui considera–se um quadrado a configuração 1x2x2

segunda etapa os quadrados são rearranjados de modo a orientar os cubinhos de aresta que os compõem. Na terceira etapa se orienta o cubinhos de arestas restantes e mais 2 cubinhos de canto quaisquer. Na quarta e última etapa os últimos 3 cubinhos de canto restantes são orientados corretamente através de comutadores. É na 3ª etapa que encontramos a complexidade deste método, pois a liberdade de movimentos é bastante diminuída, afinal o principal objetivo é não se desmontar aquilo que já está montado. Por ser um método que não prevê formas pré–determinadas, a cada vez que se inicia a resolução, diferentes configurações são obtidas. Por esta razão se torna necessário analisar muito bem como o cubo está antes de se realizar qualquer movimento e, portanto não é um método que visa a resolução do cubo no menor tempo possível.

## 5.2 Resolvendo o Cubo Mágico no menor tempo

De todos os métodos que procuram otimizar o tempo, o mais eficiente é o que foi proposto pela tcheca Jessica Fridrich no início dos anos 80. É conhecido como método $CFOP$, pois são as siglas, em inglês, de cada uma de suas 4 etapas: $C$ = Cross, $F = F2L$ (first 2 layers), $O = OLL$ (Orientation of Last Layer) e $P = PLL$ (Permutation of Last layer). A primeira etapa tem como objetivo deixar corretamente orientado os 4 cubinhos de aresta de uma determinada face escolhida, formando assim uma "cruz". Na segunda etapa o objetivo é orientar os 4 cubinhos de canto desta face escolhida juntamente com os cubinhos de aresta, adjacentes a cada um deles, da camada mediana em suas corretas orientações. Isto é feito em 4 partes, uma de cada vez, unindo–se o cubinho de canto com o seu respectivo cubinho de aresta adjacente da camada mediana e os coloca em suas posições corretas e já orientados. Ao final desta etapa já se obtém 2 camadas prontas. A terceira etapa tem como objetivo apenas orientar a face oposta àquela escolhida no início, sem se preocupar em deixar pronta a terceira camada, que é o que será feito no último passo. Na quarta etapa o objetivo é permutar os cubinhos, tanto de aresta quanto de canto da última camada de modo a colocá–los em suas posições corretas. A figura 5.1 ilustra a sequência de montagem de cada uma das 4 etapas.

Ao seguir este algoritmo, após a 1ª etapa, observa–se um conjunto relativamente pequeno de casos que sempre se repetem, isto é, existe um padrão. Para cada caso o método prevê uma sequência de movimentos específica, de modo a se atingir a próxima etapa. Por esta razão este método torna–se possível de ser memorizado e, portanto de rápida execução. Foi utilizando este método que se obteve o atual recorde mundial de montagem mais rápida do cubo mágico, de 4,90 segundos. A tabela 5.2 mostra o número de casos que cada etapa apresenta.

Embora este método traga o benefício da velocidade, é necessária a memorização

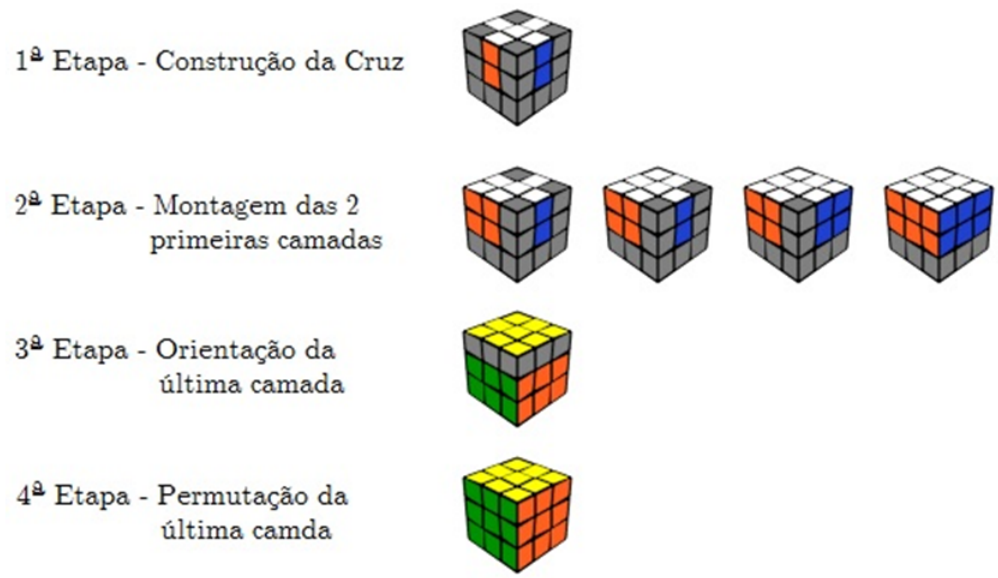


Figura 5.1: Sequência de montagem de cada uma das 4 etapas.

Tabela 5.2: Etapas do método de Fridrich

| Etapa | Número de casos |
|---|---|
| 1ª Etapa – Cross | intuitivo |
| 2ª Etapa – F2L | 41 |
| 3ª Etapa – OLL | 57 |
| 4ª Etapa – PLL | 21 |

de dezenas de sequências diferentes uma para cada caso.

## 5.3 Resolvendo o Cubo Mágico com a menor memorização

Invariavelment,e ao se manipular o cubo mágico na tentativa de resolvê–lo, algumas sequências acabam sendo memorizadas, devido à sua repetição. Entretanto, através do entendimento do funcionamento do cubo e de suas regras, algumas sequências tornam–se intuitivas, que é o caso dos comutadores e conjugados. É possível portanto, elaborar uma estratégia de resolução do cubo de Rubik apenas utilizando tais sequências. É o que iremos propor a seguir como uma proposta de resolução do cubo mágico com a menor memorização possível. Para isto utilizaremos alguns dos comutadores e conjugados analisados no Capítulo 4.

Nossa estratégia terá 5 etapas. Na primeira escolheremos uma face para iniciar, e nela posicionar e orientar os cubinhos de aresta formando a "cruz" vista no método de Fridrich. Na segunda etapa iremos posicionar e orientar os quatro cubinhos de aresta que pertencem à intersecção da camada mediana com as faces adjacentes àquela escolhida na primeira etapa. Na terceira etapa iremos posicionar e orientar os cubinhos de aresta da face oposta àquela escolhida na primeira etapa. Ao final desta etapa observaremos a formação da "cruz" em todas as seis faces do cubo. Na quarta etapa iremos apenas posicionar os cubinhos de canto, para então na quinta e última etapa orientar todos eles. Ao final desta etapa teremos o cubo resolvido. Vamos agora detalhar cada uma das etapas.

### 5.3.1 1ª Etapa: formar uma cruz na face inicial

Primeiramente escolhemos uma face para iniciar e recomenda–se escolher sempre a mesma de modo a facilitar a repetição do método. Uma sugestão é iniciar pela face branca, entretanto tal escolha não implica na perda de generalidade do método. Para formar a cruz, não há nenhuma sequência em especial, e para atingi–la é possível utilizar apenas a simples intuição.

### 5.3.2 2ª Etapa: formar uma cruz nas faces adjacentes

Para resolver a segunda etapa iremos sempre deixar para frente uma das 4 faces adjacentes àquela escolhida no início e será nela que iremos orientar os cubinhos $RF$ ou $LF$. Por exemplo, vamos escolher o cubinho laranja/verde para colocar em sua posição e orientação correta. Se ele estiver na face superior iremos observar qual das duas cores está na face frontal. Caso seja a laranja, então iremos posicioná–lo em $UF$ na face laranja. Caso seja a verde, de modo análogo, então iremos posicioná–lo em UF na face verde. Se a posição correta dele for em RF então aplicaremos a macro $U'F'UF$. Caso contrário, se a posição correta dele for em $LF$ então aplicaremos a macro $UFU'F'$. Mas caso ele esteja na camada mediana com a posição e/ou orientação errada basta aplicar qualquer uma das macros anteriores para movê–lo à camada superior. O processo se repetirá até que os quatro cubinhos de aresta da camada mediana estejam em suas posições e orientações corretas.

### 5.3.3 3ª Etapa: formar uma cruz na face oposta à inicial

Para esta etapa, como referência, deixaremos voltada para a frente a face oposta àquela escolhida no início. O objetivo será deixar os 4 cubinhos de aresta desta face em suas posições e orientações corretas. Primeiramente devemos deixar todos os quatro cubinhos orientandos corretamente, isto é, com suas cores correspondentes à face frontal, voltadas para frente. No caso de nossa sugestão deveremos deixar todos os quatro cubinhos com suas cores amarelas voltadas para frente. Para isso iremos utilizar a macro $(RU'R'U)(F'UFU')$. Esta macro irá permutar a orientação dos cubinhos que estão em $UF$ e $RF$. Uma vez orientados iremos posicioná–los corretamente utilizando a macro $(U'F')(U'F)(U'F')(U'F)U'$. Esta macro irá permutar a posição dos cubinhos que estão em $UF$ e $RF$. Ao final desta etapa observaremos a formação da "cruz" em todas as seis faces do cubo.

### 5.3.4 4ª Etapa: posicionar os cubinhos de canto

Nesta etapa iremos permutar os cubinhos de canto de modo a apenas posicioná-los corretamente sem nos preocupar com suas orientações. As macros para esta etapa permutam, tanto no sentido horário quanto no sentido anti–horário, 3 cubinhos de canto da face superior que estão em $FLU$, $FRU$ e $BRU$, sem preservar suas orientações. Para isto iremos sempre observar quais 3 cubinhos devem ser permutados de modo a serem posicionados corretamente. Uma vez entendido quais cubinhos de canto serão afetados pela macro e quais necessitam ser permutados aplicaremos os seguintes comutadores: $R'(ULU')R(UL'U')$ para o sentido horário ou $(ULU')R'(UL'U')R$ para o sentido anti-horário. O processo se repetirá até que todos os cubinhos de canto estejam corretamente posicionados. Note que não é necessário memorizar as duas macros, uma vez que para ter o efeito de uma basta aplicar a outra duas vezes.

### 5.3.5 5ª Etapa: orientar os cubinhos de canto

Nesta última etapa, utilizaremos dois conjugados que permutam a orientação dos cubinhos que estão em $FLU$ e $FRU$. De acordo com o capítulo anterior, devido à paridade, toda vez que permutamos a orientação do cubinho em $FLU$ no sentido horário, a orientação do cubinho em FRU também tem sua orientação permutada, porém no sentido anti-horário e vice-versa. As macros para esta etapa são as seguintes: Rotacionar o cubinho em $FLU$ no sentido horário é $(LD^2L'F'D^2F)U(F'D^2FLD^2L')U'$ e rotacionar o cubinho em $FLU$ no sentido anti-horário é $(F'D^2FLD^2L')U'(LD^2L'F'D^2F)U$. O processo se repetirá até que todos os cubinhos de canto estejam corretamente orientados. Note que não é necessário memorizar as duas macros, uma vez que para ter o efeito de uma basta aplicar a outra duas vezes.

### 5.3.6 Resumo

No sentido de facilitar a visualização do método, a tabela abaixo resume cada uma de suas etapas, seus objetivos e as macros que são necessárias.

Tabela 5.3: Etapas, objetivos e as macros necessárias.

| Etapa | Objetivo | Macros |
|---|---|---|
| 1ª etapa | Formar uma cruz em uma das faces. | intuitivo |
| 2ª etapa | Organizar os 4 cubinhos de aresta, na camada mediana, das faces adjacentes àquela escolhida na 1ª etapa. | $U'F'UF$ ou $UFU'F'$ |
| 3ª etapa | Organizar os cubinhos de aresta da face oposta àquela escolhida na 1ª etapa, formando uma cruz em todas as seis faces do cubo mágico. | $(RU'R'U)(F'UFU')$ ou $(U'F')(U'F)(U'F')(U'F)U'$ |
| 4ª etapa | Posicionar corretamente todos os 8 cubinhos de canto | $R'(ULU')R(UL'U')$ ou $(ULU')R'(UL'U')R$ |
| 5ª etapa | Orientar corretamente todos os 8 cubinhos de canto | $(LD^2L'F'D^2F)U(F'D^2FLD^2L')U'$ ou $(F'D^2FLD^2L')U'(LD^2L'F'D^2F)U$ |

Este método apresenta poucas macros, que por sua vez, são intuitivas. Contudo em cada etapa, de maneira geral, será necessário repetir cada macro diversas vezes, o que torna o método lento e com muitos movimentos.

# 6 Aplicação Escolar

Neste capítulo iremos apresentar, aos docentes, uma proposta didática que consiste de um método básico para resolver o cubo mágico, por exemplo, em sala de aula, já que muito provavelmente os estudantes são leigos em sua resolução. A ideia mais importante para quem esteja começando é manipular o cubo individualmente. A familiaridade é imprescindível, sempre com o objetivo de se compreender o mecanismo do cubo, isto é, como girar as faces e mover apenas um cubinho para uma determinada posição e orientação como se queira.

Devido ao fato de que é necessário uma boa abstração e noções espaciais, aconselha-se que esta proposta seja aplicada a partir do 6º Ano do Ensino Fundamental II. Muito embora não seja raro se deparar com crianças com idade inferior a 11 anos que saibam resolver o cubo mágico rapidamente.

## 6.1 Apresentação e funcionamento do cubo mágico

Apresente aos alunos as 6 faces e como são seus movimentos, tanto no sentido-horário quanto no sentido anti-horário. Diferencie os 3 tipos de cubinhos e mostre que o cubinho central determina a cor da face, e que há um padrão em relação às faces opostas: a face branca é sempre oposta à amarela, assim como a azul é oposta à verde e a laranja é oposta à vermelha. Nesta etapa deixe livremente os alunos manipularem o cubo para que eles mesmos possam criar suas hipóteses e assim compreenderem melhor o seu funcionamento.

## 6.2 Códigos de cada movimento

Apresente aos alunos as nomenclaturas tanto das faces quanto dos cubinhos. Aqui é importante ressaltar o padrão que é adotado aos códigos das faces bem como seus movimentos. Explique, por exemplo, que girar a face direita no sentido horário é feita neste sentido, porém em relação a alguém que a olharia de frente, e não em relação a quem está manipulando o cubo. Por conta deste padrão, mostre a importância de segurar o cubo corretamente, principalmente durante a execução das macros. Rotacionar o cubo durante uma sequência de movimentos seguramente acarretará em obter um resultado diferente do esperado. Uma vez entendido como são realizados os códigos em cada face do cubo é que pode-se passar para a sua resolução propriamente dita.

## 6.3 Resolução do Cubo Mágico pelo método de camadas

Este algoritmo pode ser usado sem a necessidade de se compreender o significado de cada movimento durante a execução das macros. Por conta disso, dizemos que um método quase que totalmente mecânico, exceto pela 1ª etapa que exige a intuição para concluí-la. O restante das etapas torna-se um processo memorizado.

### 6.3.1 Etapa 1: Formar uma cruz branca

Nesta primeira etapa o objetivo é alcançar, com a face branca voltada para cima, uma cruz, conforme a figura 6.1.

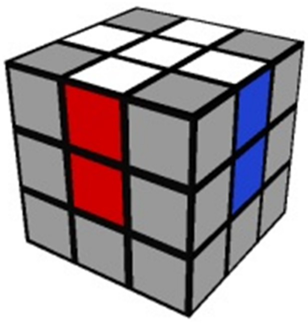

Figura 6.1: Objetivo da Etapa 1.

Oriente os alunos a manterem sempre a face branca para cima, e escolherem entre as faces vermelha, azul, verde ou laranja para ficaram voltadas para frente. A ideia é posicionar os cubinhos de aresta correta um de cada vez.

### 6.3.2 Etapa 2: Posicionar os cantos brancos

O objetivo desta etapa é organizar a 1ª camada, posicionando os cubinhos de canto corretamente, conforme a figura 6.2.

Ainda com a face branca voltada para cima, os cubinhos de canto devem ser posicionados um de cada de vez. Por exemplo, vamos iniciar pelo cubinho branco, vermelho

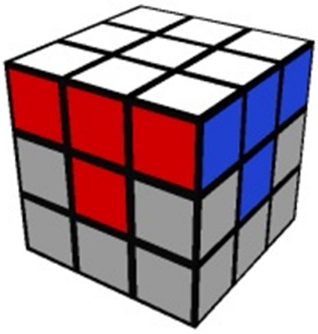

Figura 6.2: Objetivo da Etapa 2.

e azul. O cubinho que estamos procurando pode estar na face debaixo, e neste caso devemos posicioná-lo na aresta que é o encontro das 3 cores que estamos querendo posicionar, utilizando apenas os movimentos $D$ ou $D'$. As possibilidades são mostradas na figura 6.3.

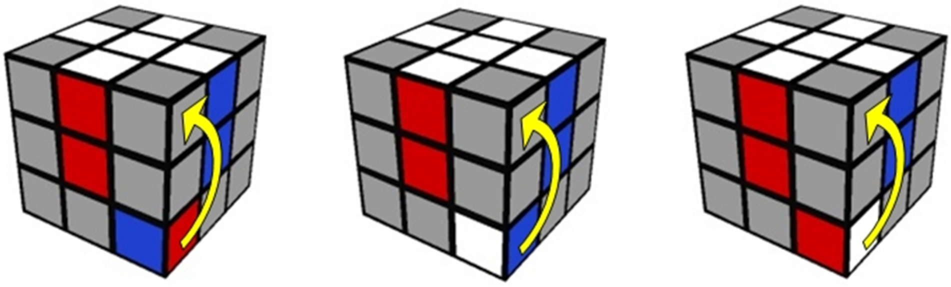

Figura 6.3: Possibilidades da Etapa 2 – cubinhos na camada debaixo.

Para levar o cubinho ao seu local correto repita, quantas vezes for necessário (no máximo 3), a seguinte macro: $R'D'RD$.

Caso o cubinho procurado não esteja na face debaixo, então ele estará na face superior, isto é, em algum dos 4 cantos da face branca, conforme a figura 6.3

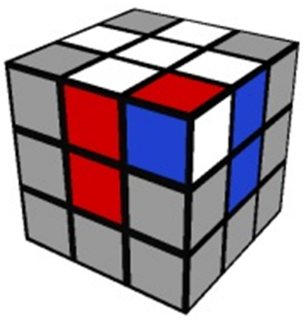

Figura 6.4: Possibilidades da Etapa 2 – cubinhos na camada superior.

Para levá-lo à camada debaixo, basta aplicar a macro: $R'D'R$. Uma vez que ele esteja na face debaixo aplicar a macro $R'D'RD$. Repetir o mesmo processo para os 4 cubinhos de canto.

### 6.3.3 Etapa 3: Resolver a camada do meio

A partir desta etapa deixaremos a face branca voltada para baixo e então o objetivo será resolver a camada mediana, posicionando corretamente os 4 cubinhos de aresta, conforme a figura 6.5.

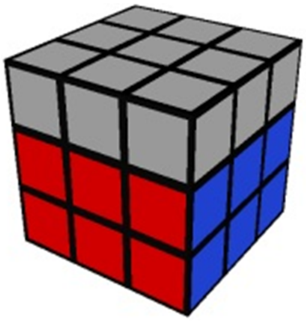

Figura 6.5: Objetivo da Etapa 3.

Da mesma forma que na etapa anterior, os 4 cubinhos de aresta serão posicionados um de cada vez. Vamos iniciar, por exemplo, com a face vermelha voltada para frente. Logo os 2 cubinhos de aresta que iremos posicionar são o vermelho/azul e o vermelho/verde. Estes cubinhos podem estar na face superior, neste caso aplicamos apenas o movimento $U$ para posicioná-los na face da frente e assim teremos os seguintes casos, conforme a figura abaixo:

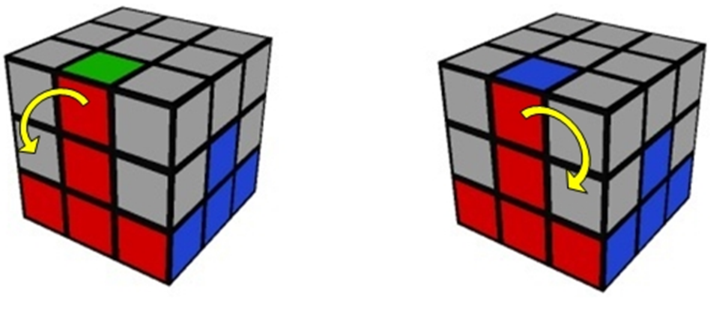

Figura 6.6: Possibilidades da Etapa 3.

Para cada caso as macros são:

- Caso 1: $(U'L'UL)(UFU'F')$
- Caso 2: $(URU'R')(U'F'UF)$

Entretanto, caso o cubinho já esteja na camada mediana, porém orientado incorretamente, então posicione um cubinho da face amarela no local correto e aplique um dos dois casos, pois assim este irá permutar com o cubinho desejado, levando-o para a face superior. Repetir o mesmo processo até posicionar os 4 cubinhos de aresta na camada mediana corretamente

### 6.3.4 Etapa 4: Formar uma cruz amarela

O objetivo desta etapa é formar uma cruz amarela na face superior. Para isto basta aplicarmos a macro $FURU'R'F'$. Pode ser necessário repeti-la até 3 vezes, dependendo da configuração que o cubo se encontra, que são as representadas na figura 6.7.

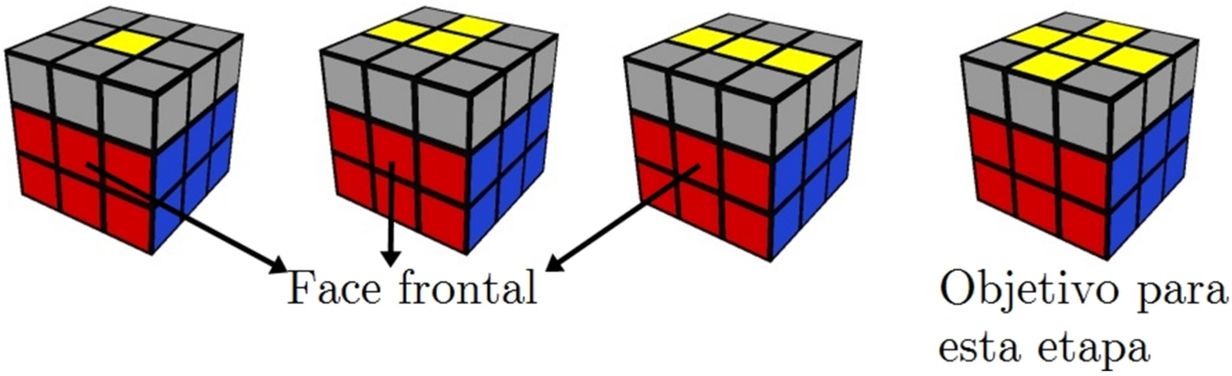


Figura 6.7: Possibilidades e objetivo da Etapa 4.

### 6.3.5 Etapa 5: Resolver a camada superior

Ao final desta etapa teremos a face amarela orientada. Para isto iremos somente aplicar o movimento U para deixar o cubo em uma das seguintes possibilidades, conforme a figura 6.8.

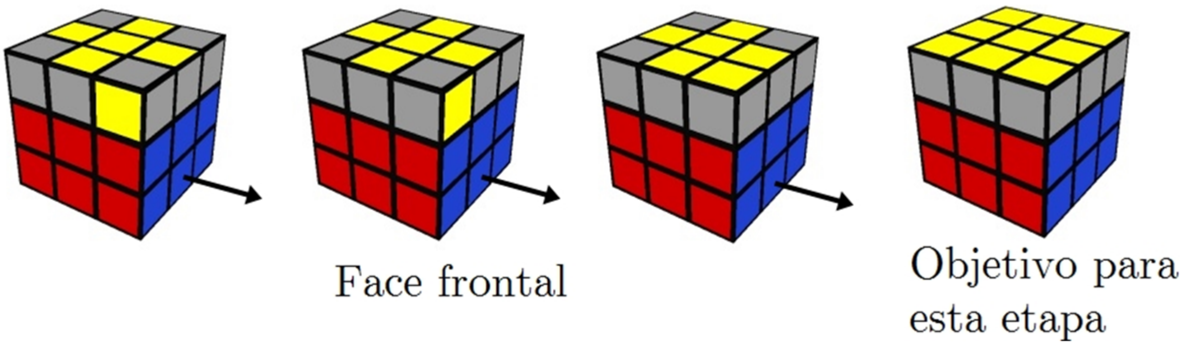


Figura 6.8: Possibilidades e objetivo da Etapa 5.

A macro para esta etapa é: $RUR'URU^2R'$. Se o objetivo não for atingido, então devemos repeti-la. Porém, antes devemos, utilizando o movimento U, deixar a face superior em uma destas 3 configurações para então executá-la novamente. Repita o processo até atingir o objetivo para esta etapa.

### 6.3.6 Etapa 6: Orientar os cubinhos de canto da camada superior

Para esta etapa devemos procurar 2 cubinhos de canto, que estejam com as mesmas cores, e deixar esta face para frente, utilizando apenas o movimento $U$. Podemos ter tanto a cor do cubinho de aresta, entre os 2 cubinhos de canto, com a mesma cor deles ou não, conforme a figura 6.9.

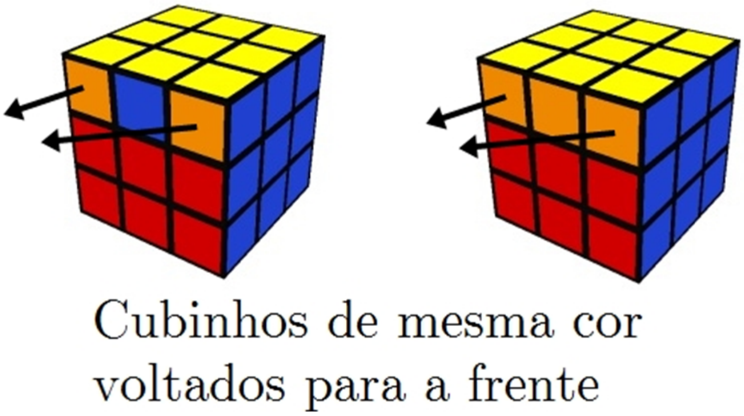


Figura 6.9: Possibilidades da Etapa 6.

Alcançada esta configuração, a macro é: $RB'RF^2R'BRF^2R^2$. Caso não haja dois cubinhos com estas características, então basta aplicar esta macro em qualquer face voltada para frente. Após esta execução haverá ao menos 2 cubinhos com a mesma cor na mesma face. Ao término desta etapa, os 4 cubinhos de canto da camada superior estarão orientados corretamente.

### 6.3.7 Etapa 7: Posicionar os cubinhos de aresta da camada superior

Nesta etapa podemos ter 3 ou 4 cubinhos de aresta a serem posicionados corretamente. A macro $RU'RURURU'R'U'R^2$ permuta apenas 3 cubinhos de aresta, deixando o quarto cubinho, que está posicionado na face de trás, inalterado. Portanto, utilizando o movimento $U$, posicione a face que já está pronta para trás antes de aplicar a macro desta etapa. Caso não haja nenhuma face montada, execute a sequência uma vez, e então teremos ao menos uma face já com a cor correta. É possível que para orientar os 3 cubinhos de aresta em suas posições corretas, seja necessário utilizar a macro por 2 vezes.

Ao final de todas as etapas o cubo mágico estará montado.

Algo que pode atrair ainda mais a atenção dos alunos para se aventurarem no desafio de resolver o cubo mágico, é sugerir uma gincana entre eles, para ver quem consegue resolver o cubo mágico. Ou até mesmo, dentre aqueles que já conseguem resolver, uma gincana para ver quem resolve o cubo mágico mais rápido.

# Referências


[1] TRAVIS, M. *The Mathematics of the Rubik's Cube.* University of Chicago, 2007.

[2] LEQUAIN, Y.; GARCIA, A. *Elementos de álgebra.* 5. ed. Rio de Janeiro: IMPA, 2010.

[3] DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna.* 4. ed. São Paulo: Atual, 2003.

[4] CHEN, J. *Group Theory and the Rubik's Cube.* Harvard, 2004.

[5] SCHULTZER, W. *Aprendendo Álgebra com o Cubo Mágico.* DM - UFSCar, 2005.

[6] TRONTO, S. *Fewest Moves Tutorial.* 01 2016.

[7] THISTLETHWAITE, M. B. *The 45-52 move strategy.* Polytechnic of the South Bank, 1981.