UNIVERSIDADE FEDERAL DO PARÁ

INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
FACULDADE DE MATEMÁTICA

RAFAEL WESLLEY BARBOSA LEITE

UMA ABORDAGEM DA TEORIA COMBINATÓRIA DE GRUPOS APLICADA NO CUBO DE RUBIK $3 \times 3 \times 3$

Belém

2022

RAFAEL WESLLEY BARBOSA LEITE

UMA ABORDAGEM DA TEORIA COMBINATÓRIA DE GRUPOS APLICADA NO CUBO DE RUBIK $3 \times 3 \times 3$

Trabalho de Conclusão de Curso, apresentado à Faculdade de Matemática do Instituto de Ciências Exatas e Naturais da Universidade Federal do Pará como requisito básico para a obtenção do título de Licenciado em Matemática.

Orientador(a) Prof(a) Juliana Silva Canella.

Belém

2022

RAFAEL WESLLEY BARBOSA LEITE

UMA ABORDAGEM DA TEORIA COMBINATÓRIA DE GRUPOS APLICADA NO CUBO DE RUBIK $3 \times 3 \times 3$

Trabalho de Conclusão de Curso, apresentado à Faculdade de Matemática do Instituto de Ciências Exatas e Naturais da Universidade Federal do Pará como requisito básico para a obtenção do título de Licenciado em Matemática.

Data da Apresentação: 20 de dezembro de 2022

Prof. Dra. Juliana Silva Canella (Orientadora)
Faculdade de Matemática, UFPA

Documento assinado digitalmente
gov.br IRENE CASTRO PEREIRA
Data: 22/12/2022 11:36:34-0300
Verifique em https://verificador.iti.br

Prof. Dra. Irene Castro Pereira (Membro)
Faculdade de Matemática, UFPA

Prof. Dr. Marcel Vinhas Bertolini (Membro)
Faculdade de Matemática, UFPA

Dedico este trabalho à minha mãe.

AGRADECIMENTOS

Gostaria de agradecer primeiramente à minha mãe, Adriana Barbosa, que desde cedo me apoiou nos estudos, e dizer que esse seu gesto foi essencial para que eu conseguisse chegar onde cheguei, e também por eu ter me tornado quem eu me tornei.

À minha namorada, Aryana Barros, por ter compreendido todas as minhas ausências durante esse processo, e por ter me dado forças para que eu não desistisse. Obrigado por tudo!

À minha orientadora Juliana Canella, que desde a iniciação científica sempre se mostrou uma pessoa muito dedicada. Obrigado pela paciência quando tive dificuldades, pelas conversas aleatórias durante as orientações, e pelas (milhares de) correções nesse trabalho. Obrigado também poder ter acreditado em mim.

Também gostaria de agradecer aos amigos que fiz durante essa jornada e que me ajudaram a chegar ao fim dela. Não citarei nomes para não acabar sendo injusto, mas saibam que todos que fizeram parte disso têm um lugar especial no meu coração. Obrigado por todas as conversas, questões resolvidas, madrugadas em claro, e também pela companhia, foi muito importante para mim.

Agradeço os ensinamentos recebidos de todos os professores da graduação, especialmente Tânia Begazo, Rogélio Guzman, Alex Sierra, Irene Castro, Marcel Vinhas e Valter Borges.

À UFPA pela oportunidade de estudar nessa maravilhosa instituição, e também a todas as outras pessoas que contribuíram para que esse meu sonho se realizasse.

Eu não vim nessa terra pra não morrer de amor.

Hélio Flanders

RESUMO

Este trabalho tem como objetivo mostrar como a Teoria de Grupos pode ser utilizada para ajudar a entender e descrever a estrutura do cubo de Rubik como um objeto matemático. Para tanto, faremos um estudo detalhado das simetrias deste quebra cabeça, e mostraremos que o mesmo pode ser resolvido de modo puramente algébrico. Além disto, discutiremos sobre o Grupo de Rubik, alguns dos seus subgrupos e resolução possível ou impossível associado a movimentos ilegais. Por fim, apresentaremos métodos computacionais para auxiliar na análise de suas propriedades.

PALAVRAS-CHAVE: Teoria de Grupos, Teoria Combinatória de Grupos, Simetrias, cubo de Rubik, GAP.

ABSTRACT

This work aims to show how Group Theory can be used to help understanding and describing the structure of the Rubik's Cube as a mathematical object. Therefore, we will make a detailed study of the symmetries of this puzzle, and we will show that it can be solved purely algebraically. In addition, we will discuss Rubik's group, some of its subgroups, possible or impossible resolution associated with illegal movements. Finally, we will present computational methods to assist in the analysis of its properties.

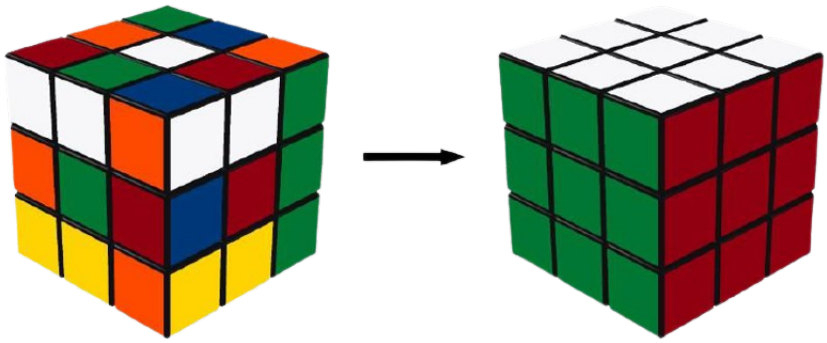
KEY WORDS: Group Theory, Combinatorial Group Theory, Symmetries, Rubik's Cube, GAP.

Sumário

Introdução

O cubo de Rubik, popularmente conhecido como *cubo Mágico*, é um quebra cabeças tridimensional inventado e patenteado pelo arquiteto húngaro Ernõ Rubik, [12], que ironicamente não possui formação Matemática, mesmo que sua criação tenha contribuído para o desenvolvimento desta. O objetivo deste quebra cabeças consiste em manipular suas faces de modo que, ao final, todas as faces do cubo estejam com a mesma cor, como podemos ver abaixo:

Figura 1: Objetivo do cubo Mágico



Fonte: Freepik

O cubo mágico, desde a década de 80, é considerado um dos *puzzles* mais vendidos do mundo[1], encantando pessoas de todas as idades. Por conta da sua popularidade, nos dias de hoje, existem competições no mundo em diversas modalidades, buscando resolver o cubo com menos movimentos ou em menor tempo. Segundo a *World Cube Association*[2], WCA, na modalidade de tempo único, o melhor tempo obtido em uma resolução, até a presente data, pertence ao chinês Yusheng Du, com incríveis 3.47 segundos.

[1] Acesso em https://www.rediscoverthe80s.com/2020/01/

[2] Acesso em https://www.worldcubeassociation.org/results/records

Desde sua criação, não demorou muito para que matemáticos percebessem a complexidade desse simples objeto, fato esse corroborado pela existência, na mesma década, de trabalhos publicados a respeito de um tratado matemático sobre o cubo mágico, [1], que analisa a estrutura deste cubo utilizando a Teoria de Grupos.

O estudo de grupos remonta ao século XIX, principalmente pelo matemático francês Evariste Galois que, [5], utilizou pela primeira vez o termo *grupo* para descrever o conjunto de todas as funções bijetoras definidas sobre um conjunto finito fixo, munido de uma operação de composição entre funções. Porém, foi o britânico Arthur Cayley, em [4], quem definiu primeiro o conceito de grupo como conhecemos na Álgebra Moderna, que diz que um grupo é um conjunto não vazio munido de uma operação binária satisfazendo certas condições, chamadas axiomas de grupo. Portanto, temos que o que Galois entendia informalmente como um grupo, de modo geral, era um caso particular dessa estrutura conhecida por *grupo de permutações*. Um resultado importante, obtido em 1830 por Galois, [5], diz que uma equação polinomial pode ser associada a algum grupo de permutações e a existência de solução algébrica desta equação depende integralmente da estrutura deste grupo. Por exemplo, é impossível resolver equações polinomiais de grau $n \geq 5$ por meio de radicais, e, por [7], podemos constatar que o grupo S_n com $n \geq 5$ não possui uma série derivada que termina no grupo trivial, e portanto, não é *solúvel*. Isto não é coincidência. O estudo das equações algébricas foi apenas o pontapé para a criação deste ramo da Matemática. No entanto, houve também contribuições para outros ramos dela, como por exemplo, para a Teoria dos Números e a Geometria. Se destacaram nesta contribuição estudiosos como Gauss, Lagrange, Poincaré, entre outros [13].

Uma parte da Teoria de Grupos se dedica em estudar simetrias, e por este motivo, pode ser aplicada em diversas áreas do conhecimento, desde Engenharias, Ciências Naturais, até mesmo em outros ramos da própria Matemática, como os grupos de Lie, que podem ser ferramenta para resolver certas equações diferenciais. Podemos aplicar também esta teoria para analisar o famoso *cubo de Rubik*, especificamente o cubo $3 \times 3 \times 3$. Este trabalho se propõe a estudar suas propriedades algébricas, bem como métodos computacionais para discuti-las.

Para tanto, dividimos essas discussões em 4 capítulos: o primeiro capítulo contém noções básicas para o desenvolvimento da Teoria Combinatória de Grupos, como grupos livres,

apresentações de grupos e exemplos, bem como diferentes tipos de produtos entre grupos. O segundo capítulo se destina a estudar grupos de permutações dada importância para a construção do grupo do cubo mágico e sua relação entre qualquer grupo. O terceiro capítulo é dedicado a dedução do *cubo de Rubik* $3\times\times3\times3$, $\mathcal{R}$: sua estrutura física, macros, orientações e como os movimentos legais e ilegais afetam a estrutura deste objeto. A partir desses conceitos, estabelecemos uma conexão entre o cubo de Rubik e os grupos de permutações finalizando com alguns de seus subgrupos. No capítulo 4, dedicado a *software* livre GAP na análise do cubo mágico, identificamos alguns dos subgrupos de $\mathcal{R}$, checamos algumas identidades e além de um método para resolver o cubo do ponto de vista computacional, mostrando assim o potencial do *software* na resolução de problemas envolvendo a Teoria Combinatória de Grupos.

Capítulo 1

Teoria Combinatória de Grupos

A teoria combinatória de grupos tem como principal objeto de estudo os chamados grupos livres e as apresentações de grupos via suas relações e seus geradores, esta última introduzida pela primeira vez em 1882 pelo matemático Walther Von Dyck em [19]. Esta teoria está repleta de problemas que, em geral, não possuem uma solução, ou são muito difíceis de resolver, como por exemplo o famoso Problema da Palavra, que busca saber quando duas palavras em um grupo representam o mesmo elemento, ou seja, são equivalentes. Outros problemas conhecidos da teoria combinatória de grupos são o Problema do Isomorfismo de Grupos e o Problema da Conjugação.

Em [14], vemos que a teoria combinatória de grupos tem suas raízes na topologia, tanto que as primeiras contribuições fortes dadas a esta área vieram de matemáticos como Poincaré, Tietze, Max Dehn, etc, todos topólogos. Isso acontece porque em alguns dos problemas de topologia, grupos definidos a partir de seus geradores e relações satisfeitas por estes geradores aparecem de forma bastante natural, como por exemplo no estudo do grupo fundamental $\pi_1(X)$ introduzido por Poincaré, em [15], temos que o grupo fundamental de uma superfície compacta orientável de gênero g pode ser definido a partir de geradores e relações, ou também quando calculamos o grupo fundamental do complemento de um nó em $\mathbb{R}^3$, via apresentação de Wirtinger [17], obtemos novamente um grupo definido a partir de seus geradores e suas relações. O termo "combinatória"é proveniente de que muitas vezes são utilizados métodos combinatórios para resolver problemas que permeiam esta área, métodos estes que são muito úteis do ponto de vista de cálculos que podem ser feitos especialmente no estudo dos grupos finitamente apresentados.

1.1 Preliminares

Nesta seção apresentaremos a definição de grupo qualquer e alguns produtos entre grupos que são importantes para o desenvolvimento deste trabalho, a saber, produtos diretos, semidiretos e entrelaçado entre grupos. Tais conceitos serão úteis para discutir a decomposição do grupo de Rubik e auxiliar na determinação de alguns de seus subgrupos como seu centro.

Os resultados desta seção podem ser encontrados em [6] e [8].

Definição 1 *Um conjunto G munido com uma operação binária*

$$G \times G \longrightarrow G$$
$$(a, b) \longmapsto ab$$

é definido como um ***grupo*** *se satisfaz as seguintes propriedades:*

1. *Associatividade:* $a(bc) = (ab)c, \ \forall\, a, b, c \in G$.
2. *Existência de um único elemento neutro* e: $\exists!\ e \in G$ *tal que* $ea = ae = a, \ \forall a \in G$.
3. *Existência de inversos:* $\forall a \in G, \exists\ b \in G$ *tal que* $ab = ba = e$.

Definição 2 *Seja $H \subset G$, G grupo. Se H é um grupo sob a mesma operação binária de G, dizemos que H é um* ***subgrupo*** *de G. Denota-se por $H \leq G$.*

Exemplo 1 *G e $\{e\}$ são subgrupos imediatos de G, também conhecidos como subgrupos triviais.*

Definição 3 *Dizemos que a* **ordem** *de um elemento x de um grupo G é n, se n é o menor inteiro positivo tal que $x^n = \underbrace{x\ x\ \ldots\ x}_{n\ \ vezes} = e$. A* **ordem** *de um grupo G é a sua cardinalidade, ou seja, a quantidade de elementos (distintos) que um grupo possui. Se um grupo G tem ordem finita, então todos os seus elementos x tem ordem finita. Denotamos a ordem n de um elemento x por $o(x) = n$ e a ordem (cardinalidade) m de um grupo por $|G| = m$, e caso este seja infinito, denotamos $|G| = \infty$.*

Definição 4 *Um subgrupo H de um grupo G é dito* ***normal*** *quando $xH = Hx$, $\forall x \in G$, denotado por $H \lhd G$.*

A importância dos subgrupos normais está no fato de que se $H \lhd G$, então o conjunto das **classes laterais** de H em G, G/H, possui estrutura de grupo. Assim, a partir da normalidade de H em G, podemos construir outro grupo que nos permite analisar G e obter informações sobre sua estrutura:

Teorema 1 *Sejam G um grupo e $H \lhd G$. O conjunto $G/H = \{aH \mid a \in G\}$ é um grupo sob a operação $(aH)(bH) = (ab)H$.*

Grupos quocientes, G/H, são importantes, pois, se G é finito e $H \neq \{e\}$, o grupo G/H é 'menor' do que G, e sua estrutura geralmente é menos complicada. Para algumas classes de grupos G que presevam o quociente, podemos imaginar que G/H é uma aproximação mais fácil de lidar do que o grupo G, e é possível deduzir propriedades deste grupo apenas estudando o quociente.

Definição 5 *Sejam G um grupo e $x, y \in G$. O elemento $y^x = yxy^{-1}$ é a* ***conjugação*** *de y por x, e $[x, y] = xyx^{-1}y^{-1} = y^x y^{-1}$ é o* ***comutador*** *de x e y.*

De modo geral, em um grupo G, se consideramos G' o conjunto gerado por todos os elementos da forma $\{[x, y] \mid x, y \in G\} \subset G$, G' tem estrutura de grupo, chamado **subgrupo dos comutadores de** G ou **subgrupo derivado de** G. Um caso particular deste conjunto é quando todos elementos comutam entre si. Este subgrupo de G é chamado **centro**, $Z(G) = \{x, y \in G \mid xy = yx\}$. Não é difícil ver que G' e $Z(G)$ são subgrupos normais de G. Quando o grupo G é exatamente igual a seu centro, dizemos que o grupo é **abeliano**. Outra importância do grupo G' é que a partir dele é possível obter uma abelianização do grupo G pois G/G' é sempre um grupo abeliano. Além disso, se $H \leq G$ é tal que G/H é abeliano, então certamente $G' \subset H$, ou em outras palavras, o subgrupo derivado será o menor subgrupo que satisfaz essa propriedade.

Definição 6 *Sejam H e K subgrupos de G. Definimos o seu produto por justaposição como $HK := \{hk \mid h \in H, k \in K\}$. Podemos também denotar esse produto por HK.*

Não é difícil ver que $\langle H \cup K \rangle \supseteq HK \supseteq H \cup K$. Dessa forma, a igualdade $\langle H \cup K \rangle = HK$ ocorre se, e somente se, $HK \leq G$:

Proposição 1 *Sejam $H, K \leq G$. Então $HK \leq G$ se, e somente se, $HK = KH$.*

Como consequências imediatas da **Proposição 1** temos que se $H, K \leq G$ e algum desses subgrupos for normal em G, então $HK \leq G$. Mais ainda, se $H, K \lhd G$ então $HK \lhd G$.

Definição 7 *Sejam $(G, *)$ e $(H, \circ)$ grupos. Uma aplicação $\varphi : G \longrightarrow H$ é um **homomorfismo** entre esses dois grupos se ela preserva a operação definida nos grupos, isto é,*

$$\varphi(a * b) = \varphi(a) \circ \varphi(b).$$

Exemplo 2 *(i) $Id : G \to G$, dada por $Id(x) = x$ é o* **homomorfismo identidade**.

(ii) $e : G \to H$, dada por $e(x) = e_H$, é o **homormorfismo trivial**.

(iii) Considere $H \lhd G$ e $\varphi : G \longrightarrow G/H$ dada por $\varphi(g) = \overline{g}$. φ é chamado **homomorfismo canônico** *ou* **projeção canônica**. *É interessante perceber que uma projeção sempre será uma sobrejeção.*

Definição 8 *Seja $\varphi : G \longrightarrow H$ um homomorfismo entre os grupos G e H. O **kernel** de φ é o conjunto*

$$\ker_\varphi := \{x \in G \mid \varphi(x) = e_H\}$$

e a **imagem** *de φ é o conjunto*

$$Im_\varphi := \{y \in H \mid \varphi(x) = y, \ \forall x \in G\}.$$

Não é difícil verificar que $\ker_\varphi \lhd G$ e $Im_\varphi \leq H$. Além disso, $\ker_\varphi = \{e\}$ se, e somente se, φ é injetor, caracterizando os **homomorfismos injetores**. Caso $Im_\varphi = H$, dizemos que φ é um **homomorfismo sobrejetor**.

Estudaremos a seguir uma classe importantíssima de homomorfismos, os isomorfismos. A importância de estudar os isomorfismos de grupos, é podermos não distinguir dois grupos que possuem exatamente a mesma estrutura e enxergá-los como sendo o mesmo grupo. Por exemplo, hoje em dia sabemos que, sendo p um número primo fixado, existe apenas um único grupo de ordem p, que é $\mathbb{Z}_p$, mas dizer isso significa que todos os outros grupos de ordem p possuem a mesma estrutura que $\mathbb{Z}_p$ e por isto não fazemos distinções sobre eles.

Definição 9 *Um homomorfismo $\varphi : G \longrightarrow H$ é dito um* ***isomorfismo*** *se é um homomorfismo bijetor. Quando conseguimos estabelecer uma bijeção entre dois grupos G e H, dizemos que eles são grupos* ***isomorfos****, e denotamos essa relação por $G \cong H$.*

Exemplo 3 *Se construirmos a tabela de multiplicação dos grupos $\mathbb{Z}/4\mathbb{Z}$ e $\mathbb{Z}_4$, vamos constatar que elas são muito semelhantes, para não dizer iguais, e isto ocorre pois é possível estabeler o seguinte isomorfismo entre os dois grupos:*

$$\begin{aligned} \varphi : \mathbb{Z}_4 &\longrightarrow \mathbb{Z}/4\mathbb{Z} \\ x &\longmapsto x + 4\mathbb{Z} \end{aligned}$$

ou seja, $\mathbb{Z}_4 \cong \mathbb{Z}/4\mathbb{Z}$, e por isto as suas tabelas serem iguais não é coincidência. De modo mais geral, podemos dizer que, dado $n \in \mathbb{N}$, tem-se que $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

Exemplo 4 *Qualquer grupo cíclico infinito é isomorfo à $\mathbb{Z}$, pois basta definir o homomorfismo $\varphi : G \longrightarrow \mathbb{Z}$ por $\varphi(a^k) = k$. Analogamente, qualquer grupo cíclico finito de ordem n é isomorfo à $\mathbb{Z}_n$. É suficiente definir o homomorfismo bijetor $\psi : G \longrightarrow \mathbb{Z}_n$ dado por $\psi(a^k) = k \ (mod\ n)$.*

Abaixo temos um teorema que diz respeito a algumas propriedades que são satisfeitas por isomorfismos, e as demonstrações omitidas podem ser encontradas em [8].

Teorema 2 *Sejam G e H grupos. Se $\psi : G \longrightarrow H$ é um isomorfismo, então as seguintes propriedades são satisfeitas:*

1. *$\psi(e_G) = e_H$;*
2. *Para todos $n \in \mathbb{Z}$ e $a \in G$, temos que $\psi(a^n) = (\psi(a))^n$;*
3. *G é abeliano $\iff$ H é abeliano;*
4. *$G = \langle a \rangle \iff H = \langle \psi(a) \rangle$;*
5. *$|a| = |\psi(a)|$;*
6. *Para um inteiro fixo k e um elemento fixo $b \in G$, a equação $x^k = b$ tem o mesmo número de soluções em G que a equação $x^k = \psi(b)$ tem em H;*

7. G e H tem exatamente o mesmo número de elementos de todas as ordens.

O chamados Teoremas do Isomorfismo entre grupos serão apresentados a seguir cuja demonstração será omitida:

Teorema 3 (1° Teorema do Isomorfismo) *Seja φ um homomorfismo entre os grupos G e H. Então a aplicação*

$$\begin{aligned} \psi : G/\ker_\varphi &\longrightarrow \varphi(G) \\ g\ker_\varphi &\longmapsto \varphi(g) \end{aligned}$$

é um isomorfismo. Isto é, $G/\ker_\varphi \cong \varphi(G)$.

Teorema 4 (2° Teorema do Isomorfismo) *Se K é um subgrupo de um grupo G e H é um subgrupo normal em G, então*

$$\frac{K}{H \cap K} \cong \frac{KH}{H}.$$

Teorema 5 (3° Teorema do Isomorfismo) *Sejam $K \leq H \leq G$ tais que $K,\ H \lhd G$. Então*

$$(G/K)/(H/K) \cong G/H.$$

Definição 10 *Seja $\alpha : G \longrightarrow G$ um homomorfismo do grupo G. Se α é bijetor, então é chamado de **automorfismo** de G. Denotamos o conjunto dos automorfismos de G por $Aut(G)$.*

Definição 11 *Considere G um grupo e g um elemento de G. O homomorfismo definido por $\psi_g(x) = gxg^{-1},\ \forall x \in G$, é chamado de **automorfismo interno** de G induzido por g. O conjunto dos automorfismos internos denotamos por $Inn(G)$.*

Note que $Aut(G)$ tem estrutura de grupo se munido da composição entre funções. Isso é fácil de enxergar pois, $id : G \longrightarrow G$ é um automorfismo que atua como elemento identidade em $Aut(G)$. Além disso, a composição de funções é associativa, e se $\varphi : G \longrightarrow G$ é um isomorfismo, $\varphi^{-1} : G \longrightarrow G$ também é. Logo, $\varphi^{-1} \in Aut(G)$, e segue que $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = id$.

Além disso, observe que $Inn(G) \leq Aut(G)$. De fato, temos que $\varphi_e(x) = e \cdot x \cdot e^{-1} = x$, logo $\varphi_e(x) = id(x),\ \forall x \in G$. Agora, suponha que $\varphi_g, \varphi_h \in Inn(G)$. Daí, temos que:

$$\begin{aligned}(\varphi_h \circ \varphi_{h^{-1}})(x) &= \varphi_h(\varphi_{h^{-1}}(x)) \\ &= \varphi_h(h^{-1}xh) \\ &= h(h^{-1}xh)h^{-1} \\ &= x \\ &= (\varphi_{h^{-1}} \circ \varphi_h)(x)\end{aligned}$$

Isto nos diz que $(\varphi_h)^{-1} = \varphi_{h^{-1}}$, e portanto

$$\begin{aligned}(\varphi_g \circ (\varphi_h)^{-1})(x) &= \varphi_g((\varphi_h)^{-1}(x)) \\ &= \varphi_g(\varphi_{h^{-1}}(x)) \\ &= \varphi_g(h^{-1}xh) \\ &= g(h^{-1}xh)g^{-1} \\ &= (gh^{-1})x(hg^{-1}) \\ &= (gh^{-1})x(gh^{-1})^{-1} \\ &= \varphi_{gh^{-1}}\end{aligned}$$

Logo, $\varphi_g \circ \varphi_{h^{-1}} \in Inn(G)$, e portanto, $Inn(G) \leq Aut(G)$.

Mais ainda, $Inn(G) \lhd Aut(G)$, pois se $\varphi \in Aut(G)$ e $\psi_g \in Inn(G)$, então

$$\begin{aligned}(\varphi \circ \varphi^{-1})(x) &= \varphi(\psi_g(\varphi^{-1}(x))) \\ &= \varphi(g\varphi^{-1}(x)g^{-1}) \\ &= \varphi(g)x\varphi(g^{-1}) \\ &= \varphi(g)x(\varphi(g))^{-1} \\ &= \psi_\varphi(g) \in Inn(G)\end{aligned}$$

Portanto, $Inn(G) \lhd Aut(G)$.

Para a próxima seção, apresentaremos alguns produtos entre grupos, importante para o desenvolvimento deste trabalho.

Produto Direto, Semidireto e Entrelaçado entre Grupos

As definições e resultados apresentados nessa subseção podem ser encontradas com mais detalhes em [6] e [12].

Definição 12 *Sejam $G_1, G_2, \cdots, G_n$ grupos. Chamamos de* ***produto direto*** *o conjunto das $n-$uplas $(g_1, g_2, \cdots, g_n)$ tais que $g_i \in G_i$. Isto é,*

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \cdots, g_n) \mid g_i \in G_i\}$$

Note que $G_1 \times G_2 \times \cdots \times G_n$ é grupo sob a operação definida por $(g_1, \cdots, g_n)(h_1, \cdots, h_n) = (g_1h_1, \cdots, g_nh_n)$, pois cada G_i é grupo, logo, vale o fechamento da operação e os axiomas de grupo.

Analogamente a decomposição de um número inteiro em fatores menores (até mesmo em fatores primos), podemos nos perguntar quando um grupo é um produto direto de outros grupos, i.e, quando $G \cong G_1 \times G_2 \times \ldots \times G_n$? Esta identificação nos permite representar um grupo por meio de outros grupos menores. Observe que se, para algum $i = 1, 2, \ldots, n$, temos que $G_i = G$, então $G_j = \{e\}$, $\forall j \neq i$, uma vez que se $|G_i| = m_i$, então segue que $|G_1 \times G_2 \times \ldots \times G_n| = \prod_{i=1}^{n} m_i$.

Teorema 6 *Sejam $G_1,\ G_2,\ \ldots, G_n$ grupos. Uma condição necessária e suficiente para que $G \cong G_1 \times G_2 \times \ldots \times G_n$ ocorra é se G possuir subgrupos $H_i \cong G_i,\ \forall i = 1, 2, \ldots, n$ que satisfaçam as seguintes condições:*

(i) $G = H_1H_2 \ldots H_n$

(ii) $H_i \lhd G,\ \forall i = 1, 2, \ldots, n$

(iii) $H_i \bigcap (H_1 \ldots H_{i-1}H_{i+1} \ldots H_n) = \{e\}$

Considere H e K grupos e $\psi : K \longrightarrow Aut(H)$ um homomorfismo com $Aut(H)$ o grupo dos homomorfismos bijetores de H, definimos como operação no conjunto $K \times H$ o seguinte produto

$$(k_1, h_1) \cdot_\psi (k_2, h_2) := (k_1k_2, h_1\psi(k_1)(h_2)).$$

Daí, $K \times H$ munido com esta operação é um grupo, chamado de **produto semidireto** de K e H. Também é denotado por $K \rtimes_\psi H$ para diferenciar do produto direto usual. Há uma diferença entre o produto direto e o produto semidireto no que diz respeito à normalidade dos grupos H_i, pois neste produto é exigido apenas que um dos subgrupos seja normal em G.

É fácil ver que o produto direto é um caso particular do produto semidireto. Se considerarmos ψ como o homomorfismo trivial, isto é, para todo $k \in K$ definimos $\psi(k)$ como

$$\begin{aligned} \varphi_k : H &\longrightarrow H \\ h &\longmapsto h \end{aligned}$$

tal que

$$\begin{aligned} (k_1, h_1) \cdot_\psi (k_2, h_2) &= (k_1 k_2, h_1 \psi(k_1)(h_2)) \\ &= (k_1 k_2, h_1 \varphi_{k_1}(h_2)) \\ &= (k_1 k_2, h_1 h_2). \end{aligned}$$

A aplicação ψ é chamada **ação** de H sobre K. Não é difícil verificar que, no produto direto $K \times H$, a ação de H sobre K é trivial. De maneira geral, podemos definir a ação de um grupo sobre um conjunto, como segue abaixo:

Definição 13 *Sejam X um conjunto e G um grupo. Dizemos que G age em X pela direita (analogamente pela esquerda), se as seguintes condições são satisfeitas:*

(i) Para $g \in G$, podemos definir uma função $\phi_g : X \longrightarrow X$;

(ii) Se $e \in G$ é o elemento identidade, então, a partir dele podemos definir uma função identidade $\phi_e : X \longrightarrow X$;

(iii) Se $g, h \in G$, então a composição $\phi_{gh} : X \longrightarrow X$ é tal que $\phi_{gh}(x) = \phi_g(\phi_h(x))$.

Somos capazes de estender ainda mais essas noções, e conseguimos obter tais generalizações a partir de um produto chamado de **produto entrelaçado**:

Definição 14 *Sejam $X = \{x_1, \cdots, x_n\}$ um conjunto finito, G um grupo, e H um grupo agindo em X. Seja também $G^n = G \times \cdots \times G$, o produto direto de G com ele próprio n*

vezes. Definimos o produto entrelaçado de G por H como $G \wr H = G^n \rtimes H$, onde H age em G^n pela sua ação definida no produto semidireto $G \rtimes_\varphi H$.

Uma observação importante é que a ação para o produto entrelaçado nesse contexto é a permutação dos índices, isto é, a ação de H sobre G^n pode ser enxergada como a função $\varphi_h : G^n \longrightarrow G^t$, definida por $\psi_h(g_1, g_2, \ldots, g_n) = (g_{h(1)}, g_{h(2)}, \ldots, g_{h(n)})$, sendo h uma permutação.

Veremos mais adiante que o grupo de Rubik poderá ser decomposto como um produto semidireto de dois grupos muito importantes, que caracterizam as permutações que movem os cubinhos, mas deixando suas orientações fixas, e também as permutações que deixam fixadas todas as posições dos cubinhos, porém mudando as suas orientações.

1.2 Grupos Livres

Nestas próximas breves seções sobre grupos livres e apresentações as referências utilizadas são [10] e [11], onde qualquer prova omitida pode ser encontrada.

Definição 15 *Um grupo F é dito **livre** sobre um subconjunto $X \subset F$ se, dado qualquer grupo G e qualquer aplicação $\theta : X \longrightarrow G$, existe um único homomorfismo $\theta' : F \longrightarrow G$ tal que $\theta'(x) = \theta(x)$, $\forall x \in X$. Em outras palavras, o seguinte diagrama é comutativo:*

$$\begin{array}{ccc} X & \xrightarrow{ic} & F \\ {\scriptstyle\theta}\downarrow & \swarrow_{\theta'} & \\ G & & \end{array}$$

Dizemos que X é uma **base** para o grupo F e podemos denotar por $|X|$ ou $r(F)$ o posto de F, que representam a quantidade de elementos na base.

Note que a função $ic : X \longrightarrow X$, dada por $ic(x) = x$, é necessariamente injetora. De fato, suponha que $ic(x_1) = ic(x_2)$ com $x_1 \neq x_2$, G um grupo com pelo menos dois elementos distintos g_1 e g_2 e $\theta : X \longrightarrow G$ tal que $\theta(x_1) = g_1$ e $\theta(x_2) = g_2$.

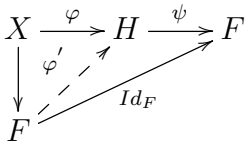
Dessa forma, $\theta' \circ ic(x_1) = g_1$ e $\theta' \circ ic(x_2) = g_2$, e daí segue que

$$\begin{aligned}(\theta' \circ ic)(x_1) = g_1 &\implies \theta'(ic(x_1)) = g_1 \\ &\implies \theta'(ic(x_2)) = g_1 \\ &\implies \theta(x_2) = g_1 \\ &\implies g_2 = g_1\end{aligned}$$

o que é um absurdo. Logo, ic é uma função injetora.

Proposição 2 *Se F é livre sobre X, então X gera F.*

Prova: Sejam $H = \langle X \rangle := \bigcap\{K \leq F \mid K \supseteq X\}$, $\varphi : X \longrightarrow H$, $\varphi' : F \longrightarrow H$ a extensão de φ e $\psi : H \longrightarrow F$. Temos o seguinte diagrama:



Note que Id_F estende $\psi \circ \varphi$ mas também ocorre que $\psi \circ \varphi'$ estende $\psi \circ \varphi$ e, como F é livre sobre X, temos que $Id_F = \psi \circ \varphi'$.

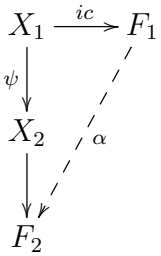
Agora, como Id_F é sobrejetora, $\psi \circ \varphi'$ também é, e portanto ψ é sobrejetora. Segue daí que $H = F$. ■

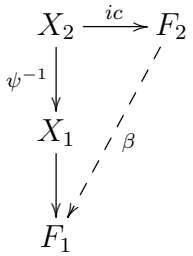
Proposição 3 *Grupos livres de mesmo posto são isomorfos. Além disso, grupos livres isomorfos possuem mesmo posto.*

Prova: Sejam F_1 livre sobre X_1 e F_2 livre sobre X_2, tais que $|X_1| = |X_2|$. Existe uma bijeção

$$\psi : X_1 \longrightarrow X_2$$

Agora, sejam α e β as extensões dadas de acordo com os seguintes diagramas





Para todo $x \in X_1$, temos

$$\begin{aligned} \beta \circ \alpha(x_1) &= \beta \circ \psi(x_1) \\ &= \psi^{-1} \circ \psi(x_1) \\ &= x_1 \end{aligned}$$

Ou seja, $\beta \circ \alpha : F_1 \longrightarrow F_1$ estende $ic : X_1 \longrightarrow F_1$. Mas temos também que a função idF_1 é uma extenção para a função ic, e desta forma, temos $\beta \circ \alpha = idF_1$. De modo totalmente análogo, concluímos que $\alpha \circ \beta = idF_2$.

Ou seja, α um homomorfismo invertível, e portanto, bijetor. Segue que $F_1 \simeq F_2$. ■

A proposição abaixo nos sugere a construção de um grupo livre a partir de um conjunto finito de geradores dados:

Proposição 4 *Se X é um conjunto não vazio, existe um grupo F e uma função $\varphi : X \longrightarrow F$ tal que F é livre sobre X e $F = \langle Im\ \varphi \rangle$.*

Prova: Seja o conjunto $X^{-1} := \{x^{-1} \mid x \in X\}$, onde $|X| = |X^{-1}|$ e $X \cap X^{-1} = \emptyset$.

Definimos em $X^{\pm} = X \cup X^{-1}$ uma palavra como sendo uma sequência finita de elementos de $X^{\pm}$, isto é

$$w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$$

onde $x_i \in X$ e $\epsilon_i = \pm 1$ e $n \geq 0$.

No caso $n = 0$, dizemos que w é uma **palavra vazia**, denotada por e. Com isso, duas palavras são *iguais* se possuem os mesmos elementos nas mesmas posições. Podemos definir uma operação entre duas ou mais palavras que será dada simplesmente pela *justaposição* entre elas, isto é, dadas duas palavras:

$$w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} \quad \text{e} \quad v = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m},$$

o produto entre w e v é definido por $w \cdot v = x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_n^{\epsilon_n} \cdot y_1^{\alpha_1} y_2^{\alpha_2} \ldots y_m^{\alpha_m}$. Também podemos convencionar que $w \cdot e = w = e \cdot w$, e o inverso de w como $w^{-1} = x_n^{-\epsilon_n} \cdots x_1^{-\epsilon_1}$.

Agora, seja S o conjunto de todas as palavras em X. Dizemos que duas palavras são equivalentes ($w \sim v$) se é possível chegar de uma palavra a outra de dois modos, com finitos passos:

1. Inserindo xx^{-1} ou $x^{-1}x$ como elementos consecutivos da palavra

2. Eliminando termos da forma xx^{-1} ou $x^{-1}x$

$\sim$ é uma relação de equivalência e a classe que contém w será denotada por $[w]$.

Definimos F como o conjunto de todas as classes de equivalência que contenham palavras do conjunto S. Se $w \sim w'$ e $v \sim v'$, segue que $wv \sim w'v'$. Podemos então definir o produto entre as classes $[w]$ e $[v]$ como $[w][v] = [wv]$. Dessa forma, $[w][e] = [w][e][w]$ e $[w][w^{-1}] = [ww^{-1}] = [e]$. Temos também que este produto é associativo, uma vez que a justaposição de palavras também é associativa, daí segue que F é um grupo sob essa operação binária.

Seja $\varphi : X \longrightarrow F$ tal que $\varphi(x) = [x]$. Vejamos que F é livre sobre X:

Suponha que $\psi : X \longrightarrow G$ é uma função de X para um grupo arbitrário G. Seja também $\overline{\alpha}$ a função entre o conjunto de todas as palavras em X para G dada por

$$\overline{\alpha}(x_1^{\epsilon_1}x_2^{\epsilon_2}\cdots x_n^{\epsilon_n}) = g_1^{\epsilon_1}\cdots g_n^{\epsilon_n},$$

onde $g_i = \psi(x_i)$. Agora, $w \sim v$ implica que $\overline{\alpha}(w) = \overline{\alpha}(v)$, pois $gg^{-1} = g^{-1}g = e_G$. Dessa forma, é possível definir a função $\alpha : F \longrightarrow G$ por $\alpha([w]) = \overline{\alpha}(w)$. Segue então que

$$\begin{aligned}
\alpha([w][v]) &= \alpha([wv]) \\
&= \overline{\alpha}(wv) \\
&= \overline{\alpha}(w)\cdot\overline{\alpha}(v) \\
&= \alpha([w])\cdot\alpha([v])
\end{aligned}$$

Ou seja, α é um homomorfismo entre F e G. E além disso

$$\begin{aligned}
(\alpha\circ\varphi)(x) &= \alpha(\varphi(x)) \\
&= \alpha([x]) \\
&= \overline{\alpha}(x) \\
&= \psi(x), \forall x \in X
\end{aligned}$$

Considere $\gamma : F \longrightarrow G$ um homomorfismo tal que $\gamma\circ\varphi = \psi$. Então $\gamma\circ\varphi = \alpha\circ\varphi$. Note que tanto $\gamma\circ\varphi$ quanto $\alpha\circ\varphi$ coincidem em Im φ e claramente $F = \langle \text{Im } \varphi\rangle$, logo $\gamma = \alpha$. ■

Existe uma classe de palavras conhecidas como **palavras reduzidas**, e elas servem para obtermos uma forma mais simples ou mais conveniente de representar os elementos de um conjunto S.

Definição 16 *Dizemos que uma palavra w em $X^{\pm}$ é **reduzida** se ela não possui pares da forma xx^{-1} ou $x^{-1}x$.*

Em uma palavra w qualquer, podemos eliminar estes termos redundantes obtendo uma palavra equivalente. Isto significa que toda classe de equivalência vai possuir uma palavra reduzida. E mais ainda, toda classe de equivalência de palavras em $X^{\pm}$ possui uma única palavra reduzida.

O próximo teorema é o mais importante desta breve introdução acerca dos grupos livres, pois é por meio dele que poderemos utilizar quocientes convenientes para representar alguns dos grupos que vamos estudar por meio do GAP.

Teorema 7 *Todo grupo é uma imagem homomórfica de um grupo livre.*

Prova: Sejam G um grupo, X um conjunto de geradores de G e F um grupo livre sobre X. Vamos denotar a palavra $x_1x_2\ldots x_n \in X \cup X^{-1}$ por $(x_1\ x_2\ldots\ x_n)_F$ e o produto em G por $(x_1\ x_2\ldots\ x_n)_G$. Seja então a aplicação de F para G dada por $\varphi([x_1x_2\cdots x_n]) = (x_1x_2\cdots x_n)_G$.

Temos φ bem definida, pois adicionar ou retirar pares de elementos inversos na palavra, significa adicionar ou retirar também em G.

Agora, temos que

$$\begin{aligned}\varphi([x_1\cdots x_n][y_1\cdots y_n]) &= \varphi([x_1\cdots x_ny_1\cdots y_n])\\ &= (x_1\cdots x_ny_1\cdots y_n)_G\\ &= (x_1\cdots x_n)_G(y_1\cdots y_n)_G\\ &= \varphi([x_1\cdots x_n])\cdot\varphi([y_1\cdots y_n])\end{aligned}$$

Ou seja, φ é um homomorfismo, e também é sobrejetor pois $G = \langle X\rangle$. ■

Corolário 1 *Todo grupo é isomorfo a um quociente de um grupo livre.*

Prova: Seja φ o homomorfismo do **Teorema 7**, e tome $K = \ker_\varphi$. Sabemos que $K \lhd F$, daí, pelo **Teorema 3**, segue que $F/K \cong G$. ■

1.3 Apresentação de Grupos

Uma vez que já temos alguns dos resultados básicos sobre grupos livres, podemos falar de apresentação de grupos. Vamos considerar X um conjunto, F o grupo livre sobre X, R um subconjunto de F, $N = \overline{R}$ o fecho normal de R em F, e $G = F/N$ um grupo quociente. Temos a seguinte definição:

Definição 17 *Dizemos que $G = \langle X \mid R \rangle$ é uma **apresentação livre**, ou simplesmente **apresentação** do grupo G. Os elementos do conjunto X chamamos de geradores e os elementos de R de relatores. Um grupo G é finitamente apresentado se possui uma apresentação onde ambos os conjuntos X e R são finitos.*

Proposição 5 *Todo grupo possui uma apresentação.*

Prova: Seja G um grupo e $X \subset G$ um conjunto de geradores de G. Seja F o grupo livre sobre X. A partir da função inclusão $ic : X \longrightarrow G$, podemos estendê-la ao homomorfismo $\varphi : F \longrightarrow G$. Temos que φ é sobrejetora, pois X gera G. Logo, pelo **Teorema 3**, segue que $F/\ker_\varphi \cong G$, ou seja, temos que $G = \langle X \mid \ker_\varphi \rangle$. ■

É válido ressaltar que a **Proposição 5** é imediata, mas que seria uma afirmação totalmente diferente caso estivesse escrito "apresentação finita" ao invés de apenas "apresentação". De fato, no caso das apresentações finitas isto não é válido de modo geral, nos restando apenas alguns casos particulares, porém que apresentam grandes vantagens de cálculo com relação a grupos que não podem ser finitamente apresentados.

Seguem abaixo alguns exemplos de grupos e suas apresentações (finitas) que podem ser encontradas em [10]:

Grupos Livres

Seja F um grupo livre de posto X. Então,

$$F = \langle X \mid \emptyset \rangle.$$

Essa apresentação para um grupo livre qualquer a partir de seus geradores é a motivação para que esses grupos sejam ditos livres, pois eles não possuem nenhuma relação entre seus elementos, exceto aquelas que de fato o definem como um grupo.

Grupos Cíclicos

Sabemos que grupos cíclicos são gerados por um elemento, então se $G = \langle a \rangle$ é um grupo cíclico de ordem n, apresentamos ele como

$$C_n = \langle a \mid a^n = 1 \rangle.$$

Esta apresentação caracteriza todos os grupos cíclicos de ordem n, então a menos de isomorfismos, existe apenas um grupo cíclico com n elementos. Por exemplo, os grupos $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ dos inteiros aditivos módulo 6 e o grupo $U(7) = \{1, 2, 3, 4, 5, 6\}$ dos inteiros multiplicativos módulo 7 são o mesmo grupo, pois ambos são cíclicos de ordem 6, e pode-se constatar que eles são isomorfos via o isomorfismo $\varphi(n) = 3^n$.

Grupo de Klein

Este grupo é 2-gerado, tendo como geradores elementos a e b satisfazendo as relações $a^2 = 1, b^2 = 1, (ab)^2 = 1$, e portanto pode ser apresentado como

$$K_4 = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1 \rangle$$

É importante saber que se existe qualquer outro grupo G que seja 2-gerado, e cujos geradores satisfaçam as mesmas relações que os geradores de K_4, então $G \cong K_4$, e a prova para este resultado de maneira mais geral pode ser consultada em [14].

Grupo Diedral D_n

Uma apresentação para o grupo diedral D_n de ordem $2n$ pode ser encontrada em [8] da seguinte maneira

$$D_n = \langle A, B \mid A^n = 1, B^2 = 1, BA = A^{n-1}B \rangle$$

Em particular, para $n = 2$, temos

$$D_2 = \langle A, B \mid A^2 = 1, B^2 = 1, BA = AB \rangle$$

Apesar das relações não serem, à primeira vista, as mesmas do grupo de Klein, podemos manipular as relações em D_2 para obter as relações de K_4, por exemplo

$$\begin{aligned} BA = AB &\implies ABA^{-1}B^{-1} = 1 \\ &\implies ABAB = 1 \\ &\implies (AB)^2 = 1 \end{aligned}$$

De onde, é equivalente dizer que

$$D_2 = \langle A, B \mid A^2 = B^2 = (AB)^2 = 1 \rangle$$

De certo modo, não fazemos distinções entre K_4 e D_2 pois, a menos de isomorfismos, ambos representam o mesmo grupo. De maneira geral, é possível verificar que dada uma apresentação de um grupo G, $G = \langle a, b, c, \ldots \mid P, Q, R, \ldots \rangle$, existem manipulações simples que não mudam o grupo ou pelo menos a classe de isomorfismo definida pela apresentação. Essas são as conhecidas *Transformações de Tietze* [11] de uma dada apresentação, que em geral tem a finalidade de, a partir de uma apresentação dada, obter uma apresentação equivalente para um mesmo grupo, utilizando as relações conhecidas. Muitas vezes é mais conveniente trabalhar com diferentes tipos de apresentações a depender do problema que está sendo analisado.

Grupo dos Quatérnios

O conjunto dos quatérnios é uma extensão do que conhecemos como números complexos, sendo elementos da forma $z = a+bi+cj+dk$, $a, b, c, d \in \mathbb{R}$ e $i,\ j$ e k são unidades imaginárias.

Agora, o grupo dos quatérnios, denotado usualmente por Q_8, é um grupo cujos elementos são identificados ao conjunto $\{1,\ i,\ j,\ k,\ -1,\ -i,\ -j,\ -k\}$ munido com a operação de multiplicação. Uma apresentação para Q_8 é dada por:

$$Q_8 = \langle x, y \mid x^4 = e,\ x^2 = y^2,\ yx = x^{-1}y \rangle$$

onde podemos ver que $i = x,\ j = y,\ k = xy$. Lembre que a tabela de multiplicação simplificada para os quatérnios é a seguinte:

*	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	-1	$-i$

Grupos Policíclicos

Uma apresentação $\langle x_1, x_2, \ldots x_n \mid R \rangle$ é chamada de **apresentação policíclica** se existe uma sequência $S = (s_1, s_2, \cdots, s_n)$, com $s_i \in \mathbb{N} \cup \{\infty\}$, e inteiros $a_{i,k}$, $b_{i,j,k}$ e $c_{i,j,k}$ tal que R é dada pelas seguintes relações:

1. $x_i^{s_i} = x_{i+1}^{a_{i,i+1}} x_{i+2}^{a_{i,i+2}} \ldots x_n^{a_{i,n}}$, para $1 \leq i \leq n$, com $s_i \leq \infty$.
2. $x_j^{-1} x_i x_j = x_{j+1}^{b_{i,j,j+1}} \ldots x_n^{b_{i,j,n}}$, para $1 \leq j < i \leq n$.
3. $x_j x_i x_j^{-1} = x_{j+1}^{c_{i,j,j+1}} \ldots x_n^{c_{i,j,n}}$, para $1 \leq j < i \leq n$.

Essa apresentação define uma classe de grupos conhecida como **grupos policíclicos**, que são caracterizados pela existência de uma cadeia descendente de subgrupos

$$G = G_1 \geq G_2 \geq G_3 \geq \cdots \geq G_{n+1} = \{e\}$$

onde o quociente G_i/G_{i+1} é cíclico.

Os grupos policíclicos fazem parte de uma classe de grupos chamados de **grupos computáveis**, no sentido de que sua estrutura tem vantagens computacionais, e sua apresentação nos permite decidir algoritimicamente problemas em geral insolúveis, como o Problema da Palavra para grupos, [10]. Veremos mais adiante que é possível encontrar uma apresentação policíclica para o grupo simétrico S_n.

Capítulo 2

Grupos de Permutações

Neste capítulo falaremos de uma classe de grupos fundamentais para o estudo do cubo de Rubik: os grupos de permutações. A partir destes grupos seremos capazes de estabelecer conexões com o cubo Mágico e provar que, de fato, a partir de uma identificação entre suas faces e movimentos, este representa um grupo. Mais especificamente, poderemos comprovar que o conjunto de movimentos possíveis no cubo com a operação de justaposição de rotações é isomorfo a algum subgrupo de S_{48}.

As principais definições e resultados deste capítulo podem ser encontrados em [6], [7] e [8].

2.1 Definição e Notação Cíclica

Definição 18 *Uma permutação de um conjunto finito A é uma função bijetora cujo domínio e contradomínio são o conjunto A.*

Exemplo 5 *Definimos a permutação α do conjunto $A = \{1, 2, 3, 4\}$ por $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 1$, $\alpha(4) = 4$. Podemos representar esta permutação pela seguinte notação*

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

no qual cada elemento $\alpha(j)$ está situado imediatamente abaixo do elemento j.

Uma outra maneira de representar permutações, que também é muito utilizada, é a partir da notação cíclica. Introduzida por Louis-Augustin Cauchy em [3], essa notação é mais comum no estudo das permutações pois são mais elegantes e por nos permitir calcular a ordem de uma permutação. A notação cíclica para α no **Exemplo 5** é $\alpha = (1234)$. Quando algum elemento é fixado por alguma permutação, ele simplesmente não aparece nos ciclos. Também cabe ressaltar que uma representação por ciclos não é única. Assim, podemos encontrar modos mais convenientes de representá-las, a depender do problema que se deseja resolver, como por exemplo, escrevendo permutações como produto de ciclos disjuntos.

Para compor duas permutações sobre o mesmo conjunto, usamos a composição de funções da direita para a esquerda. Além disso, faremos um abuso de notação e escreveremos $\alpha \circ \beta$ como $\alpha\beta$ e daí, $\alpha^2 = \alpha \circ \alpha$ e assim, sucessivamente:

Exemplo 6 *Sejam* $A = \{1, 2, 3, 4\}$. *Considere as permutações* $\alpha = (12)$ *e* $\beta = (234)$.

A composição $\alpha\beta = (12)(1234)$ *é obtida da seguinte forma:* $\alpha(\beta(1)) = 2$, $\alpha(\beta(2)) = 3$, $\alpha(\beta(3)) = 4$ *e* $\alpha(\beta(4)) = 1$. *Em outras palavras,* $\alpha\beta = (12)(234) = (1234)$.

De maneira equivalente, podemos calcular $\beta\alpha = (234)(12) = (1342)$.

Perceba que $\alpha\beta \neq \beta\alpha$ *pois, em geral, a composição de funções não é comutativa.*

Exemplo 7 *Seja* S_3 *o conjunto das bijeções sobre o conjunto* $A = \{1, 2, 3\}$ *nele mesmo. Considere as seguintes permutações:* $id = (1), \alpha = (123), \beta = (23)$.

Perceba que podemos listar todos os elementos de S_3 *a partir de* id, α *e* β. *Isto é, o conjunto de todas as permutações possíveis entre os elementos de* A *é dado por* $S_3 = \{id, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$.

Dado um conjunto finito $A = \{1, 2, \cdots, n\}$, denotamos por S_n o conjunto das funções $\alpha : A \longrightarrow A$ que são bijetoras. Podemos calcular a cardinalidade de S_n utilizando o *Princípio Fundamental da Contagem* (P.F.C.). Para $\alpha(1)$, temos n possibilidades de imagem, para $\alpha(2)$ temos $(n-1)$ possibilidades de imagem. Sucessivamente, para $\alpha(i)$, teremos $n - i + 1$ possibilidades de escolha. As possibilidades sempre diminuem pois α é uma bijeção. Usando o P.F.C., temos que a cardinalidade de S_n é

$$|S_n| = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1 = n!$$

Definição 19 *Uma permutação $\alpha \in S_n$ é chamada de* ***r-ciclo***[1] *se existem r elementos distintos $a_1, \ldots, a_r \in \{1, \ldots, n\}$ tais que $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3$, $\ldots$, $\alpha(a_{r-1}) = a_r$, $\alpha(a_r) = a_1$ com os elementos restantes fixados, isto é, $\alpha(j) = j$, para todo $j \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_r\}$. A notação para este r-ciclo é dada por $(a_1\ a_2\ a_3\ \ldots\ a_r)$.*

Definição 20 *Sejam $\alpha, \beta \in S_n$ r-ciclo e s-ciclo, respectivamente. Dizemos que α e β são ciclos disjuntos se, quando representados da forma $\alpha = (a_1 \ldots a_r), \beta = (b_1 \ldots b_s)$, temos que $\{a_1, \ldots, a_r\} \bigcap \{b_1, \ldots, b_s\} = \emptyset$.*

Abaixo, seguem algumas propriedades imediatas:

Teorema 8 *Dois ciclos disjuntos $\alpha, \beta \in S_n$ quaisquer comutam.*

Prova: Sejam $\alpha = (a_1\ a_2\ \ldots a_r)$ e $\beta = (b_1\ b_2\ \ldots b_s)$ ciclos disjuntos. Podem ocorrer três possibilidades entre α e β:

1. Considere $x \in \{a_1, a_2, \ldots, a_r\}$, $x = a_i$, para algum $1 \leq i \leq r$. Como β fixa x, então

$$\begin{aligned} (\alpha \circ \beta)(x) &= (\alpha \circ \beta)(a_i) \\ &= \alpha(\beta(a_i)) \\ &= \alpha(a_i) \\ &= a_{i+1} \end{aligned} \qquad \begin{aligned} (\beta \circ \alpha)(x) &= (\beta \circ \alpha)(a_i) \\ &= \beta(\alpha(a_i)) \\ &= \beta(a_{i+1}) \\ &= a_{i+1} \end{aligned}$$

2. Considere $x \in \{b_1, b_2, \cdots, b_s\}$, $x = b_i$, para algum $1 \leq i \leq s$. Como α fixa x, então

$$\begin{aligned} (\alpha \circ \beta)(x) &= (\alpha \circ \beta)(b_i) \\ &= \alpha(\beta(b_i)) \\ &= \alpha(b_{i+1}) \\ &= b_{i+1} \end{aligned} \qquad \begin{aligned} (\beta \circ \alpha)(x) &= (\beta \circ \alpha)(b_i) \\ &= \beta(\alpha(b_i)) \\ &= \beta(b_i) \\ &= b_{i+1} \end{aligned}$$

3. Suponha $x \notin \{a_1, \cdots, a_r\} \bigcup \{b_1, \cdots, b_s\}$. Logo

$$\begin{aligned} (\alpha \circ \beta)(x) &= \alpha(\beta(x)) \\ &= \alpha(x) \\ &= x \end{aligned} \qquad \begin{aligned} (\beta \circ \alpha)(x) &= \beta(\alpha(x)) \\ &= \beta(x) \\ &= x \end{aligned}$$

[1] Em particular, 2-ciclos frequentemente são chamados de **transposições**.

Portanto, em qualquer caso, temos que $\alpha\beta = \beta\alpha$. ■

Teorema 9 *Toda permutação de um conjunto finito pode ser escrita como um único ciclo ou como produto de ciclos disjuntos.*

Prova: Seja $\alpha \in S_n$ uma permutação do conjunto $A = \{1, \ldots, n\}$. Tome $a_1 \in A$ tal que $\alpha(a_1) = a_2$, $\alpha^2(a_1) = \alpha(\alpha(a_1)) = \alpha(a_2) = a_3$, $\ldots$, $\alpha^{n-1}(a_1) = a_n$, $\alpha^n(a_1) = a_1$, para algum $n \in \mathbb{N}$. Tal n existe pois A é um conjunto finito. Então, podemos escrever $\alpha = (a_1\ a_2\ \ldots\ a_n)\beta$. Caso $A \setminus \{a_1, a_2, \ldots, a_n\} = \emptyset$, significa que $\beta = id$ e a prova acaba aqui. Caso $A \setminus \{a_1, a_2, \ldots, a_n\} \neq \emptyset$, significa que existem $b_1,\ b_2,\ \ldots,\ b_s \in A$ que não aparecem no ciclo $(a_1\ a_2\ \ldots\ a_n)$ e, desse modo, agimos como anterior nos elementos restantes a fim de construir um novo ciclo até percorrer todos os elementos do conjunto finito A. Se, na primeira tentativa formos bem sucedidos, então α é um ciclo. Se precisarmos de mais iterações, então α é um produto de ciclos disjuntos. ■

Exemplo 8 *Consideramos* $A = \{1, 2, 3, 4, 5, 6\}$ *e*

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

Devemos escolher algum elemento do conjunto A que vai ser permutado, digamos $a_1 = 3$. *Então* $\alpha(3) = 2$, $\alpha^2(3) = \alpha(\alpha(3)) = \alpha(2) = 3$. *Uma vez que voltamos ao elemento inicial, formamos transposição. Como ainda restam elementos em A, então escolhemos outro, digamos* $b_1 = 1$. *Logo* $\alpha(1) = 5$, $\alpha^2(1) = \alpha(\alpha(1)) = \alpha(5) = 6$, $\alpha^3(1) = 1$. *Resta apenas escolher* $c_1 = 4$, *mas* α *deixa esse elemento fixo, então não é necessário colocá-lo na representação cíclica. Segue então que* $\alpha = (32)(156) = (156)(32)$.

2.2 Grupo das Permutações S_n

Nesta seção mostramos que o conjunto S_n das permutações de um conjunto finito $\{1,\ 2,\ \ldots\ n\}$ munido da composição de funções define um grupo, chamado **grupo simétrico** ou **grupo das permutações**:

Proposição 6 S_n *é um grupo sob a operação de composição de funções.*

Prova: Primeiro note que há o fechamento sob a operação binária, pois uma composição de duas bijeções α e β é por sua vez uma bijeção, e como α e β estão definidas com mesmo domínio e contradomínio, o mesmo ocorre para $\alpha \circ \beta$.

A composição de funções é associativa, então, em particular, dadas as permutações $\alpha, \beta, \gamma \in S_n$, temos que $\alpha(\beta\gamma) = (\alpha\beta)\gamma$. Note que $id : A \longrightarrow A$ assume o papel de elemento neutro sob a operação de S_n, pois, para qualquer $\alpha \in S_n$, temos que $\text{id}\ \alpha = \alpha\ \text{id}\ = \alpha$. Além disso, sabe-se que toda bijeção admite uma inversa também bijetora, ou seja, dada $\alpha : A \longrightarrow A \in S_n$, temos que $\alpha^{-1} : A \longrightarrow A \in S_n$. E com todo o anterior, temos que S_n é de fato um grupo. ■

Definição 21 *Seja $A = \{1, 2, \cdots, n\}$ um conjunto finito. O grupo S_n de todas as permutações de A é chamado* ***grupo simétrico*** *(ou* ***grupo de permutações****) de grau n.*

O próximo resultado nos mostra a importância do **Teorema** 9, pois essa forma de reescrever um elemento de S_n tem implicações muito fortes no que diz respeito a sua ordem.

Teorema 10 *Se $\alpha \in S_n$ é uma permutação tal que $\alpha = \alpha_1\alpha_2 \ldots \alpha_r$, tal que a decomposição anterior é constituída por ciclos disjuntos, então $o(\alpha) = mmc(o(\alpha_1), o(\alpha_2), \ldots, o(\alpha_r))$.*

Prova: Primeiro note que um $r-$ciclo possui ordem r. De fato, este resultado pode ser provado utilizando indução sobre r. Sejam agora α, β ciclos disjuntos de ordem r e t, respectivamente, e seja $k = mmc(o(\alpha), o(\beta))$. É claro que $\alpha^k = \beta^k = id$, já que $k \mid r$ e $k \mid t$, e como a identidade comuta com qualquer elemento, temos que $(\alpha\beta)^k = id$, e isso significa que $o(\alpha\beta)$ divide k. Suponha que $o(\alpha\beta) = p$, e note que $(\alpha\beta)^p = \alpha^p\beta^p = id$, logo $\alpha^p = \beta^{-p}$, mas por hipótese os ciclos α e β são disjuntos, então necessariamente os ciclos α^p e β^{-p} também são, pois potências não criam elementos diferentes dos que já existiam nos ciclos. Deste modo, a única possibilidade dessa igualdade ocorrer é se $\alpha^p = \beta^{-p} = id$, dessa forma, $r \mid p$ e $s \mid p$, então $mmc(r, t) \mid p$.

Primeiro mostramos que $p \mid k$, e em seguida mostramos que $k \mid p$, e portanto $p = k$. ■

Em [2] é mostrada uma apresentação relativamente simples para o grupo S_n, via relações de Moore:

Definição 22 *Seja G um grupo gerado pelo conjunto $X = \{x_1, x_2, \ldots, x_{n-1}\}$. As relações:*

1. $x_i^2 = 1$;

2. $x_i x_j = x_j x_i$, *se* $|i - j| \geq 2$;

3. $(x_i x_j)^3 = 1$.

são denominadas ***relações de Moore****.*

Desta definição, temos o seguinte teorema:

Teorema 11 *Seja G um grupo cujos geradores $x_1,\ x_2, \ldots,\ x_{n-1}$ satisfazem as relações de Moore. Então, $G \cong S_n$.*

Em particular, observe que podemos definir as transposições $\sigma_i = (i\ i{+}1)$ em S_n de modo que os elementos $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ formem um conjunto gerador para S_n. Assim, usando o **Teorema** 11, temos a seguinte maneira de apresentar o grupo simétrico de grau n:

$$S_n = \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i^2 = 1, \sigma_i\sigma_j = \sigma_j\sigma_i, (\sigma_i\sigma_j)^3 = 1 \rangle.$$

Além disso, note que esta é uma apresentação policíclica para o grupo S_n e, portanto, o Problema da Palavra é decidível em S_n.

Proposição 7 *Para $n \geq 3$, S_n não é um grupo abeliano.*

Prova: Para $n = 3$, consideremos $\alpha = (13), \beta = (23)$. Logo, $\alpha\beta \neq \beta\alpha$, e portanto S_3 não é abeliano. Mas perceba que podemos considerar essas permutações como elementos em S_n, fixando todos os elementos com $n \geq 4$. Consequentemente, teremos $\alpha, \beta \in S_n$, com $\alpha\beta \neq \beta\alpha$, e portanto, S_n não pode ser abeliano. ■

O próximo teorema mostra como todos os grupos estão relacionados com grupos de permutações, o que nos dá uma motivação para tentar entendê-los. De fato, se todos os grupos possuem ligações com grupos de permutações, nada mais natural que estudar que tipo de morfismos podemos construir entre um grupo arbitrário e S_n:

Teorema 12 (Cayley) *Todo grupo finito é isomorfo a um grupo de permutações. Em outras palavras, todo grupo finito é isomorfo à algum subgrupo de um grupo simétrico.*

Prova: Seja G um grupo qualquer de ordem n. Vamos definir a seguinte função

$$T_g : G \longrightarrow G$$
$$x \longmapsto gx$$

onde $x, g \in G$, e g é um elemento fixado. A função T_g é uma permutação dos elementos do conjunto G, isto é

$$T_g = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ gx_1 & gx_2 & gx_3 & \cdots & gx_n \end{pmatrix}$$

Considere $\overline{G} = \{T_g \mid g \in G\}$. Então $\overline{G}$ é um grupo sob a operação de composição de funções, onde o elemento identidade é a função T_e e também que $(T_g)^{-1} = T_{g^{-1}}$, pois $(T_g)^{-1} \circ T_{g^{-1}} = (T_g)^{-1}(T_{g^{-1}}(x)) = (T_g)^{-1}(g^{-1}x) = x$. Por outro lado, tem-se que $T_{g^{-1}} \circ (T_g)^{-1} = T_{g^{-1}}((T_g)^{-1}(x)) = T_{g^{-1}}(gx) = x$. E por úlitmo, como a composição de funções é associativa, temos que $\overline{G}$ é um grupo de permutações.

Considere agora

$$\varphi : G \longrightarrow \overline{G}$$
$$g \longmapsto T_g$$

$\star$ φ é injetora pois:

$$T_g = T_h \implies T_g(e) = T_h(e) \implies ge = he \implies g = h$$

$\star$ φ é sobrejetora, pois, se $y \in \overline{G}$, logo $y = T_\gamma$, com $\gamma \in G$. Basta então tomarmos $\varphi^{-1}(y) = \gamma$.

$\star$ φ também é homomorfismo, pois

$$\varphi(ab) = T_{ab}(x) = abx = a(bx) = T_a(bx) = T_a \circ T_b = \varphi(a)\varphi(b)$$

Portanto, segue que $G \cong \overline{G}$. ■

O **Teorema de Cayley**, **Teorema 12**, é importante por dois principais motivos: nos permite identificar grupos mais abstratos de uma forma mais concreta e também nos mostra que os axiomas de conjuntos adotados para caracterizar grupos é uma abstração correta do grupo de permutações. Em essência, grupos quaisquer não se diferem de algum grupo de

permutações, o que fazemos é olhar esses grupos abstratos com um outro ponto de vista, que nos permite extrair informações mais facilmente e até mesmo resolver problemas que seriam muito mais trabalhosos sem considerar o isomorfismo.

2.3 Paridades e o Grupo A_n

Nesta seção classificaremos as permutações de acordo com uma característica chamada de **paridade**, que ocorre de acordo com a quantidade de $2-$ciclos que aparecem em sua decomposição por transposições. Mostraremos também que a paridade pode ser determinada sem ambiguidades, e por isso será conveniente separar os elementos de S_n em permutações pares e ímpares.

Proposição 8 *Sempre é possível escrever $\alpha \in S_n$ como produto de transposições.*

Prova: Sabemos que α pode ser decomposto como um produto de ciclos disjuntos, então seja $\alpha_i = (a_1 a_2 \cdots a_r)$ um desses ciclos arbitrariamente escolhidos. Uma técnica que nos permite decompor α em transposições é a seguinte: $\alpha_i = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2)$. Basta repetir esse processo para os ciclos restantes que compõem α. ■

A decomposição dada pela **Proposição 8** não é única, pois por exemplo, utilizando esta técnica pode-se verificar que $(12345) = (15)(14)(13)(12)$, mas também claramente é verdade que $(12345) = (54)(52)(21)(25)(23)(13)$. Porém, existe uma grandeza invariante nas representações, que é a quantidade de transposições que forma o ciclo:

Lema 1 *Se $id = \tau_1 \tau_2 \cdots \tau_n$ onde cada τ_i é uma transposição, então n é par.*

Teorema 13 *Se uma permutação $\alpha \in S_n$ for decomposta em um número par de transposições, então qualquer outra decomposição em transposições também possui um número par de transposições. Respectivamente, o mesmo é válido para um número ímpar de transposições.*

Prova: Seja $\alpha = \tau_1 \tau_2 \cdots \tau_r = \upsilon_1 \upsilon_2 \ldots \upsilon_s$, onde τ_i, υ_j são transposições. Então, $id = \upsilon_1 \upsilon_2 \cdots \upsilon_s \tau_r^{-1} \cdots \tau_1^{-1}$. Como $\tau_i^{-1} = \tau_i$, pois a ordem de uma transposição é 2, temos que

$id = \upsilon_1\upsilon_2\cdots\upsilon_s\tau_r\cdots\tau_1$. Pelo **Lema 1**, $r+s$ é par, e portanto r e s são ambos pares ou ímpares ao mesmo tempo. ■

Como a paridade de uma decomposição por transposições está sempre bem definida, i.e., sem ambiguidades, convém categorizar as permutações de um conjunto finito levando em consideração sua paridade. Há algumas formas equivalentes de definir paridades em que algumas poder ser mais úteis, a depender do problema a ser resolvido.

Definição 23 *Seja $\alpha \in S_n$. Se na decomposição de α por transposições ocorre um número par de $2-$ciclos, então α é uma* ***permutação par****. Caso contrário, dizemos que α é uma* ***permutação ímpar****.*

Equivalentemente, também podemos definir a paridade de uma permutação a partir de uma função estabelecidade entre os grupos S_n e $\{-1, 1\}$.

Definição 24 *Seja a função sgn: $S_n \longrightarrow \{-1, 1\}$ definida por*

$$sgn(\alpha) = \prod_{1\leq i<j\leq n} \frac{\alpha(j) - \alpha(i)}{j - i}.$$

Dizemos que α é par se $sgn(\alpha) = 1$, e ímpar quando $sgn(\alpha) = -1$. A função sgn é conhecida também como função ***sinal*** *de α.*

Segue diretamente da definição que se α é uma transposição, então seu sinal é -1. Suponha, sem perda de generalidade, que $a_2 > a_1$:

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

A seguinte proposição nos será últil para descobrir quantas permutações de S_n são pares e quantas são ímpares.

Proposição 9 *A função $sgn : S_n \longrightarrow \{-1, 1\}$ é um homomorfismo.*

Prova: Devemos mostrar que dados $\alpha, \beta \in S_n$, temos $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$. De fato,

$$\begin{aligned} sgn(\alpha\beta) &= \prod_{1\leq i<j\leq n} \frac{(\alpha\beta)(j) - (\alpha\beta)(i)}{j-i} \\ &= \prod_{1\leq i<j\leq n} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{j-i} \\ &= \prod_{1\leq i<j\leq n} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{j-i} \cdot \frac{\beta(j)-\beta(i)}{\beta(j)-\beta(i)} \\ &= \prod_{1\leq i<j\leq n} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{\beta(j)-\beta(i)} \cdot \frac{\beta(j)-\beta(i)}{j-i} \\ &= \prod_{1\leq i<j\leq n} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{\beta(j)-\beta(i)} \cdot \prod_{1\leq i<j\leq n} \frac{\beta(j)-\beta(i)}{j-i} \\ &= sgn(\alpha) \cdot sgn(\beta). \end{aligned}$$

Logo, sgn é um homomorfismo. ■

Isto nos mostra que produtos de permutações que são ambas pares ou ambas ímpares é sempre par, o que é consistente com a definição que foi dada a partir do número de transposições de uma decomposição em $2-$ciclos. Também podemos observar que a permutação id é uma permutação par, pois:

$$\begin{aligned} sgn(id) &= \prod_{1\leq i<j\leq n} \frac{id(j) - id(i)}{j-i} \\ &= \prod_{1\leq i<j\leq n} \frac{j-i}{j-i} \\ &= 1. \end{aligned}$$

O resultado acima nos faz ter certeza que o conjunto das permutações ímpares não pode ser um subgrupo de S_n, pois ele não contém o elemento identidade e nem é fechado sob a operação de composição. Mas, será que o mesmo ocorre para as permutações pares? Um modo mais elegante de verificar se as permutações pares são de fato subgrupo de S_n sem verificar os axiomas de grupo é calculando o núcleo de sgn, ker_{sgn}:

Proposição 10 *O conjunto das permutações pares de S_n é um subgrupo normal de S_n. Este subgrupo também é conhecido por* ***grupo alternado*** *de grau n, denotado por A_n.*

Prova: Seja $sgn : S_n \longrightarrow \{-1, 1\}$ o homomorfismo sinal. Note que $ker_{sgn} = A_n$. Como $ker_{sgn} \lhd S_n$, segue que $A_n \lhd S_n$. ■

Corolário 2 *Para $n > 1$, exatamente metade das permutações de S_n são pares.*

Prova: Pelo **Teorema 3**, temos que $S_n/A_n \cong sgn(S_n)$. Mas, sempre haverão permutações pares e ímpares em S_n, como a identidade e alguma transposição qualquer, respectivamente.

Portanto, sgn é um homomorfismo sobrejetor. Logo,

$$\begin{aligned} S_n/ker_{sgn} \cong sgn(S_n) &\implies S_n/A_n \cong \{-1, 1\} \\ &\implies |S_n/A_n| = |\{-1, 1\}| \\ &\implies |S_n/A_n| = 2 \\ &\implies |S_n|/|A_n| = 2 \\ &\implies |A_n| = |S_n|/2 \\ &\implies |A_n| = n!/2, \end{aligned}$$

como queríamos verificar. ■

Podemos utilizar a ideia de produto semidireto para decompor o grupo simétrico em grupos menores, uma vez que já sabemos como ele se comporta.

Exemplo 9 *Note que tomando $(1\ 2) \in S_n$, temos que $\langle(1\ 2)\rangle = \{e, (1\ 2)\}$, e como $(1\ 2)$ é uma permutação ímpar, segue-se que $A_n \cap \langle(1\ 2)\rangle = \{e\}$. E também se considerarmos o conjunto $A_n \cdot \langle(1\ 2)\rangle = \{(\alpha\beta)(x) \mid \alpha \in A_n \text{ e } \beta \in \langle(1\ 2)\rangle\}$, vemos que $S_n = A_n \cdot \langle(1\ 2)\rangle$. Unindo essas informações com o fato de que $A_n \lhd S_n$, segue-se que $S_n = A_n \rtimes \langle(1\ 2)\rangle$.*

Exemplo 10 *Sejam $\mathbb{Z}_m$ o grupo dos inteiros aditivos módulo m e S_n o grupo simétrico de grau n e $X = \{x_1, x_2, \cdots, x_n\}$ um conjunto finito. O produto entrelaçado de $\mathbb{Z}_m$ por S_n é $\mathbb{Z}_m \wr S_n$, onde $\psi : S_n \longrightarrow Aut(\mathbb{Z}_m^n)$ é dada por $\psi(\alpha)(x_1, x_2, \cdots, x_n) = (x_{\alpha(1)}, x_{\alpha(2)}, \cdots, x_{\alpha(n)})$. O grupo $\mathbb{Z}_m \wr S_n$ é conhecido como* ***Grupo Simétrico Generalizado****.*

Capítulo 3

Grupo de Rubik

Nete capítulo, dividido em 5 seções, descreveremos a estrutura física do cubo de Rubik (ou cubo mágico $3 \times 3 \times 3$) e como as suas peças se comportam a medida que fazemos alguns movimentos permitidos em suas faces. Finalizamos descrevendo a estrutura do grupo de Rubik $\mathcal{R}$ e alguns de seus subgrupos.

As referências bibliográficas utilizadas para este capítulo foram [1], [12] e [18].

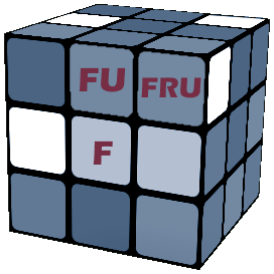
3.1 Estrutura Física Do Cubo Mágico

O cubo mágico é composto por diversos cubos menores que chamaremos de **quinas**, **meios** e **centros**. Deste modo, totalizando 26 cubos, existem 8 quinas, 12 meios e 6 centros e, para que consigamos fazer a construção do grupo de Rubik, é importante classificarmos todos esses cubos. Note que no cubo $3 \times 3 \times 3$, todas as faces possuem um centro e este centro define a cor que essa face irá possuir. Isto é, se ao olhar uma face do cubo, identificamos que a peça central é da cor branca, isto significa que toda face deverá ser branca quando o cubo estiver resolvido. Além disso, todas as quinas são cubinhos que possuem três cores e todos os meios são cubinhos que possuem duas cores então, não é possível que uma quina fique no lugar de um meio e vice-versa. É importante ressaltar que as cores de um cubo também possuem um padrão a ser seguido no qual os centros amarelo e branco serão sempre opostos, bem como os centros azul e verde, e os centros vermelho e laranja. Além disso, se posicionamos o cubo com o centro branco para cima e o centro amarelo para baixo, temos

que o centro verde fica à esquerda do centro vermelho, que fica à esquerda do centro azul, e que por sua vez fica à esquerda do centro laranja.

Como estamos interessados em rotacionar as faces do cubo para solucioná-lo, é conveniente estabelecer notações, que mais adiante serão úteis para gerarmos o grupo de Rubik. A convenção internacional, introduzida primeiramente em [18], nomea os lados do cubo utilizando como referência a face que está voltada para frente da pessoa que está resolvendo, eles são denotados pelas letras f (face frontal), b (face traseira), r (face lateral direita), l (face lateral esquerda), d (face inferior) e u (face superior). Esta notação faz sentido se usarmos os nomes em inglês, como *front*, *back*, *right*, *left*, *down* e *up*, respectivamente. Foi convencionado pela *World Cube Association* (WCA) que qualquer embaralhamento com o cubo já resolvido deve ser feito com a face verde na posição f e a face branca na posição u, e é com esse modelo padrão que desenvolveremos alguns dos exemplos mais adiante. Nos baseando nessas notações, também é mostrado em [18] que somos capazes de classificar os cubos menores citados anteriormente, levando em consideração o número de faces com as quais as peças estão tendo contato, como podemos ver abaixo:

Figura 3.1: Notação das Peças



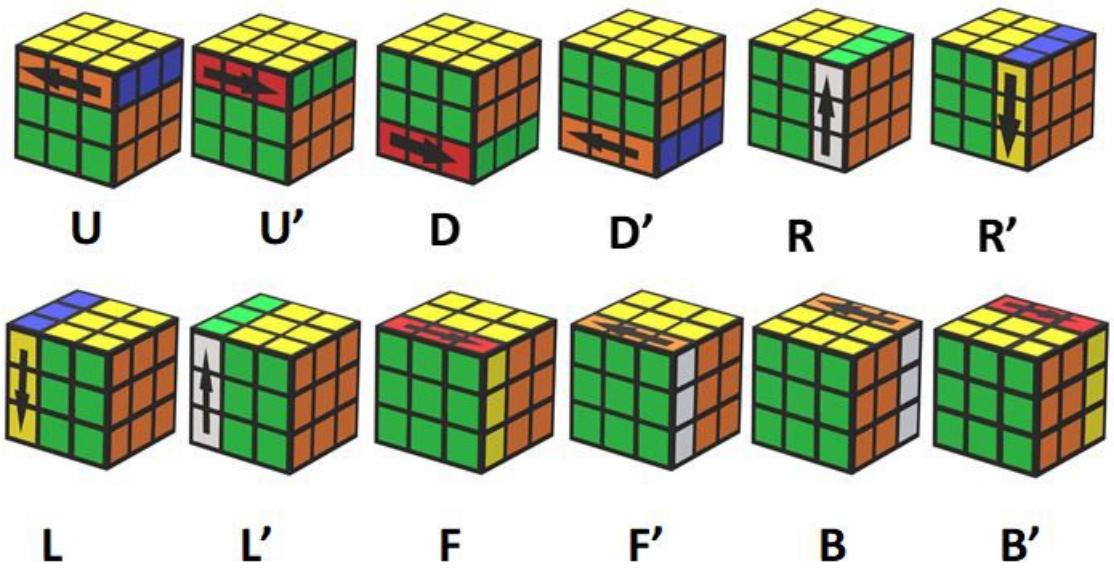
Fonte: Disponível em: https://ruwix.com/the-rubiks-cube/notation/advanced/. Acesso em: 3 Ago. 2022.

A peça central é denotada pela letra f, pois está apenas na face da frente. A peça de meio que está na parte superior é denominada fu pois pertence tanto ao topo do cubo quanto a sua face frontal. E a quina destacada é denotada por fru, não importando a ordem das letras, pois esta quina está tanto na face frontal quanto na lateral superior. Este mesmo padrão se repete para todas as peças. Então, teremos peças com nomes bld, lbu, dfr, bu e etc.

3.2 Macros

A seção **3.1** nos leva a classificação dos movimentos iniciais de rotações no cubo mágico, que são sequências de movimentos chamadas de **macros**, que utilizam das rotações de todas as faces no sentido horário ou no sentido anti-horário. As notações dos giros são bem parecidas com as próprias notações das faces, isto é, quando falamos de movimentos, a letra F significa girar a face f no sentido horário. A letra R significa girar a face r no sentido horário, e assim sucessivamente. Caso seja necessário girar uma face no sentido anti-horário, denotamos esse giro com um apóstrofo ou com o expoente -1, por exemplo, o giro R' (ou R^{-1}). Podemos ver abaixo uma classificação de todos os movimentos básicos que usamos para manipular o cubo, com as suas respectivas notações.

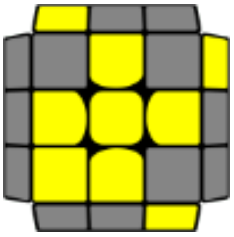
Figura 3.2: Movimentos



Fonte: Disponível em: https://i.stack.imgur.com/8i7FQ.jpg. Acesso em: 13 Nov. 2022.

Para quem já está familiarizado com o método CFOP de resolução do cubo mágico, a palavra $RUR'URU^2R'$, ou equivalentemente, $RUR^{-1}URU^2R^{-1}$, é muito importante, pois esta é uma macro que resolve o topo do cubo quando ele se encontra da seguinte forma:

Figura 3.3: OLL 27

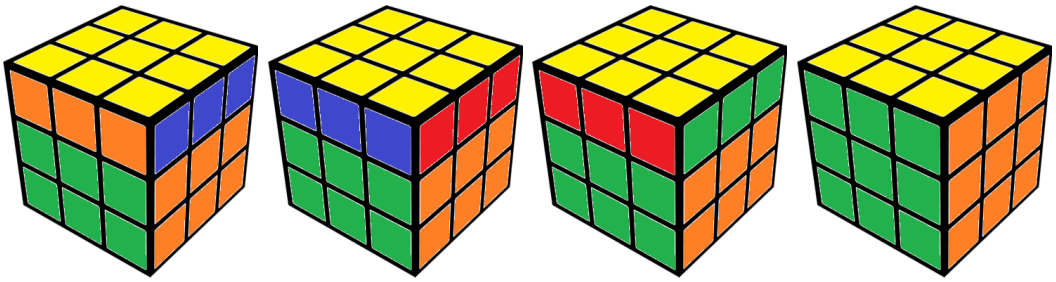


Fonte: Disponível em: https://algs.cuber.pro/333/OLL/27. Acesso em: 3 Ago. 2022.

Esta é uma configuração de topo intitulada OLL 27, abreviação para *Orientation of the last layer*, ou "sune". [1]

A permutação U no cubo mágico pode ser decomposta em ciclos da seguinte forma: perceba que nas peças de meio ela faz a seguinte troca: $fu \to lu \to bu \to ru \to fu$, e nas peças de quina $rfu \to lfu \to blu \to bru \to rfu$, e portanto $U = (rfu \;\; lfu \;\; blu \;\; bru)(fu \;\; lu \;\; bu \;\; ru)$. Observando a maneira que escrevemos o ciclo, ou até mesmo realizando os movimentos no cubo, conseguimos concluir que $|U| = 4$.

Figura 3.4: cubo quando repetimos a permutação U



Fonte: Os Autores

Se considerarmos uma outra macro qualquer no cubo, é possível sempre calcularmos a sua ordem por meio da decomposição de ciclos disjuntos. Porém, esse cálculo será mais conveniente quando identificarmos as peças do cubo com números e não com letras, como faremos adiante.

[1] Acesso livre em https://www.speedsolving.com/wiki/index.php/Sune

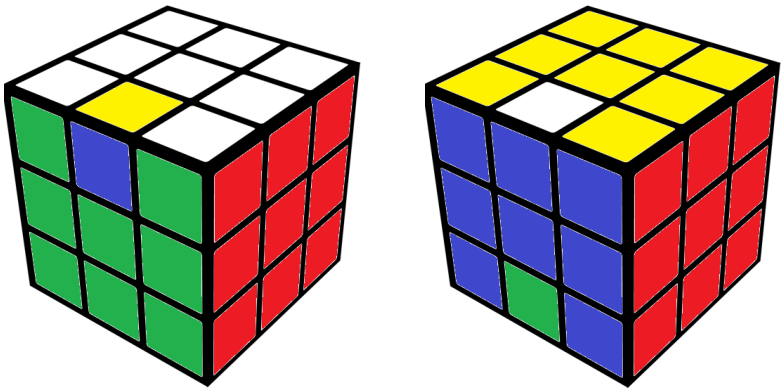
3.2.1 Comutadores e Conjugados

Existem macros que nos permitem manipular algumas peças específicas do cubo enquanto queremos preservar outras. Por exemplo, há situções em que precisamos trocar dois cubinhos de posição ou mudar a orientação de determinada peça.

Podemos fazer alguns testes no cubo e ver que nem sempre dois movimentos comutam, utilizando a **Definição 5**. Se considerarmos os elementos R e F, temos que $[R, F] = RFR^{-1}F^{-1} \neq e$. Mas por outro lado, considerando os elementos D e U, temos que $[D, U] = DUD^{-1}U^{-1} = e$. Isso ocorre para quaisquer elementos do cubo que comutam entre si.

Para um exemplo mais construtivo, vamos definir o movimento M como sendo girar a camada do meio no sentido de R^{-1} (apenas uma combinação dos elementos L^{-1} e R), e também definimos o movimento M^{-1} como sendo girar a camada do meio no sentido de R (dessa vez estamos combinando os elementos L e R^{-1}). Deste modo temos basicamente $M = L^{-1}R$ e $M^{-1} = R^{-1}L$. Aplicando o comutador $[M^{-1}, U^2] = M^{-1}U^2MU^2$, trocamos exatamente três peças de meio de lugar enquanto o restante do cubo permanece como estava. Neste caso, as peças que mudam de posição são os meios uf, ub e db.

Figura 3.5: Cubo quando aplicamos $[M^{-1}, U^2]$.



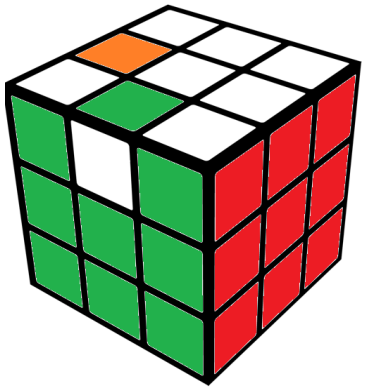
Fonte: Os Autores

Um dos exemplos mais interessantes de comutadores é o seguinte: definimos o movimento U_s como sendo mover a camada do meio no sentido de U, e similarmente U_s^{-1} sendo mover a fatia central no sentido de U^{-1}. Sejam agora

$$X = LU_s^{-1}L^2U_s^2L \qquad \text{e} \qquad Y = U.$$

Então, quando aplicamos $[X, Y] = (LU_s^{-1}L^2U_s^2L)U(L^{-1}U_s^2L^2U_sL^{-1})U^{-1}$, essa macro tem efeito somente em dois meios do cubo, que são os meios uf e ul, enquanto que o restante do cubo não se altera. Além disso, essa macro é muito especial pois ela é um comutador do tipo orientação, isto é, aplicando-a nenhuma peça do cubo sai do seu respectivo lugar, e as peças afetadas apenas são giradas. Aplicando $[X, Y]$ no cubo resolvido obtemos a seguinte configuração:

Figura 3.6: cubo quando aplicamos o comutador de orientação



Fonte: Os Autores

De modo intuitivo, uma conjugação no cubo mágico move os mesmos tipos de peças. Por exemplo, se X e Y são movimentos quaisquer e X muda de lugar três peças de meio e duas quinas então, a conjugação YXY^{-1} mudará de lugar exatamente três meios e duas quinas (não necessariamente as mesmas), independentemente de qual movimento seja Y. Essa estratégia é vantajosa quando estamos investigando modos de resolver certo caso e queremos resolver por meio de conjugações, pois já temos em mente quais tipos de peças estamos interessados em mover.

Um exemplo muito comum durante uma resolução de *speedcubing*, que é a modalidade de competição de cubo mágico visando resolvê-lo em menos tempo, é a configuração OLL 45, representada abaixo, que é resolvida por meio de conjugação:

Figura 3.7: OLL 45

Fonte: Disponível em: https://algs.cuber.pro/333/OLL/45. Acesso em: 13 Nov. 2022.

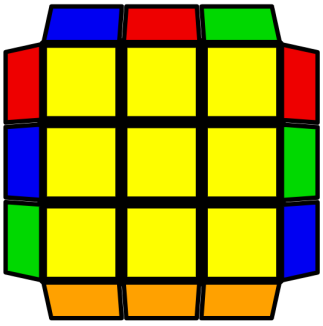
Para finalizar esta etapa, note que se não nos importamos ainda com a permutação das peças da última camada do cubo, podemos mover 4 cantos e 2 meios para resolver o topo apenas. Considere

$$X = F \quad \text{e} \quad Y = RUR^{-1}U^{-1}.$$

Perceba que Y movimenta quatro cantos sendo que dois desses cantos permanecem com as cores iniciais voltadas para cima e os outros dois cantos tem as cores que estavam pra cima trocadas. Este movimento também altera dois meios, mudando sua orientação. Daí, temos que a conjugação XYX^{-1} tem esse mesmo efeito e, de fato, ela resolve o topo quando ele se encontra nesta configuração. Caso estivéssemos investigando como resolver essa configuração por meio de conjugações, poderíamos descartar como possibilidades para conjugar elementos que não alterassem a mesma quantidade de peças que queremos mexer.

Outro exemplo também muito comum é ilustrado na figura abaixo:

Figura 3.8: PLL F



Fonte: Disponível em: http://algdb.net/puzzle/333/pll/f. Acesso em: 15 Nov. 2022.

A configuração da **Figura 3.8** é chamada PLL F, sigla para *Permutation of The Last Layer type F*. Não é difícil perceber que precisamos mudar exatamente dois meios e dois cantos. Podemos considerar os movimentos:

$$X = R^{-1}U^{-1} \qquad \text{e} \qquad Y = F^{-1}RUR^{-1}U^{-1}R^{-1}FR^2U^{-1}R^{-1}U^{-1}RUR^{-1}$$

Observe que, fazendo manipulações no cubo, o movimento Y afeta exatamente a mesma quantidade de peças que desejamos mover. Se aplicarmos a conjugação XYX^{-1} temos o mesmo efeito. De fato, esse é um dos modos mais eficientes de se resolver essa configuração seja em questão de tempo ou em questão de quantidade de movimentos.

A ideia que citamos acima também ocorre quando uma certa macro X altera várias peças formando um ciclo. Se X move quatro meios do cubo formando um ciclo, quando conjugamos essa macro por uma outra macro Y também alteramos a mesma quantidade de meios em um ciclo de mesmo tamanho.

De fato, muitos algoritmos descobertos com o uso de programas de computador se baseiam nas noções de comutadores e conjugados, uma vez que é possível filtrar os movimentos que podemos fazer, observando as peças que desejamos mudar. Mesmo que alguns algoritmos encontrados dessa forma sejam um pouco longos para executar de forma rápida, eles são relativamente mais rápidos de serem encontrados por computador.

3.3 Possibilidades de Movimentos Existentes no cubo Utilizando o Princípio Fundamental da Contagem (P.F.C.)

A partir de observações acerca da estrutura do cubo, ou também da manipulação do mesmo, isto é, girando as faces aleatoriamente utilizando movimentos básicos, percebemos que as peças centrais de cada face não mudam de posição. Por este motivo dizemos que estas são as *únicas peças fixas do cubo*. Esse fato é consequência dos seguintes resultados gerais:

Lema 2 *Sejam G um grupo finito e $g \in G$. Então $g^{-1} = g^n$, para algum $n \in \mathbb{N}$.*

Prova: Se $g = e$ é imediato, pois $e = e^{-1} = e^n, \forall n \in \mathbb{N}$. Suponha então $g \neq e$.

Como G é finito, então $g^m = e$, para algum $m \in \mathbb{N}$, com $m > 1$. Façamos $n = m - 1$, e então temos que $g \cdot g^n = e$ donde segue que $g^{-1} = g^n$. ■

Lema 3 *Seja G um grupo finito e $S \subset G$. Então $G = \langle S \rangle$ se, e somente se, todo elemento de G pode ser escrito como um produto finito de elementos de S.*

Prova: ($\Longleftarrow$) Imediato, pois se todos os elementos de G podem ser escritos como um produto finito de elementos de S, então S é um conjunto gerador para G.

($\Longrightarrow$) Suponha que $G = \langle S \rangle$. Se $g \in G$, então $g = s_1 \cdot s_2 \cdots s_j$ com $s_i \in S \cup S^{-1}$.

Para $n = 1$, temos $g = s_1$. Se $s_1 \in S$, então g pode ser escrito como produto finito de elementos de S. Se $s_1 \in S^{-1}$, isso implica que $s_1^{-1} \in S$, e também $s_1^{-1} \in \langle S \rangle$, e pelo **Lema 2** e o fato de $\langle S \rangle$ ser um grupo finito, temos que $s_1^{-1} = s_k^n$, para algum $n \in \mathbb{N}$ e $s_k \in S$. Segue daí que $g = \underbrace{s_k \cdots s_k}_{n\text{vezes}}$. Então, para $n = 1$, a base de indução é válida.

Suponha a validade para $1, 2, \cdots, j-1$. Queremos mostrar que $s_1 \cdot s_2 \cdots s_j$ pode ser escrito como um produto finito de elementos de S. Por hipótese, o produto $s_1 \cdot s_2 \cdots s_{j-1}$ pode ser escrito como produto finito de elementos de S, bem como s_j. Desta forma, podemos concluir que seu produto satisfaz a mesma propriedade, isto é, o produto $s_1 \cdot s_2 \cdots s_j$ pode ser escrito como um produto finito de elementos de S. ■

No **Lema 3**, note que S não é necessariamente um subgrupo de G, mas mesmo assim não precisamos dos seus inversos para representar os elementos de G.

Proposição 11 *Seja G um grupo finito e $S \subset G$. Suponha que as condições abaixo são satisfeitas:*

(i) Todo elemento de S satisfaz certa propriedade P;

(ii) Se $x, y \in G$ são elementos tais que x satisfaz P e y satisfaz P, então xy satisfaz P.

Então qualquer $s \in \langle S \rangle$ satisfaz P.

Prova: Pelo **Lema 3**, todo elemento de $\langle S \rangle$ pode ser escrito como $s = s_1 \cdot s_2 \cdots s_n$, para $n \in \mathbb{N}$ e $s_i \in S$. Por indução sobre n, vamos mostrar que s satisfaz P.

Caso $n = 1$, então $s_1 \in S$ satisfaz P, por hipótese.

Suponha agora que $s_1 \cdot s_2 \cdots s_{n-1}$ satisfaz P, logo temos que $(s_1 \cdot s_2 \cdots s_{n-1}) \cdot s_n = s_1 \cdot s_2 \cdots s_{n-1} \cdot s_n$ satisfaz P. ■

Podemos enxergar no cubo o conjunto S da **Proposição 11** como $\{R, L, U, D, B, F\}$. É claro que qualquer elemento de S satisfaz a propriedade P, onde P seria deixar as peças de centro fixas. Também podemos verificar que operações entre os elementos desse conjunto satisfazem a mesma propriedade. Daí, segue que todos os elementos do grupo $\langle R, L, U, D, B, F\rangle$ satisfazem P.

Usando essa informação e fato de uma peça de meio não poder se transformar em uma quina, e vice-versa, podemos tentar investigar quantas configurações são possíveis no cubo mágico. Primeiramente, se focamos na posição do cubinho urf, percebemos que há 8 possibilidades de cubinhos que podem assumir essa posição. Agora, isso significa que existem 7 possibilidades restantes para a posição ulf, 6 possibilidades para a posição ubl, e assim sucessivamente. Isto é, existem $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 8!$ modos de posicionar um cubinho em algum dos cantos. Mas além disso, podemos notar que cada uma das peças de canto pode ser girada de três modos distintos e, como podemos girar quaisquer um dos 8 cantos, na verdade existem $3^8 \cdot 8!$ modos de posicionar os cubinhos em cada canto, se levarmos em conta tanto suas posições espaciais quanto a orientação de cada peça.

De modo similar, para as 12 peças de meio, temos 12! modos de posicioná-las, mas se contarmos a orientação, cada peça pode ser girada duas vezes, e isso resulta no número $2^{12} \cdot 12!$ de possibilidades que podemos encontrar configurações para as peças de meio. E, juntando as possibilidades para as quinas e para os meios, obtemos como resultado $2^{12} \cdot 3^8 \cdot 8! \cdot 12!$ ou 519.024.040.000.000.000.000, que é aproximadamente $519 \cdot 10^{18}$ maneiras de dispor as peças de um cubo mágico. Agora, é extremamente importante ressaltar que, apesar de todas essas configurações serem existentes no cubo, nem todas são possíveis, ou válidas, quando seguimos as regras de resolver um cubo mágico. Acontece que é possível girarmos uma quina no cubo forçadamente, mas é impossível girar apenas uma quina utilizando os movimentos básicos citados anteriormente. De fato, veremos que das $519 \cdot 10^{18}$ possíveis configurações, aproximadamente 92% delas não são válidas, são posições que chamamos de "ilegais".

3.4 Estrutura do Grupo Legal de Rubik

Com as observações estabelecidas até o momento, podemos perceber que as trocas de orientações das quinas do cubo podem ser representadas pelo produto direto

$$C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 = C_3^8,$$

e as suas possíveis posições representadas por S_8. Portanto segue que todas as configurações possíveis de dispor as quinas é representado pelo produto $C_3 \wr S_8$.

Para as peças de meio podemos fazer uma análise totalmente análoga, ou seja, as orientações de meio podem ser representadas pelo produto direto C_2^{12} e suas possíveis posições por S_{12}. De maneira análoga, todas as configurações para o meio podem ser representadas pelo produto $C_2 \wr S_{12}$.

Para representarmos o **Grupo Ilegal de Rubik** $\mathcal{I}$, vamos identificá-lo por

$$\mathcal{I} = (C_3 \wr S_8) \times (C_2 \wr S_{12})$$

sendo este o grupo em que podemos tirar peças e colocar do jeito que quisermos, bem como rotacionar forçadamente quinas e meios uma vez que todas essas posições estão incluídas em $\mathcal{I}$.

Como foi citado, todas as configurações "legais" do cubo são provenientes dos movimentos fundamentais F, U, B, L, R e D, ou seja, se girarmos uma quina por exemplo, isso torna impossível de montar o cubo novamente utilizando apenas estes movimentos. Por isso é importante discutirmos a diferença entre os movimentos "legais" e "ilegais" e como eles afetam a estrutura de grupo do cubo. Para tanto, é necessário sabermos o que significa uma peça *estar orientada* de acordo com uma orientação padrão pré-estabelecida, pois a noção de orientação é fundamental para discutir posições possíveis no cubo:

Orientações

Joyner [12] nos mostra uma forma de fixar as orientações no cubo. Nas peças de meio marcamos com um +:

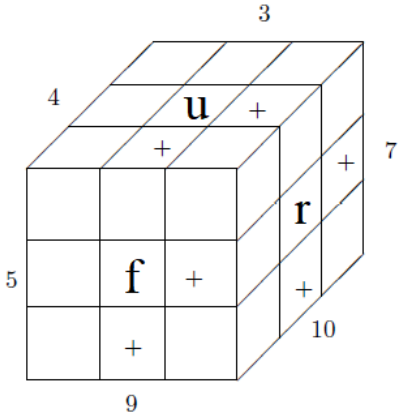
1. No lado u do cubinho uf;

2. No lado u do cubinho ur;

3. No lado f do cubinho fr;

4. Em todos os outros lados dos cubinhos que podem ser alcançados pelos anteriores por um movimento de camada de meio (movimento de fatia).

Figura 3.9: Orientação dos meios

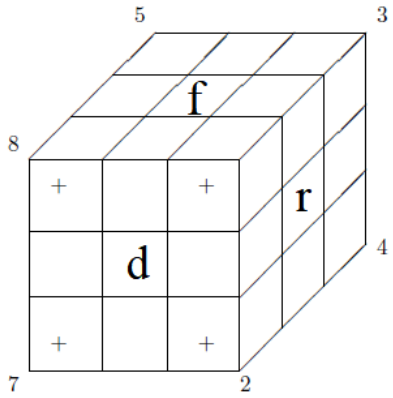


Fonte: Joyner (2002)

A numeração representa apenas uma ordem arbitrária de cada um dos 12 meios para depois podermos escrever a orientação dos meios como uma $12-$upla, mas esta ordem não é relevante nesse contexto.

Para as quinas fazemos algo semelhante, marcando com um $+$ todos os lados das quinas que estão na face d e que estão na face u:

Figura 3.10: Orientação dos cantos



Fonte: Joyner (2002)

Essas orientações são as que chamamos **orientações padrão**, e é claro que quando fazemos movimentos no cubo, as marcações que fizemos irão para outros lugares, mas vamos considerar a marcação inicial como sendo a posição para onde as marcações devem retornar.

Foi dito anteriormente que cada quina do cubo pode ser girada de três modos diferentes. Vamos considerar $v \in C_2^8$ como sendo a $8-$upla tal que $v = (v_1, \ldots, v_8)$, e v_i o número de vezes em que a $i-$ésima quina precisa ser girada para a direita para que sua marcação com + fique na posição padrão. Por exemplo, fazendo o movimento R, obtemos o $8-$upla $v = (1, 2, 2, 1, 0, 0, 0, 0)$, pois a primeira quina precisa ser girada apenas uma vez para direita para que sua marcação fique no mesmo lugar na qual havia uma marcação posição padrão antes do cubo ser mexido, a segunda quina precisa ser girada duas vezes, e assim por diante. Podemos perceber que as últimas 4 entradas são nulas, isso significa que todas essas peças já estão com a marcação + onde deveriam estar já que elas nem foram mexidas com esta macro.

Analogamente para as peças de meio, iremos considerar $w \in C_2^{12}$ a $12-$upla de orientação. Agora suas entradas consisitrão apenas de entradas com zeros e uns. No mesmo exemplo anterior, para a macro R, $w = (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$ é a $12-$upla obtida para a orientação dos meios. Dizemos que a ordem das entradas nesse contexto não é tão relevante pois estamos mais interessados nos números que são atribuídos às entradas das $n-$uplas de orientação do que a ordem das entradas em si. Isto ocorre por conta do seguinte teorema:

Teorema 14 (Primeiro Teorema Fundamental da Teoria dos cubos) *Considere* $v = (v_1, v_2, \ldots, v_8) \in C_3^8$, $r \in S_8$, $w = (w_1, w_2, \ldots, w_{12}) \in C_2^{12}$ *e* $s \in S_{12}$, *onde* v *corresponde à orientação de todas as quinas,* r *corresponde à posição de todas as quinas,* w *corresponde à orientação de todos os meios e* s *corresponde à posição de todos os meios. Então a quádrupla* (v, r, w, s) *é uma posição possível no cubo se, e somente se, as* 3 *condições abaixo são satisfeitas:*

(i) $sgn(r) = sgn(s)$;

(ii) $v_1 + v_2 + \cdots + v_8 \equiv 0 \ (mod\ 3)$;

(iii) $w_1 + w_2 + \cdots + w_{12} \equiv 0 \ (mod\ 2)$.

Em outras palavras, a quádrupla (v, r, w, s) é uma posição possível no cubo, se e somente se as permutações r e s tem a mesma paridade, a quantidade de giros nas quinas é um múltiplo de 3, e a quantidade de giros nas peças de meio é um múltiplo de 2.

Prova: ($\Longrightarrow$) Seja $v \in C_3^8, r \in S_8, w \in C_2^{12}, s \in S_{12}$ e $g \in G$, onde g é uma macro em termos dos movimentos básicos que deixa o cubo na posição (v, r, w, s). Portanto temos que $g = M_1 M_2 \cdots M_n$, onde $M_i \in \{R, L, F, B, D, U\}$.

(i) Com cada um desses movimentos, um total de quatro meios e quinas são movidos de lugar, isto é, o número de quinas movidas ao final da operação coincide com o número de meios movidos. Perceba que todas essas permutações são $4-$ciclos, que é uma permutação ímpar, daí para qualquer g, temos $sgn(r) = \prod_{k=1}^{n} sgn(M_k) = sgn(s)$, levando em consideração que permutações ímpares quando compostas com permutações ímpares resultam em uma permutação par, e permutações pares quando compostas com permutações ímpares resultam em uma permutação ímpar.

(ii) Note que se M_i corresponde ao movimento U ou D, então v permanece o mesmo, pois não há giros nas quinas. Se M_i corresponde aos movimentos R, L, F ou B, então duas quinas são movidas. Uma quina da face u é movida para baixo, e uma quina da face d é movida para cima. Desse modo, os componentes de v são ao mesmo tempo diminuídos por $1 (mod\ 3)$ e aumentados por $1 (mod\ 3)$, respectivamente. Isso significa que, para quaisquer um dos movimentos R, L, F, B, temos que

$$\sum_{k=1}^{8} v_k \equiv 1\ (mod\ 3) - 1\ (mod\ 3) \equiv 0\ (mod\ 3)$$

(iii) Para qualquer g, temos um total de quatro meios sendo reorientados, daí

$$\sum_{k=1}^{12} w_k \equiv 4\ (mod\ 2) \equiv 0\ (mod\ 2)$$

($\Longleftarrow$) Seja $A = (v, r, w, s)$, tal que as condições $(i), (ii)$ e (iii) sejam satisfeitas. Vejamos que A pode ser alcançada por movimentos básicos.

Pela condição (i) temos que $sgn(r) = sgn(s)$, então as permutações de quinas e meios são ambas pares ou ambas ímpares. Suponh que $sgn(r) = sgn(s) = 1$, pois o caso ímpar

é trivial, bastando aplicar qualquer um dos movimentos básicos que a nova permutação irá satisfazer $sgn(r) = sgn(s) = 1$.

Agora, considere um $3-$ciclo de quinas, por exemplo $M = RB^{-1}RF^2R^{-1}BRF^2R^2$, que gera o ciclo $(ulf\, urf\, urb)$, e para simplificar notação vamos denotar $ulf = a_1, urf = a_2, urb = a_3$, e o restante das quinas de $a_i, 4 \leq i \leq 8$. Para cada $a_i, 4 \leq i \leq 8$, existe um movimento x composto de no máximo dois movimentos básicos tal que a_i seja movido para a posição a_3 sem alterar as posições de a_1 e a_2. Então, aplicando o movimento xMx^{-1}, obtemos que ele cria o $3-$ciclo $(a_1\, a_2\, a_i)$, e esse $3-$ciclo pode ser obtido para qualquer a_i, isto é, $(a_1\, a_2\, a_3)$, $(a_1\, a_2\, a_4)$, $(a_1\, a_2\, a_5)$, $(a_1\, a_2\, a_6)$, $(a_1\, a_2\, a_7)$, $(a_1\, a_2\, a_8)$ podem ser obtidos a partir de um movimento x conveniente. Mas isto gera todas as permutações pares de quinas, então existe um movimento x que faz as quinas voltarem às suas devidas posições.

Um raciocínio análogo pode ser desenvolvido para as permutações de meios para mostrar que existe um movimento y apropriado que retorna todos os meios às suas posições iniciais, e o que falta fazermos é orientar as peças para que suas cores combinem com a face em que estão.

A condição (ii) nos diz que há uma conservação no total de giros, isto é, o número de giros no sentido anti horário é igual ao número de giros no sentido horário, isso sginifica que existe um movimento que gira exatamente duas quinas, e preserva a orientção e a posição do resto do cubo, por exemplo, o movimento $M_1 = (R^{-1}D^2RB^{-1}U^2B)^2$, que gira o canto ufr em $120°$ e gira o canto bdf em $-120°$. Note que M_1 pode ser modificado para obter um resultado similar para quaisquer duas quinas do cubo. Para começar a reorientar as facetas das quinas, primeiro giramos qualquer par no sentido horário e no sentido anti horário, respectivamente, de modo que eles fiquem na orientação certa. As quinas restantes ocorrerão em triplas, umas vez que as quinas odebecem $\sum_{k=1}^{8} v_k \equiv 0\ (mod\ 3)$, então teremos ou 3 giros no sentido horário, ou 3 giros no sentido anti horário. Vamos chamar de c_1, c_2 e c_3 esses cubos. As quinas restantes podem ser resolvidas por uma sequência de movimentos que giram quinas, por exemplo $M_1^* = L^{-1}D^2LBD^2B^{-1}UBD^2B^{-1}L^{-1}D^2LU^{-1}$ ou qualquer outra macro similar que tenha este efeito. A estratégia é que sabendo como a macro afeta as quinas, podemos levar quinas que estão erradas para certas posições utilizando uma macro x, ajeitá-las via uma macro de orientação, e depois retorná-la para seu lugar utilizando x^{-1}, de modo que todos os cantos estejam no seu estado resolvido.

Por (iii) temos uma conservação no número total de giros de meios, isto é, existe um número par de meios que precisam ser girados para seu estado padrão. Mas existe uma macro que muda exatamente a orientação de dois meios enquanto deixa o restante do cubo intacto, por exemplo $M_2 = LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$, então utilizando a mesma estratégia, de levar meios para as posições alteradas por M_2, alterar suas orientações, e depois retorná-las a posição inicial, podemos resolver todos os meios.

De fato é possível resolver todo o cubo conhecendo apenas duas macros, uma para orientar os meios e outra para orientar os cantos, e utilizar a estratégia: sabendo exatamente que peças essas macros afetam, movemos as peças que precisam ser movidas para estas posições, reorientamos utilizando uma macro conhecida, e após isso levamos a peça de volta para sua posição resolvida. ■

O próximo teorema nos fornece informações sobre as macros no cubo. Mais especificamente, nos dá um critério para que determinada macro seja possível:

Teorema 15 (Segundo Teorema Fundamental da Teoria dos cubos) *Uma operação no cubo é possível se, e somente se, as condições abaixo são satisfeitas:*

(1) O número total de ciclos de meios e de quinas de comprimento par, é par;

(2) O número de ciclos de quinas girados para a esquerda, é igual ao número de ciclos de quinas girados para a direita reduzido módulo 3*, se necessário;*

(3) Há um número par de ciclos que reorientam as peças de meio.

Prova: $(\Longrightarrow)$

(1) Pelo item (i) do **Teorema 14**, temos que $sgn(r) = sgn(s)$, mas isso significa que a permutação é par, logo, o comprimento dos ciclos de quinas e meios é par.

(2) Para qualquer macro M, as quinas giradas para esquerda, para a direita, ou para nenhum lado. Então o ciclo muda a soma de v_i por 2, 1 ou 0 $(mod\ 3)$, respectivamente. Pelo **Teorema 14**,

$$\sum_{k=1}^{8} v_k = 0$$

então o número de giros para a esquerda deve coincidir com o número de giros para a direita.

(3) Perceba que um ciclo de meios apenas volta para sua orientação quando é mudado por um número ímpar, pois possui duas cores. Isto é, $w_j = 1$, para algum $1 \leq j \leq 12$. Mas o **Teorema 14** nos diz que

$$\sum_{k=1}^{12} w_k = 0$$

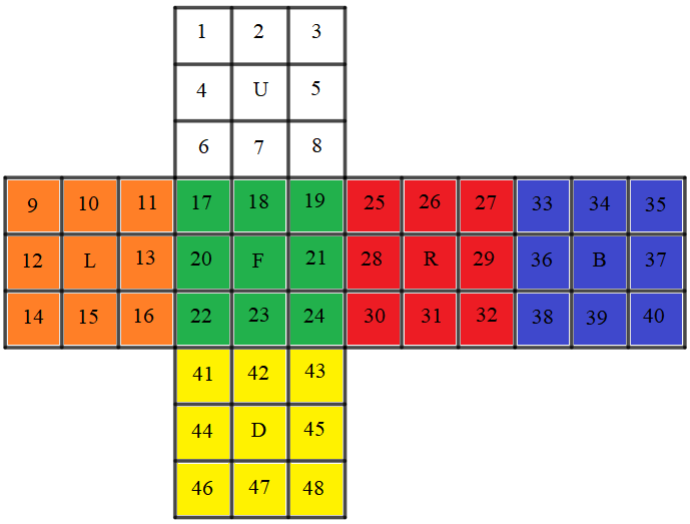
isto é, não é possível que apenas 1 meio seja reorientado sem que algum outro também seja, e de fato as peças de meio se reorientam em pares.

($\Longleftarrow$) Suponha que *(1)*, *(2)* e *(3)* sejam satisfeitas. Existe um movimento M que leva o cubo resolvido em um estado g e também um movimento M^{-1} que leva o cubo no estado g para o estado resolvido. Agora, por hipótese, se M e M^{-1} satisfazem as três condições acima, então M^{-1} também as satisfaz. Daí estas condições implicam que a operação é válida. ■

Equivalentemente, o conjunto de todas as configurações possíveis no cubo de Rubik legal tem como conjunto gerador $X = \{F, U, B, L, R, D\}$. Intuitivamente conseguimos nos convencer de que o conjunto dos possíveis movimentos que podem ser feitos no cubo utilizando combinações desses giros básicos, é um grupo, talvez com um pouco mais de esforço para enxergar a associatividade. Porém, essa estrutura ficará um pouco mais óbvia quando conseguirmos relacionar os grupos de permutações com o cubo de Rubik.

A fim de identificar o cubo de Rubik como um grupo, já foi comentado que suas peças podem ser definidas sem ambiguidades, isto é, meios não podem se tornar quinas e etc. Deste modo, mais conveniente do que usar letras para representar tais peças, é utilizar números para classificar cada um dos lados desses cubos menores, pois isto facilita *softwares* como o GAP identificar esses elementos. Então, levando em consideração que as peças centrais de cada face são fixas com relação às outras, podemos representar o cubo pelo seguinte diagrama, que pode ser encontrado de maneira similar em [12]:

Figura 3.11: Diagrama do cubo Resolvido



Fonte: Os Autores

Note que fazer um movimento U altera a disposição dos números no diagrama, fazendo as seguintes mudanças:

$$1 \to 3 \to 8 \to 6 \to 1$$

$$2 \to 5 \to 7 \to 4 \to 2$$

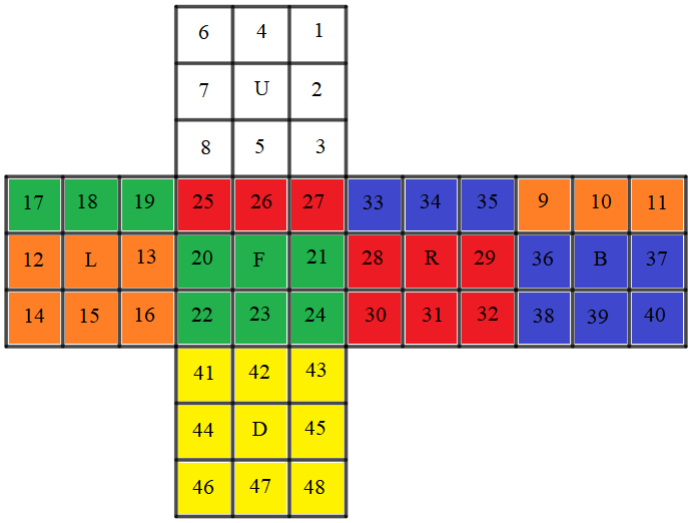
$$9 \to 33 \to 25 \to 17 \to 9$$

$$10 \to 34 \to 26 \to 18 \to 10$$

$$11 \to 35 \to 27 \to 19 \to 11.$$

É fácil ver que quando aplicarmos esse movimento, o diagrama mudará, da seguinte maneira:

Figura 3.12: Diagrama Após Aplicar U



Fonte: Os Autores

De onde, em notação de permutações, podemos escrever simplesmente como:

$$U = (1\ 3\ 6\ 8)(2\ 5\ 7\ 4)(9\ 33\ 25\ 17)(10\ 34\ 26\ 18)(11\ 35\ 27\ 19)$$

Usando raciocínio análogo, é possível representarmos todos os outros movimetos básicos do cubo nesta notação, isto é:

$$R = (25\ 27\ 32\ 30)(26\ 29\ 31\ 28)(3\ 38\ 43\ 19)(5\ 36\ 45\ 21)(8\ 33\ 48\ 24)$$
$$L = (9\ 11\ 16\ 14)(10\ 13\ 15\ 12)(1\ 17\ 41\ 40)(4\ 20\ 44\ 37)(6\ 22\ 46\ 35)$$
$$B = (33\ 35\ 40\ 38)(34\ 37\ 39\ 36)(3\ 9\ 46\ 32)(2\ 12\ 47\ 29)(1\ 14\ 48\ 27)$$
$$D = (41\ 43\ 48\ 46)(42\ 45\ 47\ 44)(14\ 22\ 30\ 38)(15\ 23\ 31\ 39)(16\ 24\ 32\ 40)$$
$$F = (17\ 19\ 24\ 22)(18\ 21\ 23\ 20)(6\ 25\ 43\ 16)(7\ 28\ 42\ 13)(8\ 30\ 41\ 11)$$

Deste modo, podemos enxergar cada movimento básico como uma permutação. Em particular, podemos enxergar cada uma dessas permutações como um elemento de S_{48}. Lembrando que, se $S \subset G$ com G um grupo, então $\langle S \rangle \leq G$ e S_n é um grupo, segue que $\mathcal{R} = \langle F, U, B, L, R, D \rangle$ também tem estrutura de grupo, conhecido como **Grupo de Rubik**. É importante observar que os elementos do cubo de Rubik não são necessariamente os padrões formados no quebra cabeças, mas sim os possíveis movimentos que podemos fazer nas suas faces. Então o grupo é formado por rotações possíveis e não configurações possíveis. Podemos destacar que o elemento identidade deste grupo corresponde a não fazer rotações nas faces, pois este "movimento"não afeta outros movimentos quando operado com os mesmos.

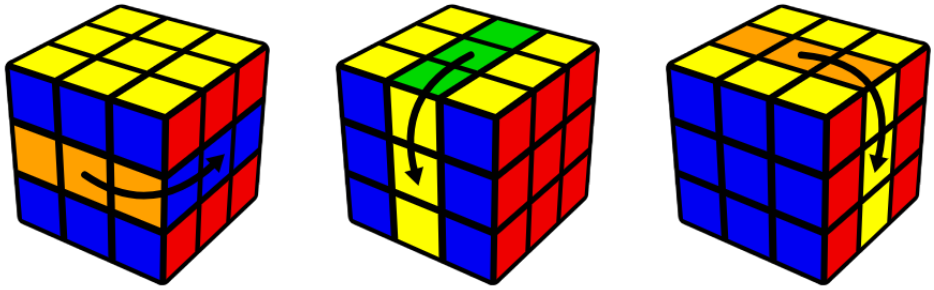
Comprovaremos mais adiante que a quantidade de elementos de $\mathcal{R}$ é muito menor que a quantidade do que a que calculamos utilizando o P.F.C., pois quando estamos limitados a utilizar apenas os movimentos básicos, descartamos a maioria das configurações que havíamos levado em consideração para fazer aquele cálculo. Via GAP facilmente poderemos comprovar que $|\mathcal{R}| = 8! \cdot 12! \cdot 3^7 \cdot 2^{10} = 43.252.003.274.489.856.000$. Note que reduzimos a potência 3^8 para 3^7 que corresponde a dizermos que apenas um terço das posições de quinas consideradas anteriomente são legais. Além disso, também reduzimos a potência 2^{12} para 2^{10} que, analogamente, representa a validade de apenas um quarto das posições de meio que contamos anteriormente.

3.5 Alguns Subgrupos do Grupo $\mathcal{R}$

3.5.1 Subgrupo das Fatias Quadradas de $\mathcal{R}$

No cubo mágico, podemos considerar os movimentos E, M e S como sendo girar a camada do meio do cubo da forma como podemos ver abaixo, respectivamente:

Figura 3.13: Slice Moves



Fonte: https://jperm.net/3x3/moves

Utilizando os elementos E^2, M^2 e S^2, temos o grupo $H^2 = \langle E^2, M^2, S^2 \rangle$, conhecido como **grupo das fatias quadradas**. Note que

$$\begin{aligned} H^2 &= \langle E^2 \rangle \cdot \langle M^2 \rangle \cdot \langle S^2 \rangle \\ &= \langle E^2 \rangle \cdot \langle S^2 \rangle \cdot \langle M^2 \rangle \\ &= \langle M^2 \rangle \cdot \langle E^2 \rangle \cdot \langle S^2 \rangle \\ &\vdots \end{aligned}$$

e que $\langle M^2 \rangle$, $\langle E^2 \rangle$, $\langle S^2 \rangle$ são normais em H^2, ou seja, $\langle M^2 \rangle$, $\langle E^2 \rangle$, $\langle S^2 \rangle \lhd H^2$. Além disso, é fácil ver que a interseção entre esses grupos dois a dois é apenas $\{e\}$, bem como cada um deles é cíclico de ordem 2. Logo, pelo **Teorema 6**,

$$H^2 \cong C_2 \times C_2 \times C_2 \cong C_2^3.$$

Portanto, também podemos afirmar que $|H^2| = 8$. Além disso, como todo grupo cíclico é abeliano e o produto direto de grupos abelianos é abeliano, é claro que H é abeliano, apesar de $\mathcal{R}$ não ser abeliano. E como sua ordem é relativamente baixa, podemos citar

explicitamente seus elementos, ou seja,

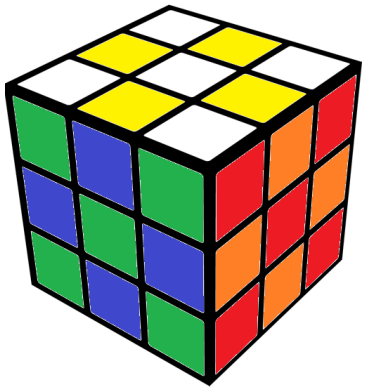
$$H^2 = \{e, M^2, E^2, S^2, M^2E^2, M^2S^2, E^2S^2, M^2E^2S^2\}$$

Abaixo temos sua tabela de Cayley:

$\circ$	e	M^2	E^2	S^2	M^2E^2	M^2S^2	E^2S^2	$M^2E^2S^2$
e	e	M^2	E^2	S^2	M^2E^2	M^2S^2	E^2S^2	$M^2E^2S^2$
M^2	M^2	e	M^2E^2	M^2S^2	E^2	S^2	$M^2E^2S^2$	E^2S^2
E^2	E^2	M^2E^2	e	E^2S^2	M^2	$M^2E^2S^2$	S^2	M^2S^2
S^2	S^2	M^2S^2	E^2S^2	e	$M^2E^2S^2$	M^2	E^2	M^2E^2
M^2E^2	M^2E^2	E^2	M^2	$M^2E^2S^2$	e	E^2S^2	M^2S^2	S^2
M^2S^2	M^2S^2	S^2	$M^2E^2S^2$	M^2	E^2S^2	e	M^2E^2	E^2
E^2S^2	E^2S^2	$M^2E^2S^2$	S^2	E^2	M^2S^2	M^2E^2	e	M^2
$M^2E^2S^2$	$M^2E^2S^2$	E^2S^2	M^2S^2	M^2E^2	S^2	E^2	M^2	e

Esse grupo também pode ser representado em termos dos movimentos básicos se considerarmos $M = L^{-1}R$, $E = D^{-1}U$, $S = F^{-1}B$, e portanto, equivalentemente, teremos $M^2 = L^2R^2$, $E^2 = D^2U^2$, $S^2 = F^2B^2$. Daí, $H = \langle L^2R^2, U^2D^2, F^2B^2 \rangle$. Uma característica estética de H é que seus elementos M^2E^2, M^2S^2, E^2S^2 e $M^2E^2S^2$, quando aplicados no cubo, criam padrões envolvendo alternâncias de cores em um estilo de tabuleiro de xadrez. O padrão abaixo é gerado no cubo pelo elemento $M^2E^2S^2$, e é chamado em [12] de *Checkerboard Pattern*.

Figura 3.14: *Checkerboard Pattern*

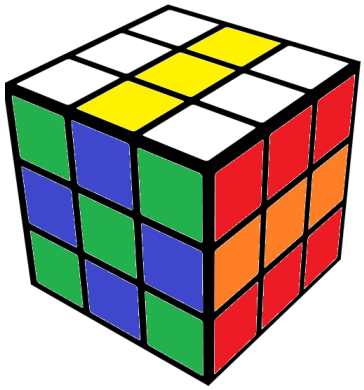


Fonte: Os Autores

Se chamamos de X o conjunto das peças de meio do cubo, e de Y o conjunto das peças de centro de cada face, podemos definir o conjunto $Z = X \cup Y$. As únicas peças do

cubo afetadas pelos movimentos em H^2 são as peças do conjunto Z, enquanto os cantos permanecem sempre permanecem fixos. Por isto, qualquer que seja o elemento de H^2 que seja aplicado no cubo, as peças de canto sempre vão estar combinando com o centro, ou com a cor oposta ao do centro. Abaixo temos outro exemplo:

Figura 3.15: Configuração gerada por M^2E^2



Fonte: Os Autores

3.5.2 Subgrupo das Fatias de $\mathcal{R}$

O **subgrupo das fatias de** $\mathcal{R}$ tem um conjunto gerador similar ao do exemplo anterior, se distinguido pelo fato dos elementos que o geram não serem elevados ao quadrado. De modo análogo, temos $H = \langle M, E, S \rangle$.

Diferente de H^2, H possui um número de elementos um pouco maior, que calcularemos via GAP no **Capítulo 4**, e ele se destaca pela simetria que forma no cubo quando aplicamos os seus elementos. O cubo tem a característica de que os cantos de uma face sempre serão iguais, e as cores opostas dos meios também serão iguais, como podemos ver nos exemplos abaixo:

É fácil perceber que os elementos de H^2 também possuem essa mesma simetria, mas as simetrias nele sempre dependem do centro de cada face, o que não ocorre com H, e deste modo, abrange tanto os casos do subgrupo das fatias quadradas quanto os casos que não dependem do centro das faces. De fato temos que $H^2 \leq H$. A seguir, utilizando o *software* GAP, exemplificaremos tal fato.

3.5.3 Subgrupo Q^* de $\mathcal{R}$

Considere o grupo $Q^* = \langle x, y \rangle$ no grupo em $\mathcal{R}$ com:

$$x = F^2R^{-1}LF^{-1}L^{-1}RU^{-1}R^{-1}LFL^{-1}RUF^2$$

$$y = FU^2F^{-1}U^{-1}L^{-1}B^{-1}U^2BUL$$

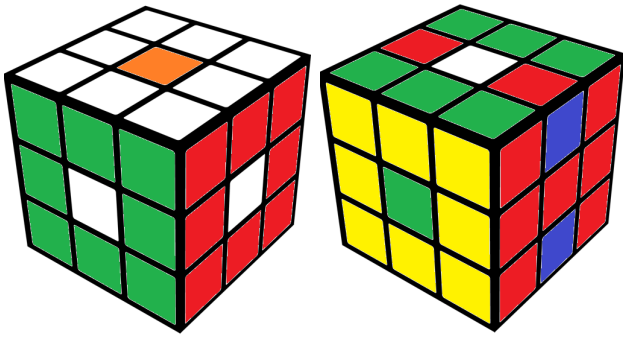
Afirmamos que $Q^* \cong Q_8$ do **Exemplo 1.3**, o qual verificaremos logo menos na seção do GAP. Estabelecido esse isomorfismo, além de encontrarmos cópias dos quatérnios no grupo de Rubik, também obtemos uma apresentação para Q^*.

3.5.4 Centro de $\mathcal{R}$

Temos duas classes especiais de subgrupos de $\mathcal{R}$ que tem efeitos nas orientações ou nas permutações das peças, e esses subgrupos são denotados por C_O e por C_P, onde C_O não tira nenhuma peça de seu lugar, mas pode mudar a orientação de alguns blocos, e C_P faz exatamente o contrário, não pode mudar a orientação de nenhum bloco, mas é capaz de mudá-los de lugar. Estes dois subgrupos serão importantes na determinação do centro de $\mathcal{R}$.

Como foi visto anteriormente, o centro de um grupo é o conjunto dos elementos de um grupo G que comutam com todos os elementos deste grupo, e que este na verdade é um subgrupo de G. Pelo fato de $\mathcal{R}$ não ser um grupo abeliano, já sabemos que $Z(\mathcal{R}) \neq \mathcal{R}$, mas podemos nos perguntar quais elementos estão em $Z(\mathcal{R})$.

Figura 3.16: Configuração gerada por dois elementos de H



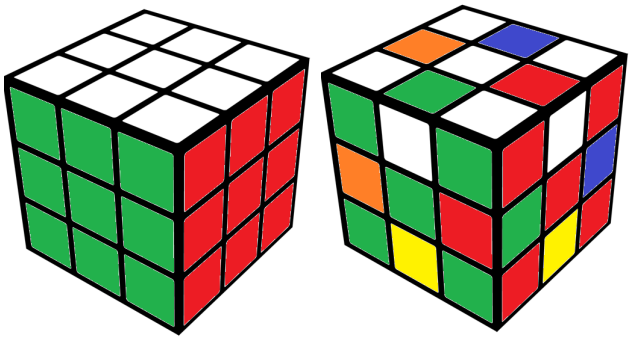
Fonte: Os Autores

Intuitivamente, por $\mathcal{R}$ ser um grupo relativamente grande, com pouco mais de $43 \cdot 10^{18}$ elementos, podemos pensar que seu centro também possui muitos elementos. Mas, na verdade, ocorre que este é um dos seus menores subgrupos, consistindo de apenas dois elementos, sendo eles a identidade e o *superflip*, isto é,

$$Z(\mathcal{R}) = \{e,\ RLFBUDRLFBUF^2R^{-1}LD^2F^{-1}R^2L^2D^2RL^{-1}F^2DR^2L^2D\},$$

que têm os seguintes efeitos no cubo:

Figura 3.17: Centro de $\mathcal{R}$



Fonte: Os Autores

Pode-se notar que os elementos do centro tem um efeito surpreendente no cubo mágico: eles não tiram nenhuma das peças do seu lugar. No caso da identidade isso é óbvio, mas no caso do *superflip*, todas as peças de meio apenas mudam de orientação, mas permanecem nos seus respectivos lugares.

Para termos certeza que de fato este subgrupo é o centro de $\mathcal{R}$ precisamos assegurar duas coisas: que todos os seus elementos comutam com os elementos de $\mathcal{R}$ e que não existem mais elementos com esta propriedade. Como a identidade está no centro de qualquer grupo, vamos focar no *superflip*, que denotaremos por s. Seja agora $r \in \mathcal{R}$, vamos analisar o elemento $rsr^{-1}s^{-1}$. Primeiramente, note que $sr^{-1}s^{-1} = sr^{-1}s$, uma vez que s tem o efeito de mudar a orientações dos meios, e pelo fato das peças de meio terem apenas duas cores, é imediato que $|s| = 2$, que implica $s = s^{-1}$.

Agora, podemos ver que $sr^{-1}s = r^{-1}$, independentemente de qual permutação seja r, uma vez que o processo que estamos fazendo é o seguinte:

$$\text{mudar orientação de meios} \longrightarrow \text{aplicar } r^{-1} \longrightarrow \text{reverter orientação de meios}$$

E portanto, obtemos que $rsr^{-1}s^{-1} = rr^{-1} = e$, ou seja, $rs = sr$. Logo s comuta com os elementos de $\mathcal{R}$. Outro modo de percebermos isso é notando que s comuta com os geradores de $\mathcal{R}$, e isso é suficiente para que s esteja no centro. Mas como podemos afirmar que não existem mais elementos com esta propriedade?

Para nos assegurar desse fato, temos a seguinte proposição, que pode ser encontrada em [12]:

Proposição 12 *O subgrupo $Z(\mathcal{R})$ consiste apenas da identidade e do superflip.*

Prova: O grupo $\mathcal{R}$ pode ser visto como um produto semidireto dos subgrupos vistos no início desta subseção, pois seus elementos consistem tanto em mudanças de posição espacial quanto em mudança de orientação de peças, isto é, $\mathcal{R} = C_O \rtimes C_P$. Considere $\psi \in Z(\mathcal{R})$. Ou seja, ψ comuta com todos os elementos tanto de C_O quanto com os elementos de C_P.

Suponha, por contradição, que ψ permuta um conjunto de peças de meio tais que o meio situado na posição P_1 ocupe o lugar do meio situado em P_2, que por sua vez ocupa o lugar do meio em P_3, e assim sucessivamente até o meio na posição P_n. Agora, se $n \neq 2$, seja $\phi \in C_O$ tal que esse elemento altera somente a orientação das peças que estão posicionadas nos lugares P_1 e P_2. Denotaremos a peça M_i com orientação invertida por $\overline{M_i}$. Se calcularmos o produto $\phi\psi$, vamos notar que ele tem como resultado alterar a orientação das peças M_n e M_1, pois aplicando essa composição temos as seguintes trocas de posições:

Posição	P_1	P_2	P_3	...	P_n
Estado Inicial	M_1	M_2	M_3	...	M_n
Estado Após ψ	M_n	M_1	M_2	...	M_{n-1}
Estado Após ϕ	$\overline{M_n}$	$\overline{M_1}$	M_2	...	M_{n-1}

Mas por outro lado, aplicando $\psi\phi$ observamos que são alteradas as orientações de M_1 e M_2, ou seja:

Por este motivo, temos que $\psi\phi \neq \phi\psi$.

Caso $n = 2$, consideramos $\phi \in C_O$ o elemento que muda a orientação das peças posicionadas em M_1 e em M, sendo M não pertencente ao ciclo $(M_1\ M_2)$. Teremos então que $\phi\psi$ orienta as peças nas posições M_2 e algum $M' \neq M_1$. Agora, por outro lado, se calculamos

Posição	P_1	P_2	P_3	...	P_n
Estado Inicial	M_1	M_2	M_3	...	M_n
Estado Após ϕ	$\overline{M_1}$	$\overline{M_2}$	M_3	...	M_n
Estado Após ψ	M_n	$\overline{M_1}$	$\overline{M_2}$	...	M_{n-1}

$\psi\phi$, obtemos a mudança de orientação das peças localizadas em M_1 e em $M'' \neq M_2$, e daí segue que em qualquer caso temos $\psi\phi \neq \phi\psi$, mas isso é uma contradição pois $\psi \in Z(\mathcal{R})$.

Com raciocício análogo, podemos tomar um elemento $\tau \in C_p$ qualquer e comprovar que $\tau\psi \neq \psi\tau$. ■

Uma outra macro que define o *superflip* pode ser descrita por

$$UR^2FBRB^2RU^2LB^2RU^{-1}D^{-1}R^2FR^{-1}LB^2U^2F^2$$

e, pelo fato de estar no centro, quando fizermos o comutador do *superflip* com qualquer outro elemento de $\mathcal{R}$, obtemos a identidade.

No seguinte capítulo, apresentaremos um *software* livre que nos ajudará na construção do grupo de Rubik. Além disso, representaremos seus subgrupos descritos nesta seção.

Capítulo 4

GAP

O *software* GAP, abreviação para *Groups, Algorithms and Progamming*, é um dos mais poderosos softwares para estudos em Álgebra, não apenas para Teoria de Grupos, mas também anéis, espaços vetoriais, sistemas de reescrita, módulos, corpos, dentre outros [9]. É uma ferramenta muito útil que surge para que possamos investigar e identificar padrões em propriedades de certos tipos de estruturas algébricas e tentar conjecturar resultados sobre eles. Apesar do principal foco do presente estudo com o GAP ser em grupos finitamente apresentados (ou até mesmo finitos!), realizar os cálculos a mão na grande maioria das vezes é uma tarefa árdua, e também um pouco desnecessária.

Este *software* possui em sua biblioteca um número gigantesco de funções disponíveis para serem usadas, e também diversos pacotes sobre os mais variados assuntos disponíveis para implementação. Além de possuir um extenso manual com mais de 1000 páginas, possui fórums ativos na internet, onde os próprios criadores do software ou usuários mais experientes promovem discussões sobre o GAP em sua totalidade, como por exemplo o fórum intitulado *"The GAP Forum mailing list"*. [1] Vale ressaltar que este é um software livre e está disponível para todos os sistemas operacionais com atualização mais dinâmica no sistema Linux.

Podemos construir qualquer grupo finitamente apresentado no GAP, pelo **Corolário 1** e pela **Proposição 5**, a partir de seus geradores e suas relações da seguinte forma: basta declarar um grupo livre que tenha $X = \{x_1, x_2, \cdots, x_n\}$ como conjunto gerador, definir o

[1] Acesso livre em https://lists.uni-kl.de/gap/info/forum.

conjunto das relações $R = \{r_1, r_2, \cdots, r_t\}$ envolvendo o conjunto X e, após isso, tomar G como o grupo quociente $G = F/R$.

Abaixo, construímos o grupo D_4 no GAP, cuja apresentação foi dada na **Seção 1.3**:

```
gap > f := FreeGroup("a", "b");
< free group on the generators [a, b] >
gap > r := [f.1^2, f.2^2, (f.1 * f.2)^2];
[a^4, b^2, (a * b)^2]
gap > G := f/r;
< fp group on the generators [a, b] >
gap > Elements(G);
[< identity... >, b, a^3 * b, a, a^3, a * b, a^2 * b, a^2]
```

O GAP também possui funções já prontas que nos permite obter informações sobre grupos rapidamente, como por exemplo, calcular a ordem de um grupo, descobrir se um subgrupo é normal em um grupo, descobrir se certo subconjunto é subgrupo, realizar operações entre elementos de um grupo, calcular sinais de permutações em grupos de permutações entre outras. Podemos tanto construir grupos quanto pedir que o GAP retorne o grupo através de uma função específica. É bem comum não sabermos se o GAP executa determinada função automaticamente, pois ele possui muitas funções para lembrarmos de todas. Porém, ele nos dá a liberdade de construir a função que precisamos a partir sua própria linguagem. Ou seja, é possível escrevermos algoritmos no GAP envolvendo funções do tipo `if, else, while, do`, etc.

Vamos construir agora o grupo de Rubik $\mathcal{R}$ utilizando as permutações obtidas para cada um dos movimentos básicos R, L, D, U, B, F. A partir daí, faremos algumas contas básicas:

```
gap> U:=( 1, 3, 8, 6)( 2, 5, 7, 4)( 9,33,25,17)(10,34,26,18)(11,35,27,19);;
gap> F:=(17,19,24,22)(18,21,23,20)( 6,25,43,16)( 7,28,42,13)( 8,30,41,11);;
gap> L:=( 9,11,16,14)(10,13,15,12)( 1,17,41,40)( 4,20,44,37)( 6,22,46,35);;
gap> R:=(25,27,32,30)(26,29,31,28)( 3,38,43,19)( 5,36,45,21)( 8,33,48,24);;
gap> B:=(33,35,40,38)(34,37,39,36)( 3, 9,46,32)( 2,12,47,29)( 1,14,48,27);;
gap> D:=(41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40);;
gap> rubik:=Group(U,F,L,R,B,D);
```

```
<permutation group with 6 generators>
gap> Order(rubik);
43252003274489856000
gap> M:=Group(R*U^2*D^-1*B*D^-1);
Group([ (1,8,17,35,19,6,9,25,11)(2,7,12,45,21,4,5,34,18,37,31,28,10,26)
(3,22,43,32,14,33,41,24,38,46,27,16,30,48,40)(15,36,44,29)(23,39)(42,47) ])
gap> Order(M);
1260
```

Do código acima, podemos confirmar que a ordem de $\mathcal{R}$ é 43.252.003.274.489.856.000 que, em sua forma fatorada, pode ser escrito como $2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$. E também podemos calcular a ordem da macro $RU^2D^{-1}BD^{-1}$, que representa a maior ordem possível no grupo de Rubik, sendo igual a 1260. Outro fato importante sobre ordem deste grupo é que não existem elementos de ordem 13 nele, pois, pelo Teorema de Lagrange [8], 13 não é um divisor de $|\mathcal{R}|$.

Quando falamos sobre o centro de $\mathcal{R}$, $Z(\mathcal{R})$, vimos que este é constituído apenas de dois elementos. Também é possível verificar isto no GAP:

```
gap> C:=Center(rubik);
Group([ (2,34)(4,10)(5,26)(7,18)(12,37)(13,20)(15,44)(21,28)(23,42)(29,36)
(31,45)(39,47) ])
gap> Order(C);
2
```

O GAP nos diz que $Z(\mathcal{R})$ é gerado pela permutação

α = (2,34)(4,10)(5,26)(7,18)(12,37)(13,20)(15,44)(21,28)(23,42)(29,36)(31,45)(39,47)

Note que em todos as transposições, os números representam a mesma peça. Por exemplo, se olharmos novamente a **Figura 3.4**, vamos perceber que os números 2 e 34 do ciclo (2 34) são a mesma peça. No diagrama, podemos notar que o número 2 representa a peça de meio *ub*, mas o número 34 também representa a peça de meio *ub*, então quando o ciclo (2 34) é aplicado, ocorre que essa peça não sai do seu lugar, mas suas cores são invertidas, e o mesmo fenômeno ocorre com as outras transposições. Outro comportamento que podemos notar é que os números correspondentes às quinas não aparecem em α, e pelo estudo dos

ciclos sabemos que isso acontece quando as peças não são afetadas, portanto, as quinas não tem sua orientação e nem sua posição trocada, uqe descreve exatamente o *superflip* que foi discutido anteriormente. Além disso, como o *superflip* é composto por transposições disjuntas, possui ordem 2.

No **Exemplo 3.5.3**, podemos também comprovar o isomorfismo entre os grupos Q_8 e Q^*. Sabemos que se dois grupos são n-gerados, e seus geradores satisfazem as mesmas relações, então eles são isomorfos. Já conhecemos uma apresentação para o grupo dos quatérnios então, basta verificarmos se os geradores de Q^* satisfazem as mesmas relações. Vamos considerar os geradores

$$\text{a} = F^2R^{-1}LF^{-1}L^{-1}RU^{-1}R^{-1}LFL^{-1}RUF^2 \quad \text{e} \quad \text{b} = FU^2F^{-1}U^{-1}L^{-1}B^{-1}U^2BUL$$

É bem simples verificar se as relações são satisfeitas, basta definirmos:

```
gap> a:=F^2*R^-1*L*F^-1*L^-1*R*U^-1*R^-1*L*F*L^-1*R*U*F^2;
(2,10,34,4)(5,7,26,18)
gap> b:=F*U^2*F^-1*U^-1*L^-1*B^-1*U^2*B*U*L;
(2,18,34,7)(4,5,10,26)
gap> Q:=Group(a,b);
Group([ (2,10,34,4)(5,7,26,18), (2,18,34,7)(4,5,10,26) ])
gap> Order(Q);
8
gap> a^4;
()
gap> a^2*b^-2;
()
gap> b*a*b^-1*a;
()
```

Isso significa que $a^4 = e$, $a^2b^{-2} = e$ e que $bab^{-1}a = e$, portanto $Q_8 \cong Q^*$.

No **Exemplo 3.5.1** pudemos calcular com certa facilidade a quantidade de elementos do subgrupo das fatias quadradas pelo fato dele ser relativamente pequeno. Porém não foi possível fazer o mesmo com o subgrupo das fatias no **Exemplo 3.5.2**. Por conveniência, vamos utilizar o GAP para obter informações sobre esse grupo.

Lembre que foi definido $H = \langle E, M, S \rangle$, mas como nossa construção no GAP depende dos movimentos básicos, vamos reescrever $H = \langle D^{-1}U, L^{-1}R, F^{-1}B \rangle$.

```
gap> x:=D^3*U;;
gap> y:=L^3*R;;
gap> z:=F^3*B;;
gap> H:=Group(x,y,z);
<permutation group with 3 generators>
gap> Order(H); 768
```

E como já sabíamos também podemos verificar a relação $H^2 \leq H$:

```
gap> a:=R^2*L^2;;
gap> b:=F^2*B^2;;
gap> c:=U^2*D^2;;
gap> H2:=Group(a,b,c);
<permutation group with 3 generators>
gap> Order(H2);
8
gap> IsSubgroup(H,H2);
true
```

Apesar de termos estudado e gerado o Grupo de Rubik considerando um grupo 6-gerado, na verdade é possível construir este grupo computacionalmente a partir de 2 geradores. Utilizamos 6 usualmente pois é mais intuitivo observar as propriedades e tentar reproduzí-las em um cubo físico. Mas, quando consideramos outros geradores, o cubo pode perder essa ideia mais tangível por exemplo, se considerarmos os geradores s e t:

$$s = L^2BRD^{-1}L^{-1} \quad \text{e} \quad t = UFRUR^{-1}U^{-1}F^{-1}.$$

Em [18], Singmaster afirma que $\mathcal{R} = \langle s, t \rangle$. Vejamos que isso de fato é verdade:

```
gap> s:= L^2*B*R*D^-1*L^-1;
(1,22,32,30,25,27,40)(2,15,12,10,39,42,20,31,28,26,29)(3,14,9,41,38,43,19)
(4, 47,23,13,45,21,5,36,34,44,37)(8,33,46,35,16,48,24)
gap> t:=U*F*R*U*R^-1*U^-1*F^-1;
(3,6,27,11,33,17)(4,18,10,7)(5,26)(8,25,19)
```

```
gap> rubikgr:=Group(s,t);
<permutation group with 2 generators>
gap> Order(rubikgr);
43252003274489856000
gap> rubik=rubikgr;
true
```

O que fizemos foi basicamente criar o grupo gerado por s e t e comprovar que ele coincide com o grupo $\mathcal{R}$, intitulado `rubik`, que foi criado no início do capítulo.

Também podemos dizer que a equivalência de macros não é trivial, ou seja, dadas duas macros X e Y, em geral não é possível dizer se $X = Y$, ou equivalentemente, $XY^{-1} = e$, apenas eliminando inversos. Por exemplo, considerando

$$\begin{aligned} \text{a} &= RUR^{-1}URUR^{-1}F^{-1}RUR^{-1}U^{-1}R^{-1}FR^2U^{-1}R^{-1}U^2RU^{-1}R^{-1} \\ \text{b} &= LU^{-1}RU^2L^{-1}UR^{-1}LU^{-1}RU^2L^{-1}UR^{-1}U^{-1} \end{aligned}$$

Temos então que

$$\begin{aligned} \text{ab}^{-1} &= (RUR^{-1}URUR^{-1}F^{-1}RUR^{-1}U^{-1}R^{-1}FR^2U^{-1}R^{-1}U^2RU^{-1}R^{-1}) \\ &\quad (URU^{-1}LU^2R^{-1}UL^{-1}RU^{-1}LU^2R^{-1}UL^{-1}) \\ &= e \end{aligned}$$

Não consguimos constatar sem muito esforço a igualdade acima, eliminando termos da forma xx^{-1}, mas podemos verificar fazendo manipulações no cubo, e também utilizando o GAP:

```
gap> a:= R*U*Rˆ-1*U*R*U*Rˆ-1*Fˆ-1*R*U*Rˆ-1*Uˆ-1* Rˆ-1*F*Rˆ2*Uˆ-1*Rˆ-1*Uˆ2*
        R*Uˆ-1*Rˆ-1;;
gap> b:= L*Uˆ-1*R*Uˆ2*Lˆ-1*U*Rˆ-1*L*Uˆ-1*R*Uˆ2*Lˆ-1*U*Rˆ-1*Uˆ-1;;
gap> a*bˆ-1;
()
```

Agora, como também é interessante resolver o cubo de Rubik do ponto de vista computacional, uma das estratégias que pode ser usada é tentar transformar uma permutação qualquer de $\mathcal{R}$ como um produto dos geradores desse grupo. Mas o conjunto de geradores que é mais conveniente neste contexto é o mais imediato, sendo $X = \{R, L, B, D, F, U\}$,

pois é possível manipular o cubo fisicamente mais facilmente com produtos desses elementos. Para isto, criamos um grupo livre F cujo conjunto gerador é X e construímos um homomorfismo entre o grupo livre F de geradores X e $\mathcal{R}$ que mapeia os geradores de F nos geradores de G. Após isto, basta que calculemos um representante da pré-imagem de uma permutação qualquer, que o GAP retornará esta mesma composição, só que decomposta em termos dos elementos do conjunto gerador que definimos inicialmente. Isto resolve o cubo, como queríamos. Este procedimento via GAP pode ser visto nas notas em [16], bem como no próprio site do GAP.

De fato, o procedimento descrito resolve o Problema da Palavra para o grupo $\mathcal{R}$, que consiste em ter uma palavra, que neste contexto são as nossas macros, e conseguir obter uma palavra equivalente a ela em termos dos geradores. Esse procedimento nos permite fazer uma composição de modo que o cubo de Rubik volte ao seu estado inicial:

```
gap> f := FreeGroup("U","L","F","R","B","D");
<free group on the generators [ U, L, F, R, B, D ]>
gap> hom := GroupHomomorphismByImages( f, rubik, GeneratorsOfGroup(f),
> GeneratorsOfGroup(rubik) );
[ U, L, F, R, B, D ] -> [ (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,
27,19), (1,17,41,40)(4,20,44,37)(6,22,46,35)(9,11,16,14)(10,13,15,12),
(6,25,43,16)(7,28,42,13)(8,30,41,11)(17,19,24,22)(18,21,23,20),
(3,38,43,19)(5,36,45,21)(8,33,48,24)(25,27,32,30)(26,29,31,28),
(1,14,48,27)(2,12,47,29)(3,9,46,32)(33,35,40,38)(34,37,39,36),
(14,22,30,38)(15,23,31,39)(16,24,32,40)(41,43,48,46)(42,45,47,44) ]
gap> x := Random( G );
(1,30,22)(2,39,12,10,26,36,7,15,23,21,34,47,37,4,5,29,18,44,42,28)
(3,11,40, 32,33,6,14,38,27,17,46,48)(8,19,25)(9,43,41)(13,20)(16,35,24)
gap> PreImagesRepresentative( hom, x );
U*F*R*U*R^-1*U^-1*F^-1*U^-1*L^-1*U^-1*B^-1*U*B*L*U^-1*L*U*F*U^-1*F^-1*L^-1*U*
F^-1*L*F*L^-1*U^-1*L^-1*U*L*U^-2*L*F*U*F^-1*U^-1*L^-2*U*L*F^-1*L*F*(L^-1*U)^2
*F^-1*L^-1*F*L*B^-1*U^-1*B*L^-1*D*F^-1*D^-1*U^-2*R*U*R^-1*U*D^-1*L^-1*B^-1*D*
L^-1*B*D^-1*B^-1*F^-1*(R*F^-1*B*U^-1*B^-1)^2*F^-1*U^-1*F^-1*U*L^-1*F*U^-1*L*D^-1
*L^-1*D*F^-1*D*R^-1*D^-1*U^-1*B*D^-1*B^-1*R^-2*U^-1*D*L.
```

Ou seja, a partir de um elemento qualquer em $\mathcal{R}$ somos capazes de decompor ele em termos dos geradores do grupo livre, e isso nos permite resolver o cubo. A decomposição dada por este método pode não ser a mais eficiente em termos do comprimento da palavra que encontramos, mas é uma solução valida.

Considerações Finais

Neste trabalho foi possível constatar que o cubo Mágico $3 \times 3 \times 3$ tem uma relação muito íntima com a Álgebra e que suas simetrias podem ser estudadas pela perspectiva da Teoria de Grupos. Desta forma, é possível determinar sem ambiguidades sua estrutura a partir de um grupo de permutações. Mais especificamente, temos que $\mathcal{R} \leq S_{48}$.

Por atrair a atenção de pessoas diversas, o cubo Mágico se apresenta como um objeto capaz de motivar o estudo de Teoria de Grupos a nivel de graduação, tornando alguns conceitos, como por exemplo, centro de um grupo, grupo de permutações, ordem, etc um pouco menos abstratos e mais tangíveis.

Além disso, a partir de alguns conceitos simples da Teoria Combinatória, é possível utilizar o GAP no auxílio e entendimento de estruturas abstratas e, portanto, podendo também ser incluída nas aulas de Álgebra uma vez que permite aos estudantes conjecturar acerca de grupos de modo mais prático, testar propriedades que se suspeitam ser verdadeiras para depois tentar uma prova algébrica.

Referências Bibliográficas

[1] Bandelow, C. *Inside Rubik's cube and beyond*. Springer Science & Business Media. 2012.

[2] Bjorner, Anders, and Francesco Brenti. *Combinatorics of Coxeter groups*. Springer Science & Business Media, 2006.

[3] Cauchy, L.A. *Mémoire Sur Le Nombre Des Valeurs Qu'une Fonction Peut Acquérir Lorsqu'on y Permute De Toutes Les Manières Possibles Les Quantités Qu'elle Renferme.* Journal de l'École polytechnique, XVIIe cahier, t. X, p. 1; 1815.

[4] Cayley, A. *On The Theory Of Groups, As Depending On The Symbolic Equation* $\theta^n = 1$. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, V.7, 42, p. 40-47. 1854.

[5] Galois, E. Neumann, Peter M. *The Mathematical Writings of Évariste Galois*. European Mathematical Society. 2011

[6] Garcia, Arnaldo, and Yves Lequain. *Elementos de Álgebra*. Instituto de Matemática Pura e Aplicada, 2006.

[7] Gonçalves, A. *Introdução à Álgebra*. Vol. 7. Instituto de Matemática Pura e Aplicada, 1979.

[8] Gallian, Joseph A. *Contemporary Abstract Algebra*. Chapman and Hall/CRC, 2021.

[9] GAP, *GAP – Groups, Algorithms, and Programming, Version 4.12.1*; 2022, https://www.gap-system.org.

[10] Holt, D.F., Eick, B. and O'Brien, E.A. *Handbook Of Computational Group Theory*. Chapman and Hall/CRC, 2005.

[11] Johnson, D.L., *Presentations Of Groups*. Vol. 15. Cambridge university press, 1997.

[12] Joyner, D. *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys*. 2002.

[13] Kleiner, Israel. *The Evolution Of Group Theory: A Brief Survey*. Mathematics Magazine 59.4 (1986): 195-215.

[14] Magnus, W., Karrass, A. and Solitar, D. *Combinatorial Group Theory: Presentations Of Groups In Terms Of Generators And Relations*. Courier Corporation, 2004.

[15] Poincaré, H. *Analysis Situs*. Paris, France: Gauthier-Villars, 1895.

[16] Schneider, C. *Minicurso Sobre O Sistema Computacional GAP*. UFMG. 2014.

[17] Santos, H. *Enlaçamentos Bordantes*. Dissertação de Mestrado, ICMC-USP. 2002

[18] Singmaster, D. *Notes on Rubik's magic cube*. Enslow Pub Incorporated, 1981.

[19] Von Dyck, W. *Gruppentheoretische Studien. Mathematische Annalen*. 1882: p.1-44.