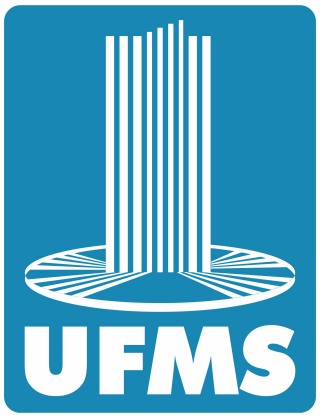


Universidade Federal de Mato Grosso do Sul

Instituto de Matemática

Programa de Pós-Graduação

Matemática em Rede Nacional

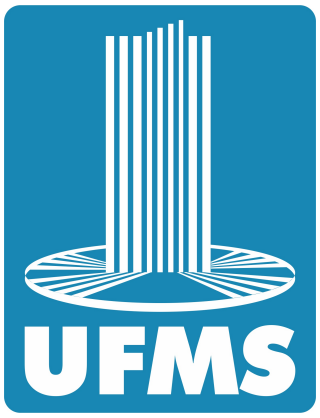
Mestrado Profissional

Jeferson Saraiva Bezerra

Tópicos em Teoria de Grupos: O Desafio do Cubo de Rubik

Campo Grande - MS

Maio de 2016



Universidade Federal de Mato Grosso do Sul

Instituto de Matemática

Programa de Pós-Graduação

Matemática em Rede Nacional
Mestrado Profissional

Jeferson Saraiva Bezerra

Tópicos em Teoria de Grupos: O Desafio do Cubo de Rubik

Orientadora: Prof.ª Dra. Elen Vivani Pereira da Silva Spreafico

Dissertação apresentada ao Programa de Pós-Graduação em matemática em Rede Nacional do Instituto de Matemática da Universidade Federal de Mato Grosso do Sul-INMA/UFMS como parte dos requisitos para obtenção do título de Mestre.

Campo Grande - MS

Maio de 2016

Tópicos em Teoria de Grupos: O Desafio do Cubo de Rubik

Jeferson Saraiva Bezerra

Dissertação apresentada ao Programa de Pós-Graduação em matemática em Rede Nacional do Instituto de Matemática da Universidade Federal de Mato Grosso do Sul-INMA/UFMS como parte dos requisitos para obtenção do título de Mestre.

Aprovado pela Banca Examinadora:

Prof. Dra. Elen Viviani Pereira Spreafico
Universidade Federal de Mato Grosso do Sul

Prof. Dr. Robson da Silva
Universidade Federal De São Paulo

Prof. Dr. Claudemir Aniz
Universidade Federal de Mato Grosso do Sul

Campo Grande – MS, 11 de Maio de 2016

Agradecimentos

Agradeço à Deus pelo dom da vida, e por ter colocado obstáculos na minha vida que pudesse suportar, e com isso, crescer pessoalmente e profissionalmente.

Aos meus pais Pedro Saraiva Bezerra e Izabel Trindade Bezerra, por me ensinarem a batalhar pelos objetivos de maneira justa e leal.

A minha namorada Rosane Barbosa de Oliveira por estar ao meu lado em todos os momentos me apoiando e auxiliando na escrita.

Minha irmã Leticia Saraiva Bezerra por me ajudar em cada dia durante este percurso.

E a minha orientadora Prof.ª Dra. Elen Vivani Pereira da Silva Spreafico por exigir o meu melhor, assim pude melhorar a escrita que não tinha muita habilidade e aprender novos conteúdos.

Resumo

Este trabalho trata essencialmente do Cubo de Rubik: Criação, Movimentos, Formato e Método de Resolução. Na abordagem desse tema, constata-se a predominância de um tratamento algébrico. Para tal, definimos algumas estruturas algébricas, entre elas Grupos. E com isso trabalharemos o Cubo de Rubik em um grupo para concluirmos que nem todas as configurações são válidas.

Palavras-chave: Cubo de Rubik, Grupo, Configurações Válidas.

Abstract

This paper mainly deals with the Rubik Cube: Creation, Movements, Format and Method. In addressing this issue, there has been a predominance of an algebraic treatment. To do this, we define some algebraic structures, including groups. And with that work the Rubik's Cube in a group to conclude that not all settings are valid.

Keywords: Rubik's Cube, Group, Valid Settings.

Sumário

Lista de Figuras

Introdução

A maioria das pessoas tem ou já viu alguém com um Cubo de Rubik. Assim, semelhante a mim, não conseguiram resolver totalmente o cubo. Com isso, trouxe esta curiosidade de trabalhá-lo e resolver alguns questionamentos: quantas posições tem o cubo? Existe algum método de resolver?

A única vez que montei o cubo por completo, foi quando usei a força física em vez da intelectual. E pude observar alguns aspectos da estrutura dele que serão apresentados ao longo desse trabalho.

O Cubo de Rubik é considerado algo difícil de ser resolvido desde sua invenção. O criador deste objeto é Erno Rubik. Por ser adaptado como brinquedo às crianças e jovens, o Cubo é o brinquedo mais vendido mundialmente, com cerca de 350 milhões de unidades desde sua existência.

O "brinquedo"é muito estudado no campo da inteligência artificial, pois almeja encontrar uma definitiva solução de montagem ao Cubo, ou até mesmo, a formulação de técnicas e meios que auxiliem em sua adequada construção. E assim, indagando as mentes mais pensantes em desvendar tal mistério.

São várias possibilidades de solução do Cubo de Rubik $3 \times 3 \times 3$, e isso faz com que o estudo torne muito mais interessante, porque para solucioná-lo devem-se explorar inúmeras situações.

De forma que todas as possibilidades do Cubo de Rubik sejam resolvidas, diversas técnicas foram aplicadas, tal que, o processo se tornasse efetivo

em tempo redutivo (diminuindo formas, excluindo formas repetidas, formas simétricas etc). O Cubo de Rubik foi submetido as mais diversas maneiras de construção desde a sua criação, sendo assim, houve o surgimento de imensas possibilidades ocasionando formas de resolvê-lo.

Atualmente é possível tentar resolver o Cubo de Rubik através do *Cubo Mágico 3D*, ou outros aplicativos para celular, ou para outro aparelho eletrônico, o que é atrativo para estudar.

No Capítulo 1 descrevemos uma revisão sobre Função, Grupos, Subgrupos, Geradores e Homomorfismo de Grupo. Mostramos alguns Grupos especiais e falamos sobre o Sinal do Homomorfismo e Grupo Alternado.

No Capítulo 2 apresentamos o Cubo de Rubik mostrando sua estrutura, movimentos e modelos semelhantes. Além disso, também descrevemos um método para resolve-lo. Por fim descrevemos o Cubo de Rubik como um grupo, desenvolvendo resultados a cerca de suas propriedades e concluirmos que nem todas as configurações são válidas.

Este trabalho foi desenvolvido baseado-se predominantemente em [5].

Capítulo 1

Neste capítulo iremos, inicialmente, apresentar alguns conceitos sobre funções e posteriormente sobre Teoria de Grupos, conceitos esses que serão utilizados no estudo do Cubo de Rubik. Para melhor compreensão das definições e propriedades serão feitos exemplos ao longo do texto.

1.1 Funções

Para entender corretamente o Cubo de Rubik, precisamos falar primeiro sobre algumas propriedades de funções.

Definição 1 *A função f de domínio D e contra-domínio R é uma regra que atribui a cada elemento $x \in D$ um único elemento $y \in R$, onde $f(x) = y$. Dizemos que y é a imagem de x e que x é imagem inversa de y.*

Note que um elemento em D tem exatamente uma imagem, mas em R pode ter $0, 1$, ou mais de uma imagem inversa.

Exemplo 1 *Considere a função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$. Se x é qualquer número real, a sua imagem é o número real x^2. Por outro lado, se y é um número real positivo, temos duas imagens inversas $\sqrt{y}$ e $-\sqrt{y}$. O*

número real 0 *tem uma única imagem inversa, a saber o número* 0; *e números negativos não tem imagem inversa.*

Podemos classificar as funções em termos de propriedades que relacionam o domínio, contradomínio e sua lei de associação: funções injetoras, sobrejetoras e bijetoras. Considere primeiramente a definição de injetividade da função.

Definição 2 *Dizemos que f é uma função injetora, se dois elementos diferentes quaisquer de D têm imagens diferentes. Em outras palavras, se para quaisquer $x_1, x_2 \in D$, tais que $x_1 \neq x_2$, valer $f(x_1) \neq f(x_2)$.*

Notemos que a contrapositiva da definição anterior é: Se $x_1, x_2 \in D$ e $f(x_1) = f(x_2)$, então $x_1 = x_2$. Normalmente usa-se essa contrapositiva, que é equivalente à definição, para verificar se f é injetora ou não.

A propriedade de injetividade garante que, se houver imagem inversa de um elemento, ela é única. Vejamos um exemplo.

Exemplo 2 *Considere a função $f : \mathbb{Z} \to \mathbb{R}$ definida por $f(x) = x + 2$. Esta função é injetora, pois se $x_1 \neq x_2$, então $x_1 + 2 \neq x_2 + 2$. Se $y \in \mathbb{R}$ é um número inteiro, então ele tem uma única imagem inversa. E se $y \in \mathbb{R}$ não é um número inteiro, então ele não tem nenhuma imagem inversa.*

Exemplo 3 *A função $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x^2$ não é injetora, pois $f(1) = f(-1)$, mas $1 \neq -1$. O número 1 tem duas imagens inversas, 1 e -1.*

Vejamos agora a definição de função sobrejetora.

Definição 3 *Uma função $f : D \to R$ é chamada sobrejetora se para cada $y \in R$, existe $x \in D$ tal que $f(x) = y$. Equivalentemente, cada elemento de R tem pelo menos uma imagem inversa.*

Exemplo 4 *A função $f : \mathbb{Z} \to \mathbb{R}$ definida por $f(x) = x$ não é sobrejetora, pois números não inteiros não têm imagens inversas. No entanto, a função $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x$ é sobrejetora.*

Exemplo 5 *A função $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x^2$ não é sobrejetora, pois não existe $x \in \mathbb{Z}$ tal que $f(x) = 2$.*

Agora, vejamos uma definição que une as duas propriedades: injetividade e sobrejetividade.

Definição 4 *Uma função $f : D \to R$ é chamada de bijetora, se é injetora e sobrejetora. Equivalentemente, cada elemento de R tem exatamente uma imagem inversa.*

Exemplo 6 *A função $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x + 1$ é bijetora.*

Exemplo 7 *Se S é qualquer conjunto numérico, então podemos definir uma função $f : S \to S$ por $f(x) = x$ para todo $x \in S$. A função é chamada de função identidade, e é bijetora.*

Podemos também considerar uma operação bem definida entre duas funções com restrições nos domínios e contradomínios: a operação composição.

Definição 5 *Sejam $f : S_1 \to S_2$ e $g : S_2 \to S_3$ duas funções. Chama-se composta de f e g a função (indicada por $g \circ f$) de S_1 em S_3 definida da seguinte maneira: $(g \circ f)(x) = g(f(x))$ para todo $x \in S_1$.*

1.2 Grupos

Nesta seção vamos mostrar alguns aspectos da Teoria de Grupos, mas especificamente a estrutura de grupo simétrico e alguns resultados sobre esse grupo para estabelecer uma estrutura para as simetrias do Cubo de Rubik.

Definição 6 *Um grupo $(G, *)$ é constituído por um conjunto não vazio G e uma operação $*$ de tal modo que:*

1. $*$ é associativa. Isto é, para quaisquer $a, b, c \in G$, $a*(b*c) = (a*b)*c$.

Exemplo 8 *A adição e multiplicação são associativas. A subtração não é associativa, pois $a - (b - c) \neq (a - b) - c$.*

2. Há um "elemento identidade". Isto é, existe $e \in G$ que satisfaz $g = e * g = g * e$ para todos $g \in G$.

Exemplo 9 *Para $(\mathbb{Z}, +), 0$ é um elemento de identidade, pois $g = 0 + g = g + 0$ para todo $g \in \mathbb{Z}$. Para $(\mathbb{R}, \cdot), 1$ é um elemento de identidade, pois $g = 1.g = g.1$ para todo $g \in \mathbb{R}$.*

3. Existência do elemento inverso. Isto é, para qualquer $g \in G$, existe um elemento $h \in G$ tal que $g * h = h * g = e$. Indiquemos $g^{'} = h$.

Exemplo 10 *Para $(\mathbb{Z}, +)$, o inverso de $n \in \mathbb{Z}$ é $-n$, pois $n+(-n) = (-n)+n = 0$. Para $(\mathbb{R}, \cdot)$, nem todos os elementos possui inversos, isto é, 0 não tem inverso. No entanto, se $x \neq 0$, então $\frac{1}{x}$ é o inverso do x pois $x.\frac{1}{x} = \frac{1}{x}.x = 1$.*

Definição 7 *Se o grupo é comutativo então ele é chamado grupo abeliano. Ou seja, se $a, b \in G$ então $a * b = b * a$.*

Vejamos agora dois lemas que caracterizam a unicidade do elemento neutro e do elemento inverso.

Lema 1 *Um grupo tem exatamente um elemento identidade.*

Demonstração: Seja $(G, *)$ um grupo, suponhamos e_1 e e_2 elementos identidades de G (sabemos que G tem pelo menos um elemento identidade, pela definição de grupo). Então, $e_1 * e_2 = e_1$ deste e_2 é um elemento identidade, por outro lado, $e_1 * e_2 = e_2$ deste e_1 é um elemento identidade. Portanto, $e_1 = e_2$, pois ambos são iguais $e_1 * e_2$. ■

Lema 2 *Se $(G, *)$ é um grupo então cada $g \in G$ tem exatamente um único inverso.*

Demonstração: Seja $g \in G$, e suponhamos g_1, g_2 seus inversos em G (sabemos que há pelo menos um inverso, pela definição de um grupo), isto é, $g * g_1 = g_1 * g = e$ e $g * g_2 = g_2 * g = e$. Por associatividade, $(g_1 * g) * g_2 = g_1 * (g * g_2)$. Como g_1, g_2 é o inverso de g, temos que $g_1 = g_1 * e = g_1 * (g * g_2) = (g_1 * g) * g_2 = e * g_2 = g_2$. Portanto $g_1 = g_2$. ■

Exemplo 11 ***a.*** *$(\mathbb{Z}/4\mathbb{Z}, +)$ e $(\mathbb{Z}/5\mathbb{Z} - \{\overline{0}\}, \cdot)$ são grupos.*
b. *$(\mathbb{Z}, +)$ é um grupo. Mas $(\mathbb{Z}, -)$ não é um grupo, pois a subtração não é associativa.*
c. *$(\mathbb{R}, \cdot)$ não é um grupo, pois 0 não tem inverso sob a multiplicação. Porém, $(\mathbb{R} - \{0\}, \cdot)$ é grupo multiplicativo.*

Definição 8 *Diz-se que um elemento $a \in A$ é regular em relação a operação $*$ se, e somente se, quaisquer que sejam os elementos x e y de A, satisfaz:*
i) $x * a = y * a \Rightarrow x = y$
ii) $a * x = a * y \Rightarrow x = y$

1.3 Subgrupos

Seja $(G, *)$ um grupo. Diz-se que um subconjunto não vazio $H \subset G$ é um subgrupo de G se:

• H é fechado para a operação $*$ (isto é, se $a, b \in H$ então $a * b \in H$);

• $(H, *)$ também é um grupo (aqui o símbolo $*$ indica a restrição da operação de G aos elementos de H).

Se e indica o elemento neutro de G, então obviamente $\{e\}$ é um grupo de G. É imediato, também, que o próprio G é um subgrupo de si mesmo. Esses dois subgrupos, $\{e\}$ e G, são chamados subgrupos triviais de G.

Lema 3 *O elemento neutro e_h de H é necessariamente igual ao elemento neutro e de G.*

Demonstração: Como $e_h * e_h = e_h = e_h * e$, e todo elemento do grupo é regular em relação a operação, então $e = e_h$. ■

Lema 4 *Dado $b \in H$, o inverso de b em H é necessariamente igual ao inverso de b em G.*

Demonstração: Seja $b \in H$ e indiquemos $b^{'}$ e $b_h^{'}$ seus inversos em G e H, respectivamente. Como porém, $b_h^{'} * b = e_h = e = b^{'} * b$ então $b_h^{'} = b^{'}$, pois os elementos do grupo são regulares com sua operação. ■

Proposição 1 *Seja $(G, *)$ um grupo. Para que uma parte não vazia $H \subset G$ seja um subgrupo de G, é necessário e suficiente que $a * b^{'}$ seja um elemento de H sempre que a e b pertencem a esse conjunto.*

Demonstração: Primeiramente suponha H é subgrupo de G. Mostremos que $a * b^{'} \in H$. Se $a, b \in H$, então $a * b_h^{'} \in H$, uma vez que , por hipótese $(H, *)$ é um grupo. Mas $b_h^{'} = b^{'}$ e, portanto, a$*b^{'} \in H$.

Como, por hipótese H não é vazio, podemos considerar um elemento $x_0 \in H$. Juntando esse fato à hipótese: $x_0 * x_0^{'} = e \in H$. Considerando agora um elemento $b \in H$, da hipótese e conclusão anterior segue que:$e * b^{'} = b^{'} \in H$.

Mostremos agora que H é fechado para a operação $*$. De fato, se $a, b \in H$, então, levando em conta a conclusão anterior, $a, b' \in H$. De onde(novamente usando a hipótese): $a * (b')' = a * b \in H$.

Falta mostrar a associatividade em H, mas isso é trivial, pois se $a, b, c \in H$, então $a, b, c \in G$ e portanto $a*(b*c) = (a*b)*c$ (já que essa propriedade vale em G). ■

Exemplo 12 *O conjunto de inteiros pares é um subgrupo de* $(\mathbb{Z}, +)$: *Afinal, os inteiros pares são um subconjunto de* $\mathbb{Z}$*, e sabemos que* $(2\mathbb{Z}, +)$ *é um grupo, pois sejam* $x, y \in 2\mathbb{Z}$ *tal que* $x = 2k$ *e* $y = 2p$ *com* $k, p \in \mathbb{Z}$*, pela Proposição 1 basta provar que* $x * y' \in 2\mathbb{Z}$*, assim* $x * y' = x + y' = 2k + (-2p) = 2(k - p)$*, logo* $x * y'$ *é par. Portanto* $x * y' \in 2\mathbb{Z}$*.*

É prática comum escrever as operações de grupo como multiplicação; ou seja, escrevemos gh ao invés de $g * h$, e chamamos isso de o "produto"de g e h. A afirmação "seja G um grupo"realmente significa que G é um grupo sob alguma operação que será escrito como multiplicação.

1.4 Geradores

Seja G um grupo e S um subgrupo de G. Agora vamos dar algumas propriedades do conjunto de geradores.

Definição 9 *Seja* G *um grupo e* S *um subconjunto de* G*. Dizemos que* S *gera* G *ou que* S *é um conjunto de geradores de* G*, se cada elemento de* G *pode ser escrito como produto finito (sob a operação do grupo) de elementos de* S *e seus inversos. Notação:* $G = \langle S \rangle$*.*

Exemplo 13 *Cada elemento de* $\mathbb{Z}$ *pode ser escrito como uma soma finita de* 1 *ou de* -1*, então* $\mathbb{Z}$ *é gerado por* 1*. Isto é,* $\mathbb{Z} = \langle 1 \rangle$*. Pela mesma razão,*

$\mathbb{Z} = \langle -1 \rangle$. *Claro, também é verdade que* $\mathbb{Z} = \langle 1, 2 \rangle$. *Em geral, há muitos conjuntos possíveis de geradores de um grupo.*

Exemplo 14 *Cada elemento de* $\mathbb{Z}/4\mathbb{Z}$ *pode ser escrito como uma soma finita de* $\overline{1}$, *então* $\mathbb{Z}/4\mathbb{Z} = \langle \overline{1} \rangle$. *Ainda que* $\mathbb{Z} = \langle 1 \rangle$ *e* $\mathbb{Z}/4\mathbb{Z} = \langle \overline{1} \rangle$, $\mathbb{Z}$ *e* $\mathbb{Z}/4\mathbb{Z}$ *não são iguais!*

Definição 10 *Um grupo* G *é cíclico se existe* $g \in G$ *tal que* $G = \langle g \rangle$.

Exemplo 15 $\mathbb{Z}$ *e* $\mathbb{Z}/4\mathbb{Z}$ *são cíclicos.*

Lema 5 *Seja* G *um grupo finito e* $g \in G$. *Então,* $g^{-1} = g^n$ *para algum* $n \in \mathbb{N}$.

Demonstração: Se $g = e$, então não há o que demonstrar. Então, suponha que $g \neq e$, assim existe m inteiro positivo tal que $g^m = e$. Como $g \neq e$, $m \neq 1$, então m>1. Seja $n = m - 1 \in \mathbb{N}$. Então, $gg^n = g^m = e$, por isso, g^n é o inverso de g. ■

Lema 6 *Seja* G *um grupo finito e* S *um subconjunto de* G. *Então,* $G = \langle S \rangle$ *se cada elemento de* G *pode ser escrito como um produto finito de elementos de* S *(isto é, os inversos dos elementos de* S *não são necessários).*

Demonstração: Se cada elemento de G pode ser escrito como um produto finito de elementos de S, então é claro que $G = \langle S \rangle$.

Por outro lado, suponha que $G = \langle S \rangle$. Isto significa que cada elemento de G pode ser escrito como um produto finito $s_1 \times s_2 \times ... \times s_n$ onde cada s_i esta em S ou é inverso de um elemento de S. O ponto básico da prova é que o inverso de um elemento de S pode também ser escrito como um produto de elementos de S pelo Lema 5. Para tornar completamente rigorosa, usaremos indução sobre n.

Suponhamos que $n = 1$. Ou $s_1 \in S$ ou $s_1^{-1} \in S$. Se $s_1 \in S$, então s_1 é escrito como um produto de um único elemento de S. Se $s_1^{-1} \in S$ então s_1 pode ser escrita como um produto finito de elementos de S. Pelo Lema 5. Assim a base da indução é verdadeira.

Agora, suponha que a afirmação é verdadeira para todos os números naturais menores que n; queremos mostrar que $s_1 \times s_2 \times ... \times s_n$ pode ser escrito como um produto finito de elementos de S. Pela hipótese de indução, $s_1 \times s_2 \times ... \times s_{n-1}$ e s_n podem serem escritos como produtos finitos de elementos de S. Portanto, o seu produto $s_1 \times s_2 \times ... \times s_n$ certamente pode também. ■

Agora, vamos ver como traduzir propriedades de geradores para todo o grupo.

Proposição 2 *Seja G um grupo finito e S um subconjunto de G. Suponha que as duas condições a seguir são satisfeitas.*

1. Cada elemento de S satisfaz alguma propriedade P.

2. Se $g \in G$ e $h \in G$, satisfaz a propriedade P, então gh satisfaz a propriedade P também.

Então, cada elemento de $\langle S \rangle$ satisfaz P.

Demonstração: Pelo Lema 5, qualquer elemento de $\langle S \rangle$ pode ser escrito como $s_1...s_n$ onde $n \in \mathbb{N}$ e cada s_i é um elemento de S. Vamos provar a proposição por indução sobre n.

Se $n = 1$, então $s_1 \in S$ satisfaz a propriedade P por hipótese.

Suponha que indutivamente $s_1...s_{n-1}$ satisfaz a propriedade P. Então, o produto $(s_1...s_{n-1})s_n$ é um produto de dois elementos que satisfazem a propriedade P, por isso satisfaz a propriedade P também.

Logo cada elemento de $\langle S \rangle$ também satisfaz P. ■

Exemplo 16 $\mathbb{Z}/5\mathbb{Z} - \{\overline{0}\}$ *é um grupo finito com a operação multiplicação, e* $\langle\overline{2}\rangle = \mathbb{Z}/5\mathbb{Z} - \{\overline{0}\}$ *pois* $\overline{2}.\overline{2} = \overline{4}$, $\overline{2}.\overline{4} = \overline{3}$, $\overline{2}.\overline{3} = \overline{1}$, $\overline{2}.\overline{1} = \overline{2}$.

1.5 Grupos Especiais

Nesta seção vamos estudar os grupos diedrais, necessário para a construção dos conceitos do Cubo de Rubik.

1.5.1 Grupo Simétrico

Seja S um conjunto não vazio e seja $G = \{f : S \to S \text{ tal que } f \text{ é bijetiva}\}$. Se $\circ$ é a operação composição de funções, isto é,

$$\begin{array}{rccc} \circ: & G \times G & \to & G \\ & (g, f) & \mapsto & g \circ f \end{array}$$

então $(G, \circ)$ é um grupo tendo

$$\begin{array}{rccc} I_S: & S & \to & S \\ & x & \mapsto & x \end{array}$$

como identidade.

Esse grupo é chamado de grupo das Permutações do conjunto S. Se $S = \{1, 2, ..., n\}$ denotaremos esse grupo por S_n, e temos que o número de elementos de S_n é exatamente $n!$

Exemplo 17 *Agora vamos mostrar que os grupos* $S_n, n \geq 3$, *são exemplos de grupos não abelianos. De fato, sejam* $f, g \in S_n$ *definidas como segue:*

$$f : \{1, 2, 3, ..., n\} \to \{1, 2, 3, ..., n\}$$

$f(1) = 3, f(2) = 1, f(3) = 2$ *e* $f(x) = x$ *para qualquer* x *tal que* $4 \leq x \leq n$, *e*

$$g : \{1, 2, 3, ..., n\} \to \{1, 2, 3, ..., n\}$$

$g(3) = 2, g(2) = 3, g(1) = 1$ *e* $g(x) = x$ *para qualquer* x *tal que* $4 \leq x \leq n$.

Então, $(g \circ f)(1) = g(f(1)) = g(3) = 2$ *e* $(f \circ g)(1) = f(g(1)) = f(1) = 3$, *e teremos que* $g \circ f \neq f \circ g$.

É usual denotar um elemento f do grupo S_n por,

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

.

Exemplo 18 *O grupo* S_3 *é composto dos seguintes* 6 *elementos:*

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_1^{-1}; \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2^{-1};$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_3^{-1}; \quad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5^{-1}; \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_4^{-1}$$

e na Tabela 1.1 temos a tábua de S_3 *com a composição de função.*

1.5.2 Simetrias do Triângulo Equilátero($S_\triangle$)

Vejamos a conexão da estrutura do grupo S_3 e as simetrias do triângulo equilátero.

Seja $P_1P_2P_3$ um triângulo equilátero. Coloque o centro de gravidade na origem 0 do espaço e chame de t_1, t_2, t_3 as retas do espaço passando pelas medianas do triângulo.

As transformações espaciais que preservam o triângulo são:

• $id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}$: as rotações planas centradas em 0, no sentido anti-horário, de ângulos zero, $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$, respectivamente.

$\circ$	e	f_1	f_2	f_3	f_4	f_5
e	e	f_1	f_2	f_3	f_4	f_5
f_1	f_1	e	f_4	f_5	f_2	f_3
f_2	f_2	f_5	e	f_4	f_3	f_1
f_3	f_3	f_4	f_5	e	f_1	f_2
f_4	f_4	f_3	f_1	f_2	f_5	e
f_5	f_5	f_2	f_3	f_1	e	f_4

Tabela 1.1: Tábua de S_3

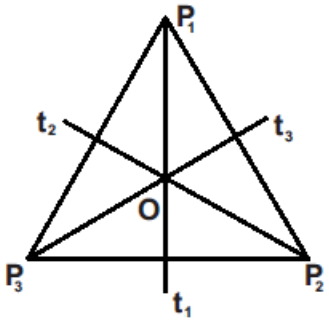


Figura 1.1: ***id***

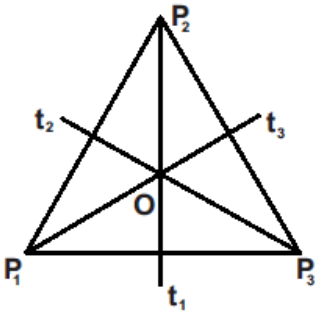


Figura 1.2: $\boldsymbol{R}_{\frac{2\pi}{3}}$

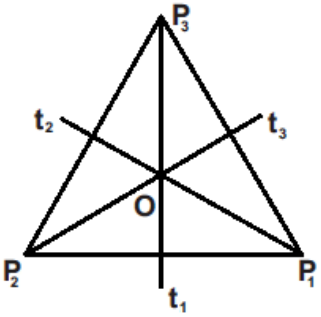


Figura 1.3: $\boldsymbol{R}_{\frac{4\pi}{3}}$

• R_1, R_2, R_3: as reflexões espaciais de ângulo π com eixos t_1, t_2, t_3, respectivamente.

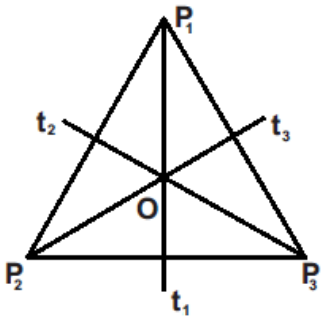


Figura 1.4: $\boldsymbol{R_1}$

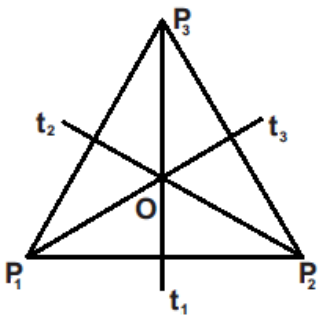


Figura 1.5: $\boldsymbol{R_2}$

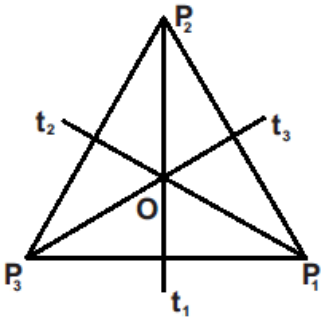


Figura 1.6: $\boldsymbol{R_3}$

Podemos ver através da Tabela 1.2, se $S_\triangle$ com a composição de funções é um grupo.

$\circ$	id	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
id	id	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	id	R_2	R_3	R_1
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	id	$R_{\frac{2\pi}{3}}$	R_3	R_1	R_2
R_1	R_1	R_3	R_2	id	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$
R_2	R_2	R_1	R_3	$R_{\frac{2\pi}{3}}$	id	$R_{\frac{4\pi}{3}}$
R_3	R_3	R_2	R_1	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$	id

Tabela 1.2: Tábua de $S_\triangle$

Por meio dela, podemos observar que a operação é fechada, que id é o elemento neutro e que o inverso de id, R_1, R_2 e R_3 são eles mesmos respectivamente, e o de $R_{\frac{4\pi}{3}}$ é o $R_{\frac{2\pi}{3}}$. Vale a associatividade, por se tratar de composição de transformações, então efetivamente se trata de um grupo. Como a tábua não é simétrica em relação a diagonal principal, então ele não é abeliano. Por

outro lado, observando que $(R_{\frac{2\pi}{3}})^2 = R_{\frac{2\pi}{3}} \circ R_{\frac{2\pi}{3}} = R_{\frac{4\pi}{3}}$, $R_1 \circ R_{\frac{2\pi}{3}} = R_3$ e $R_1 \circ (R_{\frac{2\pi}{3}})^2 = R_2$, então: $S_\triangle = \{(R_{\frac{2\pi}{3}})^0, R_{\frac{2\pi}{3}}, (R_{\frac{2\pi}{3}})^2, R_1, R_1 \circ R_{\frac{2\pi}{3}}, R_1 \circ (R_{\frac{2\pi}{3}})^2\}$. Ou seja, $S_\triangle$ é gerado por $R_{\frac{2\pi}{3}}$ e R_1.

O conjunto formado por $id, R_{\frac{2\pi}{3}}$ e $R_{\frac{4\pi}{3}}$ é um subgrupo de $S_\triangle$.

1.5.3 Simetrias do Quadrado($D_\square$)

Vejamos a conexão da estrutura de um subgrupo do S_4 e as simetrias do quadrado.

Seja $P_1P_2P_3P_4$ um quadrado. Coloque o centro de gravidade do quadrado na origem 0 do espaço e chame de d_1, d_2, m, n as retas do espaço determinadas pelas diagonais e mediatrizes do quadrado respectivamente.

As transformações espaciais que preservam o quadrado são:

• $id, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}$: as rotações planas centradas em 0, no sentido anti-horário, de ângulos zero, $\frac{\pi}{2}, \pi$ e $\frac{3\pi}{2}$ respectivamente.

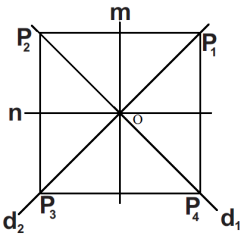


Figura 1.7: ***id***

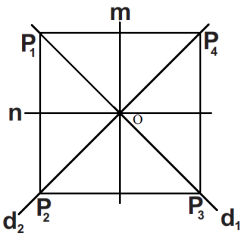


Figura 1.8: $\boldsymbol{R_{\frac{\pi}{2}}}$

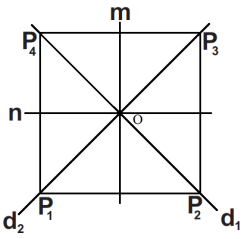


Figura 1.9: $\boldsymbol{R_\pi}$

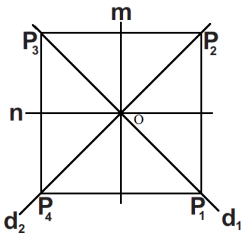
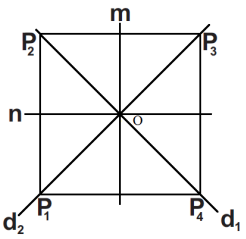
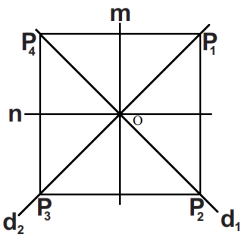
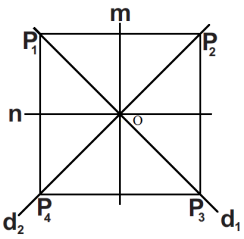


Figura 1.10: $\boldsymbol{R_{\frac{3\pi}{2}}}$

• R_1, R_2, R_m, R_n: as reflexões espaciais de ângulo π com eixos d_1, d_2, m, n, respectivamente.







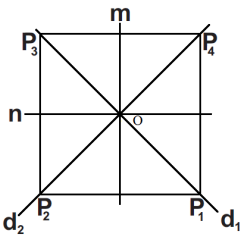


Figura 1.11: $\boldsymbol{R_1}$ Figura 1.12: $\boldsymbol{R_2}$ Figura 1.13: $\boldsymbol{R_m}$ Figura 1.14: $\boldsymbol{R_n}$

Veremos através da Tabela 1.3, se $D_\square$ com a composição de funções é um grupo.

$\circ$	id	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	R_1	R_2	R_m	R_n
id	id	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	R_1	R_2	R_m	R_n
$R_{\frac{\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	id	R_m	R_n	R_2	R_1
R_π	R_π	$R_{\frac{3\pi}{2}}$	id	$R_{\frac{\pi}{2}}$	R_2	R_1	R_n	R_m
$R_{\frac{3\pi}{2}}$	$R_{\frac{3\pi}{2}}$	id	$R_{\frac{\pi}{2}}$	R_π	R_n	R_m	R_1	R_2
R_1	R_1	R_m	R_2	R_n	id	R_π	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$
R_2	R_2	R_n	R_1	R_m	R_π	id	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$
R_m	R_m	R_2	R_n	R_1	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$	id	R_π
R_n	R_n	R_1	R_m	R_2	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$	R_π	id

Tabela 1.3: Tábua de $D_\square$

Por meio dela, podemos observar que a operação é fechada, que id é o elemento neutro e que o inverso de id, R_π, R_1, R_2, R_m e R_n são eles mesmos respectivamente, e o de $R_{\frac{3\pi}{2}}$ é $R_{\frac{\pi}{2}}$. Vale a associatividade, por se tratar de composição de transformações, então efetivamente se trata de um grupo.

Como a tábua não é simétrica em relação a diagonal principal, então ele não é abeliano. Por outro lado, observando-se que:
$(R_{\frac{\pi}{2}})^2 = R_{\frac{\pi}{2}} \circ R_{\frac{\pi}{2}} = R_\pi$, $(R_{\frac{\pi}{2}})^3 = (R_{\frac{\pi}{2}})^2 \circ R_{\frac{\pi}{2}} = R_\pi \circ R_{\frac{\pi}{2}} = R_{\frac{3\pi}{2}}$, $R_1 \circ R_{\frac{\pi}{2}} = R_m$, $R_1 \circ (R_{\frac{\pi}{2}})^2 = R_1 \circ R_\pi = R_2$ e $R_1 \circ (R_{\frac{\pi}{2}})^3 = R_1 \circ R_{\frac{3\pi}{2}} = R_n$, então: $D_\square = \{(R_{\frac{\pi}{2}})^0, R_{\frac{\pi}{2}}, (R_{\frac{\pi}{2}})^2, (R_{\frac{\pi}{2}})^3, R_1, R_1 \circ R_{\frac{\pi}{2}}, R_1 \circ (R_{\frac{\pi}{2}})^2, R_1 \circ (R_{\frac{\pi}{2}})^3\}$. Ou seja, $D_\square$ é gerado por $R_{\frac{\pi}{2}}$ e R_1.

O conjunto formado por $id, R_{\frac{\pi}{2}}, R_\pi$ e $R_{\frac{3\pi}{2}}$ é um subgrupo de $D_\square$.

1.5.4 Grupos Diedrais

O conceito de simetria de um triângulo e de um quadrado, que acabamos de observar, pode ser estendido naturalmente para um polígono regular qualquer de n lados. Tal como nos casos particulares, o número das simetrias de um polígono regular de n lados é o dobro do número de lados, portanto $2n$ no caso geral. Para descrever essas simetrias, denotemos os vértices do polígono consecutivamente por $1, 2, ..., n$ e o conjunto das simetrias por D_n. Duas simetrias bastam para gerar D_n; a rotação R de $\frac{2\pi}{n}$ radianos em torno do centro O do polígono, vide as Figuras 1.15 e 1.16;

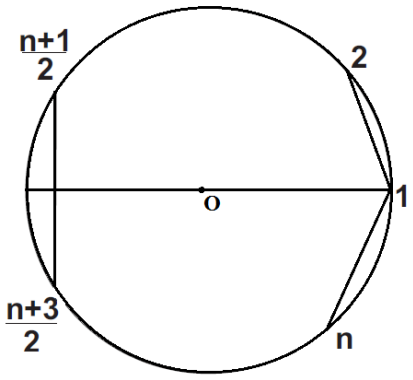


Figura 1.15: ***id***

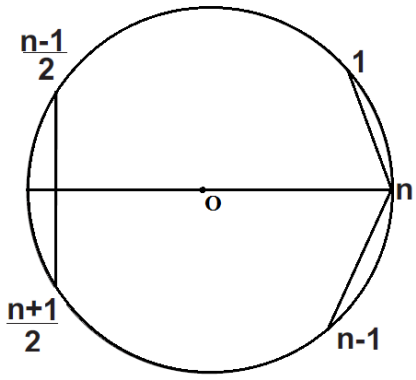


Figura 1.16: ***R***

e a reflexão X de π radianos em torno da reta x pelo vértice 1 e pelo centro do polígono, vide as Figuras 1.17 e 1.18;

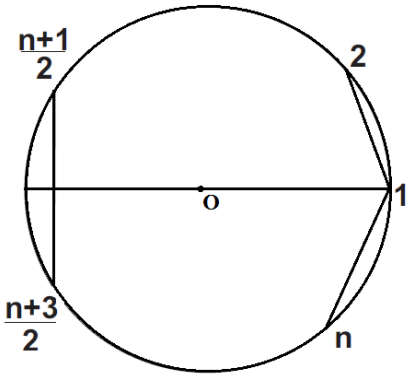


Figura 1.17: ***id***

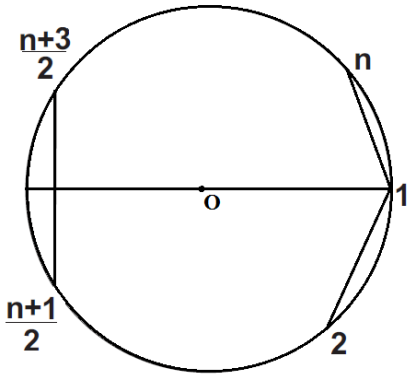


Figura 1.18: ***X***

Isso posto, pode-se demonstrar que o conjunto das simetrias do polígono é

$$D_n = \{R^0, R, R^2, ..., R^{n-1}, X, X \circ R, X \circ R^2, ..., X \circ R^{n-1}\},$$

e que esse conjunto é um grupo com a operação de composição de transformações. Ou seja, que D_n é um grupo gerado por dois de seus elementos: a rotação R e a reflexão X. Esse resultado que constitui uma generalização do que foi visto para o triângulo e o quadrado.

O grupo D_n é chamado grupo diedral de grau n. Em particular $D_3 = S_\triangle$ e $D_4 = D_\square$ são os grupos diedrais de grau 3 e 4, respectivamente.

Outro fato importante envolvendo o grupo diedral D_n é que o conjunto $R_n = \{R^0, R, R^2, ..., R^{n-1}\}$ das rotações do polígono é também um grupo em relação à composição de transformações.

1.5.5 Ciclo de Decomposição Disjunto

Há uma forma mais simples de escrever os elementos do grupo simétrico. Vejamos um exemplo.

Exemplo 19 *Considere* $\sigma \in S_{12}$ *definida por* $\sigma(1) = 12$, $\sigma(2) = 4$, $\sigma(3) = 5$,

$\sigma(4) = 2$, $\sigma(5) = 6$, $\sigma(6) = 9$, $\sigma(7) = 7$, $\sigma(8) = 3$, $\sigma(9) = 10$, $\sigma(10) = 1$, $\sigma(11) = 11$, $\sigma(12) = 8$.

Vamos escrever $i \mapsto j$ (i leva em j) significando $\sigma(i) = j$. Então,

$1 \mapsto 12$, $12 \mapsto 8$, $8 \mapsto 3$, $3 \mapsto 5$, $5 \mapsto 6$, $6 \mapsto 9$, $9 \mapsto 10$, $10 \mapsto 1$,

$2 \mapsto 4$, $4 \mapsto 2$,

$7 \mapsto 7$,

$11 \mapsto 11$.

Estes dados dizem o que σ faz a cada número. Então abreviando, temos que $\sigma = (1\ 12\ 8\ 3\ 5\ 6\ 9\ 10)(2\ 4)(7)(11)$.

Assim, (1 12 8 3 5 6 9 10), (2 4), (7), e (11) são chamados ciclos. Ao escrever a decomposição de ciclos disjuntos, deixamos de lado os ciclos com apenas um número, de modo que o ciclo de decomposição disjuntos de σ é $\sigma = (1\ 12\ 8\ 3\ 5\ 6\ 9\ 10)(2\ 4)$.

Agora, vamos realmente definir o que é um ciclo.

Definição 11 *Uma permutação $\alpha \in S_n$ é denominada um r-ciclo se existem elementos distintos $a_1, a_2, ..., a_r \in \{1, ..., n\}$ tais que $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3, ..., \alpha(a_{r-1}) = a_r$, $\alpha(a_r) = a_1$ e $\alpha(j) = j$, $\forall\ j \in \{1, ..., n\} \setminus \{a_1, a_2, ..., a_r\}$; tal r-ciclo será denotado por $(a_1...a_r)$; o número r é chamado o comprimento do ciclo. Os 2-ciclos são também chamados de transposições.*

Exemplos em S_5:

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ é um 5-ciclo, denotado por (12345); ele poderia também ser denotado por (23451), ou (34512), ou (45123), ou (51234).
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$ é um 3-ciclo, denotado por (143); ele poderia também ser denotado por (431), ou (314).
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$ é um transposição, denotado por (13); ele poderia também ser denotado por (31). O único 1-ciclo é a identidade, que denotamos por

(1) ou também por (a) com $a \in \{1, 2, 3, ..., n\}$.

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

Definição 12 *Seja $\alpha \in S_n$ um r-ciclo e seja $\beta \in S_n$ um s-ciclo; as permutações α e β são disjuntas se nenhum elemento de $\{1, ..., n\}$ é movido por ambas, isto é, $\forall\ a \in \{1, ..., n\}$, temos que $\alpha(a) = a$ ou $\beta(a) = a$.*

Lema 7 *Sejam $\alpha, \beta \in S_n$ ciclos. Se α e β são disjuntos, então $\alpha\beta = \beta\alpha$.*

Demonstração: Sejam α e β são ciclos de S_n disjuntos, com suportes iguais respectivamente a A e B. Se x é um elemento de I_n, há três hipóteses possíveis:

- $x \in A$.

Então, $(\alpha \circ \beta)(x) = \alpha(\beta(x)) = \alpha(x)$, ao passo que $(\beta \circ \alpha)(x) = \beta(\alpha(x)) = \alpha(x)$. Portanto, $\alpha \circ \beta$ e $\beta \circ \alpha$ coincidem em A.

- $x \in B$ (raciocínio análogo).

- $x \notin A$ e $x \notin B$. Neste caso, $(\alpha \circ \beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$, ao passo que $(\beta \circ \alpha)(x) = \beta(\alpha(x)) = \alpha(x) = x$. Portanto, $\alpha \circ \beta$ e $\beta \circ \alpha$ coincidem fora de A e B. ■

Exemplo 20 *Sejam $\alpha, \beta \in S_6$, definidas por $\alpha(1) = 3$, $\alpha(2) = 5$, $\alpha(3) = 4$, $\alpha(4) = 1$, $\alpha(5) = 2$, $\alpha(6) = 6$, $\beta(1) = 5$, $\beta(2) = 4$, $\beta(3) = 3$, $\beta(4) = 2$, $\beta(5) = 1$, $\beta(6) = 6$.*

Na notação de ciclo $\alpha = (1\ 3\ 4)(2\ 5)$ e $\beta = (1\ 5)(2\ 4)$. Então $\alpha\beta = (1\ 3\ 2)(4\ 5)$ e $\beta\alpha = (1\ 2)(3\ 4\ 5)$. Também podemos facilmente calcular $\alpha^2 = (1\ 4\ 3)$ e $\beta^2 = (1)$

Teorema 1 *Toda permutação $\alpha \in S_n$, exceção feita à permutação identidade, pode ser escrita univocamente (salvo quanto à ordem dos fatores) como um produto de ciclos disjuntos.*

1.6 Homomorfismo de Grupos

Definição 13 *Dá-se o nome de homomorfismo de um grupo $(G, *)$ num grupo $(J, \cdot)$ a toda aplicação ou função $f : G \to J$ tal que, quaisquer que sejam $x, y \in G$: vale $f(x * y) = f(x) \cdot f(y)$.*

Nessas condições, para simplificar a linguagem, nos referiremos a $f : G \to J$ como um homomorfismo de grupos. Quando se tratar do mesmo grupo, o que pressupõe $J = G$ e a mesma operação, então f será chamada de homomorfismo de G. Se um homomorfismo é uma aplicação injetora, então é chamado de homomorfismo injetor. E se for uma aplicação sobrejetora, de homomorfismo sobrejetor.

Exemplo 21 *A aplicação $f : \mathbb{Z} \to \mathbb{C}^*$ definida por $f(m) = i^m$ é um homomorfismo de grupos. É preciso notar, primeiro, que em casos como esses as operações são as usuais e devem ser pressupostas. Portanto, $\mathbb{Z}$ é um grupo aditivo e $\mathbb{C}^*$ um grupo multiplicativo. Como*

$$f(m+n) = i^{m+n} = i^m.i^n = f(m).f(n)$$

fica provado que se trata de um homomorfismo.

Definição 14 *Um homomorfismo $f : G \to J$ é um isomorfismo se existe um homomorfismo $h : J \to G$ tal que $f \circ h = id_J$ e $g \circ f = id_G$. Quando existe um isomorfismo entre dois grupos G e J, dizemos que G e J são isomorfos e denotamos $G \simeq J$.*

Proposição 3 *Seja $f : (G, *) \to (J, \cdot)$ um homomorfismo de grupos. Então, f é um isomorfismo se e somente se f é bijetivo.*

Definição 15 *O núcleo de um homomorfismo $\phi : G \longrightarrow H$ é definido como sendo $\{g \in G$ tal que $\phi(g) = 1_H\}$ e isso é denotado por Ker ϕ. Isto é, Ker ϕ é a imagem inversa de 1_H em G.*

Seja $\mathbb{G} = \{e, D, U, L, R, F, B, D', U', L', R', F', B', D^2, U^2, L^2, R^2, F^2, B^2\}$ conjunto dos movimentos do Cubo de Rubik.

Mostraremos no próximo capítulo que $\mathbb{G}$ munido da operação composição de movimentos é um grupo.

Exemplo 22 *O núcleo do homomorfismo $\phi_{cubo} : \mathbb{G} \longrightarrow S_{20}$ é composto por todos os movimentos do cubo de Rubik que não alteram as posições de qualquer um dos cubos. Ou seja, Ker ϕ_{cubo} consiste em todos os movimentos que afetam apenas as orientações, e não as posições do cubo.*

Teorema 2 *Se G e H são grupos e $\phi : G \longrightarrow H$ um homomorfismo, então Ker ϕ é um subgrupo de G.*

Demonstração: Basta mostrar que, se $g, h \in$ Ker ϕ, então $gh^{-1} \in$ Ker ϕ. Seja $g, h \in$ Ker ϕ, assim
$\phi(gh^{-1}) = \phi(g)\phi(h^{-1})$ pois ϕ é um homomorfismo,
$\phi(gh^{-1}) = \phi(g)\phi(h)^{-1}$ pois ϕ é um homomorfismo,
$\phi(gh^{-1}) = 1_H 1_H^{-1}$ pois $g, h \in$ Ker ϕ,
$\phi(gh^{-1}) = 1_H$,
Portanto, $gh^{-1} \in$ Ker ϕ. ■

1.7 O Sinal do Homomorfismo

Sempre é possível escrever uma permutação em 2-Ciclos. As permutações em S_n escritas como um produto de um número par de 2-ciclos são chamadas de permutações pares. Outras que são escritas como um produto de um número ímpar de 2-ciclos são chamadas permutações ímpares. Uma permutação é par ou ímpar, mas não ambos.

Fixe n, e seja $p(x_1, ..., x_n)$ um polinômio em n de variáveis $x_1, ..., x_n$.

Exemplo 23 *Se $n = 1$, $p(x_1)$ é um polinômio na variável x_1; isto é, $p(x_1) = a_m x_1^m + a_{m-1} x_1^{m-1} + ... + a_0$. Assim, $p(x_1)$ é uma soma infinita de termos do tipo ax_1^i. Se $n = 2$, então $p(x_1, x_2)$ é uma soma de termos do tipo $ax_1^i a x_2^j$.*

Em geral, $p(x_1, ..., x_n)$ é uma soma de termos do tipo $ax_1^{i_1} a x_2^{i_2} ... a x_n^{i_n}$.

Se $\alpha \in S_n$, seja p^α o polinômio definido por $(p^\alpha)(x_1, ..., x_n) = p(x_{\alpha(1)}, ..., x_{\alpha(n)})$. Isto é, simplesmente substituir x_i por $x_{\alpha(i)}$.

Exemplo 24 *Suponhamos $n = 4$, $p(x_1, x_2, x_3, x_4) = x_1^3 + x_2 x_3 + x_1 x_4$, e $\alpha \in S_4$ tem ciclo de decomposição $\alpha = (1\ 2\ 3)$. Então, $(p^\alpha)(x_1, x_2, x_3, x_4) = x_{\alpha(1)}^3 + x_{\alpha(2)} x_{\alpha(3)} + x_{\alpha(1)} x_{\alpha(4)} = x_2^3 + x_3 x_1 + x_2 x_4$.*

Exemplo 25 *Sejam $n = 4$, $p(x_1, x_2, x_3, x_4) = x_1^3 + x_2 x_3 + x_1 x_4$, $\alpha = (1\ 2\ 3)$ e $\beta = (1\ 3)(2\ 4)$. Pelo Exemplo 24, temos $p^\alpha = x_2^3 + x_3 x_1 + x_2 x_4$, assim $(p^\alpha)^\beta = x_{\beta(2)}^3 + x_{\beta(3)} x_{\beta(1)} + x_{\beta(2)} x_{\beta(4)} = x_4^3 + x_1 x_3 + x_4 x_2$. Por outro lado, $\alpha\beta = (1\ 4\ 2)$, então $p^{\alpha\beta} = x_{(\alpha\beta)(1)}^3 + x_{(\alpha\beta)(2)} x_{(\alpha\beta)(3)} + x_{(\alpha\beta)(1)} x_{(\alpha\beta)(4)} = x_4^3 + x_1 x_3 + x_4 x_2$.*

De fato, o caso do Exemplo 25 não é particular. Veja o seguinte resultado.

Lema 8 *Para quaisquer $\alpha, \beta \in S_n$, $(p^\alpha)^\beta = p^{\alpha\beta}$.*

Demonstração: Pela definição, temos $(p^\alpha)(x_1, ..., x_n) = p(x_{\alpha(1)}, ..., x_{\alpha(n)})$, assim $[(p^\alpha)^\beta](x_1, ..., x_n) = p(x_{\beta(\alpha(1))}, ..., x_{\beta(\alpha(n))})$. Como $\beta(\alpha(i)) = (\alpha\beta)(i)$, assim $[(p^\alpha)^\beta](x_1, ..., x_n) = p(x_{(\alpha\beta)(1)}, ..., x_{(\alpha\beta)(n)}) = (p^{\alpha\beta})(x_1, ..., x_n)$. ■

Para provar a nossa afirmação sobre permutações pares e ímpares, vamos aplicar o Lema 8 para um polinômio específico,

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Exemplo 26 *Se* $n = 3$, $\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.

Lema 9 *Para qualquer* $\alpha \in S_n$, $\Delta^\alpha = \pm\Delta$.

Exemplo 27 *Se* $\alpha = (1\ 3\ 2)$, *então* $\Delta^\alpha = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \Delta$. *Por outro lado, se* $\alpha = (1\ 2)$, *então* $\Delta^\alpha = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -\Delta$.

Agora, vamos provar o Lema 9. Como pode imaginar a partir dos exemplos, a ideia é combinar termos de Δ com termos de Δ^α. Isto é, para cada termo $x_i - x_j$ do produto de Δ temos $x_i - x_j$ ou seu negativo no produto de Δ^α.

Demonstração: Pela definição, temos

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j),$$

assim

$$\Delta^\alpha = \prod_{1 \le i < j \le n} (x_{\alpha(i)} - x_{\alpha(j)}).$$

A fim de mostrar $\Delta^\alpha = \pm\Delta$, devemos mostrar duas coisas. Primeira, para cada i e j com $1 \le i < j \le n$ devemos mostrar que $x_{\alpha(i)} - x_{\alpha(j)}$ ou seu negativo aparece em Δ, isto é, tanto $x_{\alpha(i)} - x_{\alpha(j)}$ ou seu negativo tem a forma $x_k - x_l$ com $1 \le k < l \le n$. Segunda, mostraremos que, para cada i e j com $1 \le i < j \le n$, $x_i - x_j$ ou seu negativo aparece em Δ^α. Como Δ e Δ^α têm a mesma quantidade de termos, estas duas declarações juntas provam que os termos de Δ e Δ^α são iguais.

Para provar a primeira, precisamos mostrar que $\alpha(i) < \alpha(j)$ ou $\alpha(j) < \alpha(i)$, mas como α é injetora e $i \neq j$ então $\alpha(i) \neq \alpha(j)$ se $1 \le i < j \le n$.

Para provar a segunda, precisamos mostrar que $x_i - x_j$ ou seu negativo pode ser escrito como $x_{\alpha(k)} - x_{\alpha(l)}$ com $1 \le k < l \le n$. Como $\alpha \in S_n$,

$\alpha^{-1} \in S_n$; em particular α^{-1} é também uma bijeção. Por hipótese, $i \neq j$, $\alpha^{-1}(i) \neq \alpha^{-1}(j)$. Seja k o menor dentre os elementos $\alpha^{-1}(i)$ e $\alpha^{-1}(j)$ e l o maior. Do que, $1 \leq k < l \leq n$ é também $x_{\alpha(k)} - x_{\alpha(l)}$ ou seu negativo. ■

Pelo Lema 9, podemos definir uma função $\epsilon : S_n \longrightarrow \{\pm 1\}$ com $\alpha\Delta = \epsilon(\alpha)\Delta$. Pelo Lema 8, $\Delta^{\alpha\beta} = (\Delta^{\alpha})^{\beta} = [\epsilon(\alpha)\Delta]^{\beta} = \epsilon(\alpha)\Delta^{\beta} = \epsilon(\alpha)\epsilon(\beta)\Delta = \epsilon(\alpha)\epsilon(\beta)$. Portanto, $\epsilon(\alpha\beta) = \epsilon(\alpha)\epsilon(\beta)$. Assim, ϵ é um homomorfismo.

Citamos no início que $\epsilon(\alpha)$ tinha algo a ver com o número de 2-ciclos em um produto decomposição de α. Agora, vamos provar isso.

Teorema 3 *Se α é um 2-ciclo, então $\epsilon(\alpha) = -1$.*

Demonstração: Primeiro, seja $\alpha = (1\ 2)$. Podemos escrever

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Agora, vamos escrever os termos onde $i = 1$ ou $i = 2$ separadamente. Então,

$$\Delta = \prod_{1 < j \leq n} (x_1 - x_j) \prod_{2 < j \leq n} (x_2 - x_j) \prod_{3 \leq i < j \leq n} (x_i - x_j)$$

$$= (x_1 - x_2) \prod_{2 < j \leq n} (x_1 - x_j) \prod_{2 < j \leq n} (x_2 - x_j) \prod_{3 \leq i < j \leq n} (x_i - x_j).$$

Portanto,

$$\Delta^{\alpha} = (x_{\alpha(1)} - x_{\alpha(2)}) \prod_{2 < j \leq n} (x_{\alpha(1)} - x_{\alpha(j)}) \prod_{2 < j \leq n} (x_{\alpha(2)} - x_{\alpha(j)}) \prod_{3 \leq i < j \leq n} (x_{\alpha(i)} - x_{\alpha(j)})$$

$$= (x_2 - x_1) \prod_{2 < j \leq n} (x_2 - x_j) \prod_{2 < j \leq n} (x_1 - x_j) \prod_{3 \leq i < j \leq n} (x_i - x_j)$$

$$= -\Delta.$$

Assim, provamos a afirmação para $\alpha = (1\ 2)$.

Podemos generalizar o argumento para qualquer 2-ciclo, mas há uma maneira mais simples. Seja α qualquer 2-ciclo. Como α é conjugado com (1 2). Isso é, $\alpha = \beta(1\ 2)\beta^{-1}$ para algum $\beta \in S_n$, e ϵ é um homomorfismo. Então $\epsilon(\alpha) = \epsilon(\beta)\epsilon(1\ 2)\epsilon(\beta^{-1}) = \epsilon(1\ 2) = -1$. ■

Visto que ϵ é multiplicativo, se $\epsilon(\alpha) = 1$, então ϵ deve ser um produto de um número par de 2-ciclos. Da mesma forma, se $\epsilon(\alpha) = -1$, então ϵ deve ser um produto de um número ímpar de 2-ciclos. Assim, ϵ é par se $\epsilon(\alpha) = 1$, e ϵ é impar se $\epsilon(\alpha) = -1$.

Exemplo 28 *(1 2) (3 1) é par, pois é produto de dois* 2*-ciclos. (1 2) é ímpar, pois é produto de um* 2*-ciclo.*

Então provamos que um elemento de S_n é par ou ímpar, mas não ambos. A ferramenta que usamos para isso foi o sinal do homomorfismo. Lembre-se que este foi um homomorfismo $\epsilon : S_n \longrightarrow \{\pm 1\}$ de tal modo que $\epsilon(\alpha) = -1$ para 2-ciclo qualquer α. Uma vez que o 2-ciclos gerar S_n, esta propriedade caracteriza o homomorfismo.

Exemplo 29 *ϵ((1 2) (1 3)) = 1 e ϵ((1 2)) = -1.*

Exemplo 30 *ϵ(1 6 3 4 2) = 1 porque (1 6 3 4 2) = (1 6)(1 3)(1 4)(1 2) é par.*

Exemplo 31 *Se α é um k-ciclo, então $\epsilon(\alpha) = (-1)^{k-1}$. Afinal, se α é um k-ciclo, então podemos escrever $\alpha = (a_1a_2...a_k) = (a_1a_2)(a_1a_3)...(a_1a_k)$.*

1.8 O Grupo alternado

Na seção anterior, definimos o que significava para um elemento de S_n ser par ou ímpar. Observemos que o produto de uma permutação par e uma

permutação ímpar é impar. O produto de duas permutações pares ou duas permutações ímpares é par. O inverso de uma permutação par é par, e o inverso de uma permutação impar é impar. Portanto, podemos definir um subgrupo de S_n que consiste em todas as permutações pares. Este grupo é chamado o grupo alternado e é denotado A_n.

Exemplo 32 *O grupo alternado A_n é o Ker de $\epsilon : S_n \longrightarrow \{\pm 1\}$.*

A_n também pode ser escrito como $A_n = \{\alpha \in S_n / \ \epsilon(\alpha) = 1\}$.

Capítulo 2

Há muitos "brinquedos"enigmáticos que tenham sido baseados no Cubo de Rubik, como por exemplo, o quebra-cabeça. Estes mistérios podem ser mais complexos ou simples do que o cubo normal. Vejamos como é a estrutura do Cubo de Rubik $3 \times 3 \times 3$.

2.1 Cubo de Rubik $3 \times 3 \times 3$

O Cubo de Rubik $3 \times 3 \times 3$ é composto por 27 pequenos cubos, que são normalmente chamadas de "cubinhos", destes 26 são visível. Ao trabalhar com o Cubo de Rubik, é útil ter uma maneira de chamar os cubinhos individualmente.

Embora pareça natural utilizar as cores nos cubinhos, na verdade é mais útil ter nomes que descrevam a localizações dos cubinhos. Os cubinhos dos cantos são chamados, muito apropriadamente, de **cubinhos de cantos** . Cada cubinho de canto tem 3 faces visíveis, e há 8 cubinhos de cantos. Veja a Figura 2.1.

Os cubinhos com duas faces visíveis são chamados **cubinhos de arestas**; há 12 cubinhos de arestas. Veja a Figura 2.2.

Finalmente, os cubinhos com uma única face visível são chamados **cubi-**

nhos centrais e há 6 cubinhos centrais. Veja a Figura 2.3.

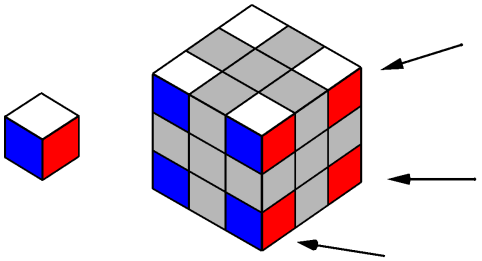


Figura 2.1: Cubinhos de Canto

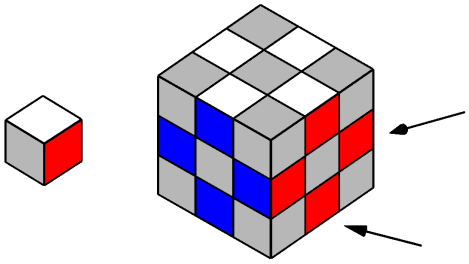


Figura 2.2: Cubinhos de Aresta

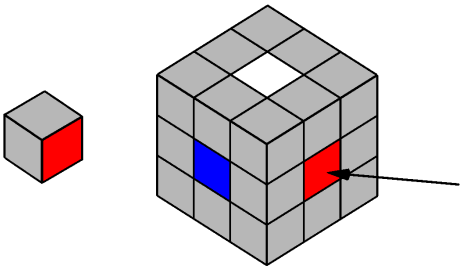


Figura 2.3: Cubinhos Centrais

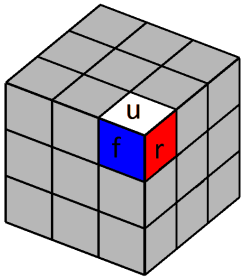


Figura 2.4: Rotulação

Agora, vamos citar as 6 faces do Cubo de Rubik. Seguindo a notação desenvolvida por David Singmaster, vamos chamá-las, a da direita (r), esquerda (l), acima (u), baixo (d), frente (f), e fundo (b). A vantagem desta nomenclatura é que cada face pode ser referido por uma única letra. Veja as Figuras 2.5 e 2.4.

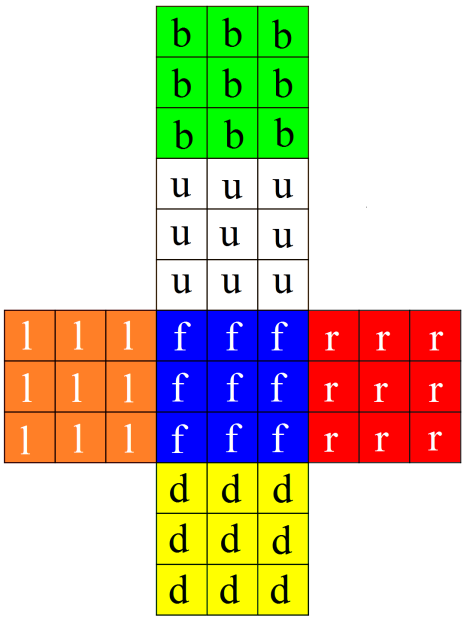


Figura 2.5: Faces do Cubo

Para citar um cubinho canto, simplesmente listamos suas faces visíveis no sentido horário. Por exemplo, no cubinho superior, direito, frontal está escrito urf. Naturalmente, podemos chamar este cubinho de rfu ou fur, às vezes, é importante que a face esteja listada primeiro, nestes casos, são **cubinhos orientados**. Ou seja, o cubinho orientado urf, rfu e fur são diferentes. Em outras situações, não importando que a face esteja listada primeiro, nesses casos, são **cubinhos não orientados** .Isto é, os cubinhos não orientados urf, rfu e fur são os mesmos.

Da mesma forma, os cubinhos de aresta e central, vamos listar apenas as faces visíveis dos cubinhos. Por exemplo, o cubinho no centro da face frontal é simplesmente chamado f, porque a sua única face visível encontra-se na parte da frente do cubo.

Também iremos falar frequentemente sobre **cubículos** . Estes são rotulados da mesma forma que cubinhos, mas descrevem o espaço em que vive o

cubinho. Assim, se o Cubo de Rubik está na configuração de partida (isto é, o Cubo de Rubik esta resolvido), então cada cubinho permanece no cubículo do mesmo nome (o cubinho urf permanece no cubículo urf, o cubinho f permanece no cubículo f, e assim por diante). Se você girar uma face do Cubo de Rubik, os cubículos não vão se mover, mas os cubinhos sim. Entretanto, quando você girar uma face do Cubo de Rubik, todos cubinhos centrais permanecera em seus cubículos.

Por fim, queremos dar nomes a alguns movimentos do Cubo de Rubik. O movimento mais básico que se pode fazer é girar uma única face. Vamos denotar de R uma rotação no sentido horário da face direita (olhando para a face direita, gire 90° no sentido horário). Da mesma forma, vamos usar a letra maiúscula L, U, D, F e B para denotar voltas no sentido horário das faces correspondentes. De modo mais geral, vamos chamar qualquer sequência contendo algumas dessas 6 letras de um **movimento** do Cubo de Rubik. Observe que, girando a face direita três vez no sentido anti-horário é o mesmo que girar uma vez no sentido horário, ou seja, aplicar R uma vez. E mais tarde, iremos descrever uma notação para esses movimentos mais complicados. Veja a Figura 2.6.

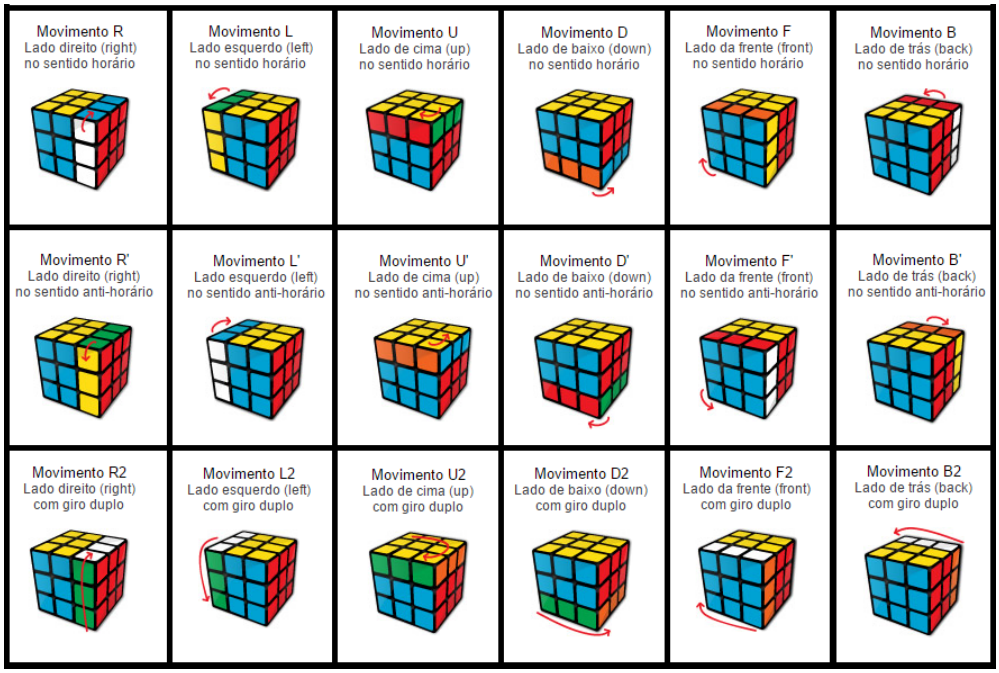


Figura 2.6: Movimentos do Cubo $3 \times 3 \times 3$

Algumas informações são imediatamente claras, por exemplo os 6 movimentos básicos mantêm os cubinhos de centro em seus cubículos. Uma vez que qualquer movimento é uma sequência destes 6 movimentos básicos, isto significa que cada movimento do Cubo de Rubik mantém os cubinhos de centro em seus cubículos. Além disso, qualquer movimento do Cubo de Rubik coloca cubinhos de cantos em cubículos de cantos e cubinhos de arestas em cubículos de arestas; ou seja, é impossível para um cubinho de canto viver em um cubículo de aresta ou para um cubinho de aresta viver em um cubículo de canto.

Usando esses dois fatos, podemos começar a descobrir as muitas configurações possíveis para o Cubo de Rubik. Vejamos, por exemplo, no cubículo urf. Teoricamente, qualquer um dos 8 cubinhos de cantos poderia residir neste compartimento. Isso deixa 7 cubinhos de cantos que poderia residir no

cubículo urb, 6 para o próximo compartimento, e assim por diante. Portanto, há $8.7.6.5.4.3.2.1 = 8! = 40320$ possíveis posicionamentos dos cubinhos de cantos. Observe que um cubinho canto pode caber em seu cubículo de 3 maneiras diferentes. Por exemplo, se as cores vermelho, branco e azul do cubinho estão no cubículo urf, então a face vermelho, branco, azul poderiam estar na face u do cubículo (e isto determina onde as outras 2 faces estão). Existem 8 cubinhos de cantos e cada um pode estar em seu cubículo em 3 formas diferentes, existem 3^8 maneiras diferentes dos cubinhos de cantos serem orientados. Portanto, existem $3^8.8!$ possíveis configurações dos cubinhos de cantos. Da mesma forma, uma vez que existem 12 cubinhos de arestas, há 12! posições dos cubinhos de arestas; cada cubinho aresta tem 2 orientações possíveis, dando 2^{12} possíveis orientações. Assim, existem $2^{12}.12!$ possíveis configurações dos cubinhos de arestas, dando um total de $2^{12}.3^8.8!.12!$ configurações possíveis do Cubo de Rubik. (Este número é cerca de $5,19 \times 10^{20}$, ou 519 quintilhões).

Embora essas configurações são teoricamente possíveis, isso não significa que podia realmente ocorrer. Vamos dizer que uma configuração do Cubo de Rubik é válida se ela pode ser alcançada por uma série de movimentos a partir da configuração inicial. Acontece que algumas possíveis configurações contadas, realmente não são válidas. Portanto, temos dois objetivos:

1. Demonstrar que algumas configurações não são válidas;
2. Encontrar um conjunto de movimentos que podem nos levar a partir de qualquer configuração válida de volta para a configuração inicial.

2.1.1 Cubo $3 \times 3 \times 3$ - Método de Resolução

Nesta seção iremos trabalhar o método de solucionar o Cubo de Rubik $3 \times 3 \times 3$, que serão dividido em alguns passos:

1° Passo: Escolha uma cor para formar a cruz, no nosso caso, a cor será a branca. Posicione o lado escolhido na parte inferior do cubo. Observe quais **cubinhos centrais** são oposto aos outros, para facilitar.

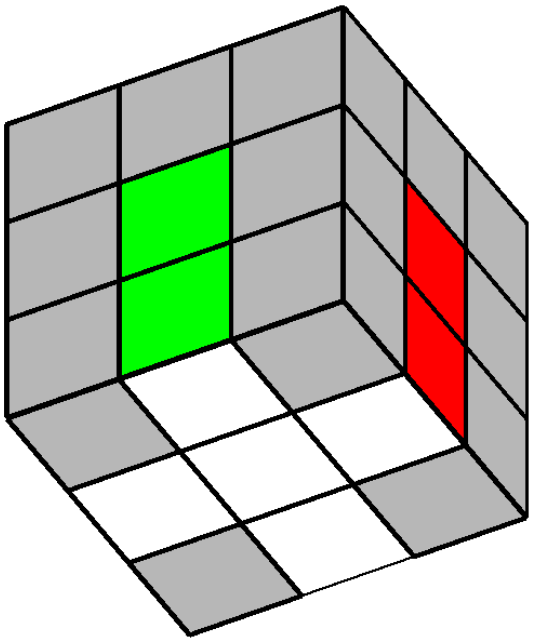


Figura 2.7: Cruz

2° Passo: O objetivo deste passo é colocar os **cubinhos cantos** que contém a cor branca em seus lugares, de modo que as cores das laterais fiquem certas e não altere a cruz. Observe à Figura 2.8.

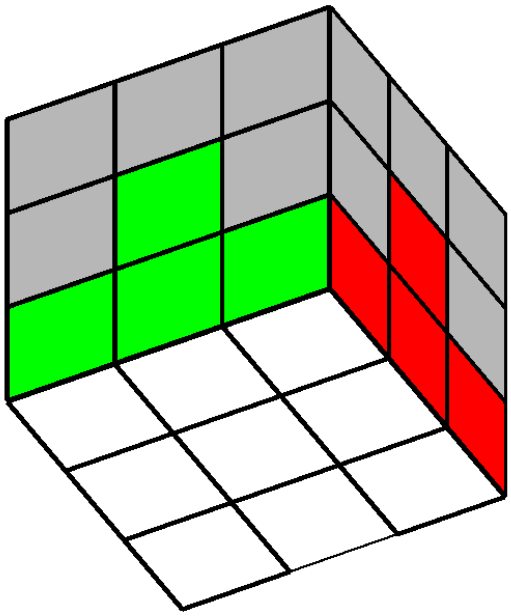


Figura 2.8: Uma face completa

3° Passo: Neste passo, vamos finalizar a camada do meio no cubo. Como a branca já está completa, as peças que faltam para completar este passo são os meios da segunda camada. Veja a Figura 2.9.

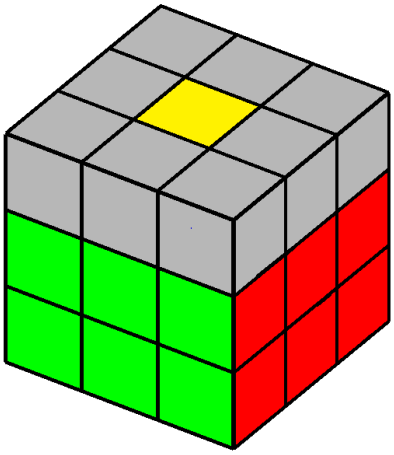


Figura 2.9: Camada do meio

Primeiro vamos procurar um **cubinho de aresta** no topo do cubo, e

encontrar o lugar que ele deverá entrar de acordo com os centros correspondentes, posicionar e aplicar a fórmula de acordo com a situação encontrada.

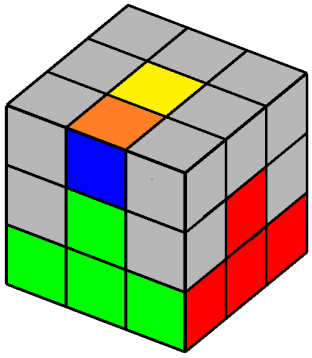


Figura 2.10: Exemplo

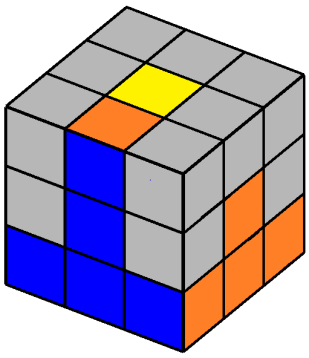


Figura 2.11: Aplicado U, U' ou U^2

Neste passo, os únicos **cubinhos de arestas** que não vão fazer parte são os amarelos, ou seja, qualquer outro que você encontrar no topo do cubo sera usado.

Mantenha a camada branca na base e procure no topo do cubo por **cubinhos de arestas** que não tenham a cor amarela. Em seguida aplicar o movimento U, U' ou U^2, mantendo a cor da lateral deste, junto com o **cubinho central** correspondente. Veja a Figura 2.11.

Às possíveis posições do **cubinho de aresta** no cubo são:

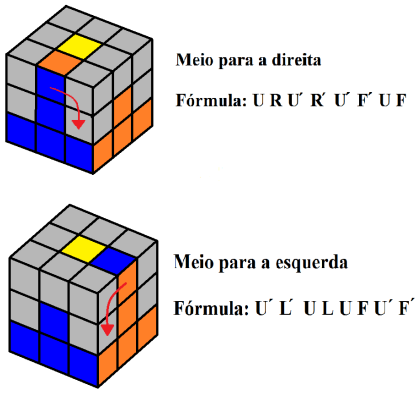


Figura 2.12: Fórmulas

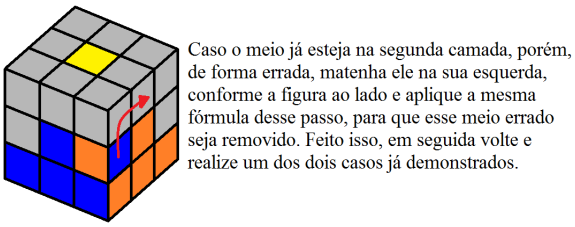


Figura 2.13: Observação

4° Passo: Agora que o cubo já está com duas camadas completas, vamos iniciar a solução da última camada. Os próximos quatro passos requerem bastante atenção, pois qualquer movimento errado pode comprometer o que já finalizamos, entretanto, são movimentos bem objetivos e fáceis de serem aplicados. Lembre-se sempre de posicionar o cubo corretamente e não errar o sentido dos movimentos.

Neste passo, vamos fazer uma cruz amarela na face de cima do cubo. É um passo muito simples, no qual você deve apenas posicionar seu cubo conforme a figura e aplicar a fórmula correspondente.

Seu cubo pode estar em 3 posições diferentes. Em qualquer um dos casos a fórmula será a mesma, a única diferença será a quantidade de vezes que ela deverá ser aplicada e a posição do cubo. Observe em qual caso seu cubo se encontra, posicione conforme a figura e aplique os movimentos.

Caso não encontre uma figura que esteja igual ao seu cubo, então o cubo não está montado na forma correta e será um dos **casos impossíveis**.

Fórmula: $FRUR'U'F'$

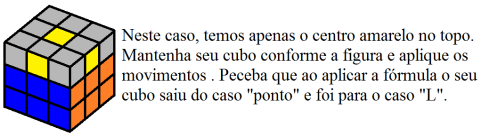


Figura 2.14: Caso Ponto

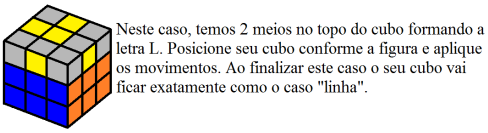


Figura 2.15: Caso L

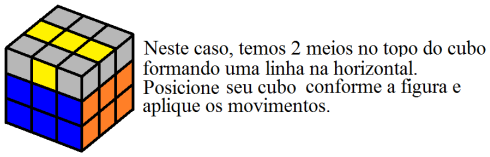


Figura 2.16: Caso Linha

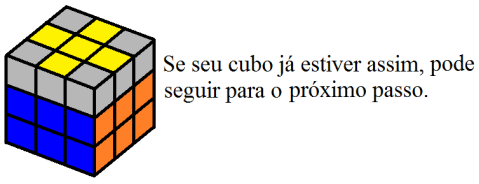


Figura 2.17: Cruz Completa

5° Passo: Neste passo, vamos finalizar a face do topo do cubo por completo,

subindo todos os **cubinhos de cantos** amarelos.

No momento não precisa se preocupar com as cores das laterais da última camada, dê atenção apenas aos **cubinhos de cantos** com a cor amarela.

O cubo pode estar em 7 posições diferentes, em qualquer um dos casos a fórmula será a mesma, a única diferença será a quantidade de vezes que ela deverá ser aplicada e a posição do cubo. Veja qual é o caso que seu cubo está, posicione conforme a figura e aplique os movimentos seguindo a sequência.

Caso você não encontre uma figura que esteja igual ao seu cubo, ocorrerá a mesma situação do passo anterior,**casos impossíveis**.

O único algoritmo que você deverá executar se chama **Sune**. Basta posicionar seu cubo conforme a figura correspondente e aplicar os movimentos.

Sune: $RUR'URU^2R'$

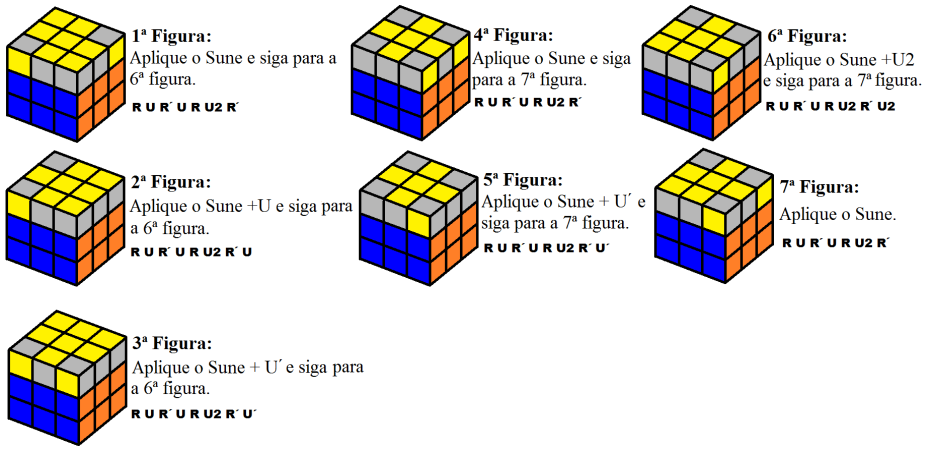


Figura 2.18: Sete posições possíveis

6° Passo: Neste passo, vamos permutar os 4 **cubinhos de cantos** da última camada. Para isso, deve encontrar um lado que tenha 2 **cubinhos de cantos** da mesma cor, posicionar este lado na sua frente e aplicar a fórmula correspondente, independentemente das demais cores da última camada e a cor da face.

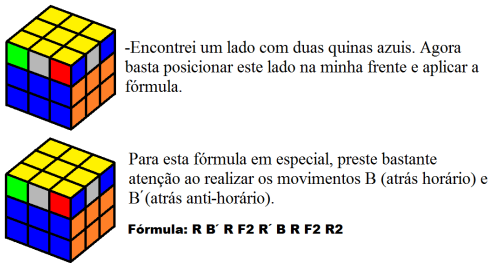


Figura 2.19: Fórmula do 6° Passo

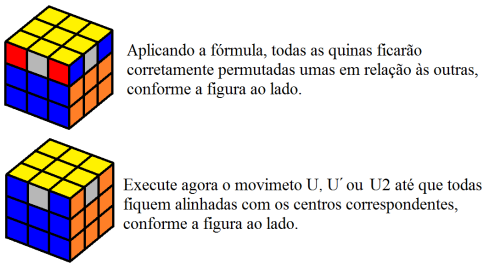


Figura 2.20: Aplicado a Fórmula

Caso não encontre um lado que tenha 2 **cubinhos de cantos** da mesma cor, mantenha o amarelo no topo e execute a mesma fórmula em qualquer posição, depois volte e procure novamente.

Se você encontrar **cubinhos de cantos** das mesmas cores (em pares) em todos os lados, é sinal que este passo já está concluído. Neste caso, alinhe os **cubinhos de cantos** com os centros correspondentes com o movimento U, U' ou U^2, e siga para o próximo passo.

7° Passo: Neste passo, encontre um lado do cubo que esteja totalmente completo, manter este lado na parte de trás, identifique qual o sentido que os outros 3 **cubinhos de arestas** errados deverão ser permutados e aplicar os movimentos correspondentes.

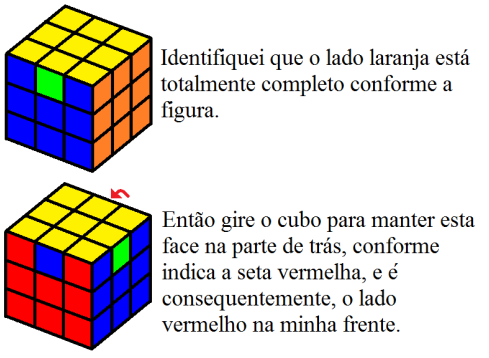


Figura 2.21: Três Faces Completas

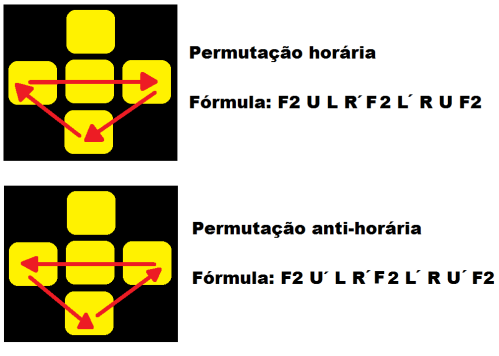


Figura 2.22: Fórmula do 7° Passo

Caso seu cubo não tenha nenhum lado totalmente completo, ou seja, quando os 4 **cubinhos de arestas** da última camada estiverem errados, mantenha o amarelo no topo e aplique uma das duas fórmulas em qualquer posição.

Depois volte ao início deste passo e procure por um lado que estará então totalmente completo.

2.1.2 Cubo de Rubik $2 \times 2 \times 2$

Este cubo $2 \times 2 \times 2$, vide Figura 2.23, é uma simplificação do Cubo de Rubik $3 \times 3 \times 3$, composto por 8 cubinhos , tendo um total de $3^8.8! = 264539520$ possibilidades, bem menos que o cubo tradicional, mas, mesmo assim difícil de ser resolvido.

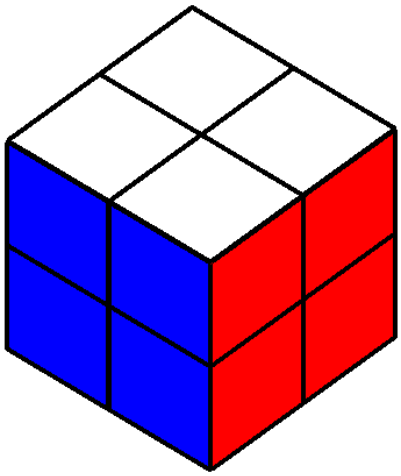


Figura 2.23: Cubo $2 \times 2 \times 2$

Diante de um cubo $2 \times 2 \times 2$, sem ter qualquer ideia do Cubo de Rubik, pensa-se em princípio ser fácil, logo depois, nota-se que não é de fato.

Sua formulação requer certa técnica e certo conhecimento do assunto. Note-se a particularidade de que com os cantos do $2 \times 2 \times 2$ pode ser dada

uma combinação que é impossibilitada no cubo $3 \times 3 \times 3$. Sendo assim, não há implicações em resolvê-lo, o cubo pode ser resolvido sem problemas, caso saiba solucionar o tradicional.

Estes 3 passos são para colocar as partes no lugar. Assim, os passos são os seguintes:

Passo 1: Como o cubo $2 \times 2 \times 2$ não possui centros e meios, devemos imaginar que uma cruz inicial na face branca já está resolvida. Sendo assim o próximo passo seria a solução das quinas brancas para finalizar a camada branca. Observe que qualquer cor poderia ser escolhida para a face. Aqui vamos sempre utilizar a face de cor branca.

Escolha um lado que esteja aparentemente mais fácil e inicie a solução, finalizando a camada com as 4 quinas brancas.

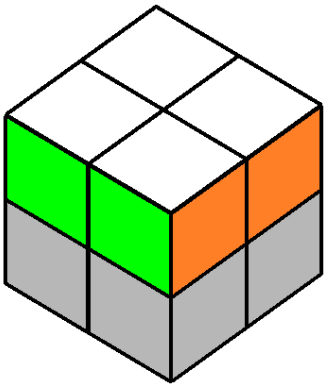


Figura 2.24: Passo 1

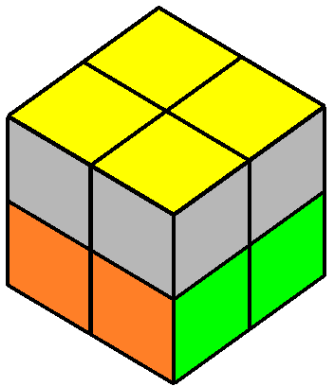


Figura 2.25: Passo 2

Passo 2: O objetivo do segundo passo é colocar todas as quinas amarelas no topo do cubo, conforme a Figura 2.25.

O único algoritmo que você deverá executar se chama **Sune:** $RUR'URU^2R'$. Basta posicionar seu cubo conforme a figura correspondente e aplicar os movimentos. Em certos casos terá que executar o algoritmo mais de uma vez.

Dica: As 7 figuras abaixo são as únicas opções que você deve encontrar em seu cubo. Caso você não encontre uma figura que esteja igual ao seu cubo, neste caso o cubo não está montado na forma correta e será um dos **casos impossíveis**.

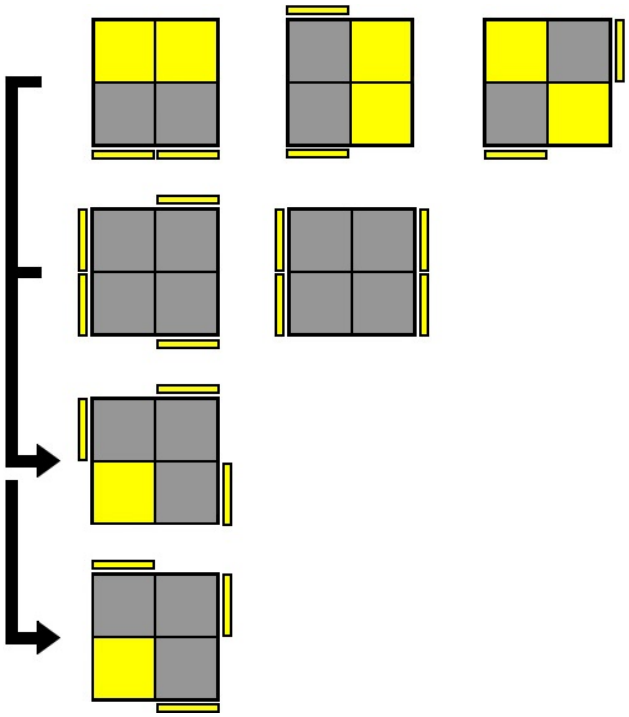


Figura 2.26: Únicos Casos Possíveis

As setas pretas representam a ordem que você deve seguir após realizar a fórmula.

Passo 3: O cubo pode estar de três formas diferentes, depois de aplicado o passo dois: Com nenhuma face lateral feita, uma face lateral concluída ou o cubo resolvido. Senão ocorrer nenhum desses casos, será a mesma situação do passo 2, **casos impossíveis**.

As setas apontam as peças que não estão no lugar:

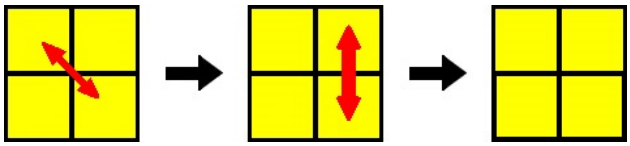


Figura 2.27: Último Passo

Basta posicionar seu cubo conforme a figura correspondente e aplicar o movimento: $RU^2R'U'RU^2R'FR'F'R$.

2.1.3 Cuboku

O Cuboku, dado na Figura 2.28, é o Cubo de Rubik em $3 \times 3 \times 3$ normal, exceto que tem todas as faces da mesma cor, mas com números. Isto é, um **Sudoku** de cada lado que é resolvido quando não há um número repetido em todos os lados.

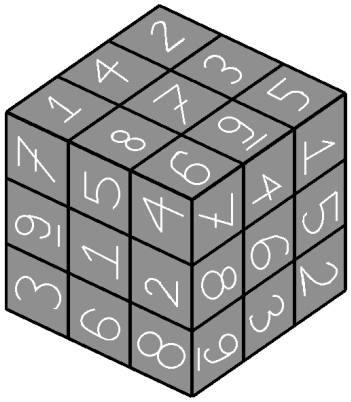


Figura 2.28: Cuboku

Construído de modo que há apenas uma solução possível. Aqui, os **cubinhos centrais** não indicam a cor da face correspondente, mas o número 5 em todos.

2.2 Fazer o Cubo de Rubik em um Grupo

Podemos fazer um conjunto de movimentos do cubo de Rubik que terá estrutura de grupo e que vamos denotar por $\mathbb{G}$. Dois movimentos serão considerados os mesmos se resultarem na mesma configuração do cubo.

Exemplo 33 *Uma torção na face no sentido horário em* $180°$ *é o mesmo que torcer a mesma face anti-horário em* $180°$.

A operação de grupo será definida: Se M_1 e M_2 são dois movimentos, então $M_1 * M_2$ é o movimento onde primeiro faz M_1, em seguida, faz M_2.

De fato. Afirmamos que $(\mathbb{G}, *)$ é um grupo.

i) Se deixarmos e ser o movimento vazio, isto é, um movimento que não altera a configuração do Cubo de Rubik, então $M * e$ significa primeiro faça M, e então não faça nada: Este é certamente o mesmo que fazer apenas o movimento M, então $M * e = M$. De modo análogo temos $e * M = M$, assim $M * e = e * M = M$. Então, $(\mathbb{G}, *)$ tem uma identidade.

ii) Se M é um movimento, podemos inverter os passos da mudança para começar um movimento $M^{'}$. Então, o movimento $M * M^{'}$, significa primeiro fazer M, e então inverter todos os passos de M. Este é o mesmo que fazer nada, assim $M * M^{'} = e$. De modo análogo temos $M^{'} * M = e$, então $M * M^{'} = M^{'} * M = e$. Portanto $M^{'}$ é o inverso de M. Logo, cada elemento de $\mathbb{G}$ tem uma inversa.

iii) Finalmente, devemos mostrar que $*$ é associativa. Recordar que um movimento pode ser definido pela mudança de configuração que provoca. Em particular, um movimento é determinado pela posição e orientação que coloca em cada cubinho.

Se C é um cubinho orientado, vamos escrever $M(C)$ para o compartimento orientado que acaba em C depois de aplicar o movimento M, com

$*$	e	R	R^2	R'	L	L^2	L'	F	F^2
e	e	R	R^2	R'	L	L^2	L'	F	F^2
R	R	R^2	R'	e	RL	RL^2	RL'	RF	RF^2
R^2	R^2	R'	e	R	R^2L	R^2L^2	R^2L'	R^2F	R^2F^2
R'	R'	e	R	R^2	$R'L$	$R'L^2$	$R'L'$	$R'F$	$R'F^2$
L	L	LR	LR^2	LR'	L^2	L'	e	LF	LF^2
L^2	L^2	L^2R	L^2R^2	L^2R'	L'	e	L	L^2F	L^2F^2
L'	L'	$L'R$	$L'R^2$	$L'R'$	e	L	L^2	$L'F$	$L'F^2$
F	F	FR	FR^2	FR'	FL	FL^2	FL'	F^2	F'
F^2	F^2	F^2R	F^2R^2	F^2R'	F^2L	F^2L^2	F^2L'	F'	e
F'	F'	$F'R$	$F'R^2$	$F'R'$	$F'L$	$F'L^2$	$F'L'$	e	F
B	B	BR	BR^2	BR'	BL	BL^2	BL'	BF	BF^2
B^2	B^2	B^2R	B^2R^2	B^2R'	B^2L	B^2L^2	B^2L'	B^2F	B^2F^2
B'	B'	$B'R$	$B'R^2$	$B'R'$	$B'L$	$B'L^2$	$B'L'$	$B'F$	$B'F^2$
U	U	UR	UR^2	UR'	UL	UL^2	UL'	UF	UF^2
U^2	U^2	U^2R	U^2R^2	U^2R'	U^2L	U^2L^2	U^2L'	U^2F	U^2F^2
U'	U'	$U'R$	$U'R^2$	$U'R'$	$U'L$	$U'L^2$	$U'L'$	$U'F$	$U'F^2$
D	D	DR	DR^2	DR'	DL	DL^2	DL'	DF	DF^2
D^2	D^2	D^2R	D^2R^2	D^2R'	D^2L	D^2L^2	D^2L'	D^2F	D^2F^2
D'	D'	$D'R$	$D'R^2$	$D'R'$	$D'L$	$D'L^2$	$D'L'$	$D'F$	$D'F^2$

Tabela 2.1

F'	B	B^2	B'	U	U^2	U'	D	D^2	D'
F'	B	B^2	B'	U	U^2	U'	D	D^2	D'
RF'	RB	RB^2	RB'	RU	RU^2	RU'	RD	RD^2	RD'
R^2F'	R^2B	R^2B^2	R^2B'	R^2U	R^2U^2	R^2U'	R^2D	R^2D^2	R^2D'
$R'F'$	$R'B$	$R'B^2$	$R'B'$	$R'U$	$R'U^2$	$R'U'$	$R'D$	$R'D^2$	$R'D'$
LF'	LB	LB^2	LB'	LU	LU^2	LU'	LD	LD^2	LD'
L^2F'	L^2B	L^2B^2	L^2B'	L^2U	L^2U^2	L^2U'	L^2D	L^2D^2	L^2D'
$L'F'$	$L'B$	$L'B^2$	$L'B'$	$L'U$	$L'U^2$	$L'U'$	$L'D$	$L'D^2$	$L'D'$
e	FB	FB^2	FB'	FU	FU^2	FU'	FD	FD^2	FD'
F	B	F^2B^2	F^2B'	F^2U	F^2U^2	F^2U'	F^2D	F^2D^2	F^2D'
F^2	B	B^2	B'	U	U^2	U'	D	D^2	D'
BF'	B^2	B'	e	BU	BU^2	BU'	BD	BD^2	BD'
B^2F'	B'	e	B	B^2U	B^2U^2	B^2U'	B^2D	B^2D^2	B^2D'
$B'F'$	e	B	B^2	$B'U$	$B'U^2$	$B'U'$	$B'D$	$B'D^2$	$B'D'$
UF'	UB	UB^2	UB'	U^2	U'	e	UD	UD^2	UD'
U^2F'	U^2B	U^2B^2	U^2B'	U'	e	U	U^2D	U^2D^2	U^2D'
$U'F'$	$U'B$	$U'B^2$	$U'B'$	e	U	U^2	$U'D$	$U'D^2$	$U'D'$
DF'	DB	DB^2	DB'	DU	DU^2	DU'	D^2	D'	e
D^2F'	D^2B	D^2B^2	D^2B'	D^2U	D^2U^2	D^2U'	D'	e	D
$D'F'$	$D'B$	$D'B^2$	$D'B'$	$D'U$	$D'U^2$	$D'U'$	e	D	D^2

Tabela 2.2

os rostos de $M(C)$ escritos na mesma ordem que os rostos de C. Ou seja, a primeira face de C deve acabar na primeira face de $M(C)$, e assim por diante.

Exemplo 34 *O movimento U coloca o ur cubinho no uf cubículo, com o rosto r do cubinho na face da frente do f cubículo e a face u do cubinho na face u do cubículo. Assim, escrevemos $U(ur) = uf$.*

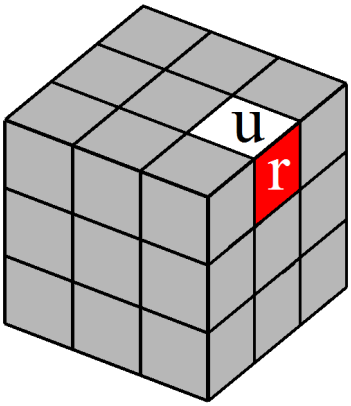


Figura 2.29: Cubo inicial

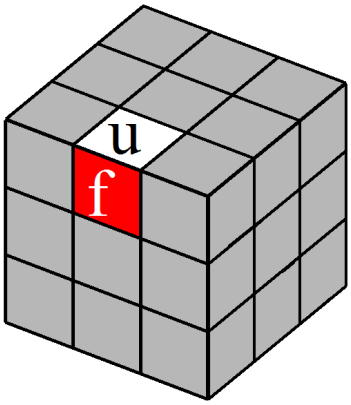


Figura 2.30: Após o movimento U

Primeiro, vamos investigar o que uma sequência de dois movimentos faz com o cubinho. Se M_1 e M_2 são dois movimentos, então $M_1 * M_2$ é o movimento em que primeiro faz M_1 e em seguida faz M_2. O movimento M_1 move C ao cubículo $M_1(C)$; o movimento M_2, em seguida, move-o para $M_2(M_1(C))$. Portanto, $(M_1 * M_2)(C) = M_2(M_1(C))$.

Para mostrar que $*$ é associativa, precisamos provar que $(M_1 * M_2) * M_3 = M_1 * (M_2 * M_3)$ para todos os movimentos M_1, M_2 e M_3. Isto é, o mesmo que mostrar $(M_1 * M_2) * M_3$ e $M_1 * (M_2 * M_3)$ fazem a mesma coisa a cada cubinho. Queremos mostrar que $[(M_1 * M_2) * M_3](C) = [M_1 * (M_2 * M_3)](C)$ para qualquer cubinho C. Sabemos do nosso cálculo acima, que $[(M_1 * M_2) * M_3](C) = M_3([M_1 * M_2](C)) = M_3(M_2(M_1(C)))$. Por outro

lado, $[M_1 * (M_2 * M_3)](C) = (M_2 * M_3)(M_1(C)) = M_3(M_2(M_1(C)))$. Assim, $(M_1 * M_2) * M_3 = M_1 * (M_2 * M_3)$. Logo, $*$ é associativa.

Portanto, $(\mathbb{G}, *)$ é um grupo.

A partir de agora, vamos apenas chamar este grupo $\mathbb{G}$, e escrever a operação como multiplicação. Por exemplo, DR significa o movimento D seguido pelo R. O movimento que torce a face da direita em 90° anti-horário é o mesmo que um movimento de torção no sentido horário na face da direita três vezes, para que possamos escrever este movimento como R^3.

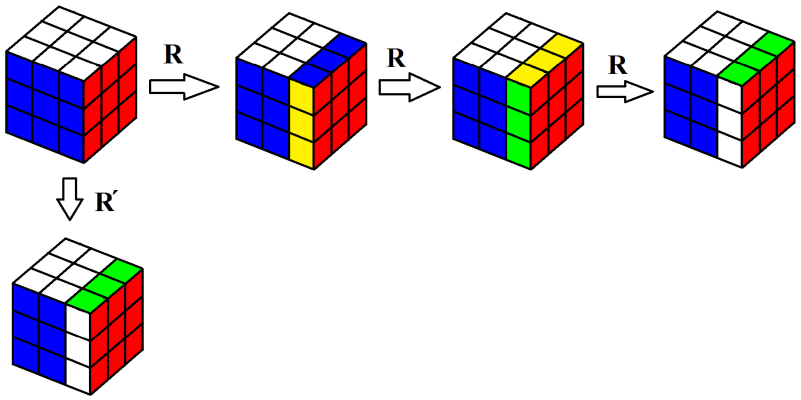


Figura 2.31: Movimentos Iguais

Calculamos que existem cerca de 519 quintilhões possíveis configurações do Cubo de Rubik (embora nem todas estas são válidas). Tentar entender um número tão grande de configurações não é tarefa fácil! Isto é útil para restringir o problema; por exemplo, em vez de olhar para todos os movimentos possíveis do Cubo de Rubik, podemos começar olhando para os movimentos que apenas envolvem torções de baixo e rostos certo.

2.2.1 Ciclo

Podemos escrever cada movimento do Cubo de Rubik usando uma notação ciclo ligeiramente modificada. Queremos descrever o que acontece com cada cubinho orientado; ou seja, queremos descrever como é o movimentos de cada cubinho e face dos cubinhos. Por exemplo, se desdobrar o cubo e desenhar a face para baixo, parece a Figura 2.32.

Se girarmos a face no sentido horário em 90° (isto é, aplicamos o movimento D), então a face para baixo, parece a Figura 2.33:

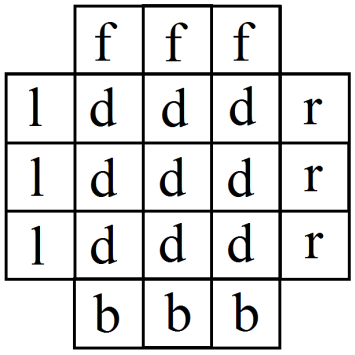


Figura 2.32: Face Inicial

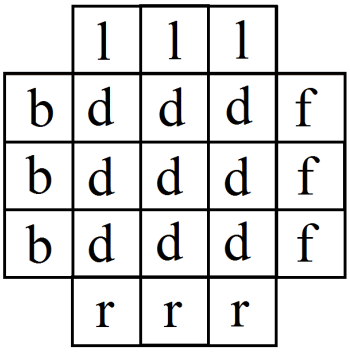


Figura 2.33: Movimento D

Assim, $D(dfr) = dlf$ pois o cubinho dlf agora está no cubículo dfr (com os cubinhos d da face nos cubículos d da face , os cubinhos l da face estão nos cubículos f, e os cubinhos f da face estão nos cubículos r). Da mesma forma, $D(drb) = dfr$, $D(dbl) = drb$ e $D(dlf) = dbl$. Se fizermos a mesma coisa para os cubinhos de arestas, encontramos $D = (dfr\ dlf\ dbl\ drb)(df\ dl\ db\ dr)$.

Exemplo 35 *Se $M \in \mathbb{G}$ é uma torção da face (de um D, U, L, R, F, B), então $\phi_{cubo}(M)$ é um produto de dois 4-ciclos. O 4-ciclo é impar, então o produto de dois 4-ciclos é par. Portanto, $\phi_{cubo}(M)$ é par. Uma vez que as voltas da cara geram todos $\mathbb{G}$, isto significa que $\phi_{cubo}(M)$ é par para todos*

$M \in \mathbb{G}$. Isto é, $\phi_{cubo}(M) \in A_{20}$ para todos $M \in \mathbb{G}$. Outra maneira de escrever este é dizer que $\phi_{cubo}(M) \in A_{20}$.

Agora, $\phi_{cubo}(M) = \phi_{canto}(M)\phi_{aresta}(M)$, então $\phi_{canto}(M)$ e $\phi_{aresta}(M)$ são ambos par ou ímpar. Ou seja, $\phi_{canto}(M)$ e $\phi_{aresta}(M)$ têm o mesmo sinal.

2.2.2 Configurações de Cubo de Rubik

A configuração do Cubo de Rubik é determinada por quatro partes:

• as posições dos cubinhos de cantos;

• as posições dos cubinhos de arestas;

• as orientações dos cubinhos de cantos;

• as orientações dos cubinhos de arestas;

O primeiro pode ser descrito por um elemento α de S_8 (isto é, o elemento de S_8 que move os cubinhos cantos, a partir de suas posições inicial para as novas posições). O segundo pode ser descrito por um elemento β de S_{12}. Agora, iremos definir a terceira e quarta. A ideia básica é a de fixar uma **orientação de partida** e uma forma sistemática de escrever como uma determinada orientação difere da orientação inicial.

Iniciaremos com os cubinhos de cantos que têm 3 possíveis orientações, e numeraremos com 0, 1 e 2. Imagine que o Cubo de Rubik está na configuração inicial e escreveremos um número sobre cada cubículo canto da face, como se segue:

1 na face u do cubículo ufl;

2 na face u do cubículo urf;

3 na face u do cubículo ubr;

4 na face u do cubículo ulb;

5 na face d do cubículo dbl;

6 na face d do cubículo dlf;

7 na face d do cubículo dfr;
8 na face d do cubículo drb;

Assim, cada cubículo canto tem exatamente uma face numerada. Nos cubinhos de cantos que têm uma face que encontram-se nos cubículos numerados, marque 0 na face do cubinho. No sentido horário, marquem 1 e 2 nas faces dos cubinhos. Conforme a Figura 2.35.

Exemplo 36 *Se olharmos diretamente para a face de baixo e desdobrar o Cubo, as faces dos cubinhos, parece com a Figura 2.32.*

Assim, as numerações dos cubículos que podemos ver, é como na Figura 2.34. E os cubinhos marcados parecem o da Figura 2.35.

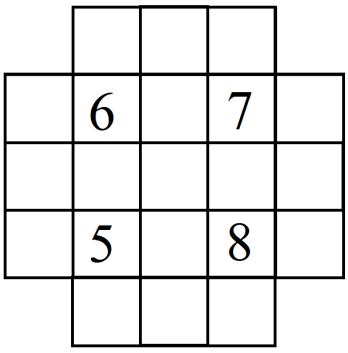


Figura 2.34: Números dos Cubinhos Canto

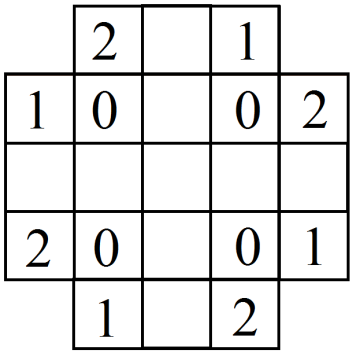


Figura 2.35: Ordem das Cores dos Cubinhos Canto

Agora, cada face do cubinho canto tem um número. Se o Cubo de Rubik estiver em qualquer configuração, descreveremos as orientações dos cubinhos de cantos como este: para qualquer i entre 1 e 8, encontrar a face do cubículo i marcado; x_i sera o número da face do cubinho vivendo neste rosto do cubículo. Escrevemos x para a ordem 8-upla $(x_1, ..., x_8)$. Observe que podemos pensar em cada x_i como contagem no sentido horário do número

que torce o cubinho i em relação ao rosto 0 na face numerada do cubículo. Observemos que ao fazer a torção sentido horário 3 vezes obtemos o cubinho na mesma orientação. Assim, devemos pensar no x_i como sendo elementos de $\mathbb{Z}/3\mathbb{Z}$. Então x é uma 8-upla de elementos de $\mathbb{Z}/3\mathbb{Z}$; escrevemos $x \in (\mathbb{Z}/3\mathbb{Z})^8$.

Exemplo 37 *Se o Cubo de Rubik esta na configuração inicial, cada* x_i *é* 0. *Também escrevemos* $x = 0$ *para cada* x_i *que é* 0.

Exemplo 38 *Aplicando* x_i *do movimento R para um cubo na configuração inicial. Dentre a configuração inicial, a face direita parece com a Figura 2.36:*

Os números do cubículo neste rosto, são os expressos na Figura 2.37.

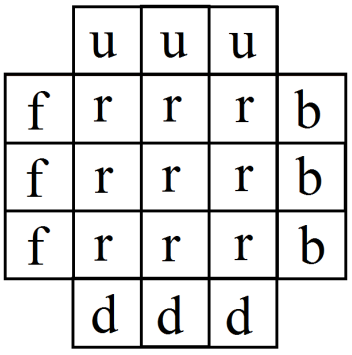


Figura 2.36: Face Inicial do Exemplo

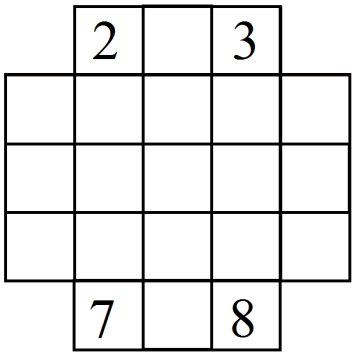


Figura 2.37: Números dos Cubinhos Canto

Portanto, a rotulagem dos cubinhos de cantos parecem com o da Figura 2.38:

Se girarmos a face direita do cubo em 90°, em seguida, os rostos dos cubinhos serão semelhantes o da Figura 2.39

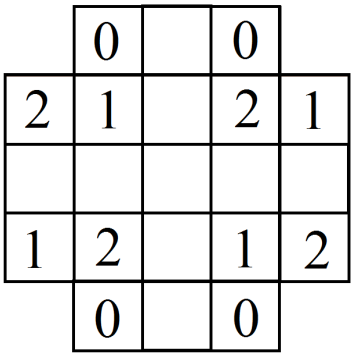


Figura 2.38: Ordem das Cores do Cubinho Canto

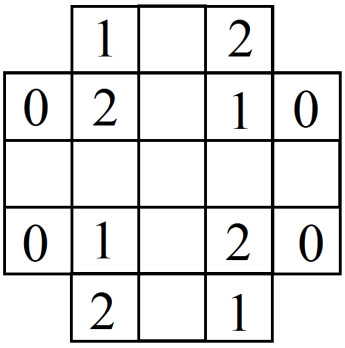


Figura 2.39: Aplicado 90° na face

Os cubinhos na face esquerda não são afetados por R, então $x_1 = 0$, $x_4 = 0$, $x_5 = 0$ e $x_6 = 0$. Agora, podemos ver dos seus diagramas que $x_2 = 1$, $x_3 = 2$, $x_7 = 2$ e $x_8 = 1$. Assim, $x = (0, 1, 2, 0, 0, 0, 2, 1)$.

Podemos fazer a mesma coisa para os cubinhos de arestas. Primeiro, rotulamos os cubículos de arestas como se segue. Escreva:

1 na face u do cubículo ub;

2 na face u do cubículo ur;

3 na face u do cubículo uf;

4 na face u do cubículo ul;

5 na face b do cubículo lb;

6 na face b do cubículo rb;

7 na face f do cubículo rf;

8 na face f do cubículo lf;

9 na face d do cubículo db;

10 na face d do cubículo dr;

11 na face d do cubículo df;

12 na face d do cubículo dl;

Cada cubinho aresta tem uma face que encontra-se em um cubículo aresta numerado; rotular este cubinho na face com 0, e rotular a outro face da cubinho 1. Em seguida, seja y_i o número da face do cubinho na face numerada do cubículo i. Isto define $y \in (\mathbb{Z}/2\mathbb{Z})^{12}$. Assim, qualquer configuração do Cubo de Rubik pode ser descrito por $\alpha \in S_8$, $\beta \in S_{12}$, $x \in (\mathbb{Z}/3\mathbb{Z})^8$ e $y \in (\mathbb{Z}/2\mathbb{Z})^{12}$. Então, vamos escrever configurações do Cubo de Rubik ordenados com 4-upla (α, β, x, y).

Exemplo 39 *A configuração inicial é (1, 1, 0, 0).*

Exemplo 40 *Suponha seu cubo na configuração inicial. Seja (α, β, x, y) a configuração do Cubo depois de fazer o movimento [D, R], que é definido como sendo $DRD^{-1}R^{-1}$.*

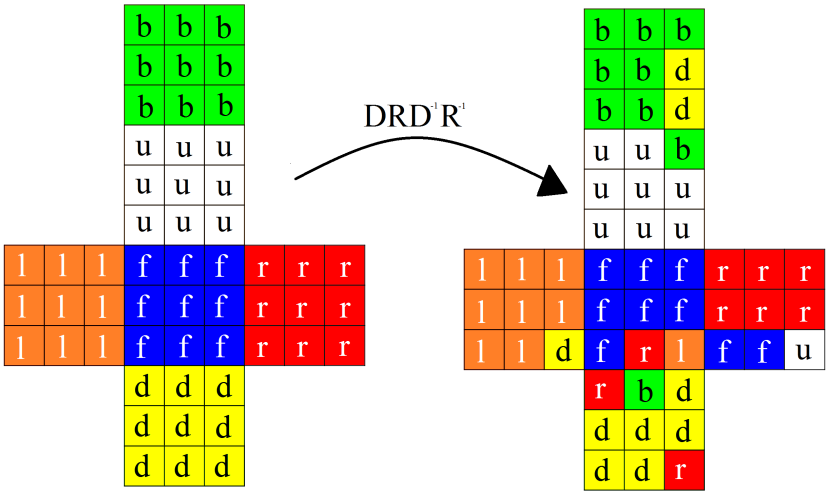


Figura 2.40: $DRD^{-1}R^{-1}$

Mostramos que $D = (dlf\ dfr\ drb\ dbl)(df\ dr\ db\ dl)$ e $R = (rfu\ ru\ rbd\ rdf)(ru\ rb\ rd\ rf)$. Portanto, $D^{-1} = (dbl\ drb\ dfr\ dlf)(dl\ db\ dr\ df)$ e $R^{-1} = (rdf\ rbd\ rub\ rfu)(rf\ rd\ rb\ ru)$. Assim,

$[D, R] = (dlf\ dfr\ lfd\ frd\ fdl\ rdf)(drb\ bru\ bdr\ ubr\ rbd\ rub)(df\ dr\ br)$

Lembre-se disso, β é um elemento de S_{12}; pensamos nele como uma bijeção do conjunto de 12 cubinhos arestas não orientados para o conjunto de 12 cubículos de arestas. E é definido: se C é um cubinho aresta não orientado no início da configuração, então $\beta(C)$ é o cubículo aresta não orientado onde C vive na configuração atual. Como qualquer elemento de S_{12}, β podem ser escritos em notação ciclo disjunta.

Neste exemplo em particular, [D, R] move o cubinho df ao cubículo dr, cubinho dr para cubículo br, e cubinho br para cubículo df. Portanto, $\beta = (df\ dr\ br)$.

Da mesma forma, α é uma bijeção do conjunto de 8 cubinhos de cantos não orientados para o conjunto de 8 cubículos de arestas não orientados. Para encontrar α, temos de descobrir o que [D, R] faz para as posições dos cubinhos de cantos. Observe que [D, R] liga as posições dos cubinhos dfl e dfr, e também liga as posições de drb e bru. Portanto, $\alpha = (drb\ bru)(dfl\ dfr)$.

Recorde-se que definimos x como se segue. Quando o cubo estava na configuração inicial, numeramos 8 cubículos cantos como este:
1 na face u do cubículo ufl;
2 na face u do cubículo urf;
3 na face u do cubículo ubr;
4 na face u do cubículo ulb;
5 na face d do cubículo dbl;
6 na face d do cubículo dlf;
7 na face d do cubículo dfr;
8 na face d do cubículo drb;

Numeramos cada um dos cubinhos cantos correspondentes com 0. A partir disso, no sentido horário rotulamos as outras duas faces 1 e 2. Por

exemplo, o rosto u do cubinho ufl é rotulado 0, de modo que o rosto f é 1 e l é 2. Agora que o cubo não está na configuração de início, definimos x_i o número do cubinho de canto no cubículo de canto i.

Na posição inicial, todas as faces do cubículo numeradas têm cubinhos de cantos com números 0. Uma vez que o movimento $[D, R]$ não afeta os cubinhos ufl, urf, ulb, ou dbl, x_1, x_2, x_4, x_5 devem ser 0. Para encontrar x_3, queremos ver qual cubinho está na cara u do cubículo ubr. Temos que $[D, R]$ coloca b na face do cubinho drb e pelo nosso esquema de numeração, o b na face do cubinho drb é numerado por 2; portanto, $x_3 = 2$. Do mesmo modo, $x_6 = 2, x_7 = 0$ e $x_8 = 2$. Assim, a 8-upla é x é (0, 0, 2, 0, 0, 2, 0, 2).

Da mesma forma, para definir y, primeiro numeramos 12 faces dos cubículos borda, quando o cubo estiver na configuração inicial:

1 na face u do cubículo ub;

2 na face u do cubículo ur;

3 na face u do cubículo uf;

4 na face u do cubículo ul;

5 na face b do cubículo lb;

6 na face b do cubículo rb;

7 na face f do cubículo rf;

8 na face f do cubículo lf;

9 na face d do cubículo db;

10 na face d do cubículo dr;

11 na face d do cubículo df;

12 na face d do cubículo dl;

Em seguida, a face do cubinho aresta correspondente rotulamos com 0 e o outro 1. Finalmente, foi definido para y ser o 12-upla $(y_1, ., ., .y_{12})$ onde y_i é o número na borda cubículo rosto i.

Como $[D, R]$ afeta apenas os df, dr e br cubinhos de arestas, sabemos imediatamente que y_{10}, y_{11} e y_6 são o único y_i que pode ser diferente de zero. Como [D, R] coloca a face b do cubículo br na face d do cubículo df, $y_{11} = 0$. Da mesma forma, y_{10} e y_6 são ambos 0. Assim, $y = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.

Suponha que seu cubo está na configuração de início e você faz o movimento M nele. Em seguida, ele acaba em uma configuração (α, β, x, y) onde $\alpha = \phi_{canto}(M)$ e $\beta = \phi_{aresta}(M)$. Portanto, provamos que, se (α, β, x, y) é uma configuração, então α e β têm o mesmo sinal.

2.3 Ações do Grupo

Se o Cubo de Rubik é alguma configuração $C = (\alpha, \beta, x, y)$, fazendo em seguida um movimento $M \in \mathbb{G}$ colocamos em alguma nova configuração. Vamos escrever esta nova configuração como $C.M$.

Suponha que o Cubo de Rubik começa na configuração C. Se fizermos o movimento M_1, a configuração do cubo torna-se $C.M_1$. Se, então fazermos um outro movimento M_2, a configuração torna-se $(C.M_1).M_2$. Por outro lado, o que temos realmente feito é iniciado com a configuração C e aplicar o movimento M_1M_2, então uma outra maneira para escrever a nova configuração é $C.(M_1M_2)$. Ou seja, acabamos de mostrar que $(C.M_1).M_2 = C.(M_1M_2)$ para todas as configurações C e todos os movimentos $M_1, M_2 \in \mathbb{G}$.

Se fizermos o movimento vazio (o elemento identidade e de $\mathbb{G}$), a configuração não muda em nada, assim $C.e = C$.

Este é um exemplo de um objeto matemático chamado uma **ação do grupo**.

Para dar uma definição formal, primeiro precisamos de algumas notações. Se S_1 e S_2 são dois conjuntos, então $S_1 \times S_2$ é o conjunto de pares ordenados

(s_1, s_2), com $s_1 \in S_1$ e $s_2 \in S_2$.

Definição 16 *A **(direita) ação do grupo** de um grupo $(G, *)$ em um conjunto A, não vazio, é uma função $A \times G \longrightarrow A$ (Isto é, dados $a \in A$ e $g \in G$, podemos produzir um outro elemento de A, que se escreve $a.g$) satisfazendo as propriedades:*

1. $(a.g_1).g_2 = a.(g_1 * g_2)$ para todos $g_1, g_2 \in G$ e $a \in A$.

2. $a.e = a$ de $a \in A$ (aqui, e é o elemento de identidade de G).

Esta é uma ação direita, em vez de uma ação esquerda pois colocamos os elementos do grupo à direita.

Na primeira condição, $a.g_1 \in A$, então $(a.g_1).g_2$ faz sentido. Por outro lado, $g_1 * g_2 \in G$, de modo $a.(g_1 * g_2)$ também faz sentido.

*Quando temos uma ação do grupo de G em um conjunto A, apenas dizemos que **G age sobre A** .*

Exemplo 41 *O grupo $\mathbb{G}$ age sobre o conjunto de configurações (α, β, x, y) do Cubo de Rubik (permitindo configurações válidas e inválidas).*

Exemplo 42 *S_n atua sobre o conjunto $\{1, ..., n\}$. A ação do grupo é definido da seguinte forma: dada $i \in \{1, ..., n\}$ e $\alpha \in S_n$, deixe $i.\alpha = \alpha(i)$. Para verificar se esta é realmente uma ação do grupo, observar que $i(\alpha\beta) = (\alpha\beta)(i) = \beta(\alpha(i)) = \beta(i.\alpha) = (i.\alpha).\beta$ e $i.1 = 1(i) = i$.*

Exemplo 43 *S_n atua sobre o conjunto de polinômios nas variáveis $x_1, ..., x_n$; na verdade, usamos esta ação para provar a existência do sinal do homomorfismo. Ou seja, se $p(x_1, ..., x_n)$ é um polinômio, definimos um novo polinômio p^α por $p^\alpha(x_1, ..., x_n) = p(x_{\alpha(1)}, ..., x_{\alpha(n)})$. Provamos que $(p^\alpha)^\beta = p^{\alpha\beta}$, e é claro que $p^1 = p$. Assim, se definirmos $p.\alpha = p^\alpha$, temos uma ação do grupo.*

Exemplo 44 *O grupo* $(\mathbb{Z}, +)$ *age sobre o conjunto* $\mathbb{R}$ *com* $a.g = g + a$ *para* $g \in \mathbb{Z}$ *e* $a \in \mathbb{R}$. *Afinal,*

$$\begin{aligned}(a.g_1).g_2 &= (a.g_1) + g_2 \\ &= (a + g_1) + g_2 \\ &= a + (g_1 + g_2) \\ &= a.(g_1 + g_2)\end{aligned}$$

para todos $g_1, g_2 \in \mathbb{Z}$ *e* $a \in \mathbb{R}$. *Além disso,* $a.0 = 0 + a = 0$ *para todos* $a \in \mathbb{R}$.

Exemplo 45 *Muitas vezes, estamos interessados no caso em que o conjunto* A *é o próprio grupo. Neste caso, dizemos o grupo que atua sobre si. Por exemplo, podemos definir uma ação do grupo da seguinte forma: para* $g \in G$ *e* $a \in G$, *definir* $a.g = ag$, *o grupo normal da multiplicação* a *e* g. *Chamaremos esta ação de* G *a si própria pela multiplicação direita.*

Definição 17 *Se* G *age em um conjunto* A, *em seguida, a órbita de* $a \in A$ *(no âmbito desta ação) é o conjunto* $\{a.g : g \in G\}$.

Exemplo 46 $\mathbb{G}$ *age sobre o conjunto de configurações do Cubo de Rubik. A órbita da configuração do início no âmbito desta ação é exatamente o conjunto de configurações válidas do Cubo de Rubik.*

Exemplo 47 *Usando um dos exemplos anteriores, o grupo* $(\mathbb{Z}, +)$ *age sobre o conjunto* $\mathbb{R}$ *com* $a.g = g + a$ *para* $g \in \mathbb{Z}$ *e* $a \in \mathbb{R}$. *Assim, a órbita de* a *é o conjunto* $\{a+g : g \in \mathbb{Z}\}$, *ou o conjunto,* $\{..., a-2, a-1, a, a+1, a+2, ...\}$. *Em particular,* $a, a+1, a-1, ...$ *têm todos a mesma órbita. Há uma órbita distinta para cada* $a \in [0, 1)$. *Portanto, podemos pensar no conjunto de órbitas como o intervalo* $[0, 1)$. *No entanto, uma vez que a órbita de* 0 *é o mesmo que a órbita de* 1, *também poderíamos pensar no conjunto de órbitas como* $[0, 1]$ *com* 0 *e* 1 *visto como o mesmo ponto.*

Definição 18 *Se uma ação do grupo tem apenas uma órbita, dizemos que a ação é transitiva (ou que o grupo atua transitivamente).*

Exemplo 48 $\mathbb{G}$ *age sobre o conjunto de pares ordenados* (C_1, C_2) *de diferentes cubinhos de cantos não orientados. Se* C_1 *e* C_2 *são dois cubinhos de cantos não orientados diferentes, aplicando um movimento* $M \in \mathbb{G}$ *envia estes cubinhos de cantos a dois cubículos de cantos diferentes* C_1' *e* C_2' *.Então, podemos definir a ação do grupo por* $(C_1, C_2).M = (C_1', C_1')$.

Da mesma forma, $\mathbb{G}$ *atua sobre o conjunto de triplos ordenadas* (C_1, C_2, C_3) *dos diferentes cubinhos cantos não orientados.*

Muitas vezes queremos provar algo sobre todos os elementos de uma órbita, por exemplo, podemos querer provar um afirmação sobre todas as configurações válidas do Cubo de Rubik. O seguinte lema pode ser útil nestas situações.

Lema 10 *Suponha que um grupo finito* G *age em um conjunto* A*, sejam* S *um conjunto de geradores de* G*, e* P *uma propriedade de tal forma que o seguinte é verdadeiro:*

Sempre que $a \in A$ *satisfaz* P *e* $s \in S$*,* $a.s$ *também satisfaz* P*. Então, se* $a_0 \in A$ *satisfaz* P*, cada elemento da órbita de* a_0 *também satisfaz* P*.*

Demonstração: Vamos definir uma nova propriedade Q da seguinte forma, digamos que $g \in G$ satisfaz propriedade Q quando o seguinte é verdadeiro.

Sempre que $a \in A$ satisfaz P, $a.g$ também satisfaz P. Basta mostrar que para cada $g \in G$ satisfaz propriedade Q. Afinal, isso significaria que, se $a_0 \in A$ satisfaz P, então $a_0.g$ satisfaz P para todos os $g \in G$, que é exatamente o que queremos mostrar.

Por hipótese, cada elemento de S satisfaz a propriedade Q. Pela Proposição 2, precisamos mostrar que, se $g, h \in G$, satisfazem a propriedade Q, então gh satisfaz a propriedade P. Então, supõem $g, h \in G$, satisfazendo a propriedade Q. Para mostrar que gh também satisfaz a propriedade Q, queremos mostrar que, se $a \in A$ satisfaz P, em seguida, $a.gh$ também satisfaz P.

Suponha que $a \in A$ satisfaz P. Como g satisfaz a propriedade Q, $a.g$ satisfaz a propriedade P. Desde h satisfaz a propriedade Q, $(a.g).h$ satisfaz a propriedade P. No entanto, a definição de uma ação do grupo, $(a.g).h = a.gh$. Então, provaremos que, se $a \in A$ satisfaz P, em seguida, $a.gh$ satisfaz P. Isso significa que gh satisfaz propriedade Q, que termina a nossa prova. ■

No caso do Cubo de Rubik, aplica-se o Lema 10 para a ação do grupo $\mathbb{G}$ no conjunto A de configurações. Em particular, se deixarmos $S = \{$D, U, L, R, F, B$\}$ e a_0 ser a configuração inicial, então podemos usar o Lema para provar todas as configurações válidas do Cubo de Rubik.

2.4 Configurações válidas de Cubo de Rubik

Agora, vamos colocar tudo que aprendemos junto para dar uma caracterização das configurações válidas do Cubo de Rubik.

Teorema 4 *Uma configuração (α, β, x, y) é válida se $sgn\ \alpha = sgn\ \beta$, $\Sigma x_i \equiv 0\ (mod\ 3)$ e $\Sigma y_i \equiv 0\ (mod\ 2)$*

O restante desta seção será dedicado a provar este teorema. Em primeiro lugar, vamos mostrar que, se (α, β, x, y) é válido, então $sgn\ \alpha = sgn\ \beta$, $\Sigma x_i \equiv 0\ (mod\ 3)$ e $\Sigma y_i \equiv 0\ (mod\ 2)$.

Lembre-se que $\mathbb{G}$ age sobre o conjunto de configurações do Cubo de Rubik. As configurações válidas formam uma única órbita desta ação. Assim, fazem sentido as declarações que fazemos sobre configurações válidas poderem ser generalizados para outras órbitas.

Lema 11 *Se* (α, β, x, y) *e* $(\alpha', \beta', x', y')$ *estão na mesma órbita, então* $(sgn\ \alpha)(sgn\ \beta) = (sgn\ \alpha')(sgn\ \beta')$.

Demonstração: Pelo Lema 10, é suficiente mostrar que, se $(\alpha, \beta, x, y) = (\alpha', \beta', x', y').M$ em que M é um dos 6 movimentos básicos, então $(sgn\ \alpha)(sgn\ \beta) = (sgn\ \alpha')(sgn\ \beta')$. Assim, $\alpha' = \alpha\phi_{canto}(M)$ e $\beta' = \beta\phi_{aresta}(M)$. Portanto, $(sgn\ \alpha')(sgn\ \beta') = (sgn\ \alpha)(sgn\ \phi_{canto}(M))(sgn\ \beta)(sgn\ \phi_{aresta}(M))$. Se M for um dos 6 movimentos básicos, então $\phi_{canto}(M)$ e $\phi_{aresta}(M)$ são ambos 4-ciclos, de modo que ambos têm sinal -1. Assim, $(sgn\ \alpha)(sgn\ \beta) = (sgn\ \alpha')(sgn\ \beta')$. ■

Corolário 1 *Se* (α, β, x, y) *é uma configuração válida, então* $sgn\ \alpha = sgn\ \beta$.

Demonstração: Esta é uma consequência direta do Lema 11 tal que qualquer configuração válida está na órbita da configuração de início (1, 1, 0, 0). ■

Lema 12 *Se* $(\alpha', \beta', x', y')$ *está na mesma órbita que* (α, β, x, y)*, então* $\Sigma x_i' \equiv \Sigma x_i\ (mod\ 3)$ *e* $\Sigma y_i' \equiv \Sigma y_i\ (mod\ 2)$.

Demonstração: Pelo Lema 10, é suficiente mostrar que, se $(\alpha', \beta', x', y')$ $= (\alpha, \beta, x, y).M$ em que M é um dos 6 movimentos básicos, em seguida, $\Sigma x_i' \equiv \Sigma x_i\ (mod\ 3)$ e $\Sigma y_i' \equiv \Sigma y_i\ (mod\ 2)$. Na Tabela 2.3 mostra o que x' e y' são se $(\alpha', \beta', x', y') = (\alpha, \beta, x, y).M$ e M é um dos 6 movimentos básicos.

M	$x^{'}$ e $y^{'}$
D	$(x_1, x_2, x_3, x_4, x_8, x_5, x_6, x_7)$
	$(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_{10}, y_{11}, y_{12}, y_9)$
U	$(x_2, x_3, x_4, x_1, x_5, x_6, x_7, x_8)$
	$(y_4, y_1, y_2, y_3, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12})$
R	$(x_1, x_7 + 1, x_2 + 2, x_4, x_5, x_6, x_8 + 2, x_3 + 1)$
	$(y_1, y_7, y_3, y_4, y_5, y_2, y_{10}, y_8, y_9, y_6, y_{11}, y_{12})$
L	$(x_4 + 2, x_2, x_3, x_5 + 1, x_6 + 2, x_1 + 1, x_7, x_8)$
	$(y_1, y_2, y_3, y_5, y_{12}, y_6, y_7, y_4, y_9, y_{10}, y_{11}, y_8)$
F	$(x_6 + 1, x_1 + 2, x_3, x_4, x_5, x_7 + 2, x_2 + 1, x_8)$
	$(y_1, y_2, y_8 + 1, y_4, y_5, y_6, y_3 + 1, y_{11} + 1, y_9, y_{10}, y_7 + 1, y_{12})$
B	$(x_1, x_2, x_8 + 1, x_3 + 2, x_4 + 1, x_6, x_7, x_5 + 2)$
	$(y_6 + 1, y_2, y_3, y_4, y_1 + 1, y_9 + 1, y_7, y_8, y_5 + 1, y_{10}, y_{11}, y_{12})$

Tabela 2.3

Em cada caso, é fácil verificar que $\Sigma x_i^{'} \equiv \Sigma x_i \ (mod\ 3)$ e $\Sigma y_i^{'} \equiv \Sigma y_i \ (mod\ 2)$.

■

Como exemplo, encontraremos $x^{'}$ quando M é o movimento R. Os cubículos da face direita parece com o da Figura 2.41:

Os cubículos são rotulados como está na Figura 2.42.

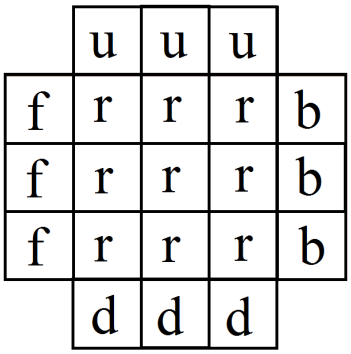


Figura 2.41: Face Direita do Cubo Inicial

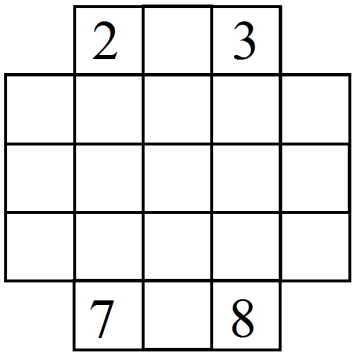


Figura 2.42: Número dos Cubinhos Canto

Portanto, se o Cubo de Rubik está na configuração (α, β, x, y), os cubinhos da face direita são rotulados:

	x_2		x_3	
x_2+2	x_2+1		x_3+2	x_3+1
x_7+1	x_7+2		x_8+1	x_8+2
	x_7		x_8	

Figura 2.43: Rotulagem

Se rodarmos esta face em 90° no sentido horário, em seguida, os cubinhos irão parecer:

	x_7+1		x_2+2	
x_7	x_7+2		x_2+1	x_2
x_8	x_8+1		x_3+2	x_3
	x_8+2		x_3+1	

Figura 2.44: Movido 90°

Assim, $x^{'} = (x_1, x_7 + 1, x_2 + 2, x_4, x_5, x_6, x_8 + 2, x_3 + 1)$. Então $\Sigma x_i^{'} \equiv \Sigma x_i + 6 \equiv \Sigma x_i \ (mod\ 3)$.

Corolário 2 *Se (α, β, x, y) é uma configuração válida, então $\Sigma x_i \equiv 0$ (mod 3) e $\Sigma y_i \equiv 0$ (mod 2).*

Demonstração: Esta é uma consequência direta do Lema 12, pois qualquer configuração válida está na órbita do início da configuração (1, 1, 0, 0). ■

Assim, provamos a ida do Teorema 4. Agora, provaremos a volta. Supondo $sgn\ \alpha = sgn\ \beta$, $\Sigma x_i \equiv 0\ (mod\ 3)$ e $\Sigma y_i \equiv 0\ (mod\ 2)$. Queremos mostrar que há uma série de movimentos que, quando aplicado a (α, β, x, y), tem-se a configuração inicial; isto é, se o Cubo de Rubik está na configuração (α, β, x, y), isto pode ser resolvido. A ideia da prova é basicamente para anotar os passos necessários para resolver o Cubo de Rubik.

Assim, provaremos estes quatro fatos:

1. Se (α, β, x, y) é uma configuração tal que $sgn\ \alpha = sgn\ \beta$, $\Sigma x_i \equiv 0\ (mod\ 3)$ e $\Sigma y_i \equiv 0\ (mod\ 2)$, em seguida há um movimento $M \in \mathbb{G}$ de tal modo que $(\alpha, \beta, x, y).M$ tem a forma $(1, \beta^{'}, x^{'}, y^{'})$ com $sgn\ \alpha^{'} = 1$, $\Sigma x_i \equiv 0\ (mod\ 3)$, e $\Sigma y_i \equiv 0\ (mod\ 2)$. Ou seja, podemos colocar todos os cubinhos de cantos nas posições certas.

2. Se $(1, \beta, x, y)$ é uma configuração com $sgn\ \beta = 1$, $\Sigma x_i \equiv 0\ (mod\ 3)$ e $\Sigma y_i \equiv 0\ (mod\ 2)$, então existe um movimento de $M \in \mathbb{G}$ de tal modo que $(1, \beta, x, y).M$ tem a forma $(1, \beta^{'}, 0, y^{'})$ com $\beta^{'} = 1$ e $\Sigma y_i \equiv 0\ (mod\ 2)$. Ou seja, podemos colocar todos os cubinhos de cantos nas orientações corretas (e posições).

3. Se $(1, \beta, 0, y)$ é uma configuração com $sgn\ \beta = 1$ e $\Sigma y_i \equiv 0\ (mod\ 2)$, então há um movimento $H \in \mathbb{G}$ tal que $(\alpha, \beta, x, y).M$ tem a forma $(1, 1, 0, y^{'})$

com $\Sigma y_i \equiv 0 \ (mod\ 2)$. Ou seja, podemos colocar toda os cubinhos arestas nas posições corretas (sem perturbar os cubinhos esquina).

4. Se $(1, 1, 0, y)$ é uma configuração com $\Sigma y_i \equiv 0 \ (mod\ 2)$, então há um movimento $M \in \mathbb{G}$ tal que $(1, 1, 0, y).M = (1, 1, 0, 0)$. Ou seja, podemos resolver o cubo!

Antes de provar, destacaremos um fato útil. Suponha que (α, β, x, y) satisfaz $sgn\ \alpha = sgn\ \beta$, $\Sigma x_i \equiv 0 \ (mod\ 3)$ e $\Sigma y_i \equiv 0 \ (mod\ 2)$. Então o Lema 11 e 12 mostram que, para qualquer $(\alpha', \beta', x', y')$ na mesma órbita que (α, β, x, y), $sgn\ \alpha' = sgn\ \beta'$, $\Sigma x_i \equiv 0 \ (mod\ 3)$ e $\Sigma y_i \equiv 0 \ (mod\ 2)$. Assim, por exemplo, na primeira afirmação acima, se pudermos provar que há um movimento $M \in \mathbb{G}$ tal que $(\alpha, \beta, x, y).M$ tem a forma $(1, \beta', x', y')$, é automático que $sgn\ \beta' = 1$, $\Sigma x_i \equiv 0 \ (mod\ 3)$ e $\Sigma y_i \equiv 0 \ (mod\ 2)$. Portanto, para terminar a prova do Teorema 4, basta que se prove as seguintes quatro proposições.

Proposição 4 *Se (α, β, x, y) é uma configuração tal que $sgn\ \alpha = sgn\ \beta$, $\Sigma x_i \equiv 0$ (mod 3) e $\Sigma y_i \equiv 0$ (mod 2), em seguida, a órbita de (α, β, x, y) contém uma configuração de forma a $(1, \beta', x', y')$.*

Proposição 5 *Se $(1, \beta, x, y)$ é uma configuração com $sgn\ \beta = 1$, $\Sigma x_i \equiv 0$ (mod 3) e $\Sigma y_i \equiv 0$ (mod 2), em seguida, a órbita de $(1, \beta, x, y)$ contém uma configuração de forma a $(1, \beta', 0, y')$.*

Proposição 6 *Se $(1, \beta, 0, y)$ é uma configuração com $sgn\ \beta = 1$ e $\Sigma y_i \equiv 0$ (mod 2), em seguida, a órbita de $(1, \beta, 0, y)$ contém uma configuração de forma a $(1, 1, 0, y)$.*

Proposição 7 *Se $(1, \beta, 0, y)$ é uma configuração com $\Sigma y_i \equiv 0$ (mod 2), em seguida, a órbita de $(1, 1, 0, y)$ contém a configuração inicial $(1, 1, 0, 0)$.*

Provaremos em ordem cada proposição. Então, em primeiro lugar queremos mostrar que podemos colocar todos os cubinhos de cantos nas posições da direita.

Lema 13 *O homomorfismo* $\phi_{canto} : \mathbb{G} \longrightarrow S_8$ *é sobrejetor.*

Demonstração: S_8 é gerado pelo conjunto S de 2-ciclos em S_8. É suficiente para mostrar que $S \subset$ Im ϕ_{canto}. Afinal, se $S \subset$ Im ϕ_{canto}, então $S_8 = \langle S \rangle \subset$ Im ϕ_{canto} . Pois Im ϕ_{canto} é um grupo, assim $\langle$Im $\phi_{canto}\rangle =$ Im ϕ_{canto}.

Então, queremos mostrar que cada 2-ciclo no S_8 está na imagem do ϕ_{canto}. Em, que deveria ter encontrado um movimento que muda apenas 2 cubinhos de cantos e deixa os outros cubinhos de cantos fixo. Um tal movimento é $M_0 = ([D, R]F)^3$, que tem decomposição ciclo disjuntos $(dbr\ urb)$ $(dr\ uf)$ $(rf\ br)$ $(lf\ df)$. Então, $\phi_{canto}(M_0) = (dbr\ urb)$. Assim, pelo menos sabemos que $(dbr\ urb)$ encontra-se na imagem do ϕ_{canto}.

Sejam C_1 e C_2 qualquer par de cubinhos de cantos. Existe um movimento de $M \in \mathbb{G}$ que envia dbr para C_1 e urb a C_2. Seja $\alpha = \phi_{canto}(M)$. Então, $\alpha(dbr) = C_1$ e $\alpha(urb) = C_2$. Como ϕ_{canto} é um homomorfismo,

$$\phi_{canto}(M^{-1}M_0M) = \phi_{canto}(M)^{-1}\phi_{canto}(M_0)\phi_{canto}(M)$$

$$= \alpha^{-1}(dbrurb)\alpha$$

$$= (\alpha(dbr)\alpha(urb))$$

$$= (C_1C_2)$$

Portanto, $(C_1C_2) \in$ Im ϕ_{canto}, que termina a prova. ■

Demonstração da Proposição 4: Pelo Lema 13, existe um movimento $M \in \mathbb{G}$ tal que $\phi_{canto}(M) = \alpha^{-1}$. De, $(\alpha, \beta, x, y).M = (1, \beta', x', y')$ para algum $\beta' \in S_{12}$, $x' \in (\mathbb{Z}/3\mathbb{Z})^8$, $y' \in (\mathbb{Z}/2\mathbb{Z})^{12}$. ■

Em seguida, provaremos a Proposição 5. A ideia base para orientar todos os cubinhos de cantos corretamente é usar os movimentos que mudam as orientações de apenas 2 cubinhos. Primeiro, temos de mostrar que existem tais movimentos.

Lema 14 *Se C_1 e C_2 são quaisquer dois cubinhos de cantos, existe um movimento de $M \in \mathbb{G}$ que altera a orientações (mas não posições) de C_1 e C_2 e que não afeta os outros cubinhos de cantos em tudo. Além disso, existe tal movimento M que gira no sentido horário C_1 e gira no sentido anti-horário C_2.*

Demonstração: Como na prova do Lema 13, a questão é primeiro encontrar um único M_0 movimento que altera as orientações de 2 cubinhos e depois conjugar M_0 para encontrar outros movimentos que mudam as orientações de 2 cubinhos. Você pode ter encontrado um tal movimento; uma possibilidade é $M_0 = (DR^{-1})^3(D^{-1}R)^3$, que possui decomposição ciclo disjuntos (dfr rdf frd) (drb rbd bdr) (df dr fr ur br dl db). Então,$\phi_{canto}(M_0) = 1$ e $\psi_{canto}(M_0)$ =(dbr brd rdb) (drf rfd fdr). Então, se $C_1 = dbr$ e $C_2 = drf$, a afirmação é verdadeira.

Agora, vamos conjugar este movimento. Existe $M \in \mathbb{G}$ que envia dbr para C_1 e drf para C_2. Temos $M' = M^{-1}M_0M$. Ao aplicar, $\psi_{canto}(M')$, temos que M' muda as orientações de C_1 e C_2 e não afeta os outros cubinhos de cantos. Especificamente, M' gira no sentido horário C_1 e gira anti-horário C_2. ■

Demonstração da Proposição 5: Suponhamos que o Cubo de Rubik é uma configuração onde pelo menos dois cubinhos cantos C_1 e C_2 têm a orientação errada. Pelo Lema 14, há um movimento que gira no sentido horário C_1, gira anti-horário C_2, e não afeta os outros cubinhos de cantos. Ao aplicar este movimento uma ou duas vezes, podemos garantir que C_1 tem a orientação correta. Uma vez que este movimento não afeta nenhum cubinhos de cantos além de C_1 e C_2, o Cubo de Rubik agora tem um a menos cubinho de canto com uma orientação incorreta. Fazendo isso várias vezes, acabamos com uma configuração $(1, \beta', 0, y')$, onde há no máximo um cubinho de canto com a orientação incorreta. Isto é, pelo menos sete dos x_i' são 0. Pelo Lema 12, $\Sigma x_i' \equiv \Sigma x_i \equiv 0 \ (mod\ 3)$, assim ele deve ser o caso que o último x_i' também é 0, portanto, a configuração do Cubo de Rubik é $(1, \beta', 0, y')$. ■

Em seguida, queremos provar Proposição 7, ou seja, queremos corrigir as posições dos cubinhos de arestas. A ideia da prova é muito semelhante ao que usamos para provar a Proposição 5. Primeiro, provamos que $\phi_{canto} : \mathbb{G} \longrightarrow S_8$ é sobrejetor. Neste caso, queremos apenas usar os movimentos que não afetam cubinhos cantos, uma vez que já fizemos um monte de trabalho para obter os cubinhos de cantos nas posições certas e orientações. Portanto, em vez de olhar diretamente para ϕ_{aresta}, olharemos para a restrição de ϕ_{aresta} para ker ψ_{canto}.

Lema 15 *A imagem de* $\phi_{aresta|Ker\,\psi_{canto}} : Ker\,\psi_{canto} \longrightarrow S_{12}$ *contém* A_{12}.

Demonstração: A_{12} é gerado pelo conjunto de 3-ciclos em A_{12}. Pelo mesmo argumento como na prova do Lema 13, basta mostrar que todos os 3-ciclo é a imagem de $\phi_{aresta|Ker\psi_{canto}}$. Como na prova do Lema 13, a estratégia é usar conjugados de um único movimento para provar.

Encontrado um movimento em que não afeta nenhum cubinho canto, mas 3 ciclos de cubinhos arestas. O movimento é $M_0 = LR^{-1}U^2L^{-1}RB^2$, que tem decomposição ciclo disjuntos $(ub\ uf\ db)$. Então, $M_0 \in Ker\ \psi_{canto}$ e $\phi_{aresta}(M_0) = (ub\ uf\ db)$. Até , se C_1, C_2, e C_3 são quaisquer 3 cubinhos cantos, há um movimento M do Cubo de Rubik que envia ub para C_1, uf para C_2, e db para C_3. Então, como $M' = M^{-1}M_0M$ tem ciclo de decomposição disjuntos $(C_1C_2C_3)$, tal que $M' \in ker\phi_{aresta}$ e $\psi_{canto}(M_0) = (C_1C_2C_3)$. Portanto $(C_1C_2C_3) \in \phi_{aresta|Ker\psi_{canto}}$ que completa a prova. ■

Observação: De fato, a imagem de $\phi_{aresta|Ker\,\psi_{canto}} : Ker\,\psi_{canto} \longrightarrow S_{12}$ é exatamente A_{12}, que permite provar usando o Corolário 1.

A Proposição 6 segue diretamente do Lema 15. A prova é exatamente a mesma ideia que a demonstração da Proposição 4.

Finalmente, provaremos a Proposição 7. Isto é bastante semelhante à Proposição 5. Primeiro, precisamos de um Lema análogo ao Lema 14.

Lema 16 *Se C_1 e C_2 são quaisquer dois cubinhos cantos, há um movimento $M \in \mathbb{G}$ que muda as orientações, mas não posições, de C_1 e C_2 e que não afeta os outros cubinhos.*

Demonstração: Encontrado um movimento que muda as orientações de 2 cubinhos de arestas, sem afetar quaisquer outros cubinhos. O movimento é

$$LR^{-1}FLR^{-1}DLR^{-1}BLR^{-1}ULR^{-1}F^{-1}LR^{-1}D^{-1}LR^{-1}B^{-1}LR^{-1}U^{-1}$$

(Este movimento é descrito com mais facilidade como $(M_RU)^4(M_RU^{-1})^4$). Chame esse movimento de M_0; que tem decomposição ciclo disjuntos $(fu$

$uf)(ub\ bu)$. $\mathbb{G}$ age transitivamente sobre o conjunto de triplos ordenados (C_1, C_2, C_3), onde C_1, C_2, e C_3 são diferentes cubinhos arestas. Em particular, se C_1 e C_2 são quaisquer dois cubinhos de arestas diferentes, existe $M \in \mathbb{G}$ que envia uf para C_1 e ub para C_2. Por MM_0M^{-1}, altera as orientações do C_1 e C_2, e não afeta os outros cubinhos em tudo. ■

O argumento que foi utilizado para provar a Proposição 5, prova a Proposição 7 também. Isto completa a prova do Teorema 4.

Observação: Anteriormente, calculamos que havia $2^{12}.3^8 8!12!$ configurações possíveis do Cubo de Rubik. Agora, o Teorema 4 diz-nos que apenas $\frac{1}{12}$ destas são válidos. Naturalmente, isto significa que existem ainda mais de 4.10^{19} configurações válidas, um número expressivamente grande ainda!

Referências Bibliográficas

[1] *DOMINGUES, Hygino H.; IEZZI, Gelson.* Álgebra moderna. 4. ed. reform. São Paulo, SP: Atual, 2003-2011.

[2] *GARCIA, Arnaldo; LEQUAIN, Yves.* Elementos de álgebra. 2. ed. Rio de Janeiro: IMPA, 2003.

[3] *GONÇALVES, Adilson.* Introdução à álgebra. 5. ed. Rio de Janeiro, RJ: Instituto de Matemática Pura e Aplicada, 2006-2012.

[4] *GARCÍA, Miguel Abreu.* Resolución rápida del cubo de rubik, Novembro 2011.

[5] *CHEN, Janet.* Group Theory and the Rubik's Cube, disponível em <http://www.math.harvard.edu/ jjchen/> acesso em 12/04/2016.

[6] *A História do Cubo de Rubik* disponível em <rubiks.com/about/the-history-of-the-rubiks-cube> acesso em 12/04/2016.

[7] *Notação do Singmaster* disponível em <docs.kde.org/stable4/pt/kdegames/kubrick/singmaster-moves.html> acesso 12/04/2016.

[8] *CERPE, Renan.* Cubo 2X2X2 - Método Básico disponível em <http://www.cubovelocidade.com.br/tutoriais/cubo-magico-2x2x2-basico.html> acesso em 12/04/2016.

[9] *CERPE, Renan.* Cubo 3X3X3 - Método Básico disponível em <http://www.cubovelocidade.com.br/tutoriais/cubo-magico-basico-metodo-camadas-1-passo-cruz-branca.html> acesso em 12/04/2016.