Universidade Federal do triângulo Mineiro
Instituto de Ciências Exatas, Naturais e Educação
Departamento de Matemática

Álgebra e o Cubo de Rubik

Robson Guimarães

Relatório para o Exame Geral de Qualificação apresentado ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional

Orientador
Prof. Dr. Leonardo Amorim Silva

2016

Universidade Federal do triângulo Mineiro
Instituto de Ciências Exatas, Naturais e Educação
Departamento de Matemática

Álgebra e o Cubo de Rubik

Robson Guimarães

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

Orientador
Prof. Dr. Leonardo Amorim Silva

2016

Catalogação na fonte: Biblioteca da Universidade Federal do Triângulo Mineiro

Lara, Robson Guimarães de Miranda
L325a Álgebra e o Cubo de Rubik / Robson Guimarães de Miranda Lara. -- 2016.
66 f. : il., fig.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) -- Universidade Federal do Triângulo Mineiro, Uberaba, MG, 2016
Orientador: Prof. Dr. Leonardo Amorim Silva

1. Matemática - Estudo e ensino. 2. Álgebra. 3. Teoria dos grupos. 4. Cubo mágico. I. Silva, Leonardo Amorim. II. Universidade Federal do Triângulo Mineiro. III. Título.

CDU 51(07)

TERMO DE APROVAÇÃO

Robson Guimarães

ÁLGEBRA E O CUBO DE RUBIK

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal do Triângulo Mineiro, pela seguinte banca examinadora:

Leonardo de Amorim e Silva

Prof. Dr. Leonardo Amorim Silva
Orientador

ARGMarques

Profª. Dra. Adriana Rodrigues da Silva
Departamento de Matemática - Universidade Federal de Uberlândia

Prof. Dr. Rafael Peixoto
Departamento de Matemática - Universidade Federal do Triângulo Mineiro

Uberaba, 29 de Agosto de 2016

Dedico à minha filha Manuela

Agradecimentos

Agradeço a Deus, em primeiro lugar, por estar sempre ao meu lado, me dando força para atingir meus objetivos e realizar meus sonhos.

Aos meus pais e irmãos por estarem sempre na torcida, apoiando e acreditando na conclusão desse projeto.

A minha esposa, por estar sempre ao meu lado durante todo esse período.

Aos amigos Wysner Max e Natália Gonçalves, parceiros nesse sonho, companheiros de viagem e de sala de aula.

Ao meu orientador, prof. Dr. Leonardo Amorim Silva, por todo apoio, dedicação, tempo e paciência. Prof. Dr. Leonardo se torna com certeza um exemplo, uma referência.

Por fim, agradeço a todos os meus amigos que de forma direta ou indireta fizeram parte desse sonho.

"A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original."

Albert Einstein

Resumo

Essa dissertação tem por objetivo mostrar como a matemática através de suas inúmeras teorias que para a grande maioria dos alunos nunca saem do campo da abstração, como por exemplo a teoria de grupos, pode ser associada a um brinquedo mundialmente famoso, o cubo de Rubik. Mostraremos que o cubo é um grupo e, posteriormente usaremos a teoria dos grupos para analisarmos qual é, realmente, a quantidade de soluções validas que podem ser utilizadas em sua resolução.

Palavras-chave: Álgebra. Teoria de Grupos. Cubo de Rubik.

Abstract

This dissertation aims to show how mathematics through his numerous theories, that for the vast majority of students never leave the abstraction field, such as group theory, can be associated with a world famous toy, the Rubik's Cube. It can be noted that the cube's movements change the settings of the faces but retain the overall shape of the cube, therefore we can represent such movements as permutations. Finally, we saw that the set of all faces permuta?ons of the Rubik's cube form a group and used the group theory to analyze what is the actual amount of valid solutions that can be used in its resolution.Writing an efficient abstract is hard work.

Keywords: Algebra. Group Theory. Rubik's Cube.

Sumário

1 Introdução

O cubo de Rubik ou cubo mágico foi criado no dia 19 de maio de 1974 pelo escultor e professor de arquitetura húngaro **Ernõ Rubik**. Rubik, aos 29 anos, trabalhava em um modelo tridimensional que o ajudaria a trabalhar com o ensino da geometria espacial aos seus alunos.

O brinquedo foi patenteado em 1977, e em seguida lançados no mercado. Hoje, existem várias versões deste brinquedo, por exemplo $(2 \times 2 \times 2)$, original $(3 \times 3 \times 3)$ e $(5 \times 5 \times 5)$.

O brinquedo foi inicialmente batizado por Cubo Mágico, pelo próprio Rubik, mas a lei de patentes da Hungria, na época regida por um governo comunista, não permitia a ampliação dos registros em caráter internacional. Por isso, quando a Ideal Toys foi registrar o brinquedo, teve de mudar o nome para cubo de Rubik. Com o lançamento do cubo mágico, surgiram também os primeiros campeonatos de resolução do desafio. Uma estudante vietcongue de 16 anos ganhou o primeiro campeonato mundial de cubo mágico, que aconteceu em Budapeste em 1982. Ela resolveu o jogo em 22,95 segundos. O atual recordista é Lucas Etter, de 14 anos, com o tempo de 4,904 segundos, mas isto entre humanos, o melhor tempo pertence a um robô criado nos Estados Unidos (2,39 segundos). Existem mais de 40 quatrilhões de combinações possíveis em um cubo mágico (são exatamente 43.252.003.274.856.000 combinações). Isso significa que se uma pessoa pegar um cubo mágico e fizer uma jogada por segundo, ela demorará pelo menos 1.400 trilhões de anos para fazer todas as movimentações possíveis. Desde a invenção do cubo mágico, em 1974, estudiosos tentam descobrir o mínimo necessário de jogadas para completar o desafio. Em julho de 2010, com a ajuda de um programa de computador, um grupo de pesquisadores chegou à conclusão: o jogo só consegue ser resolvido com um mínimo de 20 movimentações. O mais complexo cubo mágico existente é o cubo $17 \times 17 \times 17$ que foi resolvido em 7 horas, 32 minutos e 46 segundos, divididas em 5 dias por Kenneth Brandon.

O objetivo desse trabalho é usar a teoria de grupos para fazer uma discussão a respeito da quantidade de configurações possíveis que um cubo de Rukik pode assumir. No Capítulo 2, falaremos sobre alguns conceitos mais básicos de matemática que serão necessários para um melhor entendimento dos capítulos seguintes. No Capítulo 3, daremos uma breve apresentação dos conceitos de teoria de grupos que serão utilizados na modelagem do problema de estudarmos a quantidade de configurações válidas do cubo de Rubik. No Capítulo 4, demonstraremos o principal Teorema, o qual é utilizado para justificar a quantidade de configurações válidas do cubo de Rubik.

2 Relações, Aplicações e Operações

2.1 Relação Binária

Definição 2.1. *Dados dois conjuntos A e B, chamamos de* ***produto cartesiano****, e denotamos por $A \times B$ (lê-se: A cartesiano B) o conjunto formado por todos os pares ordenados (x, y) com $x \in A$ e $y \in B$.*

$$A \times B = \{(x, y) \mid x \in A \text{ e } y \in B\} \tag{2.1}$$

Definição 2.2. *Dados dois conjuntos A e B, chamamos de* ***relação*** *de A em B, todo subconjunto R de $A \times B$.*

Para indicar que $(a, b) \in R$, usaremos a notação aRb. Se $(a, b) \notin R$, escreveremos $a \not R\, b$.

Os conjuntos A e B são chamados, respectivamente de, conjunto de partida e conjunto de chegada de R.

Seja R uma relação de A em B. Chama-se **Domínio de uma relação** R, um subconjunto de A, formado por todos os elementos x para cada um dos quais existe um elemento y pertencente ao conjunto B, tal que xRy.

$$D(R) = \{x \in A \mid \exists\, y \in B : xRy\} \tag{2.2}$$

Chama-se **Imagem de uma relação** R, um subconjunto de B, formado por todos os elementos y para cada um dos quais existe um x pertencente A, tal que xRy.

$$Im(R) = \{y \in B \mid \exists\, x \in A : xRy\} \tag{2.3}$$

Exemplo 2.1. Dados os conjuntos $A = \{1, 2, 3\}$ e $B = \{1, 2, 3, 4, 5\}$, temos que: $A \times B = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (3, 1), (3, 2), (3, 3), (3, 4), (3, 5)\}$. Qualquer subconjunto do conjunto $A \times B$ é uma relação de A em B. A seguir alguns exemplos de relação de A em B. $R_1 = \emptyset$; $R_2 = \{(1, 1), (2, 2), (3, 3)\}$; $R_3 = \{(1, 3), (2, 3), (3, 3)\}$;

Se $A = B = \mathbb{Z}$, $A \times B$ é o conjunto formado por todos os pares ordenados de números inteiros, e se $A = B = \mathbb{R}$, $A \times B$ é o conjunto formado por todos os pares ordenados de números reais.

Definição 2.3. *Seja R uma relação de A em B, chama-se relação inversa de R, e indica-se por R^{-1} a seguinte relação de B em A:*

$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\} \tag{2.4}$$

Propriedades 2.1. *Decorrem diretamente da definição de relação inversa as propriedades seguintes:*

P_1: $D(R^{-1}) = Im(R)$;

P_2: $Im(R^{-1}) = D(R)$;

P_3: $(R^{-1})^{-1} = R$

2.1.1 Relação sobre um conjunto

Definição 2.4. *Quando $A = B$ e R é uma relação de A em B, diz-se que R é uma relação sobre A ou, ainda, R é uma relação em A.*

Definição 2.5. *Dada uma relação R, dizemos que a relação é:*

Reflexiva: *quando todo elemento de A se relaciona consigo mesmo. Ou seja, quando para todo $x \in A$, xRx.*

Simétrica: *se yRx sempre que xRy, ou seja, se xRy então yRx.*

Anti-simétrica: *se $x = y$, sempre que xRy e yRx. Ou seja, se xRy e yRx, então $x = y$.*

Transitiva: *se xRz sempre que xRy e yRz. Ou seja, se xRy e yRz então xRz.*

2.2 Relações de Equivalência

2.2.1 Relação de Equivalência

Definição 2.6. *Uma relação R sobre um conjunto A não vazio é chamada **relação de equivalência** sobre A se, e somente se, R é reflexiva, simétrica e transitiva. Ou seja, R deve cumprir, respectivamente, as seguintes propriedades:*

i- Se $x \in A$, então xRx;

ii- Se $x,y \in A$ e xRy então yRx;

iii- Se $x,y,z \in A$ e xRy e yRz, então xRz.

Exemplo 2.2. A Relação $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$ é uma relação de equivalência no conjunto $A = \{a, b, c\}$.

Definição 2.7. *Seja R uma relação de equivalência sobre um conjunto A. Para cada $a \in A$, o conjunto de todos os elementos $x \in A$ tais que xRa chama-se* ***classe de equivalência*** *de a e indica-se por $\bar{a}$. Ou seja,*

$$\bar{a} = \{x \in A \mid xRa\} \tag{2.5}$$

Definição 2.8. *O conjunto das classes de equivalência módulo R será indicado por A/R e chamado* ***conjunto-quociente*** *de A por R.*

Exemplo 2.3. Na relação de equivalência $R = \{(a,a),(b,b),(c,c),(a,b),(b,a)\}$ temos:

$$\begin{aligned} \bar{a} &= \{a,b\}; \\ \bar{b} &= \{a,b\}; \\ \bar{c} &= \{c\}; \end{aligned}$$

assim, $A/R = \{\bar{a},\bar{c}\} = \{\{a,b\},\{c\}\}$.

Exemplo 2.4. Considere a relaçção sobre $\mathbb{Z}$ dada por xRy $\leftrightarrow$ x $\equiv$ y (mod m), $\forall$ x,y $\in \mathbb{Z}$, m $>$ 1. Então R é uma **relação de equivalência** também chamada de **Relação de Congruência**. A relação R de congruência módulo m ($m \in \mathbb{Z}$ e $m > 1$) sobre $\mathbb{Z}$ é uma relação de equivalência.

(i) Sendo a $\in \mathbb{Z}$, efetuamos a divisão euclidiana de a por m, obtendo o quociente q e o resto r. Temos:

$$a = mq + r \text{ e } 0 \leq r < m \tag{2.6}$$

e daí vem:

$$a - r = qm \tag{2.7}$$

Portanto:

$$a \equiv r \ (mod\ m) \tag{2.8}$$

$$\bar{a} = \bar{r} \tag{2.9}$$

Concluímos que $\bar{a}$ = {x$\in$ $\mathbb{Z}$/x$\equiv$ a(mod m)} é uma classe igual a $\bar{r}$, em que r é o resto da divisão de a por m. como $r \in \{0,1,2,...,m-1\}$, vem:

$$\mathbb{Z}/\mathbb{R} = \bar{0},\bar{1},\bar{2},...,\overline{m-1} \tag{2.10}$$

(ii) Suponhamos que existam duas classes, $\bar{r}$ e $\bar{s}$, iguais em $\{\bar{0},\bar{1},\bar{2},...,\overline{m-1}\}$, representadas por elementos r e s, digamos $r < s$. Então:

$$\bar{r} = \bar{s} \quad \text{e} \quad 0 \leq r < s < m \tag{2.11}$$

De $\bar{r} = \bar{s}$ segue que $r \equiv s\ (mod\ m)$ e portanto $m|s-r$, Absurdo, pois $0 < s-r < m$, e isso é impossível.

Concluímos que $\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}$ é constituído por exatamente m elementos distintos dois a dois, ou seja:

$$\mathbb{Z}_m = \mathbb{Z}/R = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\} \tag{2.12}$$

Proposição 2.1. *Seja R uma relação de equivalência sobre A e sejam a, $b \in A$. As seguintes proposições são equivalentes:*

(i) aRb

(ii) $a \in \bar{b}$

(iii) $b \in \bar{a}$

(iv) $\bar{a} = \bar{b}$

Demonstração: Devemos provar $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow$ (i).

$(i) \Rightarrow (ii)$: É decorrência de definição de classe de equivalência.

$(ii) \Rightarrow (iii)$: Como $a \in \bar{b}$, então aRb, logo pela simetria de R, bRa, e portanto $b \in \bar{a}$.

$(iii) \Rightarrow (iv)$: Por hipótese $b \in \bar{a}$, ou seja, bRa, logo aRb. Temos que provar que $\bar{a} \subset \bar{b}$ e $\bar{b} \subset \bar{a}$.

Para provar a primeira dessas inclusões, tomemos $x \in \bar{a}$. Então xRa e, levando em conta que aRb, concluímos por transitividade de R, que xRb. Daí $x \in \bar{b}$ e $\bar{a} \subset \bar{b}$.

Analogamente se prova $\bar{b} \subset \bar{a}$.

$(iv) \Rightarrow (i)$: Como $a \in \bar{a}$ e $b \in \bar{b}$, os conjuntos $\bar{a}$ e $\bar{b}$ não são vazios. Tomemos um $x \in \bar{a} = \bar{b}$. Então xRa e xRb. Daí, pela simetria de R, aRx e xRb. A transitividade de R garante então que aRb. ■

2.2.2 Partição de um Conjunto

Definição 2.9. *Seja A um conjunto não vazio. Diz-se que uma classe F de subconjuntos não vazios de A, é uma* ***partição*** *de A se, e somente se:*

(i) Dois elementos quaisquer de F ou são iguais ou são disjuntos;

(ii) A união dos elementos de F é igual ao conjunto A.

Proposição 2.2. *Se R é uma relação de equivalência sobre um conjunto A, então A/R é uma partição de A.*

Demonstração:

Seja $\bar{a} \in A/R$. Como R é reflexiva, aRa e, portanto, $a \in \bar{a}$. Assim $\bar{a} \neq \varnothing$ para todo $\bar{a} \in A/R$.

Sejam $\bar{a}$, $\bar{b} \in A/R$ tais que $\bar{a} \cap \bar{b} \neq \varnothing$. Provaremos que $\bar{a} = \bar{b}$. De fato, seja $y \in \bar{a} \cap \bar{b}$. Então $y \in \bar{a}$ e $y \in \bar{b}$ e, portanto yRa e yRb. Daí aRy e yRb e portanto aRb. A proposição 2.1 garante então que $\bar{a} = \bar{b}$.

Provemos que $\cup_{a \in A}\bar{a} = A$.

Para cada $a \in A$, temos $\bar{a} \subset A$, portanto $\cup_{a \in A}\bar{a} \subset A$. Sendo x um elemento qualquer de A, então xRx. Daí, $x \in \bar{x}$ e por conseguinte, $x \in \cup_{a \in A}\bar{a}$, assim, $A \subset \cup_{a \in A}\bar{a}$. ■

Proposição 2.3. *Se F é uma partição no conjunto A, então existe uma relação de equivalência sobre A, tal que $A/R = F$.*

Demonstração: Seja R a relação sobre A assim definida: xRy se, e somente se, $\exists$ $E \in F$ tal que $x \in E$ e $y \in E$, ou seja, x está relacionado com y quando existe um conjunto E da partição F ao qual pertencem x e y. Provaremos que R é relação de equivalência.

Temos:

(i) Para todo x em A existe um subconjunto $E \subset A$ tal que $E \in F$ e $x \in E$, portanto xRx.

(ii) Se x e y são elementos quaisquer de A tais que xRy, então $x, y \in E$, para algum $E \in F$. Obviamente, então, $y, x \in E$. Logo yRx.

(iii) Sejam x, y e z elementos quaisquer de A tais que xRy e yRz. Isso significa que $x, y \in E$ e $y, z \in D$, para convenientes D e $E \in F$. Logo, $y \in E$ e $y \in D$. Como dois conjuntos quaisquer de F que não são disjuntos são necessariamente iguais, então $E = D$. Deste fato decorre que x e z pertencem ao mesmo conjunto de classe F de onde xRz. ■

2.2.3 Funções

Definição 2.10. *Seja f uma relação de A em B. Dizemos que f é uma **função** de A em B e denotamos por $f{:}A \to B$ se, e somente se, para todo $x \in A$ existe um único $y \in B$ tal que $(x, y) \in f$.*

Se f é uma função de A em B, escreveremos: $y = f(x)$. (lê-se: y é a imagem de x pela função f.)

Definição 2.11. *Uma função f de A em B é injetiva, se e somente se, quaisquer que sejam x_1 e x_2 de A, se $x_1 \neq x_2$, então $f(x_1) \neq f(x_2)$. Podemos definir um função injetiva de maneira equivalente da seguinte maneira: uma função f de A em B é injetiva se, e somente se, quaisquer que sejam x_1 e x_2 de A, se $f(x_1) = f(x_2)$, então $x_1 = x_2$.*

Definição 2.12. *Dizemos que uma função f de A em B é sobrejetiva se, e somente se, para todo $y \in B$ existe um elemento $x \in A$ tal que $f(x) = y$. Notemos que $f : A \to B$ é sobrejetora se, e somente se, $Im(f) = B$.*

Definição 2.13. *Dizemos que uma função f de A em B é bijetiva se, e somente se, f é injetiva e sobrejetiva. Essa definição é equivalente a: uma função f de A em B é bijetiva se, e somente se, para qualquer elemento $y \in B$, existe um único elemento $x \in A$ tal que $f(x) = y$.*

Definição 2.14. *Seja f uma função de A em B bijetiva. Definimos como a inversa da função f, e denotamos por f^{-1}, a função que associa a cada $y \in B$ um único $x \in A$.*

Definição 2.15. *Sejam as funções $f : A \to B$ e $g : B \to C$, então podemos definir uma nova função $f \circ g : A \to C$, chamada de função composta de f e g, por $(f \circ g)(x) = g(f(x))$.*

Observação 2.1. *Em alguns resultados dos Capítulos 3 e 4, escrevemos $(f \circ g)$ para denotar $g(f(x))$ em vez de $(f \circ g) = f(g(x))$. No entanto, desde que sejam consistentes, a escolha não faz uma grande diferença, todos os resultados que utilizaremos poderiam ser escritos mantendo uma única notação, porém demandaria demasiado trabalho. Usamos esta notação porque ela coincide com a convenção geralmente usada para o cubo de Rubik.*

3 Grupos

3.1 Definição e Exemplos

Definição 3.1. *Um conjunto não vazio G munido de uma operação $\star$ é um* ***grupo*** *quando as propriedades seguintes são satisfeitas:*

(i) Dados quaisquer x, $y \in G$, $x \star y \in G$, ou seja, o grupo é fechado para a operação $\star$.

(ii) Temos que $x \star (y \star z) = (x \star y) \star z$ para quaisquer $x, y, z \in G$, ou seja, a operação $\star$ é associativa.

(iii) Existe $e \in G$, chamado de elemento neutro, tal que $x \star e = e \star x = x$, para todo $x \in G$.

(iv) Dado qualquer $x \in G$, existe $x^{-1} \in G$ tal que $x \star x^{-1} = x^{-1} \star x = e$.

Diremos que um grupo $(G, \star)$ é comutativo ou abeliano se $x \star y = y \star x$ para quaisquer $x, y \in G$.

Propriedades 3.1. *Se $(G, \star)$ é um grupo, temos as seguintes propriedades:*

(i) O elemento neutro do grupo é único.

(ii) Dado $x \in G$, existe um único x^{-1} tal que $x \star x^{-1} = x^{-1} \star x = e$.

(iii) Temos que $(x^{-1})^{-1} = x$.

(iv) $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

(v) Valem as leis do cancelamento a direita e a esquerda, isto é, dados $x, y, z \in G$

$$x \star y = x \star z \Rightarrow y = z \quad \text{e} \quad y \star x = z \star x \Rightarrow y = z$$

(vi) Dados $a, b \in G$, as equações lineares $a \star x = b$ e $x \star a = b$ têm únicas soluções em G.

Demonstração:
(i) Se e_1 e e_2 são elementos neutros de $(G,\star)$, então:

$$e_1 \star e_2 = e_2, \text{ (pois } e_1 \text{ é elemento neutro)}$$
$$e_1 \star e_2 = e_1, \text{ (pois } e_2 \text{ é elemento neutro)}$$

Logo, e_1=e_2
(ii) Se y_1 e y_2 são inversos de x, então $x \star y_1 = y_1 \star x = e$, e $x \star y_2 = y_2 \star x = e$, desse modo,

$$\begin{aligned} y_1 = e \star y_1 &= (y_2 \star x) \star y_1 \\ &= y_2 \star (x \star y_1) \\ &= y_2 \star e \\ &= y_2 \end{aligned}$$

Isto é, $y_1 = y_2$
(iii)Dado $x \in G$, um elemento $y \in G$ é, por definição o inverso de x ou vice-versa, quando:

$$x \star y{=}y \star x{=}e$$

Como $x \star x^{-1} = x^{-1} \star x = e$, então $x = (x^{-1})^{-1}$.
(iv) Vamos mostrar que

$$(x \star y) \star (x^{-1} \star y^{-1}){=}(x^{-1} \star y^{-1})(x \star y) = e$$

Usando a propriedade associativa da operação em G, pode-se omitir os parênteses na equação acima, de modo que:

$$(x \star y) \star (x^{-1} \star y^{-1}) = x \star y \star x^{-1} \star y^{-1} = x \star e \star x^{-1} = e$$

(v) Como existe $x_1 \in G$ tal que $x_1 \star x = e = x \star x_1$, temos:

$$x \star y = x \star z \Rightarrow x_1 \star (x \star y) = x_1 \star (x \star z), \text{ (operando à esquerda com } x_1)$$
$$\Rightarrow (x_1 \star x) \star y = (x_1 \star x) \star z \text{ (pois } \star \text{ é associativa)}$$
$$\Rightarrow e \star y = e \star z \text{ (pois } x_1 \star x = e).$$

Isto é, $y = z$. Da mesma forma, mostra-se que $y \star x = z \star x$ implica em $y = z$.
(vi) Vamos mostrar a existência e unicidade de solução para equação $a \star x = b$; o outro caso é tratado similarmente. Seja $a_1 \in G$, com $a_1 \star a = e$. Logo o elemento $x_1 = a_1 \star b \in G$ é tal que:

$$a \star (a_1\ b) = (a \star a_1) \star b = e \star b = b$$

Isto é, x_1 é uma solução de $a \star x = b$. Suponhamos agora que $y_1 \in G$ seja outra solução. Por isso, $a \star x_1 = b$ e $a \star y_1 = b$, ou seja $a \star x_1 = a \star y_1$, Logo, por **(v)**, temos $x_1 = y_1$, mostrando a unicidade da solução. ■

Exemplos 3.1. 1− Os conjuntos $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$ são exemplos de grupos abelianos com a soma usual.
2− Para cada $n \in \mathbb{N}$, podemos definir duas operações para o conjunto $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$ dadas por $\bar{a} + \bar{b} = \overline{a+b}$ e $\bar{a}\bar{b} = \overline{ab}$. Primeiramente observemos que as operações são bem definidas: sejam $a_1, a_2, b_1, b_2 \in \mathbb{Z}_n$ tais que $\bar{a_1} = \bar{a_2}$ e $\bar{b_1} = \bar{b_2}$, temos que

$$a_1 = a_2 + n \cdot (k_1) \text{ e } b_1 = b_2 + n \cdot (k_2) \tag{3.1}$$

com $k_1, k_2 \in \mathbb{Z}$. Somando a_1 com b_1, obtemos

$$a_1 + b_1 = a_2 + b_2 + n \cdot (k_1 + k_2).$$

Ou seja

$$(a_1 + b_1) \equiv (a_2 + b_2) \mod n \ \Leftrightarrow \ \overline{a_1 + b_1} = \overline{a_2 + b_2}.$$

Logo,

$$\bar{a_1} + \bar{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \bar{a_2} + \bar{b_2}$$

Para a multiplicação temos: de 3.1 temos que

$$a_1.b_1 = (a_2 + n \cdot (k_1))(b_2 + n \cdot (k_2)) = a_2.b_2 + n \cdot (a_2.k_2 + b_2k_2 + nk_1k_2).$$

Desse modo

$$a_1.b_1 \equiv a_2.b_2 \mod n \ \Leftrightarrow \ \overline{a_1.b_1} = \overline{a_2.b_2}.$$

Portanto,

$$\bar{a_1}.\bar{b_1} = \overline{a_1.b_1} = \overline{a_2.b_2} = \bar{a_2}.\bar{b_2}.$$

Assim dados quaisquer $\bar{a}, \bar{b} \in \mathbb{Z}_n$, temos que $\overline{a+b} \in \mathbb{Z}_n$, $\bar{a}, \bar{b} \in \mathbb{Z}_n$, temos que $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$. Temos também que

$$\begin{aligned} \bar{a} + (\bar{b} + \bar{c}) &= \bar{a} + \overline{a+b} \\ &= \overline{a + (b+c)} \\ &= \overline{(a+b) + c} \\ &= \overline{a+b} + \bar{c} \\ &= (\bar{a} + \bar{b}) + \bar{c}, \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n. \end{aligned}$$

Dado $\bar{a} \in \mathbb{Z}_n$, temos que $\bar{a} + \bar{0} = \overline{a+0} = \bar{a}$. Por último, dado $\bar{a} \in \mathbb{Z}_n$ temos que $\bar{x} = \overline{n-a} \in \mathbb{Z}_n$ e que $\bar{a} + \bar{x} = \bar{a} + \overline{n-a} = \overline{a+n-a} = \bar{n} = \bar{0}$. Logo, $G = (\mathbb{Z}_n, +)$ é um grupo com a operação definida acima.

Ainda em $\mathbb{Z}_n$ como visto anteriormente dados quaisquer $\bar{a}, \bar{b} \in \mathbb{Z}_n$, temos que $\overline{ab} \in \mathbb{Z}_n$. Facilmente verificamos que $\bar{a}.(\bar{b}.\bar{c}) = (\bar{a}.\bar{b}).\bar{c}$, $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, que $\bar{a}.\bar{b} = \bar{b}.\bar{a}$, que $\bar{a}.\bar{1} = \bar{a}$. É possível mostrar ainda que, dado $\bar{a} \in \mathbb{Z}_n$, existe $\bar{b} \in \mathbb{Z}_n$ tal que $\bar{a}.\bar{b} = \bar{1}$ se, e somente se, $mdc(a, n) = 1$. Logo, o conjunto

$$U(\mathbb{Z}_n) = \{\bar{a} \in \mathbb{Z}_n : mdc(a, n) = 1\}$$

é um grupo multiplicativo abeliano.

Definição 3.2. *Consideremos um grupo G. Um subconjunto não vazio H de G é um subgrupo de G quando H, com a operação induzida de G, também é um grupo. Usaremos a notação $H < G$ para indicar que H é subgrupo de G.*

Exemplos 3.2. 1− Sob as adições usuais, temos que

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}.$$

e sob as multiplicações usuais

$$\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*.$$

2− Observe que $\mathbb{Q} \subset \mathbb{R}$, porem $(\mathbb{Q}, .)$ não é subgrupo de $(\mathbb{R}, +)$ pois as operações são distintas.

Teorema 3.1. *Seja H um subconjunto não vazio de um grupo G. Então, H é um subgrupo de G se, e somente se, uma das condições seguintes é satisfeita:*

(i) $h_1.h_2 \in H$ e $h_1^{-1} \in H$, para todo $h_1, h_2 \in H$.

(ii) $h_1.h_2^{-1} \in H$, para todo $h_1, h_2 \in H$.

Demonstração: Se H é um subgrupo de G, então H também é um grupo e, por isso as condições (1) e (2) são claramente satisfeitas. Reciprocamente, suponhamos que H satisfaz a condição (1). Logo, para qualquer $h \in H$, temos que $h^{-1} \in H$. Assim, $e{=}h.h^{-1} \in H$. Por conseguinte, $H < G$. Finalmente, se H satisfaz a condição (2), então dados h_1, $h_2 \in H$,

$$e = h_2.h_2^{-1} \in H \rightarrow h_2^{-1} = e.h_2^{-1} \in H.$$

Com isso,

$$h_1.h_2 = h_1 \, . \, (h_2^{-1})^{-1} \in H$$

Portanto, H é um subgrupo de G. ■

Definição 3.3. *Seja G um grupo. Um subgrupo H de G chama-se Normal quando*

$$ghg^{-1} \in H, \forall\, g \in G \;\; e \;\; \forall\, h \in H,$$

ou equivalentemente,

$$gHg^{-1} = \{ghg^{-1} \mid \forall\, h \in H \;\, e\, \forall\, g \in G\} \subset H.$$

Notação: *Usaremos a notação $N \lhd G$ para indicar que N é subgrupo normal de G.*

Exemplo 3.1. Se G é um grupo abeliano, então todo subgrupo H de G é normal.

Exemplo 3.2. O **centro** $Z(G) = \{x \in G : xg = gx \;\forall\, g \in G\}$ é normal.

Teorema 3.2. *Seja H um subgrupo de um grupo G. Então, as seguintes condições são equivalentes:*

(i) $H \lhd G$.

(ii) $gHg^{-1} = H, \forall\, g \in G$.

(iii) $gH = Hg, \forall\, g \in G$.

Demonstração: (i) $\Rightarrow$ (ii) Por hipótese, para cada $g \in G$, tem-se naturalmente a inclusão $gHg^{-1} \subset H$. Agora, dado $h \in H$,

$$h = g^{-1}(ghg^{-1})g \in H,$$

pois $ghg^{-1} \in H \lhd G$. Isso nos diz que $H \subset gHg^{-1}$ e, portanto $gHg^{-1} = H$.

(ii) $\Rightarrow$ (iii) Para $g \in G$, seja $x \in gH$, digamos $x = gh$ para algum $h \in H$. Logo, por hipótese,

$$xg^{-1} = ghg^{-1} \in gHg^{-1} = H$$

isto é, $xg^{-1} = h_1$, com $h_1 \in H$. Portanto $x = h_1g \in Hg$, de modo que $gH \subset Hg$. Da mesma forma, prova-se que $Hg \subset gH$. Por conseguinte, $Hg = gH$.

(iii) $\Rightarrow$ (i) Sejam $g \in G$ e $h \in H$. Como $gH = Hg$ e $gh \in Hg$, segue que $gh = h_2g$ para algum $h_2 \in H$, ou seja, $ghg^{-1} = h_2 \in H$. Portando $H \lhd G$. ■

3.2 Geradores

Definição 3.4. *Seja $(G, .)$ um grupo com a operação multiplicativa. Dados $a \in G$ e $n \in \mathbb{Z}$, define-se n-ésima potência de a, a^n, da seguinte forma:*

$$a^n = \begin{cases} e & se \quad n = 0, \\ a^{n-1}.a & se \quad n > 0, \\ (a^{-n})^{-1} & se \quad n < 0. \end{cases}$$

Se a operação em G for aditiva, então defini-se múltiplo de a, $n.a$, ao invés de potência de a. Assim,

$$n.a = \begin{cases} e & se \quad n = 0, \\ (n-1).a + a & se \quad n > 0, \\ (-n).(-a) & se \quad n < 0. \end{cases}$$

Seja G um grupo qualquer, $a \in G$. Seja $\langle a \rangle = \{a^i; i \in \mathbb{Z}\}$, assim é fácil ver que $\langle a \rangle$ é um subgrupo de G, denominado subgrupo cíclico gerado por a.

Definição 3.5. *Se para algum $a \in G, G = \langle a \rangle$, então G é dito um grupo cíclico.*

Definição 3.6. *Seja G um grupo, S um subconjunto de G. Seja H o conjunto de todos os elementos de G que podem ser representados como um produto de elementos de S, elevados a expoentes inteiros positivos, negativos ou nulos. Assim $\langle S\rangle$ será um subgrupo de G o qual diremos que é o subgrupo de G gerado por S e denotamos por $H = \langle S\rangle$.*

Exemplo 3.3. Todo elemento de $(\mathbb{Z},+)$ pode ser escrito como uma soma de uma quantidade finita de 1 ou -1, logo $\mathbb{Z} = \langle 1\rangle$, observe que $\mathbb{Z} = \langle -1\rangle$.

Podemos pensar em geradores como sendo o "núcleo" do grupo; uma vez que cada elemento do grupo pode ser escrito em termos dos geradores, informações sobre os geradores podem muitas vezes ser traduzidas para informações sobre todo o grupo.

Lema 3.1. *Seja G um grupo finito, ou seja o conjunto G é um conjunto finito, e $g \in G$. Então $g^{-1} = g^n$ para algum $n \in \mathbb{N}$.*

Demonstração: Se G é finito, digamos $G = a_1, a_2, ..., a_k$, então todo elemento $a \in G$ tem ordem finita. Fazendo $O(a_i) = n_i$ para $i = 1, ..., k$ e considerando s o produto dessas ordens $s = n_1.n_2...n_k$, temos que:

$$a_i^s = (a_i^{n_i})^r = e, \forall a \in G,$$

em que $r = n_1.n_2...n_{i-1}.n_{i+1}...n_k$. ■

Lema 3.2. *Seja G um grupo finito e S um subconjunto de G. Então $G = \langle S\rangle$ se, e somente se, todo elemento de G pode ser escrito como um produto finito de elementos de S.(Nesse caso os inversos de S não são necessários.)*

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

Reciprocamente, suponha que $G = \langle S\rangle$. Logo, todo elemento de G pode ser escrito como um produto finito $s_1.s_2...s_n$, onde cada s_i está em S ou é um inverso de um elemento de S. Provaremos isso por indução sobre n.

Se $n = 1$. Temos que $s_1 \in S$ ou ${s_1}^{-1} \in S$. Se $s_1 \in S$, então s_1 é escrito como o produto de um único elemento de S. Se $s_1^{-1} \in S$, então pelo Lema 3.1, s_1^{-1} pode ser escrito como o produto finito de elementos de S.

Suponhamos agora que a afirmação é verdadeira para todo número natural menor que n; queremos mostrar que $s_1.s_2...s_n$ pode ser escrito como um produto finito de elementos de S. Pela hipótese de indução, $s_1.s_2...s_{n-1}$ e s_n podem ser escritos como o produto finito de elementos de S, assim, $s_1.s_2...s_n$ é um produto finito de elementos de S. ■

O próximo resultado nos mostra como passar propriedades de geradores para todo o grupo.

Proposição 3.1. *Seja G um grupo finito e S um subconjunto de G. Suponha que as duas condições seguintes são satisfeitas:*

1. *Todo elemento de S satisfaz alguma propriedade P.*

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

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

Demonstração: Pelo Lema 3.2, qualquer elemento de $\langle S \rangle$ pode ser escrito como $s_1.s_2...s_n$ onde $n \in \mathbb{N}$ e cada $s_i \in S$. Provaremos a proposição usando indução sobre n.

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

Suponha, por indução, que $s_1.s_2...s_{n-1}$ satisfaz a propriedade P. Então, o produto $(s_1.s_2...s_{n-1})s_n$ é o produto de dois elementos satisfazendo a propriedade P, logo, por hipótese, satisfazem a propriedade P. ■

3.3 Grupos de Simetrias

Permutação é o termo específico usado na teoria dos grupos para designar uma bijeção de um conjunto nele mesmo. Se A indica um conjunto não vazio, denotaremos por $S(A)$ o conjunto das permutações dos elementos de A. A composição de aplicações é, neste caso, uma operação sobre $S(A)$, pois se f e g são permutações de A, ou seja, se $f : A \longrightarrow A$, e $g : A \longrightarrow A$ são bijeções, então a composta g $\circ$f : A $\longrightarrow$ A também é uma bijeção. Chama-se $(S_A, \circ)$ grupo de permutações sobre A.

Quando A tem um número finito de elementos, $A = \{x_1, x_2, ..., x_n\}$, utilizaremos o conjunto $\{1, 2, ..., n\}$ para representar as permutações dos elementos de A e denotaremos $S(A)$ por S_n.

É comum representar uma permutação $\alpha \in S_n$ por

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

Exemplo 3.4. Seja $A = \{1, 2, 3\}$. As permutações de A são

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \ \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

ou seja, $S_3 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$. Fazendo $\alpha = \alpha_6$ e $\beta = \alpha_2$, temos

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \alpha_5$$

Analogamente, $\alpha^3 = e$, $\beta^2 = e$, $\beta\alpha = \alpha_3$ e $\alpha\beta = \alpha_4$.

Definição 3.7. *Uma permutação $\alpha \in S_n$ chama-se* ***ciclo de comprimento*** *r ou r-ciclo quando existem elementos distintos a_1, a_2, ..., $a_r \in \{1, 2..., n\}$ tais que*

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

e

$$\alpha(i) = i,\ \forall\ i \in \{1, 2..., n\} - \{a_1, a_2, ..., a_r\}.$$

Em particular, um 2-ciclo chama-se transposição.

Em geral, denota-se um r-ciclo α por $\alpha = (a_1\ a_2\ ...\ a_r)$.

Exemplo 3.5. No gupo S_5, a permutação $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$ é tal que $\alpha(1) = 3$, $\alpha(3) = 5$, $\alpha(5) = 4$, $\alpha(4) = 1$ e $\alpha(2) = 2$. Logo, $\alpha = (1\ 3\ 5\ 4)$, ou seja, α é um 4-ciclo.

Exemplo 3.6. Em S_4

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1\ 2) \text{ e } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2\ 4)$$

são transposições.

Observação 3.1. Observe que se $\mu = (a_1\ a_2\ ...\ a_r) \in S_n$, então $\mu^{-1} = (a_r\ a_{r-1}\ ...\ a_1) \in S_n$

Definição 3.8. *Dois ciclos $\alpha, \beta \in S_n$, digamos $\alpha = (a_1\ a_2\ ...\ a_r)$ e $\beta = (b_1\ b_2\ ...\ b_k)$ são ditos ciclos disjuntos quando nenhum elemento de $\{1, 2, ..., n\}$ é movido por ambos. Equivalentemente, quando*

$$\{a_1, a_2, ..., a_r\} \cap \{b_1, b_2, ..., b_k\} = \emptyset$$

Exemplo 3.7. Seja $\alpha \in S_5$ dado por $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$, assim temos que $\alpha = (2\ 3)(1\ 4\ 5)$.

Proposição 3.2. *Se $\alpha, \beta \in S_n$ são ciclos disjuntos, então $\alpha\beta = \beta\alpha$.*

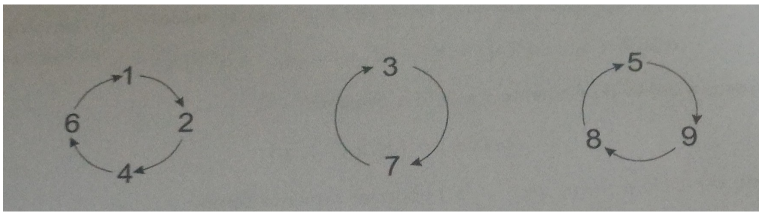
Demonstração: Devemos provar que $\alpha\beta(i) = \beta\alpha(i)$ para todo $i \in I_n$. Se $i \in I_n$ é fixado por α e β, então $\alpha(\beta(i)) = \alpha(i)$; da mesma forma $(\beta\alpha)(i) = \beta(\alpha(i)) = \beta(i) = i$. Portanto, para esse caso tem-se que $\alpha\beta(i) = \beta\alpha(i)$.
Agora, se α move o elemento i, digamos $\alpha(i) = j \neq i$, então $\beta(i) = i$, pois α e β são disjuntos. Desse modo,

$$(\alpha\beta(i)) = \alpha(\beta(i)) = \alpha(i) = j\ (\beta\alpha(i)) = \beta(\alpha(i)) = \beta(j) = j$$

Pois α move o elemento j, uma vez que se $\alpha(j) = j$, então $\alpha(i) = \alpha(j)$, com $i \neq j$ o que contradiz o fato de α ser injetora. Portanto $\alpha\beta(i) = \beta\alpha(i)$. Da mesma forma mostra-se esta igualdade quando o elemento i é movido por β. Por conseguinte, $\alpha\beta = \beta\alpha$. ■

Teorema 3.3. *Toda permutação $\alpha \in S_n - \{e\}$ pode ser escrita como um produto de ciclos disjuntos. Além disso, esta fatoração é única, a menos da ordem dos fatores.*

Demonstração: Se $\alpha \in S_n$ for um ciclo, então o resultado segue imediato. Caso contrário consideremos $O_1, O_2, ..., O_k$, as distintas α-órbitas não triviais, ou seja:



as α-órbitas com mais de um elemento. Temos então que $\alpha(O_i) = O$, para qualquer que seja $i = 1, ..., n$, definamos:

$$\mu_i(j) = \begin{cases} \alpha(j) & \text{se} \quad j \in O_i, \\ j & \text{se} \quad j \notin O_i, \end{cases}$$

Claramente, μ é um ciclo, pois se $j \notin O_i$, então $\mu(j) = j$ e, portanto, a μ_i -órbita de j é unitária, isto é, é igual a j. Temos também que O_i é uma órbita de μ_i, pois μ_i e α coincidem em O_i, e como $\alpha(O_i) = \mu(O_i) = O_i, \alpha^m$ coincide com μ_i em O_i, para todo $m \in \mathbb{Z}$. Além de $\mu_1, \mu_2, ..., \mu_k$ serem ciclos disjuntos pares vê-se claramente que $\alpha = \mu_1\mu_2...\mu_k$.

Mostremos agora a unicidade da fatoração. Suponhamos que: $\alpha = \beta_1\beta_2...\beta_l$, sendo os β_i ciclos não triviais disjuntos. Para cada $i = 1, ..., l$, chamemos de C_i a órbita não trivial de β_i. Desse modo $C_1, C_2, ..., C_l$ são órbitas não triviais de $\alpha = \beta_1\beta_2...\beta_l$. Isto significa que $l = k$ e, reordenando se necessário, temos $C_1 = O_1, C_2 = O_2, ..., C_k = O_k$. Logo $\mu_i = \beta_i$ com $i = 1, ..., k$ pois $\mu(j) = \alpha(j) = \beta(j)$ para todo $j \in O_i$. ■

Corolário 3.1. *Toda permutação $\alpha \in S_n$ pode ser escrita como produto de transposições.*

Demonstração: Pelo teorema anterior, basta mostrar que todo ciclo em S_n é um produto de transposições. Assim, dado $\mu = (a_1\ a_2\ ...\ a_r)$, temos que

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

■

Corolário 3.2. *(i) O conjunto de transposições* $\{(1\ 2), (1\ 3), ..., (1\ n), \}$ *gera* S_n.

(ii) As transposições $\{(1\ 2), (2\ 3), ..., (n-1\ n)\}$ *gera* S_n.

Demonstração: (i) Observe que $(a\ b) = (1\ a)(1\ b)(1\ a)$, assim basta utilizarmos o corolário anterior.
(ii) Observe que $(1\ k) = (k-1\ k)...(3\ 4)(2\ 3)(1\ 2)(2\ 3)(3\ 4)...(k-1\ k)$ e aplicamos a parte (i). ■

Exemplo 3.8. Notemos que a permutação $\sigma \in S_6$ dada por $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$, é tal que $\sigma = (1\ 6)(2\ 4\ 5)$. Portanto, como produto de transposições,

$$\sigma = (1\ 6)(2\ 5)(2\ 4).$$

Teorema 3.4. *Sejam* $\mu_1, \mu_2, ..., \mu_k \in S_n$ *ciclos disjuntos aos pares de comprimentos* $r_1, r_2, ..., r_k$*, respectivamente. Então, a ordem da permutação* $\alpha = \mu_1\mu_2...\mu_k$ *é igual a*

$$mmc(r_1, r_2, ..., r_k).$$

Demonstração: Como $\mu_1, \mu_2, ..., \mu_k$ são ciclos disjuntos, pela Proposição 3.2 $\mu_i\mu_j = \mu_j\mu_i$ quaisquer que sejam $i, j \in \{1, 2, ..., k\}$. Logo,

$$\alpha^s = (\mu_1\mu_2...\mu_k)^s = \mu_1^s\mu_2^s...\mu_k^s, \forall\ s \in \mathbb{Z}$$

Sendo $m = mmc(r_1, r_2, ..., r_k)$, então para cada $i \in \{1, 2, ..., k\}$, existe $\lambda_i \in \mathbb{Z}$ tal que $m = \lambda_i r_i$. Assim

$$\mu_i^m = \mu_i^{\lambda_i r_i} = (\mu_i^{r_i})^{\lambda_i} = e,$$

pois a ordem de μ_i é r_i. Logo,

$$\alpha^m = (\mu_1\mu_2...\mu_k)^m = \mu_1^m\mu_2^m...\mu_k^m = e.$$

Por outro lado, se $\alpha^t = e$, ou seja, $(\mu_1\mu_2...\mu_k)^t = e$, então

$$\mu_1^t\mu_2^t...\mu_k^t = e.$$

Mas como os ciclos $\mu_1, \mu_2, ..., \mu_k$ são disjuntos, obtemos que

$$\mu_i^t = e, \forall\ i \in \{1, 2, ..., k\}$$

Portanto, a ordem de μ_i divide t, isto é, r_i divide t. Mas, como m é o mínimo múltiplo comum de $r_1, r_2, ..., r_k$, então m deve necessariamente dividir t, de modo que $m \leq t$. Portanto, a ordem de $\alpha = \mu_1\mu_2...\mu_k$ é igual a m. ■

Exemplo 3.9. Considere $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 7 & 1 & 4 & 6 & 2 \end{pmatrix}$. Como $\tau = (1\ 3\ 8\ 2\ 5)(4\ 7\ 6)$, em que $\mu_1 = (1\ 3\ 8\ 2\ 5)$ e $\mu_2 = (4\ 7\ 6)$ são ciclos disjuntos de comprimento 5 e 3, respectivamente, temos que a ordem de τ é $mmc(3,5) = 15$.

Teorema 3.5. *Se $\alpha, \sigma \in S_n$, então $\alpha\sigma\alpha^{-1}$ é a permutação obtida aplicando α aos elementos dos ciclos que aparecem na fatoração de σ. Em particular, $\alpha\sigma\alpha^{-1}$ e σ têm a mesma estrutura de ciclos.*

Demonstração: Consideremos $\tau = \alpha\sigma\alpha^{-1}$, assim, se $\sigma(i) = j$, então

$$(\tau\alpha)(i) = (\alpha\sigma\alpha^{-1})\alpha(i) = (\alpha\sigma)(i) = \alpha(j).$$

Desse modo, desde que $(a_1\ a_2\ ...\ a_r)$ seja um ciclo na decomposição de σ, temos que $(\alpha(a_1)\ \alpha(a_2)\ ...\alpha(a_r))$ é um ciclo na decomposição de $\alpha\sigma\alpha^{-1}$. Portanto, a fatoração em ciclos de τ é obtida substituindo-se x por $\alpha(x)$ na decomposição de σ. Por isso, τ e σ têm a mesma estrutura de ciclos. ■

Exemplo 3.10. Dadas as permutações em S_6

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

vamos determinar $\alpha\sigma\alpha^{-1}$ usando o Teorema 3.5 e pelo método tradicional. Como $\sigma = (4\ 5\ 6)$, então

$$\alpha\sigma\alpha^{-1} = (\alpha(4)\ \alpha(5)\ \alpha(6)) = (6\ 1\ 4) = (1\ 4\ 6)$$

Pelo método tradicional temos,

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

e

$$\begin{aligned} \alpha\sigma\alpha^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 2 & 6 & 3 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 6 & 5 & 1 \end{pmatrix} \\ &= (1\ 4\ 6). \end{aligned}$$

3.4 Homomorfismos de Grupos

Homomorfismo de grupos é uma forma de relacionar dois grupos G_1 e G_2, no sentido que se possam obter informações algébricas de G_2 a partir de propriedades algébricas conhecidas de G_1, ou vice-versa.

Definição 3.9. *Sejam $(G_1, \star)$ e $(G_2, *)$ dois grupos. Uma função $f : G_1 \to G_2$ chama-se homomorfismo de G_1 em G_2 quando $f(a \star b) = f(a) * f(b)$, para todo a, $b \in G_1$*

Proposição 3.3. *Seja $f : G_1 \to G_2$ um homomorfismo de grupos. Então:*

(1) $f(e_1) = e_2$, sendo e_i o elemento neutro de G_i

(2) $f(a^{-1}) = f(a)^{-1}$, para todo a $\in G_1$.

(3) $Im(f) = \{f(a) : a \in G_1\}$ é um subgrupo de G_2.

(4) Se H é um subgrupo de G_2, então a imagem inversa $f^{-1}(H)$ de H por f, $f^{-1}(H) = \{x \in G_1 : f(x) \in H\}$, é um subgrupo de G_1.

Demonstração: (1) Como $e_1 = e_1.e_1$, então:

$$f(e_1) = f(e_1.e_1) = f(e_1).f(e_1)$$

Logo, $f(e_1)$ é necessariamente a identidade de G_2, ou seja, $f(e_1) = e_2$

(2) Para todo $a \in G_1, a.a^{-1} = e_1$. Assim,

$$f(a_1.a^{-1}) = f(e_1) = e_2,$$

ou seja, $f(a).f(a^{-1}) = e_2$, o que significa que $f(a^{-1}) = f(a)^{-1}$

(3) Sendo $f(e_1) = e_2$, então $Im(f) \neq \emptyset$. Agora, dados $x, y \in Im(f)$ existem $a, b \in G_1$ tais que $f(a) = x$ e $f(b) = y$. Por isso,

$$x.y^{-1} = f(a).f(b)^{-1} = f(a).f(b^{-1}) = f(a.b^{-1})$$

de maneira que, $x.y^{-1} \in Im(f)$ e $Im(f) < G_2$

(4) Como $e_2 \in H$ e $f(e_1) = e_2$, então $f^{-1}(H) =\neq \emptyset$. Consideremos então $a, b \in f^{-1}(H)$. Assim, por definição, $f(a) \in H$ e $f(b) \in H$. Como H é subgrupo de G_2, $f(b)^{-1} = f(b^{-1})$ também está em H, de modo que:

$$f(a.b^{-1}) = f(a).f(b^{-1}) = f(a).f(b)^{-1} \in H$$

Portanto, $a.b^{-1} \in f^{-1}(H)$, implicando que $f^{-1}(H) < G$. ■

Definição 3.10. *O núcleo de um homomorfismo f: $G_1 \to G_2$ é definido como sendo $ker(f)$ = $\{g \in G_1 : f(g) = e_2\}$, ou seja, $ker(f)$ é a imagem inversa de e_2.*

Teorema 3.6. *Seja $f : G_1 \to G_2$ um homomorfismo de grupos. Então:*

(1) $ker(f) = e_1$ se, e somente se, f é injetora.

(2) $ker(f) \lhd G_1$.

Demonstração: (1) Suponhamos que $ker(f) = \{e_1\}$, e sejam $x_1, x_2 \in G_1$. Temos que

$$\begin{array}{rcl} f(x_1) = f(x_2) & \Rightarrow & f(x_1).f(x_2)^{-1} = e_2 \\ & \Rightarrow & f(x_1).f(x_2^{-1}) = e_2 \\ & \Rightarrow & f(x_1.x_2^{-1}) = e_2 \end{array}$$

Mas, $f(x_1.x_2^{-1}) = e_2$ implica que $x_1.x_2{}^{-1} \in ker(f) = e_1$, de modo que $x_1.x_2{}^{-1} = e_1$, ou seja, $x_1 = x_2$. Portanto, f é injetora. Reciprocamente, dado $x \in G_1$,

$$x \in ker(f) \Leftrightarrow f(x) = e_2 = f(e_1).$$

Como por hipótese f é injetora, $f(x) = f(e_1)$ nos diz que $x = e_1$, e portanto $ker(f) = \{e_1\}$.
(2) Por 3.3 temos que $ker(f)$ é um subgrupo de G_1. Agora, para $g \in G_1$ e $h \in ker(f)$, temos

$$f(ghg^{-1}) = f(g).f(h).f(g^{-1}) = f(g).e_2.f(g^{-1}) = f(g).f(g)^{-1} = e_2.$$

■

Definição 3.11. *Um homomorfismo de grupos $f : G_1 \to G_2$ bijetivo chama-se **isomorfismo**. Em particular, um isomorfismo $f : G \to G$ denomina-se **automorfismo** de G. Dois grupos G_1 e G_2 são ditos isomorfos quando existir um isomorfismo entre eles.*

A noção de isomorfismo de grupos é bastante valiosa pois ela nos fornece um modo de verificar quando dois grupos são essencialmente os mesmos, ou seja, quando eles possuem as mesmas propriedades algébricas.

Exemplo 3.11. Considere o grupo $G_1 = (\mathbb{Z}_4, +)$, temos que:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Podemos reescrever a tabela de adição acima da seguinte forma: usaremos o símbolo * em vez de $+$ para adição, e vamos escrever $e = \bar{0}$, $a = \bar{1}$, $b = \bar{2}$, e $c = \bar{3}$. Assim, obtemos a seguinte tabela:

Faremos a mesma coisa para $G_2 = (\mathbb{Z}_5^*, .)$, o conjunto de unidades *mod* 5. As unidades *mod* 5 são $\bar{1}$, $\bar{2}$, $\bar{3}$ e $\bar{4}$. Observe que adicionando duas unidades, não obtemos necessariamente outra unidade; por exemplo, $\bar{1} + \bar{4} = \bar{0}$, e $\bar{0}$ não é uma unidade. No

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$.$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{3}$	$\bar{1}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{1}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{2}$	$\bar{4}$

entanto, se você multiplicar duas unidades, você sempre terá uma unidade. Assim, podemos escrever uma tabela de multiplicação de $G_2 = (\mathbb{Z}_5^*, .)$. Assim, obtemos a seguinte tabela:

Novamente, podemos reescrever isso usando novos símbolos. Usaremos * representar a multiplicação, e $e = \bar{1}$, $a = \bar{2}$, $b = \bar{4}$ e $c = \bar{3}$. Assim a tabela de multiplicação de $G_2 = (\mathbb{Z}_5^*, .)$ fica como segue:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Assim podemos observar que $G_1 = (\mathbb{Z}_4, +)$ e $G_2 = (\mathbb{Z}_5^*, .)$ são essencialmente os mesmos, ou seja G_1 é isomorfo a G_2.

3.4.1 O Sinal de um Homomorfismo

Vimos que S_n é gerado por 2-ciclos em S_n, ou seja, qualquer permutação em S_n pode ser escrita como um produto finito de 2-ciclos. Porém, qualquer permutação de S_n pode ser escrita como um produto finito de 2-ciclos de várias maneiras.

Algumas permutações em S_n podem ser escritas como um produto de um número par de 2 ciclos, chamamos essas permutações de *permutações pares*. Outras permutações de S_n podem ser escritas com um produto de um número ímpar de 2-ciclos, chamamos essas permutações de *permutações ímpares*. Até o momento, parece não haver nenhuma razão para que uma permutação não possa ser ao mesmo tempo tanto par como ímpar. No entanto, uma permutação sempre será par ou ímpar, e nunca par e ímpar aos mesmo tempo.

Para demonstrarmos a afirmação anterior usaremos o seguinte argumento:
Fixe n, e seja $p(x_1, ..., x_n)$ um polinômio em n variáveis $x_1, ..., x_n$.

Se $n = 1$, $p(x_1)$ é um polinômio na variável x_1; isto é, $p(x_1) = a_m x_1^m + a_{m-1}x_1^{m-1} + \cdots + a_0$. Portanto, $p(x_1)$ é uma soma de termos da forma $a_i x_1^i$.

Se $n = 2$, então $p(x_1, x_2)$ é uma soma de termos da forma $a_{ij}x_1^i x_2^j$.

Em geral, $p(x_1, ..., x_n)$ é uma soma de termos da forma $a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$.

Se $\sigma \in S_n$, seja p^σ o polinômio definido por $(p^\sigma)(x_1, ..., x_n) = p(x_{\sigma(1)}, ..., x_{\sigma(n)})$, ou seja, simplesmente substituímos x_i por $x_{\sigma(i)}$.

Exemplo 3.12. Suponha $n = 4$, $p(x_1, x_2, x_3, x_4) = x_1^3 + x_2x_3 + x_1x_4$, e $\sigma \in S_4$ dado por $\sigma = (1\ 2\ 3)$. Então, $(p^\sigma)(x_1, x_2, x_3, x_4) = x_{\sigma(1)}^3 + x_{\sigma(2)}x_{\sigma(3)} + x_{\sigma(1)}x_{\sigma(4)} = x_2^3 + x_3x_1 + x_2x_4$.

Lema 3.3. *Para qualquer $\sigma, \tau \in S_n$, $(p^\sigma)^\tau = p^{\sigma\tau}$.*

Demonstração: Pela definição, $(p^\sigma)(x_1, x_2, ...x_n) = p(x_{\sigma(1)}, ..., x_{\sigma(n)})$, logo $[(p^\sigma)^\tau] = p(x_{\tau(\sigma(1))}, ..., x_{\tau(\sigma(n))})$. Além disso, $\tau(\sigma(i)) = (\sigma\tau)(i)$, logo $[(p^\sigma)^\tau](x_1, x_2, ...x_n) =$
$= p(x_{(\sigma\tau)(1)}, ..., x_{(\sigma\tau)(n)}) = (p^{\sigma\tau})(x_1, ...x_n)$. ■

Para provarmos a afirmação sobre permutações pares e ímpares, aplicaremos o Lema 3.3 para um polinômio específico dado por

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

Exemplo 3.13. Se $n = 3$, $\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.

Exemplo 3.14. Se $\sigma = (1\ 3\ 2)$, então $\Delta^\sigma = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \Delta$. Por outro lado, se $\sigma = (1\ 2)$, então $\Delta^\sigma = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -\Delta$.

Lema 3.4. *Para qualquer $\sigma \in S_n$, $\Delta^\sigma = \pm\Delta$.*

Demonstração: Por definição,

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

logo,

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

Assim, para mostrar que $\Delta^\sigma = \pm\Delta$, devemos mostrar duas coisas. Primeiramente que, para cada i e j com $1 \le i < j \le n$, devemos mostrar que $x_{\sigma(i)} - x_{\sigma(j)}$ ou seu oposto aparece em Δ; ou seja, $x_{\sigma(i)} - x_{\sigma(j)}$ ou seu oposto tem a forma $x_k - x_l$ com $1 \leq k < l \leq n$. Em seguida, devemos mostrar que, para cada i e j com $1 \leq i < j \leq n$, $x_i - x_j$ ou seu negativo aparece em Δ^σ. Uma vez que Δ e Δ^σ têm o mesmo número de termos, as duas afirmações juntas provam o resultado.

Para provarmos a primeira afirmação, precisamos mostrar que $\sigma(i) < \sigma(j)$ ou $\sigma(j) < \sigma(i)$, ou seja, devemos mostrar que $\sigma(i) \neq \sigma(j)$ se $1 \leq i < j \leq n$. Porém isso é verdade uma vez que σ é injetiva e $i \neq j$.

Para a segunda afirmação, precisamos mostrar que $x_i - x_j$ ou seu negativo podem ser escritos como $x_{\sigma(k)} - x_{\sigma(l)}$, com $1 \leq k < l \leq n$. Uma vez que $\sigma \in S_n$, $\sigma^{-1} \in S_n$, e portanto, σ^{-1} também é uma bijeção. Assim, uma vez que $i \neq j$, $\sigma^{-1}(i) \neq \sigma^{-1}(j)$. Seja k o menor número entre $\sigma^{-1}(i)$ e $\sigma^{-1}(j)$, e seja l o maior. Assim, $1 \leq k < l \leq n$ e $x_i - x_j$ será $x_{\sigma(k)} - x_{\sigma(l)}$ ou seu negativo. ■

Pelo Lema 3.4 podemos definir uma aplicação $\epsilon : S_n \to \{\pm 1\}$ dada por $\Delta^\sigma = \epsilon(\sigma)\Delta$, ou seja, se $\Delta^\sigma = \Delta$, então $\epsilon(\sigma) = 1$, se $\Delta^\sigma = -\Delta$, teremos $\epsilon(\sigma) = -1$. Pelo Lema 3.3 $\Delta^{\sigma\tau} = (\Delta^\sigma)^\tau = [\epsilon(\sigma)\Delta]^\tau = \epsilon(\sigma)\Delta^\tau = \epsilon(\sigma)\epsilon(\tau)\Delta$. Portanto, $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$. Assim, ϵ é um homomorfismo. Chamaremos esse homomorfismo de *sinal do homomorfismo.*

Afirmamos inicialmente que $\epsilon(\sigma)$ tinha algo a ver com o número de 2-ciclos na decomposição de σ. O teorema seguinte provará esse fato.

Teorema 3.7. *Se σ é um 2-ciclo, então $\epsilon(\sigma) = -1$.*

Demonstração: Primeiramente, seja $\sigma = (1\ 2)$. Seja

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

Podemos escrever Δ como segue

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

Além disso,

$$\begin{aligned} \Delta^\sigma &= (x_{\sigma(1)} - x_{\sigma(2)}) \prod_{2<j\leq n}(x_{\sigma(1)} - x_{\sigma(j)}) \prod_{2<j\leq n}(x_{\sigma(2)} - x_{\sigma(j)}) \prod_{3\leq i<j\leq n}(x_{\sigma(i)} - x_\sigma(j)) \\ &= (x_2 - x_1) \prod_{2<j\leq n}(x_2 - x_j) \prod_{2<j\leq n}(x_1 - x_j) \prod_{3\leq i<j\leq n}(x_i - x_j) \\ &= -\Delta \end{aligned}$$

Assim, provamos o resultado para $\sigma = (1\ 2)$.

Poderíamos generalizar o argumento acima para um 2-ciclo qualquer, mas existe um caminho mais fácil. Seja σ um 2-ciclo, $\sigma = (a_i\ a_j)$, temos que $(a_i\ a_j) = (1\ a_j\ 2\ a_i)(1\ 2)(1\ a_i\ 2\ a_j)$, ou seja, σ é o conjugado de $(1\ 2)$. Assim, $\sigma = \tau(1\ 2)\tau^{-1}$, para algum $\tau \in S_n$. Uma vez que ϵ é um homomorfismo, $\epsilon(\sigma) = \epsilon(\tau)\epsilon(1\ 2)\epsilon(\tau)^{-1} = \epsilon(1\ 2) = -1$. ■

Assim, se $\epsilon(\sigma) = 1$, então σ deve ser um produto de um número par de 2-ciclos. Analogamente, se $\epsilon(\sigma) = -1$, então σ deve ser um produto de um número ímpar de 2-ciclos. Portanto, σ é par se, e somente se, $\epsilon(\sigma) = 1$ e σ é ímpar se, e somente se, $\epsilon(\sigma) = -1$.

3.5 O Grupo Alternado

Na seção anterior, definimos o que significa para um elemento de S_n ser par ou ímpar. Lembre-se que $\sigma \in S_n$ é definido como sendo par se ele pode ser escrito como um produto de um número par de 2-ciclos, e é definido como sendo ímpar se ele pode ser escrito como um produto de um número ímpar de 2-ciclos.

Exemplo 3.15. A permutação $(1\ 2)(1\ 3)$ é par, uma vez que é um produto de dois 2-ciclos. Já a permutação $(1\ 2)$ é ímpar, uma vez que é um produto de um 2-ciclo.

Provamos anteriormente que um elemento de S_n é par ou ímpar, mas não ambos. A ferramenta que usamos para isso foi o homomorfismo que chamamos de sinal do homomorfismo. Lembre-se que este era um homomorfismo $\epsilon : S_n \to \{\pm 1\}$ tal que $\epsilon(\sigma) = -1$ para qualquer 2-ciclo. Uma vez que os 2-ciclos geram S_n, esta propriedade caracteriza os homomorfismos.

Assim, ϵ é um homomorfismo e $\epsilon(\sigma) = -1$ se σ é ímpar, e $\epsilon(\sigma) = 1$ se σ é par.

Exemplo 3.16. Temos que $\epsilon((1\ 2)(1\ 3)) = 1$ e $\epsilon((1\ 2)) = -1$.

Exemplo 3.17. Temos também que $\epsilon(1\ 6\ 3\ 4\ 2) = 1$ pois $(1\ 6\ 3\ 4\ 2) = (1\ 2)(1\ 4)(1\ 3)(1\ 6)$ é par.

Exemplo 3.18. Observe que se σ é um k-ciclo, então $\epsilon(\sigma) = (-1)^{k-1}$.

Observação 3.2. Observe que o produto de uma permutação par e uma permutação ímpar é ímpar. O produto de duas permutações pares ou duas permutações ímpares é par. A inversa de uma permutação par ainda á par, e a inversa de uma permutação ímpar é ímpar. Portanto, podemos definir um subgrupo de S_n que consiste em todas as permutações pares. Este grupo é conhecido como grupo alternado e é denotado por A_n.

Teorema 3.8. *Se $n \geq 3$, então A_n contém todos os 3-ciclos. Além disso, todo elemento em A_n é um produto de 3-ciclos.*

Demonstração: Pelo exemplo acima sabemos que todo 3-ciclo é uma permutação par, logo pertence a A_n.

Para a outra parte, é suficiente mostrar que o produto de quaisquer duas transposições é um produto de 3-ciclos; isso porque um elemento de A_n é um produto de um número par de transposições. Sejam $\mu_1 = (a_1\ a_2)$ e $\mu_2 = (a_3\ a_4)$ transposições de S_n. Se μ_1 e μ_2 são disjuntas (este caso exclui $n = 3$), então

$$\mu_1\mu_2 = (a_1\ a_2)(a_3\ a_4) = (a_1\ a_2)(1)(a_3\ a_4).$$

Mas, como $e = (1) = (a_2\ a_3)(a_2\ a_3)$, temos que

$$\mu_1\mu_2 = (a_1\ a_2)(a_2\ a_3)(a_2\ a_3)(a_3\ a_4) = (a_2\ a_3\ a_1)(a_3\ a_4\ a_2).$$

Caso contrário (este caso inclui $n = 3$), consideremos $\mu_1 = (a_1\ a_2)$ e $\mu_2 = (a_2\ a_3)$; logo

$$\mu_1\mu_2 = (a_1\ a_2)(a_2\ a_3) = (a_1\ a_2\ a_3).$$

Assim, toda permutação de A_n pode ser escrita como produto de 3-ciclos. ■

Exemplo 3.19. Vamos escrever a permutação

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 8 & 2 & 7 & 3 & 6 & 5 \end{pmatrix} \in S_8$$

como produto de 3-ciclos. Primeiramente, notemos que

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

Observe que $\mu_1 = (1\ 4\ 2)$ e $\mu_2 = (3\ 8\ 5\ 7\ 6)$ são permutações pares, de modo que $\alpha = \mu_1\mu_2 \in A_8$. Agora, $\mu_2 = (3\ 8\ 5\ 7\ 6) = (6\ 3)(3\ 7)(5\ 3)(3\ 8)$. Assim,

$$\mu_2 = (6\ 3)(3\ 7)(5\ 3)(3\ 8) = (6\ 3\ 7)(5\ 3\ 8).$$

Portanto,

$$\alpha = \mu_1\mu_2 = (1\ 4\ 2)(6\ 3\ 7)(5\ 3\ 8).$$

3.6 Ações de Grupos

Definição 3.12. *Uma* ***ação de grupo (à direita)*** *de um grupo $(G, *)$ sobre um conjunto (não-vazio) A é uma aplicação $A \times G \to A$ satisfazendo duas 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. *$a.e = a$ para $a \in A$, onde e é o elemento neutro de G.*

Observe que a primeira condição, $a.g_1 \in A$, logo $(a.g_1).g_2$ faz sentido. Por outro lado, $g_1 * g_2 \in G$, logo $a.(g_1 * g_2)$ também faz sentido.

Quando temos uma ação de um grupo G sobre um conjunto A, diremos apenas que "G age sobre A".

Exemplo 3.20. S_n age sobre o conjunto dos polinômios nas variáveis $x_1, ..., x_n$; de fato, usamos anteriormente está ação para provarmos a existência do homomorfismo *sinal do homomorfismo*. Ou seja, se $p(x_1, ..., x_n)$ é um polinômio, definimos p^σ por $p^\sigma(x_1, ..., x_n) = p(x_{\sigma(1)}, ..., x_{\sigma(x_n)})$ o que nos dá novamente um polinômio nas variáveis $x_1, ..., x_n$.

Exemplo 3.21. Algumas vezes, estaremos interessados no caso em que o conjunto A é o próprio grupo. Neste caso, podemos dizer que o grupo age sobre si mesmo. Por exemplo, podemos definir uma ação do grupo da seguinte forma: para $g \in G$ e $a \in G$, definimos $a.g = ag$, a operação normal do grupo de a e g. Chamamos esta ação de G sobre si mesmo de *multiplicação direita*.

Exemplo 3.22. O grupo $(\mathbb{Z}, +)$ age sobre o conjunto $\mathbb{R}$ por $a.g = g + a$ para todo $g \in \mathbb{Z}$ e $a \in \mathbb{R}$

Pois

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

para quaisquer $g_1, g_2 \in \mathbb{Z}$ e $a \in \mathbb{R}$. Alem disso, $a.0 = 0 + a = a$ para todo $a \in \mathbb{R}$.

Observação 3.3. Intuitivamente uma ação de um grupo G sobre um conjunto A significa que qualquer elemento a em G age como uma permutação sobre A de modo compatível com a operação de grupo em G.

Definição 3.13. *Se G age sobre um conjunto A, então a órbita de $a \in A$ (sob está ação) é o conjunto $\{a.g : g \in G\}$.*

Exemplo 3.23. No exemplo 3.22, mostramos que $(\mathbb{Z}, +)$ age sobre $\mathbb{R}$ por $a.g = g + a$ para todo $g \in \mathbb{Z}$ e $a \in \mathbb{R}$. Assim, a órbita de a é o conjunto $\{a + g : g \in \mathbb{Z}\}$, ou seja, o conjunto $\{..., a - 2, a - 1, a, a + 1, a + 2, ...\}$. Em particular, a, $a + 1$, $a - 1$,... têm a mesma órbita. Existe uma órbita distinta para cada $a \in [0, 1)$. Portanto, podemos pensar no conjunto das órbitas como o intervalo $[0, 1)$. No entanto, uma vez que a órbita do 0 é a mesma que a órbita do 1, podemos pensar no conjunto de órbitas de $[0, 1]$ com 0 e 1 visto como o mesmo ponto. Uma maneira de visualizar isso é imaginar dobrar o intervalo $[0, 1]$ formando um círculo de modo que os pontos 0 e 1 coincidam. Assim, é natural que se pense no conjunto de órbitas desta ação como formando um círculo.

Definição 3.14. *Se a ação de grupo tem somente uma órbita, diremos que a ação é transitiva ou que o grupo age transitivamente.*

Muitas vezes queremos provar algo sobre todos os elementos de uma órbita, o lema seguinte pode ser útil nestas situações.

Lema 3.5. *Seja G um grupo finito que age sobre um conjunto A, e seja S um conjunto de geradores de G. Seja P uma propriedade tal que a seguinte afirmação seja verdade:*

Sempre que $a \in A$ satisfaz P e $s \in S$, $a.s$ também satisfaz P

Então, se $a_0 \in A$ satisfaz P, todo elemento na órbita de a_0 também satisfaz P.

Demonstração: Vamos definir uma nova propriedade Q da seguinte forma: diremos que $g \in G$ satisfaz a propriedade Q quando a seguinte afirmação for verdadeira:

Sempre que $a \in A$ satisfaz P, $a.g$ também satisfaz P.

Assim, basta mostrar que todo $g \in G$ satisfaz a propriedade Q. Afinal de contas, isso significaria que, se $a_0 \in A$ satisfaz P, então $a_0.g$ satisfaz P para todo $g \in G$, que é exatamente o que queremos mostrar.

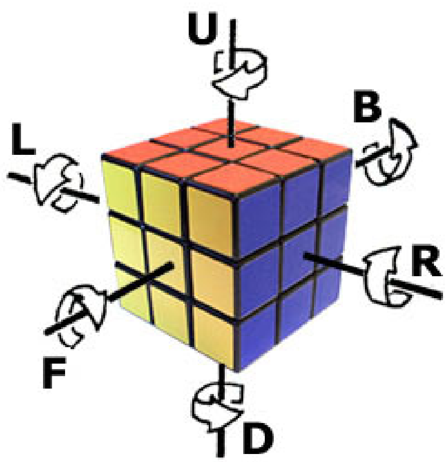
Por hipótese, todo elemento de S satisfaz a propriedade Q. Pela Proposição 3.1, precisamos mostrar que se $g, h \in G$ satisfazem a propriedade Q, então gh também satisfaz a propriedade Q. Assim, suponha que $g, h \in G$ satisfazem a propriedade Q. Para mostrar que gh também satisfaz precisamos mostrar que se $a \in A$ satisfaz a propriedade P, então $a.gh$ também satisfaz P.

Suponha que $a \in A$ satisfaz P. Uma vez que g satisfaz Q, $a.g$ satisfaz P e como h satisfaz Q, $(a.g).h$ satisfaz P. No entanto, pela definição de ação de grupo, $(a.g).h = a.gh$. Portanto provamos que se $a \in A$ satisfaz P, então $a.gh$ satisfaz P. Isto significa que gh satisfaz Q, que é o que queríamos mostrar. ■

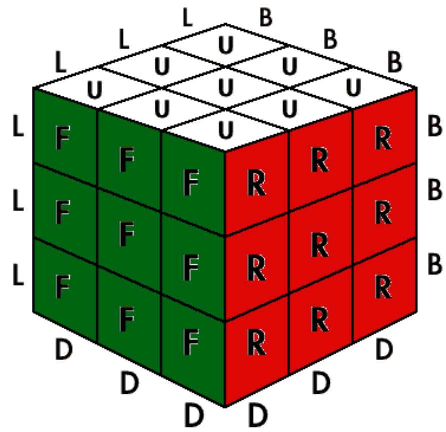
4 Cubo de Rubik

O cubo de Rubik é formado por 27 pequenos cubos, que chamaremos de *cubinhos*, dos quais 26 são visíveis. Para facilitar o estudo identificaremos os cubinhos visíveis de acordo com a quantidade de faces que ficam expostas. Os cubinhos com três faces visíveis estão localizados nos cantos, nos vértices do cubo, portanto, chamaremos esses cubinhos de *cubinhos de canto*, existem 8 cubinhos de canto. Os cubinhos com duas faces visíveis, são aqueles com uma face visível em cada uma de duas faces adjacentes do cubo de Rubik, serão chamados de *cubinhos de borda*, no cubo de Rubik existem 12 cubinhos de borda. Por fim os cubinhos que possuem apenas uma face visível, e que se localizam na parte central das faces serão chamados de *cubinhos centrais*. No cubo de Rubik existem 6 cubinhos centrais.

Usaremos a notação de David Singmaster para as faces do cubo de Rubik, as faces serão chamadas de direita (r - right), esquerta (l - left), acima (u - up), abaixo (d - down), frente (f - front) e costas (b - back), conforme figura a seguir. Cada face do cubo de Rubik a partir de agora será chamada apenas pela inicial do nome em inglês da face.



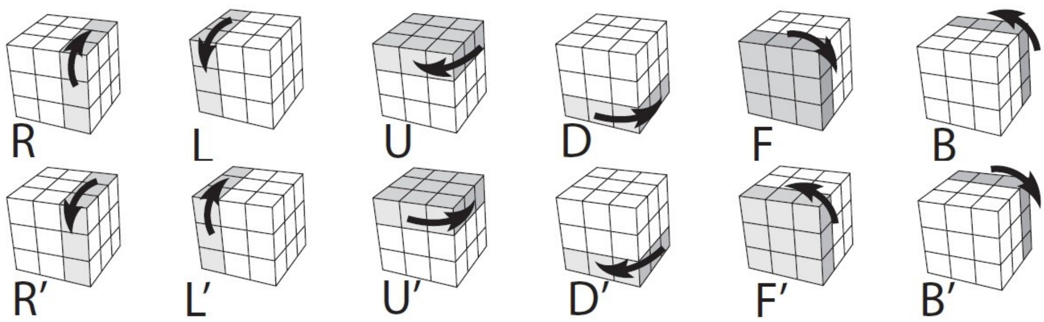
Para citar um cubinho de canto, listaremos suas faces visíveis no sentido horário, por exemplo o cubinho nas faces superior, a direita e frontal será escrito na forma urf, logicamente esse cubinho também pode ser escrito na forma rfu ou fur. Se indicarmos uma face como referência, as notações urf e rfu são diferentes, nesses casos os cubinhos serão chamados de cubinhos orientados. Caso não haja necessidade e a ordem das faces não importar, os cubinhos serão não orientados e urf e rfu representaram o mesmo cubinho.



Da mesma forma para citarmos os cubinhos de borda e os cubinhos centrais usaremos as letras correspondentes às faces, por exemplo o cubinho central localizado na face frontal será chamado de f, e o cubinho de borda localizado entre as faces acima e direita será chamado de ur.

Usaremos também o termo *cubículo*, que serão rotulados como os cubinhos, mas irão descrever o espaço em que o cubinho mora. Quando o cubo de Rubik estiver na configuração inicial (o cubo de Rubik resolvido), então cada cubinho mora no cubículo de mesmo nome (o cubinho urf mora no cubículo urf, o cubinho f mora no cubículo f e assim por diante). Se girarmos uma face do cubo de Rubik, os cubinhos irão se mover, mas os cubículos não. Observe que ao girar uma face do cubo de Rubik, os cubinhos centrais permanecem sempre no mesmo lugar.

Finalmente, daremos nomes aos movimentos de cubo de Rubik. O movimento mais básico que se pode fazer é girar uma única face. Vamos usar R para denotar uma rotação no sentido horário da face à direita (olhando para a face direita, girar 90° no sentido horário). Da mesma forma, vamos usar o letras maiúsculas L, U, D, F e B para denotar rotações de 90° no sentido horário das outras faces.



Observe que os 6 movimentos básicos irão manter os cubinhos de centro em seus cubículos. Uma vez que qualquer movimento é uma sequência destes 6 movimentos básicos, isso significa que cada movimento de cubo de Rubik mantém os cubinhos de centro em seus cubículos. Além disso, qualquer movimento do cubo de Rubik coloca cubinhos de canto em cubículos de canto e cubinhos de borda em cubículos de borda, é impossível um cubinho de canto, através de movimentos no cubo de Rubik, morar em um cubículo de borda ou para um cubinho de borda morar em um cubículo de canto.

Já observamos que os 6 movimentos básicos mantêm os cubinhos de centro em seus cubículos. Como qualquer movimento é uma sequência destes 6 movimentos básicos 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 canto em cubículos de canto e cubinhos de borda em cubículos de borda. Usando esses dois fatos, podemos começar a descobrir quantas configurações possíveis tem o cubo de Rubik. Vejamos, por exemplo, no cubículo urf, teoricamente, qualquer um dos 8 cubinhos de canto podem morar neste cubículo, assim sobram 7 cubinhos de canto que pode morar no cubículo urb, 6 para o próxima cubículo de canto, e assim por diante. Portanto, há $8.7.6.5.4.3.2.1 = 8!$ possíveis posicionamentos dos cubinhos canto. Note que um cubinho de canto pode morar em seu cubículo de 3 maneiras diferentes. Por exemplo, se um cubinho vermelho, branco, e azul encontra-se no cubículo urf, ou a face vermelha, ou a face branca, ou a face azul poderia morar na face u do cubículo (e isso determina onde as outras 2 faces moram). Como existem 8 cubinhos de canto e cada um pode morar no seu cubículo de 3 formas diferentes, existem 3^8 maneiras diferentes que os cubinhos de canto poderiam ser orientados. Portanto, existem $3^8.8!$ possíveis posições dos cubinhos de canto. Da mesma forma, uma vez que existem 12 cubinhos de borda, existem 12! posições dos cubinhos de borda; cada cubinho de borda tem 2 orientações possíveis, nos dando 2^{12} possíveis orientações dos cubinhos de borda. Logo, existem $2^{12}.12!$ possíveis configurações dos cubinhos de borda, dando um total de $2^{12}3^8 8!12!$ configurações possíveis do Cubo de Rubik. (Este número é de cerca de $5,19 \times 10^{20}$, ou 519 quintilhões!)

Embora essas configurações são teoricamente possíveis, isso não significa que as mesmas podem realmente ocorrer. Diremos que uma configuração do cubo de Rubik é **válida** desde que possa ser conseguida por uma série de movimentos da configuração inicial. Acontece que algumas dessas configurações teoricamente possíveis que contamos anteriormente não são realmente válidas.

Cubo de Rubik e a Teoria de Grupos

Podemos associar os movimentos do cubo de Rubik a um Grupo que denotaremos por $(\mathcal{G}, *)$. Os elementos de $\mathcal{G}$ são os movimentos possíveis do cubo de Rubik. Dois movimentos serão considerados iguais se resultarem na mesma configuração do cubo. Por exemplo, girar uma face 180° no sentido horário resulta na mesma configuração de um giro de 180° no sentido anti-horário. A operação do grupo será definida da seguinte forma: se M_1 e M_2 são dois movimentos, então $M_1 * M_2$ é o movimento em que primeiro faremos M_1 e em seguida M_2.

Observemos que de fato o cubo de Rubik é um grupo

$\mathcal{G}$ é fechado, uma vez que, se M_1 e M_2 são movimentos do cubo, $M_1 * M_2$ também é.

Se, denotarmos por e o elemento neutro (o movimento que não altera a configuração do cubo), então $M * e$ significa primeiro o movimento M e depois não fazer outro movimento, isto é certamente o mesmo que executar somente o movimento M, logo $M * e = M$ e portanto $(\mathcal{G}, *)$ tem elemento neutro.

Para qualquer movimento M, podemos inverter os passos, executar os passos de M ao contrário, e assim executar o movimento M', de modo que o movimento M' coloca o cubo na configuração anterior ao movimento M, ou seja executar o movimento M e em seguida o movimento contrario M', o cubo não sofrerá alteração na sua configuração, assim sendo $M * M' = e$, assim sendo M' é o movimento inverso de M.

Por fim, mostraremos que $*$ é associativa. Vale lembrar que cada movimento é definido pela mudança de configuração do Cubo de Rubik que ele provoca.

Se C é um cubinho orientado, chamaremos de $M(C)$ o cubículo orientado em que C se encontra após o movimento M ser executado, com as faces de $M(C)$ escritas na mesma ordem que as faces de C, ou seja, a primeira face de C deve acabar na primeira face de $M(C)$. Por exemplo, o movimento R coloca o cubinho ur no cubículo br, com a face u do cubinho localizado na face b do cubículo e a face r do cubinho localizada na face r do cubículo. Assim sendo, $R(ur) = br$.

Primeiro, vamos investigar o que uma sequencia de dois movimentos faz com o cubo. Dados M_1 e M_2, dois movimentos, e $M_1 * M_2$ é o movimento dado pelo movimento

M_1 seguido do movimento M_2. O movimento M_1 move C para o cubículo $M_1(C)$ e o movimento M_2, move C do cubículo $M_1(C)$ para o cubículo $M_2(M_1(C))$. Portanto $M_1 * M_2 = M_2(M_1(C))$.

Para mostrar que $*$ é associativa, temos que provar que $(M_1 * M_2) * M_3 = M_1 * (M_2 * M_3)$, para quaisquer movimentos M_1, M_2 e M_3, ou seja, que $(M_1 * M_2) * M_3$ e $M_1 * (M_2 * M_3)$ provocam o mesmo a qualquer cubinho. Mostraremos, então que $[(M_1 * M_2) * M_3)](C) = [(M_1 * (M_2 * M_3))](C)$ para quaisquer cubinhos. Sabe-se 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, $[M1 * (M2 * M3)](C) = [(M2 * M3)]M1(C) = M3(M2(M1(C)))$, então, temos que $(M_1 * M_2) * M_3 = M_1 * (M_2 * M_3)$ e, portanto, $*$ é associativa.

Logo, verificamos que $(\mathcal{G}, *)$ é um grupo.

Usaremos, a partir de agora a notação $\mathcal{G}$ para indicar o grupo $(\mathcal{G}, *)$ e DR, por exemplo, para indicar o movimento D seguido do movimento R. O movimento que gira a face r $90°$ no sentido anti-horário é o mesmo que o movimento que girar R três vezes no sentido horário e portanto será representado por R^3.

Exemplo 4.1. Uma prova formal da afirmação feita anteriormente de que qualquer movimento do cubo de Rubik mantém os cubículos centrais em seus cubículos é dada da seguinte forma: seja $S = \{D, U, L, R, F, B\} \subset \mathcal{G}$. Todo elemento $M \in S$ satisfaz a propriedade "M mantém todos os cubinhos de centro em seus cubículo." Se $M_1, M_2 \in \mathcal{G}$ são movimentos que mantêm todos os cubinhos centrais em seus cubículos, então $M_1 * M_2$ certamente manterá todos os cubículos de centro em seus cubículos. Uma vez que $\mathcal{G} = \langle S \rangle$, a Proposição 3.1 nos diz que todo elemento de $\mathcal{G}$ manterá os cubinhos de centro em seus cubículos.

Podemos escrever cada movimento do cubo de Rubik, com uma notação de ciclos levemente modificada. Assim, queremos descrever o que acontece com cada cubinho orientado, ou seja, queremos descrever onde cada cubinho esta depois de um movimento e o que acontece com suas faces.

Por exemplo, se desdobrarmos o cubo e mostrarmos a face abaixo (d - down),

	f	f	f	
l	d	d	d	r
l	d	d	d	r
l	d	d	d	r
	b	b	b	

e girarmos essa face 90° no sentido horário, ou seja, aplicar o movimento D, a face que continua visível é a face abaixo.

	l	l	l	
b	d	d	d	f
b	d	d	d	f
b	d	d	d	f
	r	r	r	

Então $D(dlf) = dfr$, porque o cubinho dlf agora ocupa o cubículo dfr, ou seja, a face d do cubinho esta ocupando a face d do cubículo, a face l do cubinho ocupando a face f do cubículo e a face f do cubinho ocupando a face r do cubículo. Da mesma forma, $D(dfr) = drb$, $D(drb) = dbl$ e $D(dbl) = dlf$. Se fizermos a mesma coisa para os cubinhos de borda, encontramos $D = (dlf\ dfr\ drb\ dbl)(df\ dr\ db\ dl)$.

4.0.1 As configurações do cubo de Rubik

Temos que a configuração do cubo de Rubik é determinada por quatro informações, que são:

- A posição dos cubinhos de canto
- A posição dos cubinhos de borda
- A orientação dos cubinhos de canto
- A orientação dos cubinhos de borda

A primeira pode ser descrita como um elemento σ de S_8 (isto é, um elemento de S_8 que move os cubinhos de canto a partir de suas posições originais, para as suas novas posições). A segunda pode ser descrito como um elemento τ de S_{12}. O que precisamos agora é entender o que acontece na terceira e quarta informações.

A ideia é fixar uma orientação de partida, e a partir daí escrever de uma forma sistemática como uma determinada orientação difere da orientação original.

Comecemos pelos cubinhos de canto, cada cubinho de canto tem três possíveis orientações, que serão numeradas da seguinte forma 0, 1 e 2. Vamos entender o que esses números significam. Imagine o cubo de Rubik na sua configuração inicial, escreveremos um número em uma face de cada cubículo de canto, assim como descrito a seguir:

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

Agora, cada cubículo de canto tem exatamente uma face numerada. Cada cubinho de canto agora tem uma face situada sob uma face numerada de um cubículo. Nesta face do cubinho, marque o número 0, em seguida, no sentido horário marque a próxima face desse cubo com 1, e por último, a última face desse cubo com o número 2.

Exemplo 4.2. Se olharmos diretamente para a face de baixo e desdobrar o cubo, as faces dos cubinhos ficariam assim:

	f	f	f	
l	d	d	d	r
l	d	d	d	r
l	d	d	d	r
	b	b	b	

Assim, as numerações dos cubículo ficariam como segue:

	6		7	
	5		8	

Portanto, as faces dos cubinhos ficariam

	2		1	
1	0		0	2
2	0		0	1
	1		2	

Agora, cada face de cada cubinho de canto tem um número. No cubo de Rubik, em qualquer configuração, podemos descrever as orientações dos cubinhos de canto da seguinte forma: para qualquer i, com $1 \leq i \leq 8$, encontre o cubículo com a face numerada com o número i, seja x_i o número da face do cubinho que está localizado na face numerada desse cubículo. Agora escreveremos a 8-upla ordenada $(x_1, x_2, ..., x_8)$. Observe que podemos pensar cada x_i como sendo o número de giros no sentido horário das faces do cubinho i de tal maneira que a face 0 do cubinho coincida com a face numerada do cubículo. Mas um cubinho que é girado três vezes sempre é orientado da mesma maneira que um cubinho que foi girado 0 vezes. Assim, podemos pensar no x_i como sendo um elemento de $\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$. Então, x é uma 8-upla de elementos de $\mathbb{Z}/3\mathbb{Z}$, escreveremos $x \in (\mathbb{Z}/3\mathbb{Z})^8$.

Exemplo 4.3. Se o cubo de Rubik está na configuração de inicial, cada x_i é 0. Podemos escrever $x = 0$ denotar que cada x_i é 0.

Exemplo 4.4. Veremos o que acontece com cada x_i quando aplicamos o movimento R para um cubo na configuração inicial. Na configuração inicial, para a face à direita temos:

	u	u	u	
f	r	r	r	b
f	r	r	r	b
f	r	r	r	b
	d	d	d	

Os números dos cubículo nesta face são

	2		3	
	7		8	

Portanto, a numeração dos cubinhos de canto ficariam:

	0		0	
2	1		2	1
1	2		1	2
	0		0	

Se girarmos a face à direita do cubo em 90º, então a face do cubo ficaria

	1		2	
0	2		1	0
0	1		2	0
	2		1	

Observe que os cubinhos na face esquerda não são afetados por R, logo $x_1 = 0$, $x_4 = 0$, $x_5 = 0$, e $x_6 = 0$. Agora, podemos ver pelos nossos 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 seguir o mesmo raciocínio para os cubinhos de borda. Primeiro, vamos rotular os cubículos de borda como se segue:

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

Agora, cada cubinho de borda tem uma face situada sob uma face numerada de um cubículo; neste face do cubinho marque o número 0, e na outra face da cubinho marque o número 1. Assim, seja y_i o número da face do cubinho que está localizada na face numerada do cubículo i. Logo, teremos que $y \in (\mathbb{Z}/2\mathbb{Z})^{12}$.

Logo, qualquer configuração do cubo de Rubik pode ser descrita por $\sigma \in S_8$, $\tau \in S_{12}$, $x \in (\mathbb{Z}/3\mathbb{Z})^8$ e $y \in (\mathbb{Z}/2\mathbb{Z})^{12}$. Portanto escreveremos as configurações de cubo de Rubik como 4-uplas ordenadas (σ, τ, x, y).

Exemplo 4.5. A configuração inicial é descrita por $(1, 1, 0, 0)$.

Exemplo 4.6. Imagine que o cubo está na configuração inicial e seja (σ, τ, x, y) a configuração do cubo depois de fazer o movimento $[D, R]$, o qual é definida pelo movimento $DRD^{-1}R^{-1}$. Vamos encontrar σ, τ, x e y.

Como sabemos, $D = (dlf\ dfr\ drb\ dbl)(df\ dr\ db\ dl)$ e $R = (rfu\ rub\ rbd\ rdf)(ru\ rb\ rd\ rf)$. Além disso $D^{-1} = (dbl\ drb\ dfr\ dlf)(dl\ db\ dr\ df)$ e $R^{-1} = (rdf\ rbd\ rub\ rfu)(rf\ rd\ rb\ ru)$. Logo

$$[D, R] = (dlf\ dfr\ lfd\ frd\ fdl\ rdf)(drb\ bru\ bdr\ ubr\ rbd\ rub)(df\ dr\ br) \tag{4.1}$$

Lembremos que τ é um elemento de S_{12}; assim, pensamos nele como um bijeção de um conjunto com 12 cubinhos de borda não orientados para um conjunto de 12 cubículos de borda. Assim, ele é definido por: se C é um cubinho de borda não orientado na configuração inicial, então $\tau(C)$ é o cubículo de borda não orientado onde C está na configuração atual. Como qualquer elemento de S_{12}, τ pode ser escrito em notação de ciclos disjuntos.

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

Analogamente, pensamos em σ como uma bijeção de um conjunto com 8 cubinhos de canto não orientados para um conjunto de 8 cubículos de canto não orientados. Para encontrar σ, devemos descobrir o que $[D, R]$ faz com as posições dos cubinhos de canto. Observe que $[D, R]$ muda as posições dos cubinhos dfl e dfr, e também muda as posições de drb e bru. Portanto, $\sigma = (drb\ bru)(dfl\ dfr)$.

Pela definição de x que foi dada anteriormente temos que na posição inicial, todos as faces numeradas dos cubículos tem cubinhos com faces numeradas com o 0. Uma vez que o movimento $[D, R]$ não afeta os cubinhos ufl, urf, ulb ou dbl, temos que x_1, x_2, x_4 e x_5 devem ser 0. Para encontrarmos x_3, queremos descobrir qual face do cubinho está sob a face u do cubículo ubr. Por (4.1) temos que $[D, R]$ coloca a face b do cubinho drb sob a face u do cubículo ubr; pelo nosso método de numeração, a face b do cubinho drb é numerada com o 2, logo $x_3 = 2$. Analogamente, $x_6 = 2$, $x_7 = 0$ e $x_8 = 2$. Portanto $x = (0, 0, 2, 0, 0, 2, 0, 2)$.

Analogamente, vamos encontrar y utilizando o método de numeração descrito acima. Uma vez que $[D, R]$ afeta somente os cubinho de borda df, dr e br temos que somente y_{11}, y_{10} e y_6 podem ser diferentes de zero. Como $[D, R]$ coloca a face b do cubinho br sob a face d do cubículo df, $y_{11} = 0$. Analogamente, $y_{10} = 0$ e $y_6 = 0$. Portanto $y = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.

Uma questão que pode surgir é "Por que usarmos a notação de (σ, τ, x, y) para descrever as configurações do cubo de Rubik uma vez que parece muito mais fácil obtê-las diretamente de (4.1)?". A principal razão é que escrever σ, τ, x e y separadamente nos permite reconhecer padrões mais facilmente e consequentemente prová-los.

Podemos definir um homomorfismo $\phi_{canto} : \mathcal{G} \to S_8$ da seguinte maneira: qualquer movimento em $\mathcal{G}$ certamente reorganiza os cubinhos de canto de alguma forma, assim, define uma permutação dos 8 cubinhos de canto não orientados. Ou seja, qualquer $M \in \mathcal{G}$ define uma permutação $\sigma \in S_8$. Assim $\phi_{canto}(M) = \sigma$ é um elemento de S_8 o qual descreve o que M faz com o cubinhos de canto não orientados. Por exemplo, sabemos que $[D, R]$ tem uma decomposição em ciclos disjuntos $(dlf\ dfr\ lfd\ frd\ fdl\ rdf)(drb\ bru\ bdr\ ubr\ rbd\ rub)(df\ dr\ br)$. Portanto $\phi_{canto}(M) = (dlf\ dfr)(drb\ bru)$.

Analogamente definimos um homomorfismo $\phi_{borda} : \mathcal{G} \to S_{12}$ de tal forma que $\phi(M)$ é um elemento de S_{12} o qual descreve o que M faz com os 12 cubinhos de borda não orientados. Por exemplo $\phi_{borda}([D, R]) = (df\ dr\ br)$.

Por fim, definimos um homomorfismo $\phi_{cubo} : \mathcal{G} \to S_{20}$, o qual descreve permutações dos 20 cubinhos, 12 de borda e 8 de canto, não orientados. Por exemplo, $\phi_{cubo}([D, R]) = (dlf\ dfr)(drb\ bru)(df\ dr\ br)$.

Assim, dado $M \in \mathcal{G}$ o movimento de girar uma face (ou seja, M é D, U, L, R, F ou B), então $\phi_{cubo}(M)$ é o produto de 2 4-ciclos. Como um 4-ciclo é ímpar, o produto de 2 4-ciclos será par. Assim, $\phi_{cubo}(M)$ é par. Uma vez que os giros das faces geram $\mathcal{G}$, isto significa que $\phi_{cubo}(M)$ é par para todo $M \in \mathcal{G}$, ou seja, $\phi_{cubo}(M) \in A_{20}$ para todo $M \in \mathcal{G}$.

Observe que $\phi_{cubo}(M) = \phi_{canto}(M)\phi_{borda}(M)$, sendo assim $\phi_{canto}(M)$ e $\phi_{borda}(M)$ são ambos pares ou ambos ímpares, ou seja, $\phi_{canto}(M)$ e $\phi_{borda}(M)$ têm o mesmo sinal.

Suponha o cubo na configuração inicial e faça um movimento M de tal forma que termina na configuração (σ, τ, x, y) onde $\sigma = \phi_{canto}(M)$ e $\tau = \phi_{borda}(M)$. Assim temos que se (σ, τ, x, y) é uma configuração válida, então σ e τ têm o mesmo sinal.

Uma vez que A_n consiste de todos os elementos pares de S_n, A_n pode ser descrito como $\{\sigma \in S_n : \epsilon(\sigma) = 1\}$.

Observe também que o núcleo do homomorfismo $\phi_{cubo} : \mathcal{G} \to S_{20}$ consiste de todos os movimentos do cubo de Rubik que não altera as posições de quaisquer cubinhos, ou seja, $ker(\phi_{cubo})$ consiste de todos os movimentos os quais alteram somente orientações e não as posições dos cubinhos.

Consideremos agora alguma configuração $C = (\sigma, \tau, x, y)$, fazendo um movimento $M \in G$ colocamos o cubo de Rubik em uma nova configuração, denotaremos está nova configuração por $C.M$.

Supondo o cubo na configuração C, aplicando o movimento M_1, obtemos a configuração $C.M_1$. Aplicando outro movimento M_2, obtemos a configuração $(C.M_1).M_2$. Por outro lado, o que realmente fizemos é dada uma configuração C e aplicamos o movimento M_1M_2, assim podemos escrever a nova configuração por $C.(M_1M_2)$, ou seja, mostramos que $(C.M_1)M_2 = C.(M_1M_2)$ para qualquer configuração C e movimentos $M_1, M_2 \in G$. Seja $e \in G$ onde e é o movimento que não altera a configuração, temos que $C.e = C$. Sendo assim, mostramos que o grupo $\mathcal{G}$ age sobre o conjunto das configurações do cubo de Rubik.

Observe que a órbita de uma configuração inicial sob essa ação é exatamente o conjunto das configurações válidas do cubo de Rubik.

4.1 Configurações Válidas do Cubo de Rúbik

O objetivo dessa seção será usar os conceitos e propriedades apresentados anteriormente para caracterizarmos as configurações válidas do cubo de Rubik. Para isso, provaremos o seguinte teorema:

Teorema 4.1. *Uma configuração (σ, τ, x, y) é válida se, e somente se, o sinal de sigma é igual o sinal de τ, $\sum x_i \equiv 0\ (mod\ 3)$ e $\sum y_i \equiv 0\ (mod\ 2)$.*

Usaremos o resto desta seção para demonstrarmos o teorema anterior. Primeiro mostremos que se (σ, τ, x, y) é válida, então o sinal de σ é igual ao sinal de τ, $\sum x_i \equiv 0\ (mod\ 3)$ e $\sum y_i \equiv 0\ (mod\ 2)$. No processo, vamos provar alguns fatos um pouco mais gerais que serão úteis para provarmos a recíproca do teorema.

Lembremos que $\mathcal{G}$ age sobre o conjunto de configurações do cubo de Rubik. As configurações válidas formam uma única órbita desta ação.

Lema 4.1. *Se (σ, τ, x, y) e (σ', τ', x', y') estão na mesma órbita, então $\epsilon(\sigma)\epsilon(\tau) = \epsilon(\sigma')\epsilon(\tau')$.*

Demonstração: Pelo Lema 3.5, é suficiente mostrar que se

$$(\sigma', \tau', x', y') = (\sigma, \tau, x, y).M,$$

onde M é um dos movimento básicos, então $\epsilon(\sigma)\epsilon(\tau) = \epsilon(\sigma')\epsilon(\tau')$. Observe que $\sigma' = \sigma\phi_{canto}(M)$ e $\tau' = \tau\phi_{borda}(M)$. Portanto

$$\epsilon(\sigma')\epsilon(\tau') = \epsilon(\sigma)\epsilon(\phi_{canto}(M))\epsilon(\tau)\epsilon(\phi_{borda}(M)).$$

Se M é um dos seis movimentos básicos, então $\phi_{canto}(M)$ e $\phi_{borda}(M)$ são ambos 4-ciclos, portanto ambos têm sinal -1. Portanto $\epsilon(\sigma')\epsilon(\tau') = \epsilon(\sigma)\epsilon(\tau)$. ■

Corolário 4.1. *Se (σ, τ, x, y) é uma configuração válida, então $\epsilon(\sigma) = \epsilon(\tau)$.*

Demonstração: Isto é uma consequência imediata do lema acima uma vez que qualquer configuração válida está na mesma órbita da configuração inicial $(1, 1, 0, 0)$.

Lema 4.2. *Se* (σ', τ', x', y') *está na mesma órbita que* (σ, τ, x, y)*, então* $\sum x'_i \equiv \sum x_i \ (mod\ 3)$ *e* $\sum y'_i \equiv \sum y_i \ (mod\ 2)$*.*

Demonstração: Seguindo a ideia do lema anterior, é suficiente mostrar que se $(\sigma', \tau', x', y') = (\sigma, \tau, x, y).M$ onde M é um dos seis movimentos básicos, então $\sum x'_i \equiv \sum x_i \ (mod\ 3)$ e $\sum y'_i \equiv \sum y_i \ (mod\ 2)$. Abaixo segue uma tábua mostrando o que acontece com x' e y' se $(\sigma', \tau', x', y') = (\sigma, \tau, x, y).M$ onde M é um dos seis movimentos básicos. Em cada caso, é fácil ver que $\sum x'_i \equiv \sum x_i \ (mod\ 3)$ e $\sum y'_i \equiv \sum y_i \ (mod\ 2)$

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	$(x_1, x_2, x_8 + 1, x_3 + 2, x_4 + 1, x_6, x_7, x_5 + 2)$
	$(y_6 + 1, y_2, y_3, y_4, y_1 + 1, y_9 + 1, y_7, y_8, y_5 + 1, y_{10}, y_{11}, y_{12})$

Como exemplo, vamos ver como encontrar x' quando M é o movimento R. Assim, os cubículos da face da direita ficariam como abaixo:

	u	u	u	
f	r	r	r	b
f	r	r	r	b
f	r	r	r	b
	d	d	d	

Os cubículos são numerados como segue:

	2		3	
	7		8	

Portanto, se o cubo de Rubik está na configuração (σ, τ, x, y), os cubinhos sob a face direita são numerados como segue:

	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	

Se rotacionarmos essa face em 90° no sentido horário, então os cubinhos ficam como segue:

	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	

Portanto, $x' = (x_1, x_7+1, x_2+2, x_4, x_5, x_6, x_8+2, x_3+1)$. Logo, $\sum x'_i = \sum x_i + 6 \equiv \sum x_i \ (mod\ 3)$. ■

Corolário 4.2. *Se (σ, τ, x, y) é uma configuração válida, então $\sum x_i \equiv 0 \ (mod\ 3)$ e $\sum y_i \equiv 0 \ (mod\ 2)$.*

Demonstração: Isto é uma consequência do lema acima, uma vez que uma configuração válida está na órbita da configuração inicial $(1, 1, 0, 0)$. ■

Assim, provamos uma direção do Teorema 4.1. Agora vamos mostrar a recíproca. Suponha que $\epsilon(\sigma) = \epsilon(\tau)$, $\sum x_i \equiv 0 \ (mod\ 3)$ e $\sum y_i \equiv 0 \ (mod\ 2)$. Queremos mostrar que existe uma série de movimentos que, quando aplicados a (σ, τ, x, y), nos darão a configuração inicial, ou seja, se o cubo de Rubik está na configuração (σ, τ, x, y), ele pode ser solucionado. A ideia da demonstração é basicamente anotar os passos necessários para solucionar o cubo de Rubik. Assim, vamos provar as seguintes afirmações:

1. Se (σ, τ, x, y) é uma configuração tal que $\epsilon(\sigma) = \epsilon(\tau)$, $\sum x_i \equiv 0 \ (mod\ 3)$ e $\sum y_i \equiv 0 \ (mod\ 2)$, existe um movimento $M \in \mathcal{G}$ tal que $(\sigma, \tau, x, y).M$ é da forma

$(1, \tau', x', y')$ com $\epsilon(\tau') = 1$, $\sum x_i' \equiv 0$ $(mod\ 3)$ e $\sum y_i' \equiv 0$ $(mod\ 2)$. Ou seja, podemos colocar os cubinhos de canto nas posições corretas.

2. Se $(1, \tau, x, y)$ é uma configuração com $\epsilon(\tau) = 1$, $\sum x_i \equiv 0$ $(mod\ 3)$ e $\sum y_i \equiv 0$ $(mod\ 2)$, existe um movimento $M \in \mathcal{G}$ tal que $(1, \tau, x, y).M$ é da forma $(1, \tau', 0, y')$ com $sgn\ \tau' = 1$ e $\sum y_i' \equiv 0$ $(mod\ 2)$. Ou seja, podemos colocar os cubinhos de canto nas orientações corretas (e posições).

3. Se $(1, \tau, 0, y)$ é uma configuração com $\epsilon(\tau) = 1$ e $\sum y_i \equiv 0$ $(mod\ 2)$, existe um movimento $M \in \mathcal{G}$ tal que $(1, \tau, 0, y).M$ é da forma $(1, 1, 0, y')$ com $\sum y_i' \equiv 0$ $(mod\ 2)$. Ou seja, podemos colocar todos os cubinhos de borda nas posições corretas (sem perturbar os cubinhos de canto).

4. Se $(1, 1, 0, y)$ é uma configuração com $\sum y_i \equiv 0$ $(mod\ 2)$, existe um movimento $M \in \mathcal{G}$ tal que $(1, 1, 0, y).M$ é da forma $(1, 1, 0, 0)$. Que significa que podemos solucionar o cubo.

Porém, antes de provarmos estas afirmações, destacamos o seguinte fato. Suponha-se que (σ, τ, x, y) satisfaz $\epsilon(\sigma) = \epsilon(\tau)$, $\sum x_i \equiv 0$ $(mod\ 3)$ e $\sum y_i \equiv 0$ $(mod\ 2)$. Então, os Lemas 4.1 e 4.2 mostram que, para qualquer (σ', τ', x', y') na mesma órbita que (σ, τ, x, y),$\epsilon(\sigma') = \epsilon(\tau')$, $\sum x_i' \equiv 0$ $(mod\ 3)$ e $\sum y_i' \equiv 0$ $(mod\ 2)$. Assim, por exemplo, na primeira afirmação acima, se provarmos que existe um movimento $M \in \mathcal{G}$ de tal modo que $(\sigma, \tau, x, y)M$ tem a forma $(1, \tau', x', y')$, é imediato que $\epsilon(\tau') = 1$, $\sum x_i' \equiv 0$ $(mod\ 3)$, e $\sum y_i' \equiv 0$ $(mod\ 2)$. Portanto, para finalizar a demonstração do Teorema 4.1, basta que provemos as seguintes proposições.

Proposição 4.1. *Se (σ, τ, x, y) é uma configuração com $\epsilon(\sigma) = \epsilon(\tau)$, $\sum x_i \equiv 0$ $(mod\ 3)$ e $\sum y_i \equiv 0$ $(mod\ 2)$, então a órbita de (σ, τ, x, y) contém alguma configuração na forma $(1, \tau', x', y')$.*

Proposição 4.2. *Se $(1, \tau, x, y)$ é uma configuração com $\epsilon(\tau) = 1$, $\sum x_i \equiv 0$ $(mod\ 3)$ e $\sum y_i \equiv 0$ $(mod\ 2)$, então a órbita de $(1, \tau, x, y)$ contém alguma configuração da forma $(1, \tau', 0, y')$.*

Proposição 4.3. *Se $(1, \tau, 0, y)$ é uma configuração com $\epsilon(\tau) = 1$ e $\sum y_i \equiv 0$ $(mod\ 2)$, então a órbita de $(1, \tau, 0, y)$ contém alguma configuração da forma $(1, 1, 0, y')$.*

Proposição 4.4. *Se $(1, 1, 0, y)$ é uma configuração com $\sum y_i \equiv 0$ $(mod\ 2)$, então a órbita de $(1, 1, 0, y)$ contém alguma configuração da forma $(1, 1, 0, 0)$.*

Provaremos estas afirmações em ordem, assim a primeira que provaremos é que podemos colocar os cubinhos de canto nas posições corretas.

Lema 4.3. *O homomorfismo $\phi_{canto} : \mathcal{G} \to S_8$ é sobrejetor.*

Demonstração: Pelo Corolário 3.2, S_8 é gerado por um conjunto S de 2-ciclos em S_8. Assim, é suficiente mostrar que $S \subset Im\ \phi_{canto}$. De fato, se $S \subset Im\ \phi_{canto}$, então $S_8 = \langle S \rangle \subset \langle Im\ \phi_{canto} \rangle$, além disso, como $\langle Im\ \phi_{canto} \rangle$ é um grupo, temos que $\langle Im\ \phi_{canto} \rangle = Im\ \phi_{canto}$.

Assim, queremos mostrar que cada 2-ciclo de S_8 pertence a imagem de ϕ_{canto}. Observe que o movimento $M_0 = ([D, R]F)^3 = (dbr\ urb)(dr\ uf)(br\ rf)(df\ lf)$ muda apenas 2 cubinhos de canto e deixa os outros cubinhos de canto fixo. Então, $\phi_{canto}(M_0) = (dbr\ urb)$. Assim, pelo menos $(dbr\ urb)$ encontra-se na imagem de ϕ_{canto}.

Sejam C_1 e C_2 um par qualquer de cubinhos do canto. É fácil perceber que sempre existe um movimento $M \in \mathcal{G}$ o qual envia dbr para C_1 e urb para C_2. Seja $\sigma = \phi_{canto}(M)$, assim, $\sigma(dbr) = C_1$ e $\sigma(urb) = C_2$. Uma vez que ϕ_{canto} é um homomorfismo, temos

$$\begin{aligned} \phi_{canto}(M^{-1}M_0M) &= \phi_{canto}(M)^{-1}\phi_{canto}(M)_0\phi_{canto}(M) \\ &= \sigma^{-1}(dbr\ urb)\sigma \\ &= (\sigma(dbr)\ \sigma(urb)) \\ &= (C_1\ C_2) \end{aligned}$$

Portanto, $(C_1\ C_2) \in Im\ \phi_{canto}$, o que termina a demonstração. ■

Demonstração da Proposição 4.1: Pelo lema anterior, existe um movimento $M \in \mathcal{G}$ tal que $\phi_{canto}(M) = \sigma^{-1}$. Assim, $(\sigma, \tau, x, y).M = (1, \tau', x', y')$ para algum $\tau' \in S_{12}$, $x' \in \mathbb{Z}_3^8$ e $y' \in \mathbb{Z}_2^{12}$. ■

Em seguida, vamos provar a Proposição 4.2. A ideia aqui é orientar todos os cubinhos de canto corretamente usando movimentos que mudam as orientações de apenas 2 cubinhos. Em primeiro lugar, temos de mostrar que existem tais movimentos.

Lema 4.4. *Sejam C_1 e C_2 dois cubinhos de canto quaisquer, existe um movimento $M \in \mathcal{G}$, que altera as orientações (mas não as posições) de C_1 e C_2 e que não afeta os outros cubinhos de canto. Além disso, existe tal movimento M que gira C_1 no sentido horário e C_2 no sentido anti-horário.*

Demonstração: Como na prova do Lema anterior, a questão é primeiramente encontrar um único movimento M_0, que altera as orientações de 2 cubinhos e depois conjugar M_0 para encontrar movimentos que mudam as orientações de 2 cubinhos. Um movimento com essa propriedade é dado por $M_0 = (DR^{-1})^3(D^{-1}R)^3$, o qual tem uma decomposição em ciclos disjuntos dada por $(dfr\ rdf\ frd)(drb\ rbd\ bdr)(df\ dr\ fr\ ur\ br\ db\ dl)$. Assim, $\phi_{canto}(M_0) = 1$ e $\psi_{canto}(M_0) = (dbr\ rdb\ brd)(drf\ rfd\ fdr)$, onde a aplicação ψ mostra o que o movimento M_0 faz com as orientações dos cubinhos de canto dbr e drf. Logo, se $C_1 = dbr$ e $C_2 = drf$, o lema é verdadeiro.

Agora, vamos conjugar este movimento. Como sempre existe um movimento $M \in \mathcal{G}$ que envia dbr para C_1 e drf para C2. Seja $M' = M^{-1}M_0M$, pelo Teorema 3.5 podemos encontrar $\psi_{canto}(M')$, podemos ver que M' muda as orientações do C_1 e C_2 e não afeta os outros cubinhos de canto. Especificamente, M' gira C_1 no sentido horário e C_2 no sentido anti-horário. ■

Demonstração da Proposição 4.2: Suponha que o cubo de Rubik está em uma configuração em que pelo menos dois cubinhos de canto C_1 e C_2 não estão nas orientações corretas. Pelo Lema 4.4, existe um movimento que gira C_1 no sentido horário, gira C_2 no sentido anti-horário e não afeta os outros cubinhos de canto. Aplicando este movimento uma ou duas vezes, podemos garantir que C_1 tem a orientação correta. Uma vez que este movimento não afeta nenhum cubinho de canto, além de C_1 e C_2, o cubo de Rubik agora tem um cubinho de canto a menos com uma orientação incorreta. Fazendo isso várias vezes, acabamos com uma configuração $(1, \tau', x', y')$, onde há no máximo um cubinho de canto com orientação incorreta. Isto é, pelo menos, 7 dos x_i' são 0. Pelo Lema 4.2, $\sum x_i' \equiv \sum x_i \equiv 0\ (mod\ 3)$, assim este é o caso em que o último x_i' também é 0, logo a configuração do cubo de Rubik é $(1, \tau', 0, y')$. ■

Agora, iremos provar Proposição 4.3; ou seja, queremos corrigir as posições dos cubinhos de borda. A ideia da demonstração é muito semelhante ao que usamos para provar a Proposição 4.2. Lembre-se que, nesse caso, primeiro provamos que ϕ_{canto} é sobrejetora. Neste caso, queremos usar somente movimentos que não afetam os cubinhos de canto, uma vez que já obtemos os cubinhos de canto nas posições e orientações corretas. Portanto, em vez de olhar diretamente para ϕ_{borda}, vamos olhar para ϕ_{borda} restrito a $ker\ \psi_{canto}$.

Lema 4.5. *A imagem de* $\phi_{borda} : ker\psi_{canto} \to S_{12}$ *contém* A_{12}.

Demonstração: Pelo Teorema 3.8 temos que A_{12} é gerado por um conjunto de 3-ciclos em A_{12}. Pelo mesmo argumento da demonstração do Lema 4.3, é suficiente mostrar que todo 3-ciclo está na imagem de $\phi_{borda}|_{ker\ \psi_{canto}}$. Como na demonstração do Lema 4.3, a estratégia é usar a conjugação de um único movimento.

Temos que $M_0 = LR^{-1}U^2L^{-1}RB^2$ é um movimento de cubinhos de borda, o qual é um 3-ciclo, e que não afeta nenhum cubinho de canto que tem decomposição em ciclos disjuntos dada por $(ub\ uf\ db)$. Então, $M_0 \in ker\psi_{canto}$, e $\phi_{borda}(M_0) = (ub\ uf\ db)$. Agora, se C_1, C_2 e C_3 são quaisquer 3 cubinhos de borda, existe um movimento M do cubo de Rubik que envia ub para C_1, uf para C_2, e db para C_3. Então, seja $\sigma = \phi_{borda}(M)$, temos

$$
\begin{aligned}
\phi_{borda}(M^{-1}M_0M) &= \phi_{canto}(M)^{-1}\phi_{borda}(M)_0\phi_{borda}(M) \\
&= \sigma^{-1}(ub\ uf\ db)\sigma \\
&= (\sigma(ub)\ \sigma(uf)\ \sigma(db)) \\
&= (C_1\ C_2\ C_3)
\end{aligned}
$$

Portanto, $(C_1\ C_2\ C_3) \in Im\phi_{borda}|_{ker\psi_{canto}}$, o que completa a demonstração. ■

Assim, a Proposição 4.3 segue diretamente do Lema 4.5. (A prova é exatamente a mesma ideia que a prova da Proposição 4.1.)

Por último, provaremos a Proposição 4.4. A qual é similar a Proposição 4.2; antes precisamos de um lema parecido com o Lema 4.4.

Lema 4.6. *Se C_1 e C_2 são dois cubinhos quaisquer, existe um movimento $M \in G$ o qual muda as orientações (mas não a posições) de C_1 e C_2 e que não altera os outros cubinhos.*

Demonstração: Queremos primeiramente encontrar um movimento que muda as orientações de 2 cubinhos de borda sem afetar quaisquer outros cubinhos, um tal movimento é dado por

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

Chamaremos este movimento de M_0, ele tem uma decomposição em ciclos dada por $(fu\ uf)(bu\ ub)$. Assim, dados C_1 e C_2 são quaisquer cubinhos de borda diferentes, existe $M \in \mathcal{G}$ enviando uf para C_1 e ub para C_2. Assim, MM_0M^{-1} altera as orientações de C_1 e C_2 e não afeta todos os outros cubinhos.

Agora, o argumento que foi utilizado para provar a Proposição 4.2 prova a Proposição 4.4 também. Isso completa a prova do Teorema 4.1.

5 Considerações Finais

Neste trabalho, fizemos o estudo de uma aplicação da teoria de grupos para a investigação da quantidade de possíveis configurações de um brinquedo mundialmente conhecido, o cubo de Rubik.

Abordamos conceitos elementares de matemática assim como alguns conceitos um pouco mais avançados da álgebra, como o estudos de algumas propriedades envolvendo a teoria de grupos.

Tivemos como objetivo também mostrar que algumas perguntas que podem aparecer no nosso cotidiano, por exemplo na manipulação de um brinquedo bastante popular, podem ser respondidas através de conceitos matemáticos abstratos que nem sempre são muito atrativos para os estudantes mas que quando usados de maneiras corretas nos fornecem belíssimas soluções.

Observamos por fim que, antes de toda a analise de validade de movimentos, tínhamos que o total de possibilidades de se colocar os cubos em suas posições era dado por $3^8 * 8! * 2^{12} * 12!$, e que esse total de possibilidades poderia ser dividido em 24 partes iguais, visto que, σ poderia ser par ou impar, τ pode ser par ou impar, x $\in \mathbb{Z}_3$ e y $\in \mathbb{Z}_2$. Assim sendo 2*2*3*2 = 24. Apos estudo e demonstração da validade do teorema 4.1 temos que para que os movimentos da resolução do cubo sejam validos σ e τ possuem o mesmo sinal, portanto, temos somente 2 possibilidades de isso acontecer e, $\sum x_i \equiv 0\ (mod\ 3)$ e $\sum y_i \equiv 0\ (mod\ 2)$, logo somente um resto nos interessa tanto para o somatório de x quanto para o somatório de y, portanto, dos 24 grupos antes analisados somente 2 são validos. portanto somente 1/12 de $3^8 * 8! * 2^{12} * 12!$ de soluções são válidas.

Referências

[1] CHEN, Janet. Group Theory and the Rubik's Cube. 2004.

[2] DOMINGUES, Hygino H.; IEZZI, Gelson. Álgebra moderna. São Paulo: Editora Atual, 2003.

[3] IEZZI, Gelson; MURAKANI, Carlos. Fundamentos da Matemática Elementar: conjuntos e funções. Atual Editora: São Paulo: 2005.

[4] VIEIRA, Vandenberg Lope. Álgebra abstrata para licenciatura. Campina Grande: EDUEPB, 2013.

[5] http://www.cubovelocidade.com.br/info/historia-do-cubo-magico.html

[6] http://guiadoscuriosos.com.br/blog/2014/05/19/40-curiosidades-dos-40-anos-do-cubo-magico/

[7] http://www.matematica.br/historia/grupos.html