# O GRUPO DE PERMUTAÇÕES E UMA APLICAÇÃO NO CUBO DE RUBIK

HELENA DUARTE VILELA[1]; ANDREA MORGADO[3]

[1] *Universidade Federal de Pelotas - helvilela@gmail.com*
[3] *Universidade Federal de Pelotas - andrea.morgado@ufpel.edu.br*

## 1. INTRODUÇÃO

A teoria de grupos é uma teoria clássica dentro da Álgebra Abstrata. Essa teoria surgiu nos trabalhos sobre a solubilidade por radicais de equações polinomiais de Evariste Galois (1811-1832), entretanto quem atribuiu o primeiro conceito moderno de grupo foi Arthur Cayley (1821-1895) com a frase "Um grupo é definido por meio de leis que combinam seus elementos". Um exemplo importante dessa definição é o grupo de permutações, no qual alguns resultados envolvendo esse conceito podem ser visualizados no cubo de Rubik. Por sua vez, o cubo de Rubik é um quebra-cabeça tridimensional inventado por Ernő Rubik em 1974 e é conhecido por seu desafio de reverter a um estado de cores uniformes cada uma de suas faces. Podemos associar os movimentos no cubo de Rubik a um subgrupo do grupo de permutações. Neste trabalho, exploramos uma aplicação de um resultado envolvendo o grupo de permutações no cubo de Rubik.

## 2. METODOLOGIA

Este trabalho foi conduzido por meio de um estudo de diversos tópicos abordados nos livros e artigos incluídos na bibliografia, com foco específico na aplicação ao Cubo de Rubik. O processo de pesquisa envolveu não apenas a leitura e análise das fontes, mas também a interpretação e adaptação dos conceitos ao contexto do projeto.

## 3. RESULTADOS E DESENVOLVIMENTO

A seguir serão apresentadas algumas definições e resultados que serão aplicados ao Cubo de Rubik. Estes resultados são clássicos da literatura e podem ser encontrados nas referências [1], [2] e [4].

**Definição 1:** Seja $G$ um conjunto não vazio munido de uma operação $* : G \times G \to G$. Dizemos que $(G, *)$ é um *grupo* se satisfizer:
(i) Para quaisquer elementos $x$, $y$ e $z \in G$ tem-se que $(x * y) * z = x * (y * z)$;
(ii) Existe $e \in G$ tal que $x * e = x = e * x$, para todo $x \in G$;
(iii) Para todo $x \in G$, existe $x' \in G$ tal que $x * x' = e = x' * x$.

Mais ainda, se $(G, *)$ é um grupo tal que para quaisquer $x, y \in G$ tem-se $x * y = y * x$, dizemos que $(G, *)$ é um *grupo abeliano ou comutativo*.

**Definição 2:** Sejam $(G, *)$ um grupo e $H$ um subconjunto não vazio de $G$. Dizemos que $H$ é um *subgrupo de* $G$ se $(H, *)$ é um grupo.

Seja $S$ um conjunto não vazio de um grupo $(G, *)$. Definimos o conjunto gerado por $S$ como:

$$\langle S \rangle = \{x_1 * x_2 * \ldots * x_n : x_i \in S \text{ ou } x_i \in S^{-1}\}, \text{ onde } S^{-1} = \{x_i^{-1} : x_i \in S\}.$$

É provado que $\langle S \rangle$ é um subgrupo de $G$ denomidado *subgrupo gerado por* $S$.

Consideremos $x \in G$ e $n$ um número inteiro. Definimos $x^n$ da seguinte maneira: se $n = 0$, então $x^0 = e$; se $n > 0$, então $x^n = x^{n-1} * x$; se $n < 0$, então $x^n = (x^{-n})'$, onde $(x^{-n})'$ denota o elemento simétrico de $x^{-n}$ em relação à operação $*$ do grupo $G$.

**Definição 3:** Nas condições anteriores definimos a *ordem do elemento* $x \in G$ como sendo, se existir, o menor número inteiro positivo $n$ tal que $x^n = e$ e neste caso denotaremos $\mathcal{O}(x) = n$. No caso de tal número inteiro não existir dizemos que a ordem de $x$ é infinita e denotaremos $\mathcal{O}(x) = \infty$.

Um importante exemplo de grupos é o grupo de permutações. A seguir apresentaremos sua definição e alguns conceitos e resultados importantes para o trabalho.

**Grupo de Permutações:** Seja $S$ um conjunto finito com $n$ elementos. Definimos $S_n$ como sendo o conjunto de todas as bijeções (ou permutações) de $S$ sobre si mesmo, ou seja, $S_n = \{f : S \to S : \ f \text{ é função bijetiva}\}$. Temos que $S_n$ é um grupo munido da operação de composição de funções chamado *grupo das permutações de* $n$ *elementos*. É fácil verificar que a composição de funções é associativa, o elemento neutro de $S_n$ é a função identidade e todo elemento possui inverso pois estamos considerando apenas as funções bijetivas de $S$ em $S$.

**Ciclo e Comprimento do Ciclo:** Um ciclo é uma permutação que move elementos em uma sequência cíclica, deixando todos os outros elementos não envolvidos no ciclo fixos. Por exemplo, se $(a_1\, a_2\, \ldots\, a_r)$ é um ciclo em $S_n$, temos que $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \cdots, \sigma(a_{r-1}) = a_r, \sigma(a_r) = a_1$ e $\sigma(i) = i$, para todo $i \in S - \{a_1\, a_2\, \ldots\, a_r\}$. Neste caso, dizemos que $\sigma$ é um $r$-ciclo e que seu comprimento é $r$, pois número total de elementos envolvidos no ciclo é $r$. Além disso, a ordem de um $r$-ciclo é $r$. Um exemplo de $3$-ciclo em $S_5$ é dado por $(1\ 2\ 3)$, onde $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, $4 \mapsto 4$ e $5 \mapsto 5$.

Dizemos que os ciclos $\sigma = (a_1 a_2 \cdots a_{k-1} a_k)$ e $\tau = (b_1 b_2 \cdots b_{l-1} b_l)$ em $S_n$ são *disjuntos* se $\{a_1, a_2, \cdots, a_{k-1}, a_k\} \cap \{b_1, b_2, \cdots, b_{l-1}, b_l\} = \emptyset$.

**Teorema 1:** Seja $\sigma$ uma permutação em $S_n$. Então, $\sigma$ pode ser escrita de forma única como um produto de ciclos disjuntos.

**Teorema 2:** Sejam $\sigma_1, \ldots, \sigma_t \in S_n$ ciclos disjuntos de comprimentos $r_1, \ldots, r_t$, respectivamente. A ordem do produto $\sigma_t \ldots \sigma_1$ é igual ao $\mathrm{mmc}(r_1, \ldots, r_t)$, onde $\mathrm{mmc}$ é a abreviação de mínimo múltiplo comum.

**Cubo de Rubik:** A seguir, exploraremos a estrutura do cubo, nomearemos suas faces e delinearemos os movimentos fundamentais. Os resultados trabalhados aqui podem ser encontrados em [3] e [5]. As faces do cubo serão denominadas como Front (F), Back (B), Upper (U), Down (D), Left (L) e Right (R).

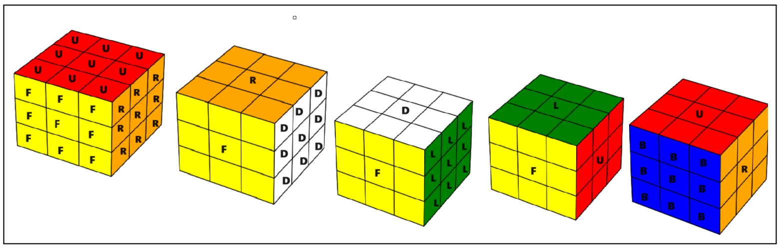

Figura 1: Faces do cubo

As faces do cubo podem girar um quarto ou meia volta, tanto no sentido horário quanto anti-horário. Os movimentos de um quarto de volta no sentido horário são indicados por $F$, $B$, $U$, $D$, $L$ e $R$. Já as rotações no sentido anti-horário, que representam o movimento inverso, são denotadas por $K'$ para uma face $K$. A sequência de movimentos no cubo pode ser expressa usando essas notações. Vamos destacar o movimento $U$ e seu respectivo inverso $U'$. As demais faces são movidas de maneira análoga, porém em direções diferentes. Para uma compreensão adequada, considere que o cubo está inicialmente em sua forma homogênea antes de efetuar qualquer movimentação. O movimento designado por $U$ consiste em girar a face superior (Upper) no sentido horário por um quarto de volta. O movimento inverso, indicado por $U'$, implica girar essa mesma face por um quarto de volta no sentido anti-horário.

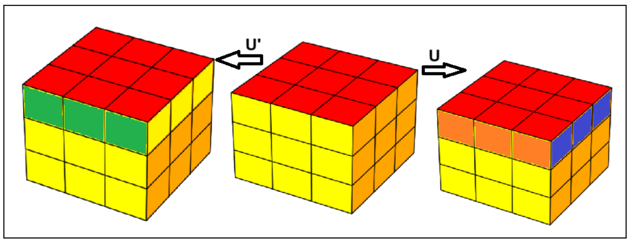


Figura 2: Movimento $U$ e $U'$

Utilizando as definições acima, podemos analisar as permutações das facetas do Cubo de Rubik. Os movimentos $R$, $L$, $F$, $B$, $U$ e $D$ correspondem a permutações específicas das facetas do cubo. Estes movimentos podem ser vistos como permutações das 54 faces visíveis, das quais 6 permanecem fixas. Podemos planificar o cubo e atribuir números às faces que podem ser permutadas:

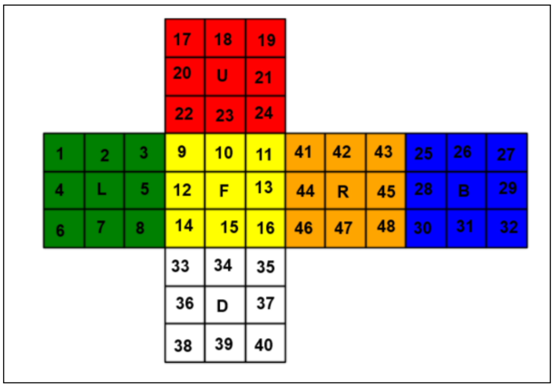


Figura 3: Cubo planificado

Obtemos correspondências para cada movimento, a seguir apresentamos somente as que serão usadas neste trabalho.

$$\begin{aligned}
U &= (1,25,41,9)(2,26,42,10)(3,27,43,11)(22,17,19,24)(20,18,21,23)\\
U' &= (18,20,23,21)(17,22,24,19)(27,3,11,43)(2,10,42,26)(1,9,41,25)\\
R &= (11,19,30,35)(13,21,28,37)(16,24,25,40)(46,41,43,48)(44,42,45,47)\\
R' &= (44,47,45,42)(46,48,43,41)(16,40,25,24)(13,37,28,21)(11,35,30,19)
\end{aligned}$$

Assim, cada movimento específico do Cubo de Rubik pode ser formalmente descrito por uma permutação das facetas numeradas, conforme a planificação apresentada.

**Definição 4:** Definimos o *grupo de Rubick* como sendo o subgrupo de $(S_{48}, \circ)$ gerado pelo conjunto $X = \{R, L, F, B, U, D\}$ , ou seja,

$$\mathcal{GR} =< R, L, F, B, U, D >= \{x_1 x_2 \cdots x_n : x_i \in X \text{ ou } x_i \in X^{-1}\}.$$

Chamaremos de macro um elemento de $\mathcal{GR}$, ou seja, uma sequência de movimentos no cubo é descrita pela ordem dos códigos de rotação, escritos da esquerda para a direita, considerando a face frontal como referência (durante a execução de uma macro, a face frontal não deve ser alterada). Assim, vamos utilizar o Teorema 2 para determinar a ordem da macro $T = URU'R'$. Notemos que podemos escrever a macro $T$ como:

$$T = (1, 25, 27, 43, 17, 19)(11, 35, 41, 46, 24, 16)(13, 18, 21)(26, 42, 44)$$

onde $T$ é composto por dois $6$ ciclos e dois $3$-ciclos. Pelo Teorema 2, a ordem de $T$ é dada por $\mathcal{O}(T) = \mathrm{mmc}(6, 6, 3, 3) = 6$.

## 4. CONCLUSÕES

Este trabalho proporcionou uma ampliação significativa do conhecimento sobre a teoria de grupos, aplicada de forma concreta a um problema prático, que normalmente não é abordado nos cursos de Licenciatura em Matemática. Ademais, permitiu uma nova perspectiva sobre o uso da álgebra, demonstrando como conceitos teóricos podem ser aplicados de maneira inovadora e prática, como no caso da manipulação do cubo de Rubik.

## 5. REFERÊNCIAS BILIOGRÁFICAS

[1] ARMSTRONG, M.A. **Groups and Symmetry**. New York: Springer-Verlag, 1988.

[2] GARCIA, A., LEQUAIN, Y. **Elementos de Álgebra**. 6ª edição. Rio de Janeiro: IMPA, 2012.

[3] GRIMM, L.G.H.M. **Cubo Mágico: Propriedades e Resoluções envolvendo Álgebra e Teoria de Grupo**. Rio Claro, 2016. Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exata.

[4] GONÇALVES, A. **Introdução à Álgebra**. 5ª edição. Rio de Janeiro: IMPA, 2012.

[5] SANTOS, J.O. **Álgebra no Cubo de Rubik**. Macapá, 2010. Monografia (Licenciatura Plena em Matemática) - Universidade Federal do Amapá.