FUNDAÇÃO GETULIO VARGAS
ESCOLA DE MATEMÁTICA APLICADA

LUCA ESCOPELLI

CUBO DE RUBIK COMO UM GRUPO ALGÉBRICO

Rio de Janeiro
2023

LUCA ESCOPELLI

CUBO DE RUBIK COMO UM GRUPO ALGÉBRICO

Trabalho de conclusão de curso apresentada para a Escola de Matemática Aplicada (FGV/EMAp) como requisito para o grau de bacharel em Matemática Aplicada.

Área de estudo: álgebra.

Orientador: Moacyr Alvim

Rio de Janeiro

2023

Agradecimentos

Lembre de agradecer a quem te apoiou, como, por exemplo, orientador, família, agência de fomento, professores conselheiros.

"Se eu vi mais longe, foi por estar sobre ombros de gigantes."
Isaac Newton

Resumo

Segundo a o resumo deve ressaltar o objetivo, o método, os resultados e as conclusões do documento. A ordem e a extensão destes itens dependem do tipo de resumo (informativo ou indicativo) e do tratamento que cada item recebe no documento original. O resumo deve ser precedido da referência do documento, com exceção do resumo inserido no próprio documento. (. . .) As palavras-chave devem figurar logo abaixo do resumo, antecedidas da expressão Palavras-chave:, separadas entre si por ponto e finalizadas também por ponto. Deve ser redigido na terceira pessoa do singular e quanto a sua extensão, o resumo deve ter de 150 a 500 palavras.

Palavras-chave: latex. abntex. editoração de texto.

Abstract

É a tradução do resumo para o inglês (Abstract), com a finalidade de facilitar a divulgação do trabalho em nível internacional.

Keywords: latex. abntex. editoração de texto.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ABNT	Associação Brasileira de Normas Técnicas
abnTeX	ABsurdas Normas para TeX

Lista de símbolos

Γ	Letra grega Gama
Λ	Lambda
ζ	Letra grega minúscula zeta
$\in$	Pertence

Sumário

1 Introdução

O cubo de Rubik, também conhecido como cubo mágico, é um brinquedo inventado em 1974 por Ernő Rubik, um professor húngaro de arquitetura. O objeto foi criado com a intenção de desenvolver a capacidade de visualização espacial em seus alunos. Ao começar a brincar com sua nova invenção, o professor rapidamente percebeu a complexidade que o brinquedo poderia tomar com apenas alguns movimentos, tanto que levou mais de 30 dias para conseguir solucionar o puzzle. Ainda antes da invenção de Rubik, Larry D. Nichols já havia desenvolvido um objeto semelhante a uma versão 2x2x2 do cubo, com uma estrutura utilizando imãs para segurar as peças, porém não conseguiu obter a mesma popularidade da versão 3x3x3.

Desde sua invenção, o cubo foi um objeto de admiração por todas as pessoas que o conhecem. Por se tratar de um objeto com uma mecânica simples, mas com uma enorme complexidade, se tornou um dos brinquedos mais populares de todo o mundo. Esse fascínio pelo "não tão simples" cubo foi o que motivou o desenvolvimento desse estudo em relação à invenção de Rubik e suas variações.

O presente trabalho utiliza das ferramentas da teoria dos grupos, dentro do estudo da álgebra, aplicadas ao cubo para encontrar propriedades interessantes do objeto. A teoria dos grupos introduz o conceito de um grupo matemático, que consiste em um conjunto de elementos juntos de uma operação, de tal forma que a operação seja associativa, exista um elemento neutro e todo elemento possua seu inverso. Com isso em mente, é possível trabalhar com o cubo como um grupo, em que cada estado de embaralhamento é um elemento do conjunto e as operações são os movimentos de rotação das faces.

Uma das interessantes propriedades do cubo e objeto de estudo desse trabalho é o chamado "número de Deus". Esse número se refere ao número mínimo de movimentos suficiente para resolver qualquer estado de embaralhamento do cubo, i.e. independente do estado inicial do cubo, existe uma sequência de movimentos de tamanho menor ou igual à esse valor que resolve o puzzle. Para o cubo tradicional (3x3x3) esse número foi provado ser 20 (ROKICKI et al., 2014). Será apresentado como foi feito esse processo de descoberta e como técnicas semelhantes podem ser aplicadas na variação mais simples, o cubo de Nichols (2x2x2,) para descobrir seu Número de Deus, que é o objetivo principal desse estudo.

O trabalho está dividido da seguinte forma:

Seção 2 - Introdução à teoria de grupos: O conteúdo em questão sera apresentado, contemplando suas definições, propriedades e os principais atributos que serão utilizados para o problema principal.

Seção 3 - Análise de estudos anteriores: Será feita uma passagem pelos estudos anteriores relacionados a esse conteúdo para compreender as técnicas utilisadas e dificuldades encontradas.

Seção 4 - Apresentação dos experimentos: As técnicas e conteúdos aprensentados pelas seções anteriores serão utilizadas em experimentos para conseguir o valor do Número de Deus para o Cubo 2x2x2.

Seção 5 - Conclusão: Será apresentado os resultados obtidos pelo estudo além de desafios encontrados e possíveis futuros avanços no assunto.

2 Introdução à teoria de grupos

2.1 Definição

Um grupo é definido como um conjunto não-vazio (G) junto de uma operação binária ($\cdot$) que leva dois elementos de G a outro elemento do grupo e que respeita as 3 propriedades mostradas a seguir. Podemos escrever o grupo G com a notação (G, $\cdot$) para indicar que o grupo é formado pelo conjunto G e pela operação $\cdot$.

Um grupo sempre deve respeitar as propriedades de associatividade, existência de elemento neutro e existência de inverso.

Associatividade: Sejam a, b e c elementos quaisquer de G, devemos ter que:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$$

Existência de elemento neutro: Todo grupo deve possuir um elemento neutro (e) que leve qualquer elemento nele mesmo, assim temos:

$$a \cdot e = e \cdot a = a \quad \forall a \in G$$

Existência de elemento inverso: Para todo elemento a de um grupo deve existir no mesmo grupo o elemento inverso a^{-1} que leve-o ao elemento neutro, temos então:

$$\forall a \in G, \quad \exists a^{-1} \in G$$
$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

2.1.1 Exemplos

1. Grupo dos inteiros com a operação de soma ($\mathbb{Z}$, +):

$$a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Z}$$
$$0 = e, \quad a + 0 = 0 + a = a \quad \forall a \in \mathbb{Z}$$
$$a + (-a) = (-a) + a = 0 \quad \forall a \in \mathbb{Z}$$

2. Grupo dos racionais com a operação de soma $(\mathbb{Q}, +)$:

$$a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Q}$$
$$0 = e, \quad a + 0 = 0 + a = a \quad \forall a \in \mathbb{Q}$$
$$a + (-a) = (-a) + a = 0 \quad \forall a \in \mathbb{Q}$$

3. Grupo dos reais não nulos com a operação de multiplicação $(\mathbb{R}^*, \cdot)$:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in \mathbb{R}^*$$
$$1 = e, \quad a \cdot 1 = 1 \cdot a = a \quad \forall a \in \mathbb{R}^*$$
$$a \cdot a^{-1} = a^{-1} \cdot a = 0 \quad \forall a \in \mathbb{R}^*$$

Note que nesse caso não podemos incluir o 0 pois não possui inverso.

Apesar dos exemplos acima serem compostos por conjuntos de infinitos elementos, isso não é necessário, podemos ter grupos de qualquer tamanho, veja:

4. Grupo trivial $(\{0\}, +)$:

$$0 + (0 + 0) = (0 + 0) + 0 = 0$$
$$0 = e, \quad 0 + 0 = 0 + 0 = 0$$
$$0 + 0 = 0 + 0 = 0$$

Note que esse é um grupo de um conjunto com apenas 1 elemento. Além disso, percebemos que para qualquer operação sempre é possível criar um grupo trivial com o conjunto sendo apenas o elemento nulo da respectiva operação.

5. Grupo do anel das classes de congruência módulo 2 com a operação de soma $(\mathbb{Z}_2, +)$:

$$a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Z}_2$$
$$0 = e, \quad a + 0 = 0 + a = a \quad \forall a \in \mathbb{Z}_2$$
$$a + (-a) = (-a) + a = 0 \quad \forall a \in \mathbb{Z}_2$$

Note que nesse exemplo o conjunto possui apenas 2 elementos (0 e 1) e esse caso pode ser estendido para qualquer valor de congruência, indicando que o conjunto de um grupo pode ser de qualquer tamanho.

6. Grupo do anel das classes não nulas de congruência módulo p, sendo p primo, com a operação de multiplicação $(\mathbb{Z}_p^*, \cdot)$:

Multiplicação é associativa.

1 é elemento neutro da multiplicação, então $1 = e$ nesse caso.

Pelo pequeno teorema de Fermat $a^{p-1} \equiv 1 \pmod{p}$, portanto $a \cdot a^{p-2} \equiv 1 \pmod{p}$ $\implies a^{p-2} \equiv a^{-1}$

2.2 Subgrupos

Dado um grupo G, chamamos H de um subgrupo de G (indicamos por $H \leq G$) se H está contido em G ($H \subseteq G$) e H é um grupo com a mesma operação associada a G.

Como H deve ser um grupo também, é necessário que o elemento neutro esteja em H ($e \in H$). Além disso, como G é subconjunto de G e é um grupo, temos que G é subgrupo de G. Assim, podemos afirmar que todo grupo possui 2 subgrupos triviais, apenas o elemento neutro e o próprio grupo.

$$\{e\} \leq G \quad \forall G$$
$$G \leq G \quad \forall G$$

Chamamos de subgrupos próprios (ou não-triviais) todos os subgrupos diferentes dos mecionados acima.

Temos que um subconjunto H de G é subgrupo se e somente se:

- O elemento neutro pertence a H ($e \in H$)
- A operação de dois elementos de H leva a um elemento em H ($ab \in H \quad \forall a, b \in H$)
- O inverso de qualquer elemento de H está em H ($a^{-1} \in H \quad \forall a \in H$)

Note que a associatividade em H vem diretamente da associatividade em G.

2.2.1 Exemplos

O conjunto dos inteiros é subconjunto dos racionais. Como os dois conjuntos formam, individualmente, grupos com a operação de soma, podemos falar que os inteiros são um subgrupo dos racionais nessa operação. Além disso, ambos são subgrupos dos reais, que por sua vez são subgrupos dos complexos.

O conjunto definido por $n\mathbb{Z} = \{nx | x \in \mathbb{Z}\},\ n \in \mathbb{Z}$ é subgrupo dos inteiros com a operação de soma, veja:

$$n0 = 0$$

$$na + nb = n(a + b)$$

$$n(-a) = -na$$

Percebemos acima que as 3 propriedades são satisfeitas.

Um detalhe importante a se notar, sabemos que o anel das classes de congruência módulo 2 (exemplo 5 de grupo) é um subconjunto dos inteiros, no entanto não é considerado um subgrupo pois as operações em questão são diferentes. Note que em um caso o inverso de 1 é -1 e no outro é o próprio 1.

Um exemplo de subgrupo envolvendo anéis pode ser obtido considerando as classes módulo 4 ($\{0, 1, 2, 3\}$) com a operação de soma, em que podemos tomar o subgrupo próprio ($\{0, 2\}$), pois:

$$0 = e$$

$$2 + 2 \equiv 0 \quad (mod\ 4)$$

Como vemos, o subconjunto possui o elemento neutro, todas operações de elementos do subconjunto levam a outro elemento do subconjunto e todos elementos possuem inverso dentro do subconjunto.

2.3 Conjunto gerador de um grupo

Definimos como conjunto gerador de um grupo um subconjunto S tal que todos elementos do grupo G podem ser obtidos por uma combinação finita dos elementos de S, ou seus inversos, sob a operação do grupo. Escrevemos então $G = \langle S \rangle$.

No caso particular de S ser um conjunto unitário ($S = \{s\}$) temos que:

$$G = \langle S \rangle = \langle \{s\} \rangle = \{s^n | n \in \mathbb{Z}\}$$

Nesse caso, chamamos G de grupo cíclico e denotamos apenas por $G = \langle s \rangle$.

Para os casos gerais, temos que:

$$\langle S \rangle = \{s_1 s_2 \cdots s_n | n \in \mathbb{N}, s_i \in S \cup S^{-1}\}$$

Sendo S^{-1} o conjunto dos inversos de S. Note que, como consequência direta da definição, $\langle S \rangle = \langle S^{-1} \rangle$.

2.3.1 Exemplos

- $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

  O grupo dos inteiros com a operação de soma é ciclíco gerado pelo elemento 1 (ou pelo -1).

- $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$

  O grupo dos múltiplos de n com a operação de soma é ciclíco gerado pelo elemento n (ou pelo -n).

- Potências de $2 = \langle 2 \rangle = \langle 2^{-1} \rangle$

  O grupo das potências de 2 é gerado pelo 2 considerando a operação de multiplicação.

- $\langle \{2, 3\} \rangle$

  O grupo do produto entre potências de 2 e potências de 3 é gerado pelo conjunto $\{2, 3\}$ junto com a operação de multiplicação.

Esse conceito fornece uma ferramenta prática muito importante para criação de grupos interessantes para determinados problemas. Visto que, dado um conjunto e uma operação que faça sentido, podemos gerar um grupo utilizando a ideia de conjunto gerador sem a preocupação de conhecer todos elementos individualmente. Mais adiante, veremos a aplicação dessa ideia no estudo em questão.

2.4 Classes laterais

Dado um subgrupo H de G ($H \leq G$), definimos as classes laterais à esquerda ou à direita de H, respectivamente, como:

Dado $x \in G$:

$$xH = \{x \cdot h | h \in H\}$$

$$Hx = \{h \cdot x | h \in H\}$$

As classes laterais são subconjuntos de G, no entanto, não são subgrupos, pois não possuem o elemento neutro. Podemos perceber isso, pois $x, h \in G \implies xh \in G \implies xH \subset G$, porém $x \notin H \implies xh \notin H \implies e \notin xH$, logo xH não é subgrupo (para a classe à direita é analogo). Um detalhe importante é de que consideramos $x \notin H$, isso pode ser utilizado, visto que, caso $x \in H$ teremos que $xH = H$ e não faz sentido considerarmos a classe lateral nesse caso.

Além disso, forma-se um bijeção natural entre H e xH. Note que $x \in G \implies x^{-1} \in G$ logo $xh_1 = xh_2 \implies x^{-1}xh_1 = x^{-1}xh_2 \implies h_1 = h_2$, portanto a cardinalidade de qualquer classe lateral é a mesma e é igual à cardinalidade de H.

Temos também que dados $x, y \in G \backslash H$ com $x \notin yH$ então as classes laterais xH e yH não possuem elementos em comum. Vamos provar isso por contradição.

$$h_1, h_2 \in H, \quad xh_1 = yh_2 \implies x = yh_2h_1^{-1} \implies x \in yH$$

Absurdo, logo $xH \cap yH = \emptyset$.

Além disso, se $x \in yH$ então $xH = yH$, pois $\exists h_1$ tal que $x = yh_1 \implies xH = yh_1H = yH$.

Como todo elemento de G pode gerar sua classe lateral, e acabamos de verificar que todas as classes laterais são disjuntas (desconsiderando os casos de classes equivalentes) e possuem a mesma cardinalidade (igual à cardinalidade de H), temos que as classes laterais formam uma partição muito interessante do grupo G original. Adicionalmente, como todo subgrupo possui classes laterais, temos para cada subgrupo uma partição diferente do grupo principal.

Essa propriedade é muito interessante para o nosso problema, pois permite a divisão do desafio em desafios menores e disjuntos. Veremos mais adiante como isso é feito na prática.

3 Estudos anteriores

4 Apresentação dos experimentos

Nosso objeto de estudo é o cubo mágico de dimensões 2x2x2. Como a ideia do trabalho é aplicar a teoria de grupos ao cubo, nosso primeiro desafio é transformar o objeto em um grupo algébrico.

Antes de fazer isso, vamos entender como é a estrutura dessa versão menor do brinquedo. O 2x2x2 é formado apenas por 8 cubinhos menores, cada um possuindo 3 cores e dispostos nos vértices do cubo. Fazendo uma comparação com o 3x3x3, é como se só tivéssemos as peças de canto do cubo. Dado esse formato, temos uma diferença bem relevante que é a de não possuir peças fixas, portanto, não há definição prévia de qual face deverá ser qual cor quando o cubo estiver resolvido. Com isso, podemos "fixar" uma peça para simplificar o problema e evitar casos que são iguais exceto por uma operação de rotação do cubo. Essa fixação será feita tomando uma peça qualquer e mantendo sempre ela no lugar correto, ou seja, antes de executar movimentos no cubo, vamos rotacioná-lo para colocar a peça no lugar estabelecido sem executar movimentos. Em seguida, vamos aplicar movimentos no cubo que não alterem a posição dessa peça (verificaremos adiante como isso é feito).

Para fazer isso, vamos utilizar a mesma ideia dos estudos anteriores. Os elementos do grupo são representados por uma sequência de movimentos e cada uma dessas sequências gera um embaralhamento no cubo a partir do estado inicial (resolvido). No nosso grupo, o elemento neutro é representado pela não execução de movimentos, ou seja, manter o cubo resolvido. Como notação, vamos utilizar I para representar esse caso (uma referência à matriz identidade). Da mesma forma que já vimos para o cubo tradicional, os movimentos são associativos e cada movimento possui um inverso (girar a mesma face no sentido oposto e o mesmo número de vezes).

Essa ideia de transformar o cubo em um grupo é exatamente a mesma que apresentamos para a versão 3x3x3, no entanto, o que vamos diferenciar aqui serão os movimentos. Já apresentamos na versão tradicional que os movimentos possíveis são relacionados às faces R, L, F, B, U, D. Porém, no cubo 2x2x2, girar a face da direita no sentido horário gera o mesmo resultado de girar a face esquerda no anti-horário, exceto por uma rotação do cubo. O mesmo ocorre para os outros pares de faces opostas e outros sentidos de rotação de face. Com isso, podemos simplificar nosso caso e utilizar somente os movimentos R, F e U, i.e. o grupo é gerado apenas por esses movimentos $G_2 = \langle R, F, U \rangle$. Note que, com esses movimentos, a peça do canto traseiro, inferior, esquerdo nunca será movida, portanto essa será a peça que teremos fixada, como mencionado anteriormente.

5 Conclusão

Parte final do trabalho, apresenta as conclusões correspondentes aos objetivos ou hipóteses.

Referências

ROKICKI, Tomas et al. The Diameter of the Rubik's Cube Group Is Twenty. **SIAM Review**, v. 56, n. 4, p. 645–670, 2014. DOI: 10.1137/140973499. Disponível em: <https://doi.org/10.1137/140973499>.

"