Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Grupos e algumas aplicações

Victor Rafael Araujo de Noronha
Mestrado Profissional em Matemática: PROFMAT/SBM

Orientadora: **Profa. Dra. Eunice Cândida Pereira Rodrigues**

Trabalho financiado pela Capes

Cuiabá - MT

Julho de 2014

Grupos e algumas aplicações

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Victor Rafael Araujo de Noronha e aprovada pela comissão julgadora.

Cuiabá, 15 de agosto de 2014.

Profa. Dra. Eunice Cândida P. Rodrigues
Orientador

Banca examinadora:

Profa. Dra. Eunice C. Pereira Rodrigues
Profa. Dra. Luciene Pinheiro Lopes
Profa. Dr. Martinho da Costa Araújo

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

N852g Noronha, Victor Rafael Araujo de.
Grupos e algumas aplicações / Victor Rafael Araujo de Noronha. -- 2014
xiii, 42 f. : il. color. ; 30 cm.

Orientadora: Eunice Cândida Pereira Rodrigues.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2014.
Inclui bibliografia.

1. Grupo. 2. Números negativos. 3. Cubo mágico. 4. Criptografia. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Dissertação de Mestrado defendida em 17 de Julho de 2014 e aprovada pela banca examinadora composta pelos Professores Doutores

---

Profa. Dra. Eunice Cândida Pereira Rodrigues

Profa. Dra. Luciene Pinheiro Lopes

Prof. Dr. Martinho da Costa Araújo

A minha avó (in memorian) que, mesmo não estando mais entre nós, participou desta vitória.

Agradecimentos

Embora um dissertação seja um trabalho individual, nada teria sido possível sem a ajuda e a generosidade constantes de muitos, a quem quero deixar aqui o meu imenso agradecimento.

A Deus, pelo dom da vida e por em permitir mais essa conquista.

Aos meus pais, Valdir e Eliane, pela sabedoria, pelo amor e pelo apoio ilimitado.

Ao meu irmão, João Paulo, pelo estímulo e carinho.

A minha orientadora, Eunice, pela competência e ajuda na construção do meu conhecimento.

Aos meus professores do PROFMAT, que conseguiram transmitir seus conhecimentos.

Aos meus familiares, pelo afeto e suporte.

Aos meus amigos de turma do mestrado, pelo coleguismo e apoio.

Aos meus amigos: Gisa, Leila, Saullo, Jonas, Daniela, Jonatas, Rodolfo, Lorrayne, Crisanvânia, Patrícia, Rodney e Elton, pela amizade e por me proporcionarem momentos de imensas alegrias.

À CAPES, pelo suporte financeiro.

Lutam melhor os que têm belos sonhos.

Che Guevara.

Resumo

Neste trabalho apresenta-se algumas aplicações da teoria de grupos, que poderão utilizadas por professores do ensino básico, na elaboração de atividades envolvendo algumas propriedades da álgebra. Para a realização deste, antes de qualquer aplicação, necessitou-se da introdução de conceitos básicos e exemplos de grupos. A partir daí, mostra-se porque o produto de dois números inteiros negativos é sempre um número positivo, apresenta-se as aplicações da teoria de grupo no cubo mágico e finalmente aborda-se a referida teoria na criptografia.

Palavras chave: Grupo, Números negativos, Cubo mágico, Criptografia.

Abstract

The present paper aims at presenting some group theory applications, which can be used by Elementary School teachers during preparation of activities related to algebra and its properties. The development of this study needed the presentation of basic concept and some examples of groups. After that, we could show why the product of two negative numbers is always a positive one. We presented the application of group theory on a magic cube. Finally, we approached the already presented theory in encryption.

Keywords: Group, Negative Numbers, Magic Cube, Encryption.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

$\forall$: Para todo.

$\exists$: Existe algum.

$\mathbb{N}$: Números Naturais.

$\mathbb{Z}$: Números Inteiros.

$\mathbb{Q}$: Números Racionais.

$\mathbb{I}$: Números Irracionais.

$\mathbb{R}$: Números Reais.

$\mathbb{C}$: Números Complexos.

$S_{\triangle}$: Grupo de rotações no triângulo.

$x \mid y$: x divide y.

$a \equiv b \ mod \ R$: a é congruente a b módulo R.

X/S : Conjunto quociente de X por S.

$\mathbb{Z}_m$: Conjuntos da classes de congruência módulo m.

$\bar{a}$: Elemento de $\mathbb{Z}_m$.

$G =< a >$: Grupo G gerado pelo elemento a.

$(a_1 \ \ a_2 \ \ a_3 \ \ ... \ \ a_r)$: r-ciclo.

$\#(B)$: Cardinalidade de B.

D_S : Grupo de rotações no quadrado.

$(m, \ n)$: Máximo divisor comum dos números inteiros m e n.

Introdução

Embora não conste, diretamente, como um dos temas a ser abordado pelos Parâmetros Curriculares Nacionais, mas na teoria de grupo verifica-se as propriedades associativa, existência de um elemento neutro, existência do simétrico e comutativa, que são abordados no ensino básico, e frequentemente são negligenciadas ou, não é conseguido fazer uma contextualização de tais propriedades. Assim, nosso foco neste trabalho será justificar algumas propriedades matemáticas através da álgebra, mostrar a importância da álgebra em atividades lúdicas.

Para atingirmos o objetivo proposto, organizaremos este trabalho como segue.

No primeiro capítulo introduziremos conceitos e resultados que fazem parte da literatura usual da teoria de grupos e que serão necessários para o desenvolvimento de nosso trabalho.

No capítulo 2 abordaremos um exemplo de grupo, que é o grupo da permutações, que servirá de suporte teórico para as aplicação da teoria de grupo no Cubo de Rubik.

No último capítulo, o principal capítulo deste trabalho, será dedicado as aplicações da teoria de grupo. Este capítulo será dividido em três seções. Na primeira seção, mostraremos por que o produto de dois números inteiros negativos resulta um número positivo. Na segunda seção apresentaremos uma aplicação do grupo das permutações no Cubo de Rubik, exploraremos o grupo de Rubik, e na conclusão desta seção concluiremos quantos elementos tem o conjunto que forma o Grupo de Rubik, ou seja, quantas são as posiçoes do cubo formada através de movimentos de rotação das facetas do cubo. Na terceira seção aplicaremos a teoria de grupos na criptografia em especial nos criptossistemas de transformação afim.

O enfoque principal deste trabalho será apresentar uma proposta de material de apoio, para que professores de matemática possam utilizá-lo em seus estudos, para elaborarem um roteiro de aplicação em sala de aula e para os alunos do Ensino Médio,

um instrumento de motivação'.

Capítulo 1

Preliminares

Neste capítulo mencionamos alguns conceitos e propriedades da teoria de grupos importantes para o desenvolvimento dos capítulos subsequentes. Os resultados apresentados aqui já fazem parte da literatura usual da área, por isso quase todas as demonstrações serão omitidas. Em razão disso, indicamos algumas referências nos quais estes resultados podem ser encontrados, isto é, vejam referências [2], [4], [5], [6], [7], [9], [11].

1.1 Noções básicas de teoria de grupo

Definição 1 :

Seja G um conjunto não vazio e

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (x, y) &\longmapsto x * y \end{aligned}$$

uma operação em G. Dizemos que G é um grupo [1] *em relação a essa operação se, e somente se:*

i) $a * (b * c) = (a * b) * c, \forall a, b, c \in G$;

ii) Existe $e \in G$ *de maneira que* $a * e = e * a = a, \forall a \in G$;

iii) $\forall a \in G, \exists\ b \in G$ *tal que* $a * b = b * a = e$;

Se para um grupo $(G, *)$ [2] *verifica-se também a propriedade:*

iv) $a * b = b * a, \forall a, b, \in G$.

[1] Definição retirada de (6)

[2] Escrevemos $(G, *)$ para dizer que G é um grupo

Dizemos que o grupo $(G, *)$ é um grupo abeliano.

Assim um conjunto G com uma operação será um grupo se for satisfeita a propriedade associativa, se existir um, e somente um elemento neutro e se todo elemento de G tem simétrico. Se ainda valer a propriedade comutativa o conjunto será um grupo abeliano.

Apresentaremos a seguir alguns conjuntos que, munidos de uma operação, representam grupos:

1. Os conjuntos dos números inteiros, racionais e reais com a operação de adição são grupos, ou seja, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ representam um grupo, além disso em todos eles são válidas a propriedade comutativa, assim podemos chamá-los de grupos aditivos abelianos. O conjunto dos números naturais ($\mathbb{N}$) com a mesma operação não é um grupo pois nenhum elemento tem simétrico, no citado conjunto.

2. Os conjuntos dos números racionais e reais, agora com a operação de multiplicação também representam grupos abelianos, ou seja, $(\mathbb{Q}^*, .)$, $(\mathbb{R}^*, .)$ representam um grupo, além disso em todos eles são válidas a propriedade comutativa, assim podemos chamá-los de grupos multiplicativos abelianos. Porém, o conjunto dos números inteiros ($\mathbb{Z}^*$) com a mesma operação não é um grupo uma vez que os únicos elementos invertíveis em $\mathbb{Z}$ são 1 e -1, isto é, $\forall\ a\ \in\ \mathbb{Z}^*,\ a \neq \{1, -1\}, a$ não tem inverso. Vale ressaltar que, no conjunto $\mathbb{Z}^* \cup \{0\}$, com a referida operação, são válidas algumas propriedades, a saber:

   M_1) $\forall\ a,\ b,\ c\ \in \mathbb{Z},\ a.(b.c) = (a.b).c$ (Associativa);

   M_2) $\forall\ a\ \in\ \mathbb{Z},\ a.1 = 1.a = a$ (Existência do elemento neutro); . M_3) $\forall\ a,\ b\ \in \mathbb{Z},\ a.b = b.a$ (Comutativa).

   AM) A multiplicação é distributiva em relação à adição, ou seja,

   $$a.(b + c) = a.b + b.c;\ \forall\ a,\ b,\ c\ \in \mathbb{Z}$$

   .

3. Considere $P_1P_2P_3$ um triângulo equilátero, com centro em O e chame E_1, E_2, E_3 as retas passando pelas medianas do triângulo.

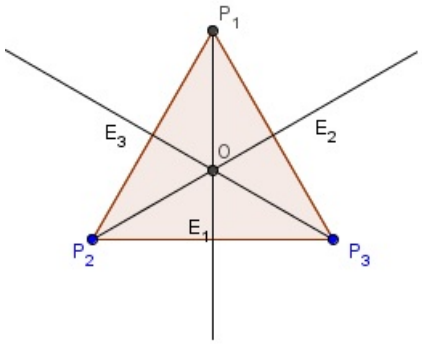
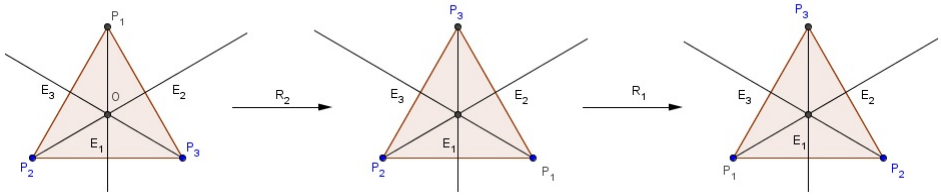


Figura 1.1: Triângulo Equilátero

Considere agora as transformações geométricas que preservam o triângulo:

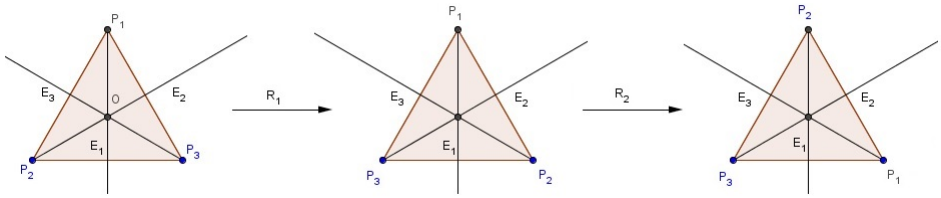
- As rotações planas centradas em O, no sentido anti-horário, id , $R_{\frac{2\pi}{3}}$, $R_{\frac{4\pi}{3}}$ de ângulos 0, $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$, respectivamente.
- As rotações espaciais, R_1, R_2, R_3, de ângulo π com eixos E_1, E_2, E_3, respectivamente.

Daí temos que o conjunto $S_{\triangle} := \left\{id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}},\ R_1,\ R_2,\ R_3\right\}$ com a operação de composição representa um grupo, porém não é abeliano pois:

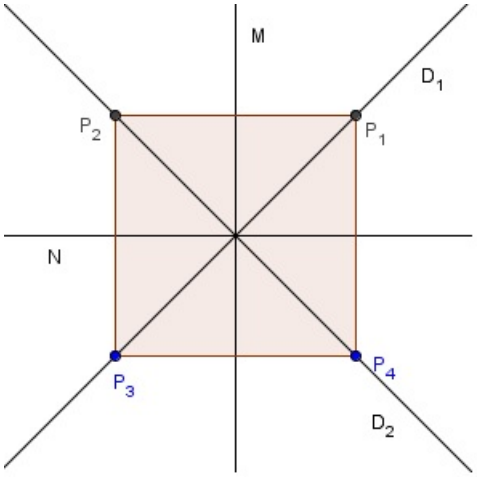


Isto é, $R_1 \circ R_2 = R_{\frac{2\pi}{3}}$.

Agora fazendo , $R_2 \circ R_1$ resulta em $R_{\frac{4\pi}{3}}$, ou seja:



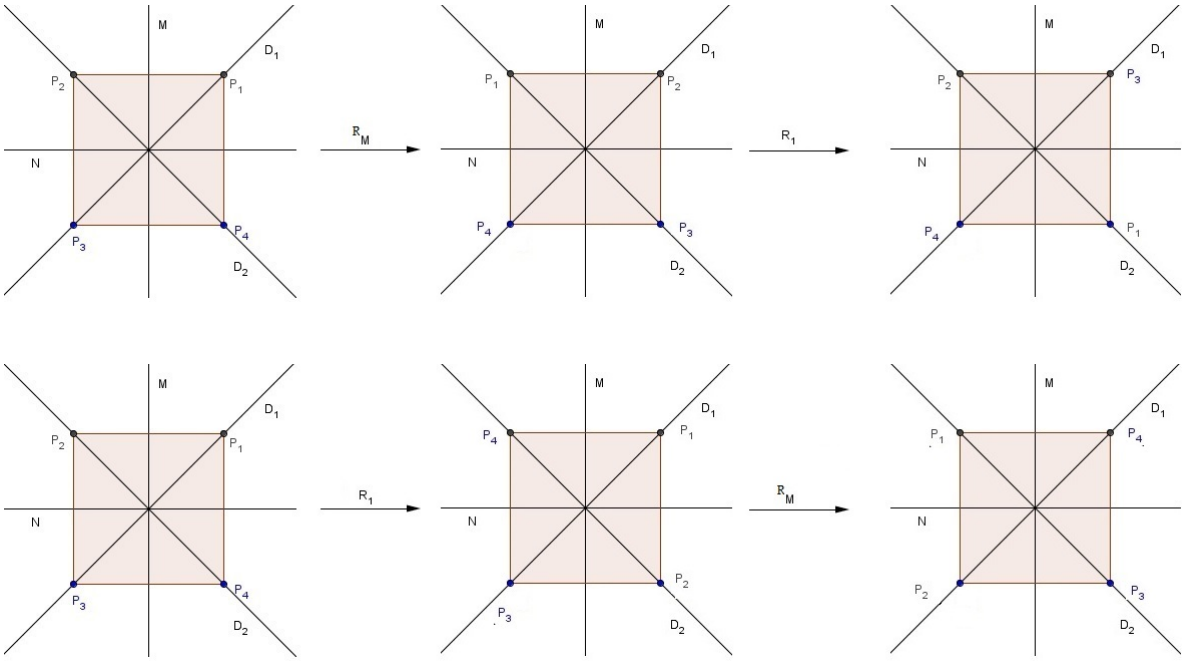
4. Seja $P_1P_2P_3P_4$ um quadrado com o centro de gravidade na origem O do espaço e chame de D_1, D_2, M, N as retas do espaço determinadas pelas diagonais e pelas mediatrizes do quadrado.



Considere agora as transformações que preservam o quadrado:

- As rotações planas centradas em O, id, $R_{\frac{\pi}{2}}$, R_{π}, $R_{\frac{3\pi}{2}}$, no sentido anti-horário, de ângulos zero, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$, respectivamente.
- As rotações espaciais, R_1, R_2, R_M, R_N, de ângulo π comos eixos D_1, D_2, M, N, respectivamente.

É fácil perceber que o conjunto $D_S := \left\{id, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}, R_1, R_2, R_M, R_N\right\}$ com a operação de composição de funções é um grupo, da mesma maneira que a do triângulo, este grupo não é abeliano, pois temos que $R_1 \circ R_M = R_{\frac{3\pi}{2}}$ e $R_M \circ R_1 = R_{\frac{\pi}{2}}$, isto é, $R_1 \circ R_M \neq R_M \circ R_1$, conforme segue abaixo:



1.1.1 Parte histórica sobre grupos abelianos

Grupos comutativos são chamados Abelianos em homenagem ao matemático norueguês Niels Henrik Abel (1802 - 1829). Abel estava interessado na questão da solubilidade das equações polinomiais. Num documento escrito em 1828 ele provou que se todas as raízes de uma dada equação podem ser expressas como funções racionais $\varphi,\ g, ...,\ h$ de uma delas, digamos x, e se para quaisquer duas dessas raízes, $\varphi(x)$ e $g(x)$, a relação $\varphi(g(x)) = g(\varphi(x))$ sempre se verifica, então a equação é solúvel por radicais. Abel mostrou que cada uma dessas funções na verdade permuta as raízes da equação; daí essas funções são elementos do grupo de permutações das raízes. Foi essa propriedade de comutividade nesses grupos de permutação assosciada a equações solúveis que levou Camille Jordan em seu tratado de álgebra de 1870 a dar o nome a tais grupos de abelianos; o nome então tem sido dado a grupos comutativos em geral.

Abel foi atrído a matemática ainda adolescente e logo superou todos os professores da Noruega. Ele por fim recebeu um prêmio, viagem do governo para estudar em qualquer lugar do mundo em 1825 e rumou para Berlim, onde se tornou amigo de August Crelle, o fundador do mais influente jornal de matemática alemão. Abel contribuiu com numerosos escritos para o jornal de Crelle durantes os anos seguintes, incluindo muitos artigos no campo das funções elípticas, cuja teoria ele criou praticamente sozinho. Abel retornou a Noruega em 1827 sem emprego e com muita dívidas. Ele entretanto continuou a escrever brilhantes artigos, mas morreu de tuberculose aos 26 anos, dois dias antes de Creller conseguir um emprego para ele em Berlim.

Para que possamos exibir mais um exemplo de grupo, iremos antes apresentar alguns conceitos necessários para o entendimento.

1.2 Classes de equivalência

Definição 2 : *Dados dois conjuntos X e Y, é chamado de relação* [3] *de X em Y todo subconjunto S do produto cartesiano* $X \times Y$.

Considerando X o conjunto dos números inteiros e Y o conjunto dos números

[3] Definição retirada de (2)

naturais, então o conjunto

$$S = \left\{(x, y) \in \mathbb{Z} \times \mathbb{N} / x^2 + y^2 = 25\right\}$$

é uma relação de $\mathbb{Z}$ em $\mathbb{N}$, onde os elementos são:

$$S = \{(-5, 0), (-4, 3), (-3, 4), (0, 5), (3, 4), (4, 3), (5, 0)\}$$

Graficamente, percebemos que o produto cartesiano $\mathbb{Z} \times \mathbb{N}$ são pontos da circunferência de centro O e raio 5 e a relação são os 7 pontos sobre ela, conforme figura abaixo.

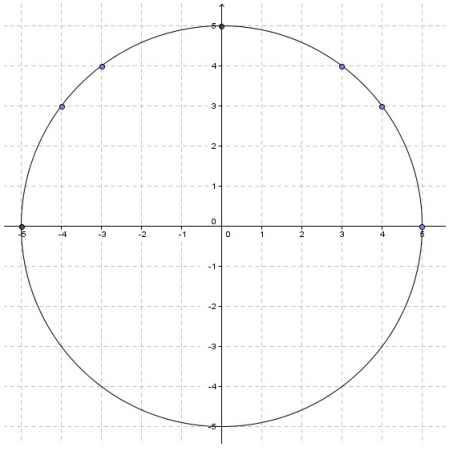


Figura 1.2: Exemplo de relação

Podemos definir uma relação S de um conjunto X nele mesmo, um exemplo disso é a relação $S = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} / x^2 + 1 = 9\right\}$, onde percebemos que a mesma é definida de $\mathbb{R}$ em $\mathbb{R}$. Este tipo de relação merece destaque, pois ela representa uma relação de equivalência, que é um conceito muito importante na matemática.

Definição 3 : *Dizemos que a relação S sobre um dado conjunto X é uma relação de relação de equivalência* [4] *sobre X se ela cumpre as seguintes condições:*

i) $(x, x) \in S$*, para todo* $x \in X$ *(Reflexiva);*

ii) se x e y são elementos de X tais que$(x, y) \in S$*, então* $(y, x) \in S$ *(Simétrica);*

iii) se x, y e z são elementos de X tais que $(x, y) \in S$ *e* $(y, z) \in S$*, então* $(x, z) \in S$ *(Transitiva).*

[4] Definição retirada de (5)

Portanto para que uma relação seja de equivalência, ela tem que satisfazer as propriedades reflexiva, simétrica e transitiva.

A relação $S = \{(a,\ a),\ (b,\ b),\ (c,\ c),\ (a,\ c),\ (c,\ a)\}$ é uma relação de equivalência sobre $X = \{a,\ b,\ c\}$.

A seguir verificaremos se a relação $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} / x - y\ \acute{e}\ par\}$ é de equivalência, isto é, se a relação cumpri as propriedades reflexiva, simétrica e transitiva. Vejamos:

i) Para qualquer $x \in \mathbb{Z}$, temos que $x - x = 0$, e 0 é um número par, daí temos que S é reflexiva.

ii) Suponhamos que $(x, y) \in S$ para $x, y \in \mathbb{Z}$, então $x - y$ é par, como o oposto de qualquer inteiro também é par então $-(x - y)$ é par e consequentemente $y - x$ é par, portanto $(y, x) \in S$, o que segue que S é simétrica;

iii) Suponhamos que $(x, y) \in S$ e $(y, z) \in S$ para $x, y, z \in \mathbb{Z}$, assim temos que $x-y$ e $y-z$ são pares, como a soma de dois números pares é par, então $(x-y)+(y-z) = x-z$ é um número par, portanto $(x, z) \in S$, o que segue que S é transitiva.

Logo S é uma relação de equivalência.

Considerando agora a relação $S = \{(x,\ y) \in \mathbb{Z}^* \times \mathbb{Z}^* / mdc(x,\ y) = 1\}$, verificamos que este relação é simétrica, mas não é reflexiva pois, por exemplo, $mdc(6,\ 6) = 6 \neq 1$, e também não é transitiva, porque $mdc(16,\ 21) = 1$ e $mdc(21,\ 26) = 1$, porém $mdc(16,\ 26) = 2 \neq 1$. Assim concluímos que S não é uma relação de equivalência.

Fazendo uma análise da relação de equivalência $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} / x - y\ \acute{e}\ par\}$, se pegarmos um elemento de $\mathbb{Z}$, como por exemplo, o número 5, todos os elementos do conjunto $\mathbb{Z}$, que relacionam com 5, segundo a relação de equivalência S dada, formam um conjunto que chamamos de classe de equivalência, assim o conjunto $\{...\ -5,\ -3,\ -1,\ 1,\ 3,\ 5, ...\}$ é a classe de equivalência do 5 segundo a relação S.

Definição 4 : *Dado uma relação de equivalência S sobre um conjunto X, chamamos de classe de equivalência* [5] *de $a \in X$ segundo a relação S, que denotamos $\bar{a}$, o conjunto $\{x \in X / xRa\}$.*

Definição 5 : *O conjunto formado por todas classes de equivalência módulo S, é chamado de conjunto quociente de X por S* [6]*, e denotamos por X/S.*

[5] Definição retirada de (5)
[6] Definição retirada de (5)

Voltando a relação de equivalência $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} / x - y \text{ é } par\}$, vamos determinar a classe de equivalência de cada número inteiro. Pela definição de classe temos que $\bar{0} = \{y \in \mathbb{Z} / yR0\}$ e pela relação S temos que $y-0$ é par, daí $\bar{0} = \{..., -2,\ 0,\ 2,\ 4, ...\}$. Da mesma maneira encontramos $\bar{1}$, basta achar os inteiros y tais que $y-1$ é par, assim $\bar{1} = \{..., -5, -3, -1,\ 1,\ 3,\ 5,\ ...\}$, obtendo $\bar{2} = \{...,\ -8,\ -6,\ -4,\ -2,\ 0,\ 2,\ 4,\ 6,\ 8,\ ...\}$, o que verificamos que $\bar{0} = \bar{2}$ e é fácil concluir que $\bar{n} = \bar{0}$, se n for par. Encontrando agora $\bar{3}$, obtemos $\bar{3} = \{...,\ -5,\ -3,\ -1,\ 1,\ 3,\ 5, \therefore\}$ que é igual ao $\bar{1}$ o que é fácil concluir que $\bar{n} = \bar{1}$, se n for ímpar. Deste modo, temos que o conjunto de todas as classes de equivalência de $\mathbb{Z}$ terá apenas dois elementos $\bar{0}$ e $\bar{1}$, este cojunto é o *conjunto quociente de* $\mathbb{Z}$ *por* S , que representamos por $\mathbb{Z}/S = \{\bar{0},\ \bar{1}\}$.

Na relação de equivalência $S = \{(a,\ a),\ (b,\ b),\ (c,\ c),\ (a,\ c),\ (c,\ a)\}$,temos que, $\bar{a} = \{a,\ c\}$, $\bar{b} = \{b\}$, e $\bar{c} = \{a,\ c\}$ e consequentemente $X/S = \{\{a,\ c\},\ \{b\}\}$.

Teorema 1 : *Seja S uma relação sobre X e $a,\ b \in X$. Então as seguintes proposições são equivalentes:*

i) $(a,\ b) \in S$ *ii)* $a \in \bar{b}$ *iii)* $b \in \bar{a}$ *iv)* $\bar{a} = \bar{b}$

1.3 Partição de um conjunto

Definição 6 : *Seja X um conjunto não vazio. Diz-se que uma classe f de subconjuntos não vazios de X é um partição* [7] *de X se:*

i) dois membros quaisquer de f são iguais ou são disjuntos;

ii) a união dos membros de f é igual a X.

A partir da definição acima percebemos que $f = \{(-\infty,\ 3),\ [3,\ 4),\ [4,\ 5],\ (5, +\infty)\}$ é uma partição de $\mathbb{R}$.

A seguir apresentaremos dois teoremas que relacionam conjunto quociente e partição.

Teorema 2 : *Se S é uma relação de equivalência sobre X, então o conjunto quociente X/S é uma partição de X.*

Teorema 3 : *Se f é uma partição de X, então existe uma relação S de equivalência sobre X de modo que $X/S = f$.*

[7] Definição retirada de 2

1.4 Relação de congruência módulo m

A Teoria das Congruências é um vasto campo da matemática, inserido na Teoria dos Números. Abrange propriedades e teoremas cujo entendimento e aplicabilidade variam dos níveis mais básicos aos mais avançados. Porém como a proposta deste trabalho está voltada para o ensino básico, nos restringiremos apenas a itens úteis para esse fim. Em matemática, aritmética modular (chamada também de aritmética do relógio) é um sistema de aritmética para inteiros, onde os números "voltam pra trás"quando atingem um certo valor, o módulo.

O matemático suiço Euler foi o pioneiro na abordagem de congruência por volta de 1750, quando ele explicitamente introduziu a ideia de congruência módulo um número natural N. A aritmética modular foi desenvolvida posteriormente por Carl Friedrich Gauss em seu livro Disquisitiones Arithmeticae, publicado em 1801.

Definição 7 : *Sejam a e b dois números inteiros e m um número inteiro positivo maior que 1. Dizemos a e b são congruentes módulo m* [8] *se o m divide a diferença $a-b$. Quando os inteiros a e b são congruentes módulo m, escrevemos*

$$a \equiv b \mod m$$

Por exemplo, $21 \equiv 13 \mod 2$ pois, $2|21-13$ e $21 \not\equiv 13 \mod$ pois, $3 \nmid 21-13$. Dizer que $m|a-b$ é equivalente dizer que os restos da divisão de a por m e b por m são iguais.

Um exemplo, do dia a dia, seria os relógios analógicos que trata-se de um caso de congruência, módulo 12. Note que 13 horas é congruente a 1 hora, no módulo 12. Ambos divididos por 12, deixam resto 1 e que 17 horas é congruente a 5 horas, módulo 12. Tanto 17, como 5, divididos por 12, deixam resto 5, e assim, sucessivamente.

$$1 \equiv 13 \equiv 25 \; mod \; 12$$

$$5 \equiv 17 \equiv 29 \; mod \; 12$$

Assim, as horas marcadas num relógio analógico constituem também um caso clássico de congruência, nesse caso, com módulo 12.

[8] Definição retirada de (2)

Da definição 3 decorre que $S = \{(a,\ b) \in \mathbb{Z} \times \mathbb{Z} / a \equiv b\ mod\ m\}$ é uma relação de equivalência. De fato,

1. Temos que $a \equiv a\ mod\ m$, pois $m \mid a - a = 0$. Assim é reflexiva;

2. Se $a \equiv b\ mod\ m$, então $b \equiv a\ mod\ m$, pois, como $m \mid a - b$ então m divide o oposto, e daí $m \mid b - a$. Logo vale a propriedade simétrica.

3. Se $a \equiv b\ mod\ m$ e $b \equiv c\ mod\ m$, então $a \equiv c\ mod\ m$, pois como $m \mid a - b$ e $m \mid b - c$ então m divide a soma, daí $m \mid (a - b) + (b - c) = a - c$, portanto S é transitisa.

Definição 8 : *A relação de congruência módulo m sobre $\mathbb{Z}$ determina um conjunto quociente $\mathbb{Z}/S$ que é indicado por $\mathbb{Z}_m$, ou seja, $\mathbb{Z}_m$ é o conjunto de todas as classes de equivalência sobre S.*

Proposição 4 : *O conjunto $\mathbb{Z}_m$ tem exatamente m elementos, isto é,*

$$\mathbb{Z}_m = \left\{\bar{0},\ \bar{1},\ \bar{2},\ ...,\ \overline{m-1}\right\}$$

.

Demonstração: i) Dado $a \in \mathbb{Z}$, efetuemos a divisão euclidiana de a por m. Sendo q o quociente e r o resto dessa divisão, temos: $a = mq + r$, como $0 \leq r < m$ logo, $a - r = mq$, isto é, $a \equiv r\ mod\ m$, ou ainda, $\bar{a} = \bar{r}$. Como $r \in \{0,\ 1,\ 2,\ ...,\ m-1\}$, temos que $\bar{a} \in \mathbb{Z}_m \Longrightarrow \bar{a} \in \left\{\bar{0},\ \bar{1},\ \bar{2},\ ...,\ \overline{m-1}\right\}$

ii) Suponhamos agora que existam duas classes iguais em $\left\{\bar{0},\ \bar{1},\ \bar{2},\ ...,\ \overline{m-1}\right\}$, isto é: $\bar{r} = \bar{s}$ com $0 \leq r < s < m$. Neste caso, temos: $\bar{r} = \bar{s} \Longrightarrow r \equiv s\ mod\ m \Longrightarrow m \mid s - r$. Como $0 < s - r < m$, então isto é impossível.

Logo, o número de elementos de $\mathbb{Z}_m$ é exatamente m.

1.5 Função φ de Euler e a congruência módulo m

Procurar os inversos dos elementos invertíveis em $(\mathbb{Z}_m,\ \cdot)$ não é tarefa fácil. A seguir mostraremos um função que nos auxilia nesta busca. Uma abordagem sobre a função que segue pode ser encontrada em [3], [9] e [11].

Definição 9 : *Dado $m \in \mathbb{N}$, designaremos $\varphi(m)$ a quantidade de números naturais entre 0 e $m-1$ que são primos com m. Isto define uma importante função, chamada de função fi de Euler:*

$$\varphi : \mathbb{N}^* \to \mathbb{N} \text{ tal que } \varphi(m) = \#((m,\ n) = 1)$$

onde $\#((m,\ n) = 1)$ é a quantidade de elementos m tal que $(m,\ n) = 1$.

Corolário 5 : *Pela definição, temos que $\varphi(m) \leq m - 1$, além disso:*

i) $\varphi(m) = m - 1$ se, e somente se, m é primo.

ii) Se $m = pq$, com p e q primos, então $\varphi(m) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

iii) Se $n = p^k$, isto é, se n é potência de um primo p, então $\varphi(n) = \varphi(p^k) = p^k - p^{k-1}$.

Teorema 6 *(Euler)***:** *Sejam $m,\ a \in \mathbb{N}$ com $m > 1$ e $(a,\ m) = 1$. Então,*

$$a^{\varphi(m)} \equiv 1 \ mod\ m.$$

O Teorema de Euler pode ser usado para determinar o inverso de alguns elementos $a \in \mathbb{Z}_n$, pois

$$a^{\varphi(n)} \equiv 1 \ mod\ n \iff a^{-1} \equiv a^{\varphi(n)-1} \ mod\ n.$$

Apresentaremos a seguir um exemplo para calcular o inverso de $\bar{7} \in \mathbb{Z}_{10}$.

$$\bar{7}^{-1} \equiv \bar{7}^{\varphi(10)-1} \equiv \bar{7}^{4-1} \equiv \bar{7}^3 \equiv 343 \equiv 3 \ mod\ 10.$$

Ou seja, $\bar{7}^{-1} = \bar{3}$, uma vez que $\bar{7} \times \bar{3} = \bar{21} = \bar{1}$.

1.6 Operações em $\mathbb{Z}_m$

Definição 10 : *Sejam $\bar{x}$ e $\bar{y}$ elementos do conjunto $\mathbb{Z}_m$, assim a operação $(\bar{x} + \bar{y})$, chamada adição módulo m* [9]*, é o resto da divisão $x + y$ por m, ou seja $\overline{x + y}$.*

Por exemplo, sejam $\bar{3},\ \bar{4} \in \mathbb{Z}_5$ então $\bar{3} + \bar{4}$ é um elemento $\mathbb{Z}_5$ o qual é igual a $\bar{7} = \bar{2}$.

[9] Definição retirada de (11)

A tabela abaixo, chamada de *tábua da adição módulo 5* [10], mostra a soma de todos elementos de $\mathbb{Z}_5$.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabela 1.1: Adição em $\mathbb{Z}_5$

Definição 11 : *Sejam $\bar{x}$ e $\bar{y}$ elementos do conjunto $\mathbb{Z}_m$, a operação $(\bar{x} \cdot \bar{y})$, chamada de multiplicação módulo m* [11]*, é o resto da divisão $x \cdot y$ por m, ou seja, $\overline{x \times y}$.*

Por exemplo $\bar{3} \cdot \bar{4}$ é um elemento do conjunto $\mathbb{Z}_5$, sendo $\bar{12} = \bar{2}$, pois a divisão de 12 por 5 deixa resto 2.

Da mesma maneira, construindo a tábua da multiplicação módulo 5, temos:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tabela 1.2: Multiplicação em $\mathbb{Z}_5$

Voltando agora aos exemplos de grupos, podemos mostrar que $(\mathbb{Z}_m, +)$, isto é, o conjuntos $\mathbb{Z}_m$, munido da operação de adição módulo m, é um grupo, chamado *grupo aditivo das classes de restos módulo m*, e mais, é um grupo abeliano.

Agora, o $\mathbb{Z}^*{}_m$ munido da operação de multiplicação nem sempre é um grupo. Considerando o conjunto $\mathbb{Z}^*{}_{10}$, temos que $(\mathbb{Z}^*{}_{10}, \cdot)$ não é um grupo pois, temos que $\bar{5} \cdot \bar{1} = \bar{5} \cdot \bar{3} = \bar{5} \cdot \bar{5} = \bar{5} \cdot \bar{7} = \bar{5} \cdot \bar{9} = \bar{5}$, isto é, o elemento neutro não é único. Existe outra maneira averiguar que $(\mathbb{Z}^*{}_{10}, \cdot)$ não é grupo, basta ver que $\bar{2} \cdot \bar{5} = \bar{0}$, que não pertence a $\mathbb{Z}^*{}_{10}$.

[10] A barra dos elementos foram omitidas na tabela para não carregar a figura
[11] Definição retirada de (11)

Proposição 7 : $(\mathbb{Z}_m{}^*, \cdot)$ *é um grupo, se, e somente se, o* m *for um número primo.*

Demonstração: ($\Longrightarrow$) Suponhamos que $(\mathbb{Z}_m{}^*, \cdot)$ é um grupo e que m não é primo. Então existem dois números naturais r e s, ambos maiores do que 1, de modo que, $m = rs$. Desta igualdade resulta que $\bar{0} = \bar{m} = \bar{r}\bar{s}$ o que é absurdo pois $\bar{0} \notin \mathbb{Z}^*{}_m$.

($\Longleftarrow$) Tomemos $\bar{r},\ \bar{s}\ \in \mathbb{Z}^*{}_m$. Se tivéssemos $\bar{r}\bar{s} = \bar{0}$, então teríamos $rs \equiv 0\ mod\ m$ o que equivale a dizer que $m|rs$. Como m é primo, então $m|r$ ou $m|s$ ou seja $\bar{r} = \bar{0}$ ou $\bar{s} = \bar{0}$ o que é impossível. Logo $\mathbb{Z}^*{}_m$ é fechado para a multiplicação definida em $\mathbb{Z}_m$.

1.7 Subgrupos

Dado um conjunto G, tal que $(G, *)$ seja um grupo. Podemos encontrar um conjunto H, tal que $H \subset G$, de tal maneira que $(H, *)$ também seja um grupo, por exemplo, seja $G = \mathbb{Z}$ e $H = \{-2,\ -1,\ 0,\ 1,\ 2\}$, temos que, $(H,\ +)$ é um grupo, pois obedece as mesmas propriedades de G e chamamos H de *subgrupo de* G [12].

Definição 12 : *Seja* $(G, *)$ *um grupo. Dizemos que um subconjunto não vazio,* $H \subset G$ *é um subgrupo de* G*, se, e somente se:*

i) $\forall a,\ b \in H \Longrightarrow a\ *\ b \in H$

ii) $(H, *)$ *também é um grupo.*

Apresentaremos um resultado mais conveniente para verificar que um subconjunto H é um subgrupo de G.

Teorema 8 : *Seja* H *um subconjunto não-vazio de grupo* G*. Então* H *é um subgrupo de* G *se e somente se as duas condições seguintes são satisfeitas:*

i) $h_1 * h_2\ \in\ H,\ \forall\ h_1,\ h_2\ \in\ H$*;*

ii) $h^{-1}\ \in\ H,\ \forall\ h\ \in H$*.*

Segue abaixo alguns exemplos de subgrupos:

1. Se G é um grupo, então $\{e\}$ e G são subgrupos de G.

2. $(2\mathbb{Z},\ +)$ [13] é um subgrupo de $(\mathbb{Z},\ +)$. De maneira mais geral, se n é um inteiro qualquer, $(n\mathbb{Z},\ +)$ é um subgrupo de $(\mathbb{Z},\ +)$.

[12] Definição retirada de (2)

[13] $2\mathbb{Z}$ é o conjunto dos múltiplos de 2, ou seja, pares

3. $\{id,\ R_1\}$ e $\left\{id,\ R_{\frac{2\pi}{3}},\ R_{\frac{4\pi}{3}}\right\}$ são subgrupos do grupo de rotações do triângulo.

4. $\{id,\ R_\pi\}$ e $\left\{id,\ R_{\frac{\pi}{2}},\ R_\pi,\ R_{\frac{3\pi}{2}}\right\}$ são subgrupos do grupo de rotações do quadrado.

1.8 Grupos cíclicos

Definição 13 : *Um grupo G chama-se cíclico* [14] *se existe um elemento $a \in G$ de maneira que $G =< a >$. O elemento a é dito gerador de G.*

O grupo multiplicativo $G = \{-1,\ 1\}$ é ciclico uma vez que $\{(-1)^m\ /\ m \in \mathbb{Z}\ \} = \{-1,\ 1\}$.

Existem alguns resultados imediatos importantes que devemos considerar:

i) Todo grupo cíclico é abeliano, mas a recíproca não é verdadeira;

ii) Um grupo cíclico pode conter mais de um gerador. Por exemplo: $\bar{3}$ e $\bar{5}$ são geradores de $(\mathbb{Z}_7,\ +)$;

iii) Se G é um grupo aditivo gerado por a, então $G = \{ma\ tal\ que\ m\ \in\ \mathbb{Z}\}$.

Teorema 9 : *Seja a um elemento de um grupo multiplicativo G. Se a ordem de a é $m > 0$, então $< a >$ é um grupo finito de ordem m dado por $< a >= \left\{e,\ a,\ a^2,\ ...,\ a^m\right\}$.*

[14] Definição retirada de (2)

Capítulo 2

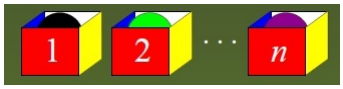
Grupos de permutações

2.1 Permutações de um conjunto

Definição 14 : *Seja B um conjunto não vazio. Chama-se permutação de B toda aplicação bijetora de B em B.*

Podemos pensar em arranjos como um conjunto de caixas numeradas 1, 2, 3, ..., n cada uma contendo uma única bola.

Permutar é tirar todas as bolas para fora, depois recolocá-las na mesma caixa ou em outra diferente, cada caixa contendo exatamente uma bola.



A aplicação idêntica de B, isto é, a aplicação

$$\begin{array}{rcl} I_B : B & \longrightarrow & B \\ x & \longmapsto & I_B(x) = x \end{array} \quad , \ \forall\ x \in B$$

é denominada permutação indêntica.

A permutação representar tirar todas as bolas das caixas e recolocá-las todas na mesma caixa.

Quando $B = \{1,\ 2,\ 3,\ ...,\ n\}$, indicaremos uma permutação τ de B pela notação matricial:

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

Assim, no exemplo das caixas, representaríamos esta permutação da seguinte forma:

$$\begin{pmatrix} 1 & 2 & ... & n \\ 2 & 1 & ... & n \end{pmatrix}$$

Com esta notação, a permutação idêntica de B escreve-se

$$I_B = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ 1 & 2 & 3 & ... & n \end{pmatrix}$$

O número total de permutações de um conjunto finito B com n elementos é igual ao produto dos n primeiros inteiros positivos, isto é:

$$1 \,.\, 2 \,.\, 3 \,.\, ... \, n \;=\; n!$$

Denotaremos os conjuntos das permutações do conjunto B, contendo n elementos, como S_B ou S_n.

2.2 Permutação inversa

Definição 15 : *Seja $B = \{1,\ 2,\ 3,\ ...,\ n\}$, e γ um permutação de B, então a inversa de γ será a permutação:*

$$\gamma^{-1} = \begin{pmatrix} \gamma(1) & \gamma(2) & \gamma(3) & ... & \gamma(n) \\ 1 & 2 & 3 & ... & n \end{pmatrix} \;=\; \begin{pmatrix} \gamma^{-}1(1) & \gamma^{-1}(2) & \gamma^{-1}(3) & ... & \gamma^{-1}(n) \\ 1 & 2 & 3 & ... & n \end{pmatrix}$$

Exemplo 1:

Se o conjunto $B = \{1,\ 2,\ 3,\ 4,\ 5\}$, então uma permutação de B é:

$$\varphi \;= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

A permutação inversa de φ é a aplicação bijetora:

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

Exemplo 2:

Seja $B = \{1,\ 2,\ 3,\ 4\}$. Considere as permutações:

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \text{ e } \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

As aplicações compostas $\varphi \circ \psi : B \longrightarrow B$ e $\psi \circ \varphi : B \longrightarrow B$ são bijetoras e, portanto, também são permutações de B. Temos:

$$\varphi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

$$\psi \circ \varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Observe que $\varphi \circ \psi \neq \psi \circ \varphi$.

2.3 Notações de ciclo

As matrizes são convenientes para descrever permutações. Mas há um modo mais simples: a notação de cliclos.

Um ciclo pode ser pensado como uma série de transições de estado que acaba por retornar ao estado inicial.

Por exemplo, considere a permutação

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

Voltando a pensar nas caixas com bolas, esta permutação faz o seguinte: A bola que estava na caixa 1 vai para a caixa 3, a bola que estava na caixa 3 vai para a caixa 4, a bola que estava na caixa 4 vai para a caixa 1, a bola que estava na caixa 2 vai para a caixa 2. Repare no modo como as bolas das caixas 1,3 e 4 transitam em círculo.

Podemos representar o trânsito das bolas como

$$\sigma : 1 \Longrightarrow 3 \Longrightarrow 4 \Longrightarrow 1$$

significando que a bola da caixa 1 vai para a caixa 3, que a bola da caixa 3 vai para a caixa 4, a bola da caixa 4 vai para a caixa 1 e a bola da caixa 2 continua na caixa 2.

Melhor ainda, podemos simplesmente escrever

$$\sigma : (1\ 3\ 4)$$

significando a mesma coisa. Esta é chamada de *notação de ciclos de* σ.

Na notação de ciclo os n elementos entre parênteses formam um *n-ciclo*

Da mesma forma das matrizes, os 3-ciclos $(1\ 3\ 4),\ (3\ 4\ 1),\ (4\ 1\ 3)$ são iguais. E convenientemente, começamos um ciclo pelo menor elemento.

Assim escrevendo a permutação $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \end{pmatrix} = (1\ 2)(4\ 6\ 5)$. Vemos que esta permutação consiste em um 2-ciclo e um 3-ciclo.

2.4 Grupo das permutações de um conjunto

Os elementos do conjunto das permutações S_n possuem algumas caracterizações, as quais seguem.

Definição 16 : *Seja* $B = \{1,\ 2,\ 3,\ ...,\ n\}$. *Uma permutação* α *de* S_n *é chamado de r-ciclo se existem elementos distintos* $a_1,\ a_2,\ ...,\ a_r \in \{1,\ ...,\ n\}$ *tais que* $\alpha(a_1) = a_2,\ \alpha(a_2) = a_3,\ ...,\ \alpha(a_{r-1}) = a_r,\ \alpha(a_r) = a_1$.

Definição 17 : *Duas permutações* α *e* $\beta \in S_n$ *são disjuntos de* x *é movido por uma e fixado por outra. Em símbolos, se* $\alpha(x) = x$ *e se* $\beta(x) \neq x$, *então* $\alpha(x) = x$.

Um exemplo relacionado com a definição anterior é, se em S_5 os ciclos (1 3 4) e (2 5) são disjuntos e os ciclos (1 3 5) e (2 5), não são disjuntos, pois o elemento 5 é

movimento por ambos.

Proposição 10 : *Seja $\alpha \in S_n$, $\alpha \neq I_B$. Então α é igual a um produto de ciclos disjuntos de comprimentos ≥ 2.*

Proposição 11 : *Todo elemento de S_n é produto de transposições, isto é, S_n é gerado por transposições.*

O conjunto das permutações de S_n tem estrutura de grupo, como mostra o teorema abaixo.

Teorema 12 : *Seja B um conjunto não vazio e $S_n = \{\tau : B \longrightarrow B \ / \ \tau$ é bijetora$\}$. Então*

i) $(S_B, \circ)$ é um grupo, onde $\circ$ é a operação composição.

ii) Se $\#(B) > 2$, então $(S_B, \circ)$ não é abeliano.

Demonstração:

i) É imediato que dados $\tau_1, \tau_2, \tau_3 \in S_B$, valem: a) $(\tau_1 \circ \tau_2) \circ \tau_3 = \tau_1 \circ (\tau_2 \circ \tau_3)$ (assosciativa). b) $\tau_1 \circ I_B = I_B \circ \tau_1$ (existência do elemento neutro, denotado por I_B). c) $\tau_1 \circ {\tau^{-1}}_1 = {\tau^{-1}}_1 \circ \tau_1 = I_B$ (${\tau^{-1}}_1$ é inverso de τ).

ii) Se o conjunto B tem mais de dois elementos, o grupo $(S_B, \circ)$ não é abeliano. Como $\#(B) > 2$, façamos $B = \{b_1, b_2, b_3\} \cup B'$. Considere as permutações τ e $\rho \in S_B$, assim definidas: $\tau(b_1) = b_2,\ \tau(b_2) = b_3,\ \tau(b_3) = b_1,\ \tau(x) = x, \forall x \in B - B'$ $\rho(b_1) = b_2,\ \rho(b_2) = b_3,\ \rho(b_3) = b_1,\ \rho(x) = x, \forall x \in B - B'$ Temos: $(\tau \circ \rho)(b_1) = \tau(\rho(b_1)) = \tau(b_2) = b_3$ $(\rho \circ \tau)(b_1) = \rho(\tau(b_1)) = \rho(b_2) = b_1$ Portanto, $\tau \circ \rho \neq \rho \circ \tau$, isto mostra que o grupo $(S_B, \circ)$ não é abeliano.

Consideremos o grupo $S_3 = \{id,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$. Sejam $\alpha = (1\ 2\ 3)$ e $\beta = (1\ 2)$, temos: $\alpha^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$, $\alpha^3 = (1\ 3\ 2)(1\ 2\ 3) = id$, $\beta^2 = (1\ 2)(1\ 2) = id$, $\beta\alpha = (1\ 2\ 3)(1\ 2) = (2\ 3)$, $\alpha\beta(1\ 2)(1\ 2\ 3) = (1\ 3)$, $\alpha^2\beta = (1\ 3\ 2)(1\ 2) = (2\ 3)$

Observe que foi verificado acima que α e β geram o grupo S_3, isto é, que todos os elementos do grupo são produtos finitos de fatores iguais a α ou β.

Dados duas permutações é possível operá-las, isto é, suponhamos que o conjunto a ser permutado seja $\{1,\ 2,\ 3,\ 4,\ 5\}$. Desejamos fazer $\sigma = (1\ 2\ 4)(3\ 5)$ seguido de $\tau =$

(1 3 5)(2 4), que é, obter a composição dessas permutações. Basta seguir, cada elemento do conjunto e ver onde ele irá parar.

Por exemplo, σ leva 1 no 2 e τ leva 2 no 4, logo 1 vai no 4. Em seguida, σ leva o 4 no 1 e τ leva o 1 no 3, então 4 vai no 3. Depois σ leva 3 no 5 e τ leva 5 no 1, fechando o ciclo. Ainda, σ leva 2 no 4 e τ leva 4 no 2, logo o 2 não se move. Como temos apenas 5 elementos, o 5 também não se move.

Portanto $\sigma \circ \tau = (124)(35) \circ (135)(24) = (1\ 4\ 3)$.

2.5 Permutações pares e ímpares

Definição 18 : *Seja σ uma permutação. Se σ pode ser fatorada com um número par de transposições, então dizemos que σ é um permutação par. Se σ pode ser fatorada com um número ímpar de transposições, então ela é chamada permutação ímpar. Em geral, a fatoração de uma permutação em transposições não é única.*

Pode ser demonstrado que, a composição de permutações pares resulta numa permutação par. A composição de permutações ímpares e a composição de uma permutação par com uma permutação ímpar resultam em uma permutação ímpar.

Proposição 13 : *Se A_n é o conjunto de todas as permutações pares em S_n então A_n é um subgrupo de S_n.*

De fato, A_n é um subgrupo de S_n pois, de acordo com o Teorema 8 temos que, dados $\alpha,\ \gamma \in A_n \Rightarrow \alpha \circ \gamma \in A_n$. Além disso, se $\alpha \in A_n \Rightarrow \alpha^{-1} \in A_n$. O citado grupo é denomidado grupo alternado de grau n.

Pode ser mostrado que a quantidade de elementos deA_n é $\frac{n!}{2}$. (Ver [4])

Seja o grupo S_4 de permutações com 24 elementos. Então A_4 tem 12 elementos, a saber: $id, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4), (1\ 3\ 4), (1\ 4\ 3), (1\ 2\ 3), (1\ 3\ 2), (2\ 3\ 4)$, $(2\ 4\ 3), (1\ 2\ 4)$ *e* $(1\ 4\ 2)$.

Capítulo 3

Aplicações

3.1 Por que $(-a).(-b) = ab$?

Hoje em dia, os números negativos são comuns no dia a dia. Estão presentes nas medidas de temperaturas, altitudes, deslocamentos, calendário, fuso horário, questões de natureza contábil. Mas nem sempre foi assim. Os números negativos tem a origem incerta, existem registros de obras envolvendo tais números, pelos chineses, 200 a.C., mas somente no século XVII é que os matemáticos passaram a usar os negativos com desembaraço. O próprio nome desses números nos mostram o quantos eles foram vistos com desconfiança, pois *números negativos* representa negação, ou seja, não número.

O ensino dos números negativos é um grande desafio para nós professores, pois a não compreensão do conceito de números negativos, faz com que o aluno crie outras dificuldades. Segundo Borba(2009), a aprendizagem dos números inteiros relativos é importante à compreensão de outros conceitos matemáticos e para a resolução de diversos problemas como os que envolvem álgebra, funções e o cálculo de quantidades. Constata-se então, que a não compreensão dos números inteiros, além de dificultar a aprendizagem de outros conceitos, prejudica também a resolução de situações que envolvem as operações nesse conjunto, como a multiplicação e a divisão. Uma dificuldade que temos, em relação aos números negativos, é repassar aos alunos a famosa *regra de sinal da multiplicação*, pois muitas vezes esta regra é imposta aos alunos, sem justificativas. O aluno por sua vez, apenas memoriza tal regra, o que torna sem sentido as operações com números negativos. Alguns livros didáticos trazem ilustrações para justificarem a regra de sinais, estas ilustrações são bons artifícios didáticos, mas que na maioria das vezes, tornam-se regras

de memorização. Aresentaremos abaixo algumas dessas ilustrações:

1. Considere (+) sendo amigo e (-) sendo inimigo. Assim:

   - O amigo de meu amigo é meu amigo, ou seja (+).(+)=(+);
   - O amigo de meu inimigo é meu inimigo, ou seja (+).(-)=(-);
   - O inimigo de meu amigo é meu inimigo, ou seja (-).(+)=(-);
   - O inimigo de meu inimigo é meu amigo, ou seja (-).(-)=(+);

2. Considere um ganho representado por um número positivo e a perda por um número negativo, considere ainda o tempo no futuro por um número positivo e no passado por um número negativo, assim:

   - Se uma pessoa perde 5 reais por dia, então daqui 3 dias terá perdido 15 reais, ou seja (-5).(+3)=-15;
   - Se uma pessoa perde 5 reais por dia, então há 3 dias estava com 15 reais a mais, ou seja (-5).(-3)=+15.

3. Considere a sequência: $3.(-2) = -6, 2.(-2) = -4, 1.(-2) = -2, 0.(-2) = 0$. Continuando a sequência teremos, $-1.(-2) = 2, -2.(-2) = 4$.

Iremos apresentar agora, uma maneira algébrica que responde a pergunta que foi colocada como título desta seção, *Porque* $(-a).(-b) = ab$*?*. Consequentemente, justificar a regra de sinal da multiplicação.

Pois bem, vimos no capítulo anterior que $(\mathbb{Z},\ +)$ é um grupo abeliano e que, mesmo $(\mathbb{Z},\ .)$ não sendo grupo, verificam-se algumas propriedades, que seguem: existência do elemento neutro, que é o número 1, além disso a multiplicação é distributiva em relação à adição (veja exemplo 2 da seção 1.1). Estas informações são relevantes para mostrarmos que $(-a).(-b) = ab$.

Inicialmente mostraremos que $a.0 = 0,\ \forall\ a\ \in \mathbb{Z}$:

Considere a um número inteiro qualquer, assim $a + a.0 = a.1 + a.0 = a(1 + 0) = a.1 = a = a + 0$, portanto $a + a.0 = a + 0$ e fazendo o cancelamento, temos que $a.0 = 0$. Agora podemos mostrar que $(-1).a = -a$ para todos número inteiro a:

Considere a um número inteiro qualquer, assim $a + (-1).a = 1.a + (-1)a = [1 + (-1)].a = 0.a = 0$. Assim a e $(-1)a$ são simétricos, pois $a + (-1).a = 0$, ou seja, $(-1)a =$

$-a$ e $a = -[(-1)a]$. Em particular, fazemos $a = -1$, temos que $(-1).(-1) = -(-1) = 1$, generalizando, temos $(-a).(-b) = (-1).a.(-1).b = (-1).(-1).ab = 1.ab = ab$.

Com isso terminamos a desmonstração, e concluímos que o produto de dois números inteiros negativos é sempre um número inteiro positivo. Alguns professores podem achar que esta demonstração é muito abstrata para apresentar aos seus alunos, mas se o professor partir de casos particulares, conseguirá o entendimento dos mesmos.

3.2 Cubo de Rubik

O cubo mágico foi inventado, em 1974, pelo arquiteto hungaro Erno Rubik, na intenção de ilustrar para seus alunos o conceito de terceira dimensão. A primeira peça era feita de madeira, com as faces de 6 cores diferentes, a fazer os primeiros movimentos, Erno percebeu ter criado um quebra-cabeça, ao qual demorou cerca de um mês para conseguir voltar o cubo a sua configuração original. Em 1980, iniciou-se a produção industrial e a distribuição mundial do Cubos, em apenas dois anos são vendidos 100 milhões de cubos e hoje o cubo mágico é considerado um dos brinquedos mais populares do mundo.

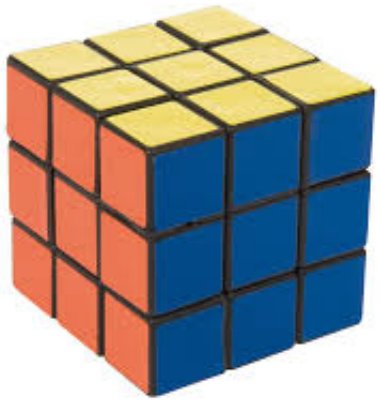


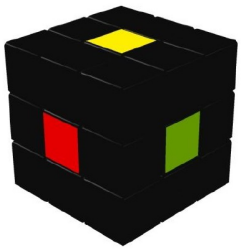
Figura 3.1: Cubo Mágico

A versão mais comum do cubo de Rubik, é a $3 \times 3 \times 3$, que é formado por 6 faces de cores distintas, com 27 cubinhos, sendo 9 cubinhos em cada face. Cada cubinho tem 6 facetas [1], mas só são visíveis as facetas que apontam para fora do cubo. Diferenciamos os cubinhos de 4 maneiras:

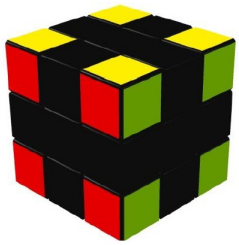
- 1 cubinho virtual, que está no centro do cubo, e não é possível vê-lo;

[1] Designaremos facetas como sendo as faces dos cubinhos

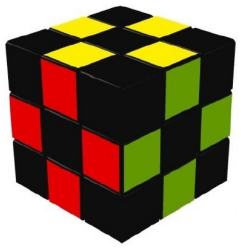
- 6 cubinhos centrais, com uma faceta visível;
- 8 cubinhos de cantos, com 3 facetas visíveis;
- 12 cubinhos arestas, com 2 facetas visíveis.



(a) Cubinhos Centrais



(b) Cubinhos de Canto



(c) Cubinhos Arestas

Figura 3.2: Tipos de cubinhos

Indicamos as faces do cubo com a primeira em inglês de sua posição, assim:

- A face voltada para nós (face frontal), chamamos de *Front* e indicamos por **F**;
- A face oposta à Front chamamos de *Back* e indicamos por **B**;
- A face superior chamamos de *Under* e indicamos por **U**;
- A face inferior chamamos de *Down* e indicamos por **D**;
- A face do lado direito chamamos de *Right* e indicamos por **R**;
- A face do lado esquerdo chamamos de *Left* e indicamos por **L**.

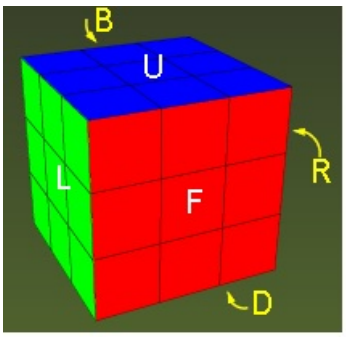


Figura 3.3: As faces do Cubo

Os movimentos do cubo ocorre quando giramos qualquer face do cubo, no sentido horário ou anti-horário, $\frac{1}{4}$ de volta, meia volta, $\frac{3}{4}$ de volta ou a volta completa. É fácil

perceber que o movimento $\frac{3}{4}$ de volta no sentido horário é igual ao movimento $\frac{1}{4}$ de volta no sentido anti-horário e que o movimento volta completa retorna o cubo a posição inicial. Assim todos esses movimentos se resumem apenas ao movimentos $\frac{1}{4}$ de volta e meia volta, nos sentido horários o anti-horários e o movimento não fazer nada, isto é, a posição inicial do cubo, chamaremos este movimento de identidade, e indicaremos I. Indicaremos os movimentos de um quarto de volta em sentido horário pelas iniciais das faces, ou seja, F, B, U, D, L e R, indicaremos ainda os movimentos de meia volta por F^2, B^2, U^2, D^2, L^2, R^2 e os movimentos de um quarto de volta no sentido anti-horário por F^{-1}, B^{-1}, U^{-1}, D^{-1}, L^{-1}, R^{-1}.

(a) Movimento R

(b) Movimento U^{-1}

Figura 3.4: Movimentos R e U^{-1}

Devemos obsevar que no cubo os movimentos alteram a configuração das facetas dos cubinhos, mas preservam a forma geral do cubo, por isso são chamados simetrias [2] do cubo e nem todas as configurações são possíveis. Por exemplo, cubinhos de aresta não podem ser trocados com os de cantos, etc.

Para resolver o cubo basta encontrar uma sequência dos movimentos acima tal que, o cubo retorne a sua posição original. Uma sequência de movimento feita no cubo poderia ser F seguido da L seguido da D seguido da U, iremos escrever esta sequência como FLDU, como se quiséssemos "multiplicar"F por L por D por U.

A busca por uma sequência que resolva o cubo é um desafio de milhões de pessoas pelo mundo, adepto desse quebra cabeça. Existem algumas maneiras de resolver o cubo:

1º: Método empírico: é o método adotado pela maioria das pessoas, elas vão criando suas próprias estratégias para tentar chegar ao seu objetivo.

2º: Método estratégico: usar um conjunto de sequências pré definidas para realizar tarefas específicas com o cubo a fim de levá-lo gradativamente à solução.

[2] Transformação geométrica que mantém inalteradas a forma, as dimensões ou quaisquer outras propriedades de uma figura

3º Método algébrico: encontrar a solução fazendo as contas. Requer conhecimentos aprofundados da Teoria de Grupos.

Neste trabalho não iremos focar com a solução do cubo, mas sim mostrar que alguns elementos da Álgebra podem ser aplicados nos movimentos do cubo de Rubik. Usaremos estes elementos para mostrar quantas são as configurações totais das facetas do cubo.

3.2.1 Grupo de Rubik

Certos conjuntos de permutações também formam grupos. Nesta seção mostra que o conjunto de todas as posições possíveis de um cubo mágico forma um grupo.

Proposição 14 : *O conjunto de todas as permutações das facetas do Cubo forma um grupo* $\Re$ *chamado Grupo de Rubik.*

O conjunto, que formará o referido grupo, consiste dos movimentos L, R, F, B, U, D e de todas as sequências formadas a partir destes movimentos. Assumindo que duas sequências que produzem o mesmo resultado são vistas como iguais, por exemplo F e F^5 são o mesmo elemento do grupo $\Re$.

De fato, os movimentos L, R, F, B, U, D e de todas as sequências formadas a partir destes movimentos são associativa, a figura abaixo ilustra a associatividade destes movimentos:

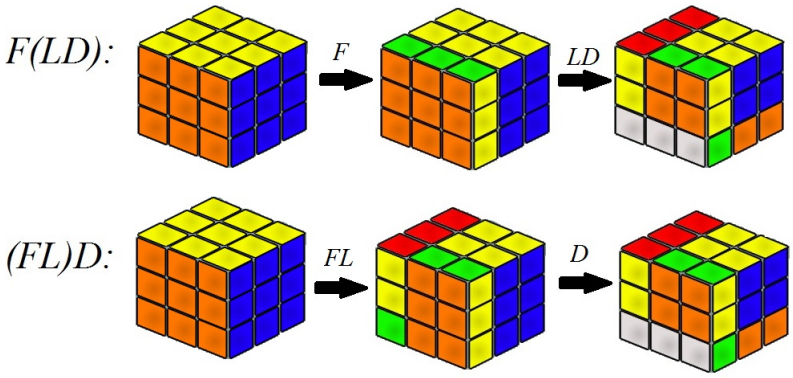


Figura 3.5: Sequências associativas

Percebemos então que $F(LD) = (FL)D$, ou seja, obedece a propriedade associativa.

Existe um elemento neutro, que é o fazer nada, isto é, deixar o cubo inalterado. Indicamos esse movimento por I, e o chamamos identidade, apresentamos abaixo um exemplo que verifica a existência do elemento neutro:

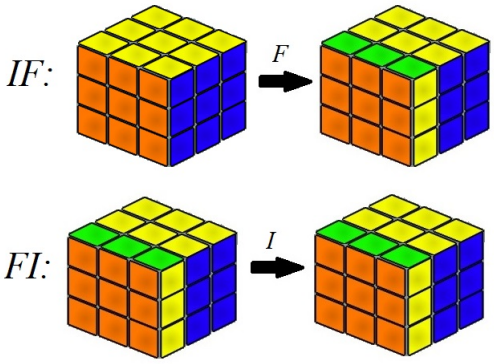


Figura 3.6: Existência do elemento neutro

Verifica-se também que todos os elementos tem um inverso, ou seja, dada uma sequência de movimento, existe outra sequência tal que retorne o cubo a posição inicial (I), onde para desfazer uma seqüência de movimentos, devemos executar em ordem reversa os opostos dos movimentos individuais, assim F^{-1} é o inverso de F, ou seja $FF^{-1} = I$ e $(U^{-1}L^{-1}F^{-1})$ é o inverso da sequência (FLU), ou seja $(FLU)(U^{-1}L^{-1}F^{-1}) = I$. A figura abaixo apresenta movimentos inversos:

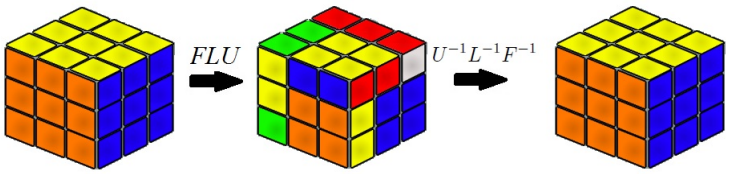


Figura 3.7: Elemento invertível

Portanto, pela definição 1, o cubo de mágico é um grupo denominado Grupo de Rubik. No entanto, ele não é *abeliano*, pois existem sequências que não são comutativas, por exemplo $LF \neq FL$, como mostra a figura 3.8.

Em relação a paridade o Grupo de Rubik é um grupo de permutação par, percebemos isso ao observar o efeito de F nas facetas da face frontal $(FurFrdFldFul)(FrFdFlFu)$ que representa uma permutação par, conforme figura 3.9.

Apresentaremos outros exemplo que percebemos a paridade no cubo:

i) A sequência $(L^2F^2)^3$, onde este movimento troca apenas dois pares de cubo, fomando assim permutação par, $(Ul\ Dl)(Uf\ Df)$, como podemos ver na figura 3.10:

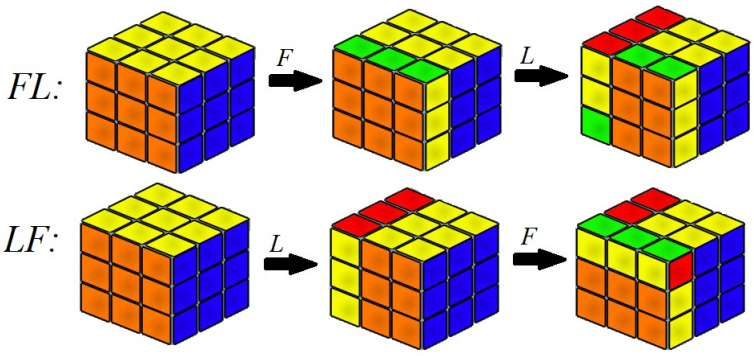


Figura 3.8: Sequências não comutativas

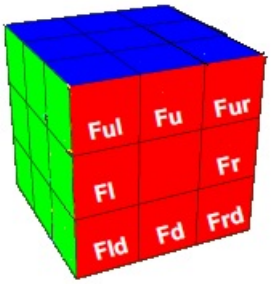


Figura 3.9: Paridade no cubo

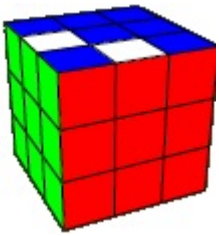


Figura 3.10: Sequência $(L^2F^2)^3$

ii) A sequência $BU^{-1}F^{-1}UB^{-1}U^{-1}FU$ que troca ciclicamente três cubinhos, conforme a figura 3.11.

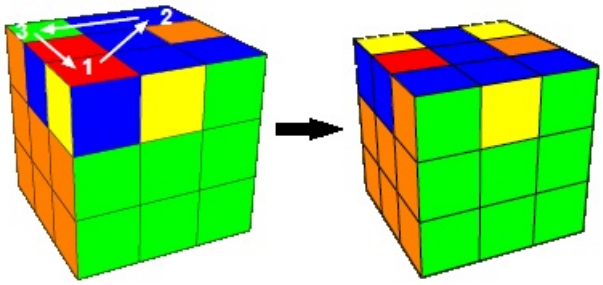


Figura 3.11: Sequência $BU^{-1}F^{-1}UB^{-1}U^{-1}FU$

Após o movimento acontece a permutação $(Ulf\ Ulb\ Urb)$ que também é uma permutação par, pois pode ser fatorada em um número par de transposições.

Apresentaremos agora alguns resultados importantes em relação a paridade do Grupo de Rubik:

i) Não existe nenhuma combinação de movimentos que consiga trocar apenas um par de cubinhos.

De fato, pois isso só aconteceria se a permutação fosse ímpar, e o conjunto das permutações ímpares não forma um grupo, pelo fato de I ser uma permutação par, ou seja não existe um elemento neutro no conjunto das permutações ímpares.

E desse resultado podemos concluir que de todas a configurações dos cubo apenas a metade pode ser feita através de movimentos de rotação, ou seja as permutações pares.

ii) Não é possível girar um único cubinho de aresta deixando os demais como estão.

Podemos perceber isso na figura 3.12, após o movimento F, vemos que dois pares de flechas azuis invertem suas posições, ou seja estes dois pares de cubinhos foram girados.

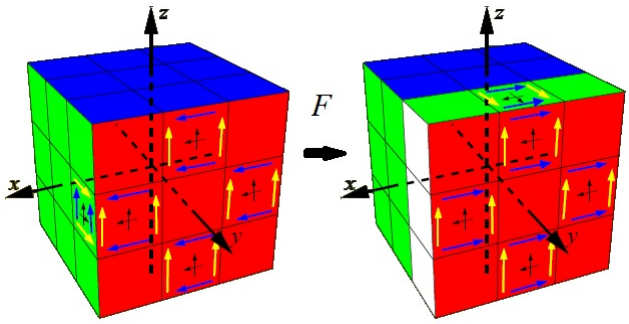


Figura 3.12: Movimento F

Um outro exemplo que ilustra este resultado é a sequência

$$FUD^{-1}L^2U^2D^2RU^{-1}R^{-1}D^2U^2L^2DU^{-1}F^{-1}U$$

onde o gera a permutação $(Fu\ Uf)(Lu\ Ul)$, como mostra a figura 3.13.

Sendo assim, apenas $\frac{1}{2}$ das orientações das arestas poderão ser formadas através das sequências de movimentos, pois para cada giro de uma aresta necessariamente terá outro giro de outra aresta.

iii) A rotação dos cubinhos de canto deve ser congruente a zero módulo 360°.

Para ver isso, marcamos os 4 cubinhos do topo e os 4 cubinhos de baixo e giramos uma face adjacente, como mostra a figura 3.14.

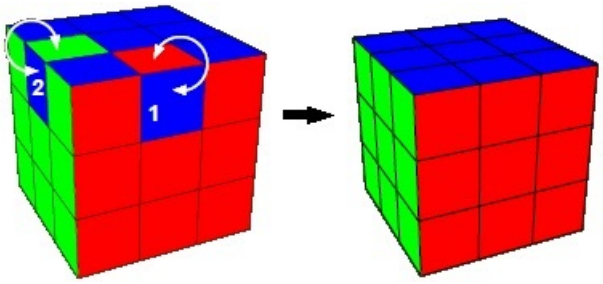


Figura 3.13: Movimento $FUD^{-1}L^2U^2D^2RU^{-1}R^{-1}D^2U^2L^2DU{-}1F^{-1}U$

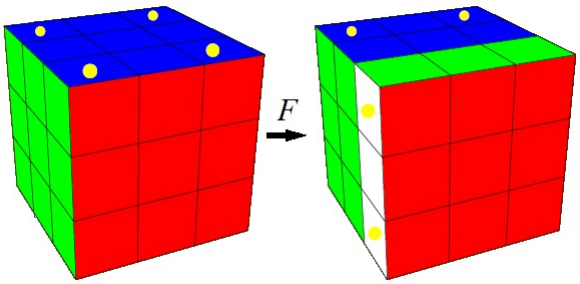


Figura 3.14: Paridade dos Cantos

Olhando para um canto ao longo de uma reta passando pelo vértice e pelo centro do cubinho, há 3 possíveis orientações para um cubinho: A marca está em cima ou em baixo: o cubinho não sofreu rotação (0°); a marca está girada 120° no sentido horário; A marca está girada 240° no sentido horário.

Se somarmos todos esses números para os oito cantos, teremos um múltiplo de 360°, ou seja a rotação total será congruente a zero. De fato, observe que dois cantos foram girados de 120° e dois de 240°.

Assim concluímos que sempre que um cubinho de cantos girar 120° no sentido horário, necessariamente outro cubinho tem que girar 120°no sentido anti-horário, ou seja, 240° no sentido horário. Um exemplo disso é a sequência $F^{-1}DFLDL^{-1}ULD{-}1L^{-1}F^{-1}D^{-1}FU^{-1}$ que gera a permutação $(Luf\ Flu\ Ufl)(Ruf\ Ufr\ Frd)$, que é uma permutação par, onde o primeiro ciclo gira o cubinho no sentido horário e o segundo ciclo gira o anti-horário.

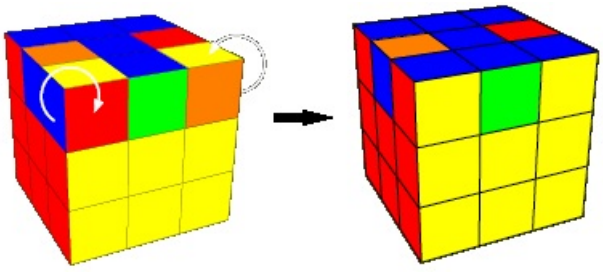


Figura 3.15: Movimento $F^{-1}DFLDL^{-1}ULD{-}1L^{-1}F^{-1}D^{-1}FU^{-1}$

Sendo assim, apenas $\frac{1}{3}$ das orientações das arestas poderão ser formadas através das sequências de movimentos, pois para cada giro, no sentido horário, de um cubinho de canto necessariamente terá outro giro, no sentido anti horário, de outro cubinho.

Depois de todos estes resultados podemos concluir quantos elementos tem o conjunto que forma o Grupo de Rubik, ou seja, quantas são as posições do cubo formada através de movimentos de rotação das facetas.

Primeiro consideraremos as posições dos cubinhos, ou seja, existe 8 posições para os de cantos e 12 posições para as arestas, um total de 8!12! rearranjos. Consideraremos agora a rotações dos cubinhos, nos cubinhos de canto existem 3 possíveis de rotação, ou seja, 3^8 possibilidades, já as arestas existem 2 possíveis rotações, ou seja, 2^{12} possibilidades. Que totaliza 8! 12! 3^8 2^{12} rearranjos.

Agora iremos retirar as restrições quantos as paridades: Apenas $\frac{1}{2}$ são permutações pares, apenas $\frac{1}{2}$ dos cubinhos arestas terão a orientação correta e nos cubinhos de cantos apenas $\frac{1}{3}$ terão a orientação correta. Portanto, quantidade total de posições possíveis de serem formadas através de sequências dos movimentos F, B, U, D, L, R é:

$$\frac{8!\ 12!\ 3^8\ 2^{12}}{2\ .\ 2\ .\ 3} = 43.252.003.274.489.856.000\ \textit{posições}$$

3.3 Criptografia e os criptossistemas

Nesta seção iremos fazer uma abordagem histórica da criptografia, mostrando a evolução dos métodos de cifragem, dando enfase aos Criptossistemas de transformação afim, que é uma aplicação do grupo Z_m, fornecendo dados para que o Professor de Matemática possa ter ideias de como introduzir este assunto no ensino básico.

3.3.1 Um pouco de história

A palavra CRIPTOGRAFIA vem do grego, *Kriptós*: escondido, oculto e *grápho*: grafia e definimos como a arte ou ciência de escrever mensagens em cifras ou códigos, de modo que somente a pessoa autorizada possa decifrar e ler as mensagens. A mensagem a ser enviada é chamada de *texto-original* e a mensagem codificada é chamada de *texto-cifrado*.

Um dos primeiros textos sobre códigos secretos foi escrito pelo geógrafo e histori-

ador grego Herótodo (485 a.C. - 420 a. C.),na sua obra "As Histórias de Herótodo", onde ele retrata a história do conflito entre a Pérsia e a Grécia no século V antes de Cristo. Vejamos a história contada por Herótodo:

> O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz deperceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os gregos. (SINGH, 2007, p. 20)

Esta história contada por Herótodo não se trata de uma comunicação secreta pois, foram obtidas através de ocultação de mensagem, que chamamos de *estenografia*, que a arte ou ciência de ocultar mensagens. E com a evolução da estenografia chegamos a ciptografia, que é o nosso foco neste trabalho.

O primeiro código secreto que se tem notícia foi utilizado pelo militar e governante romano Júlio César (100 a.C. - 44 a.C.), na época da transição do final do período republicano da Roma Antiga. Júlio César é considerado por muitos o maior gênio militar da história. Um dos motivos que pode justificar esse adjetivo é o fato dele utilizar um recurso para codificar mensagens com o objetivo de manter segredos de natureza militar. No livro As vidas dos Césares, escrito no século II por Suetônio, um dos recursos utilizados por César consistia numa substituição de cada letra do alfabeto por outra, três posições adiante, a partir do que as três últimas letras do alfabeto fazem corresponder às três primeiras. Na prática, a letra a é substituída pela letra d; a letra b, pela e; a letra c, pela f e assim sucessivamente.

No século IX, o matemático árabe AL-Kindi escreveu o livro, *Um manuscrito sobre a decifração de mensagens criptográficas*, nesse livro o método das análises das frequências, o qual permite romper todas as cifras de substituição monoalbabética, ou seja, cifras de substituição a partir das quais cada letra do texto claro é substituída por outra letra no texto cifrado, de forma constante.

Em meados de 1440, o arquiteto italiano Leon Battista Albertin (1404 - 1472) escreveu um ensaio do que acreditava ser um novo tipo de cifra. Alberti propôs a utilização de dois ou mais alfabetos cifrados, usados alternadamente, para confundir os criptoanalistas. O avanço principal do método de Alberti consiste em não permitir que a mesma letra do texto original apareça como uma única letra do alfabeto cifrado, ou seja, ele é o primeiro personagem que se tem notícia que utilizou a cifra de substituição polialfabética.

A primeira máquina criptográfica que se tem registro foi inventada no século XV pelo arquiteto italiano Leon Alberti, um dos criadores da cifra polialfabética. A máquina era composta de dois discos de cobre. O maior era fixo e o outro, o menor, era móvel. Cada disco continha o alfabeto ao longo da sua borda; no disco maior, o alfabeto original em letras maiúsculas e, no menor, o alfabeto cifrado em letras minúsculas. A figura 3.16 mostra uma dessa máquinas.

Figura 3.16: Disco de cifras usado na guerra civil americana

Em 1918, o inventor alemão Arthur Scherbius e seu amigo Richard Ritter criaram uma máquina de cifras mecânica, basicamente uma versão elétrica do disco de Alberti, mais tarde vendida como máquina Enigma. Em 1925, Scherbius produziu a Enigma em grande escala, pois as autoridades alemãs acreditavam na segurança absoluta que ela proporcionava. Trinta mil máquinas foram adquiridas, nas duas décadas da 2ª guerra, pela exército alemão.

3.3.2 Criptossistemas

Nesta seção iremos apresentar algumas ferramentas que usaremos para codificar e decodificar uma mensagem, assim iremos apresentar algumas definição e resultados no ajudará em tais tarefas.

Na criptografia, o processo de converter um texto original para um texto cifrado é chamado de codificação ou cifragem, e o processo de reverter é chamado de decodificação ou decifragem.

Definição 19 : *Sejam P o conjunto de todas as possíveis mensagens unitárias* **u** *do texto original e C todas as possíveis mensagens unitárias* **c** *do texto cifrado, assim a correspondência biunívoca*

$$f : P \to C \text{ tal que } f(u) = c$$

é o processo de codificação. E a correspondência biunívoca

$$f^{-1} : C \to P \text{ tal que } f^{-1}(c) = u$$

é o processo de decodificação. Qualquer uma dessa bijeções de P sobre C recebe o nome de Criptossistemas.

Normalmente substituimos as letras do alfabeto usado por números inteiros $0, 1, 2, ...$, para torna mais a construção do criptossistema f. As barras dos elementos de $\mathbb{Z}_m$ serão omitidas ao longo do texto, para não carregar o mesmo.

Fazendo a correspondência identidade entre o alfabeto $A = \{A, \mathcal{B},\ C,\ ...,\ X,\ Y,\ Z\}$ e o conjunto dos números inteiros $\mathbb{Z}_{27} = \{0,\ 1\ 2,\ 3,\ ...,\ 26,\ 27\}$ chegamos:

A	B	C	...	K	...	X	Y	Z
$\updownarrow$	$\updownarrow$	$\updownarrow$		$\updownarrow$		$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	...	10	...	24	25	26

Teorema 15 : *Sejam $m \in \mathbb{N}$ e $a,\ b \in \mathbb{Z}_m$ fixados. Se $mdc(a,\ m) = 1$, então a função $f : \mathbb{Z}_m \to \mathbb{Z}_m$ dada por $f(x) = ax + b$ é um criptossistema.*

Demonstração: Como $mdc(a,\ m) = 1$ temos que existe $a^{-1} \in {\mathbb{Z}^*}_m$ tal que $a.a^{-1} = 1$. Assim

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

onde $b^{-1} = -ab^{-1}$, é tal que $f \circ f^{-1} = f^{-1} \circ f = I_{\mathbb{Z}_m}$; isto é, f^{-1} é a função inversa de f.

O criptossistema $f(x) = ax+b$ é chamado de transformação afim, onde o par $(a,\ b)$ é chamado de chave de codificação. Quando $m = 27$, $a = 1$ e $b \in \mathbb{Z}_{27}$ o criptossistema $f(x) = x + b$ caímos nas famosas Cifras de César.

Apresentaremos agora um exemplo de criptossistemas, codificaremos o texto original PROFMAT, com a chave de codificação (2, 4). Primeiramente faremos a correspondência numérica

P	R	O	F	M	A	T
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
15	17	14	5	12	0	19

agora passaremos a codificar o texto original usando a função $f(x) = 2x+4$, onde x representa o correspondente numérico da mensagem original e $f(x)$ representa o correspondente numérico da mensagem codificada. Daí:

$$f(15) = 2.15 + 4 = 34 \equiv 7 \ mod\ 27$$

$$f(17) = 2.17 + 4 = 38 \equiv 11 \ mod\ 27$$

$$f(14) = 2.14 + 4 = 32 \equiv 5 \ mod\ 27$$

$$f(5) = 2.5 + 4 = 14$$

$$f(12) = 2.12 + 4 = 28 \equiv 1 \ mod\ 27$$

$$f(0) = 2.0 + 4 = 4$$

$$f(19) = 2.19 + 4 = 42 \equiv 15 \ mod\ 27$$

Fazendo novamente a correspondência numérica, temos:

7	11	5	14	1	4	15
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
H	L	F	O	B	E	P

Portanto o texto original PROFMAT cifrado com a chave (2, 4) é HLFOBEP

Iremos agora decodificar esta mensagem HLFOBEP. Primeiro calculamos a inversa da função $f(x) = 2x + 4$ que é a função $f^{-1}(x) = 2^{-1} - 4.2^{-1}$. Daí calculando os

inversos temos:

$$2^{-1} \equiv 2^{\varphi(27)-1} \equiv 2^{1}7 \equiv 14 \ mod \ 27$$

$$-4.2^{-1} \equiv -4.14 \equiv 23.14 \equiv 322 \equiv 25 \ mod \ 27$$

Assim $f^{-1} = 14x + 25$ e fazendo:

$$f^{-1}(7) = 14.7 + 25 = 123 \equiv 15 \ mod \ 27$$

$$f^{-1}(11) = 14.11 + 25 = 179 \equiv 17 \ mod \ 27$$

$$f^{-1}(5) = 14.5 + 25 = 95 \equiv 14 \ mod \ 27$$

$$f^{-1}(14) = 14.14 + 25 = 221 \equiv 5 \ mod \ 27$$

$$f^{-1}(1) = 14.1 + 25 = 39 \equiv 12 \ mod \ 27$$

$$f^{-1}(4) = 14.4 + 25 = 81 \equiv 0 \ mod \ 27$$

$$f^{-1}(15) = 14.15 + 25 = 235 \equiv 19 \ mod \ 27$$

Portanto após decodificar o texto cifrado, chegamos em 15 17 14 5 12 0 27 que fazendo a relação numérica chegamos, no texto original PROFMAT.

Considerações Finais

Neste trabalho apresentamos aplicações da teoria de grupos, e concluímos que é possível aplicar alguns conceitos desta Teoria nas salas de aula do Ensino Médio.

Ao apresentar uma maneira algébrica de mostrar porque o produto de dois números negativos é sempre um número positivo, verificamos que, realizar esta operação não é tão simples assim, e por isso a maioria dos professores, talvez influenciados por livros mais antigos, optam por simplesmente fazer com que os seus alunos decorem a regra, o que gera dificuldades para a compreensão e aplicação correta nas operações. Portanto, é papel do professor ter o maior número de estratégias possíveis para melhorar a compreensão do conteúdo para os alunos.

Ao abordar o uso da teoria de grupos no cubo mágico, mostramos uma contextualização do ensino de álgebra através dos movimentos do cubo de Rubik. Conseguimos mostrar nesta seção que algumas propriedades da álgebra, que pareciam sem importância, podem ser aplicados em várias ações do dia a dia. Apresentamos também uma possibilidade da inserção de jogos no ensino de Matemática, que fará com que o aluno tenha mais interesse no ensino de Álgebra. Quando eu estava escrevendo sobre o cubo, propus uma atividade, com meus alunos do 3º ano do Curso Técnico em Agropecuária Integrado ao Ensino Médio do IFMT/Campus São Vicente, onde foi verificado as propriedades algébricas no cubo mágico, através das permutações do Grupo de Rubik, e através destas propriedades encontrar a quantidades totais das permutações possiveis no cubo. E o resultado da aula foi surpreendente, pois os alunos se interessaram muito pelo assunto, conseguiram perceber a ligação da teoria de grupo com os movimentos do cubo, e ficaram muito surpresos com a quantidade possíveis de configuração do cubo.

Finalmente ao abordar os segredos da criptografia, conseguimos mostrar uma maneira de despertar o interesse do aluno para a Álgebra, pois é de fácil compreensão e instiga o aluno cifrar e decifrar mensagens secretas. Acredito que uma atividade simples

de codificação e decoficação de mensagens, usando os criptossistemas de transformação afim, por exemplo, tornará as aulas de Matemática mais atrativa para os alunos do ensino médio.

Este trabalho não teve a intenção de servir como material pedagógico para ser usado em sala de aula. O objetivo foi criar uma fonte que forneça, ao professor, um suporte no planejamento de suas aulas e que ajude o professor a responder alguns questionamento envolvendo álgebra. E para trabalho futuro, pretendemos elaborar e disponibilizar algumas atividades, envolvendo os assuntos aqui abordados, que possam servir como material pedagógico a ser usado em sala de aula.

Referências Bibliográficas

[1] BORBA, Rute, O que pode influenciar a compreensão de conceitos: o caso dos números relativos In: BORBA, Rute e GUIMARÃES, Gilda, **A pesquisa em Educação Matemática: repercussões na sala de aula** , São Paulo: Cortez, 2009.

[2] DOMINGUES, H. H. e IEZZI, G., **Álgebra Moderna**,4 ed., São Paulo: Atual, 2003.

[3] FIGUEIREDO, Luiz Manoel Silva, **Números primos e Criptografia de chave pública**, Rio de Janeiro: Universidade Federal Fluminense, 2006.

[4] GARCIA, Arnaldo e Lequain, Yves, **Elementos de álgebra**, Associação Instituto de Matemática Pura e Aplicada, 2003.

[5] GOMES, Olimpio Ribeiro e SILVA, Jhone Caldeira, **Estrutura Algébricas para Licenciatura**, Brasília: Editora do Autor, 2008.

[6] GONÇALVES, Adilson, **Introdução à álgebra**, 5 ed., Rio de Janeiro: IMPA, 2008.

[7] HEFEZ, Abramo, **Elementos de Aritmética**, 2 ed., Rio de Janeiro: SBM, 2011.

[8] LIMA, Elon Lages, **Meu Professor de Matemática e outras histórias**, 5 ed., Rio de Janeiro: SBM, 2006.

[9] SANTOS, José Plínio de Oliveira, **Introdução à teoria dos números**, 3 ed., Rio de Janeiro: IMPA, 2010.

[10] SCHULTZER, Waldeck, **Aprendendo Álgebra com o Cubo Mágico** , Uberlândia, 2005. http://www.dm.ufscar.br/ waldeck/rubik Consultado 02/02/2014

[11] SILVA, Valdir Vilmar da, **Números: Construções e Propriedades**, Goiânia: Editora da UFG, 2003.

[12] SINGH, Simon; tradução de Jorge Calife, **O livro dos Códigos**, 6 ed., Rio de Janeiro: Record, 2007.