UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
PROFMAT- Mestrado Profissional em Matemática em Rede Nacional

Grupos, simetrias e quadrados mágicos

Zelia Fernanda Domingos da Silva

RIO DE JANEIRO/RJ
2020

Zelia Fernanda Domingos da Silva

Grupos, simetrias e quadrados mágicos

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-graduação em Matemática PROFMAT da UNIRIO, como requisito para a obtenção do grau de MESTRE em Matemática.

Orientador:Silas Fantin
Doutor em Matemática

RIO DE JANEIRO/RJ
2020

Catalogação informatizada pelo(a) autor(a)

S586 Silva, Zelia Fernanda Domingos da
Grupos, simetrias e quadrados mágicos / Zelia Fernanda Domingos da Silva. -- Rio de Janeiro, .

Orientador: Silas Fantin.
Dissertação (Mestrado) - Universidade Federal do Estado do Rio de Janeiro, Programa de Pós-Graduação em Matemática, .

1. Grupos. 2. Simetrias. 3. Subgrupos. 4. Permutação. 5. Quadrado Mágico. I. Fantin, Silas, orient. II. Título.

Zélia Fernanda Domingos da Silva

Grupos, simetrias e quadrados mágicos

Trabalho de Conclusão de Curso apresentado ao Programa de Pós graduação em matemática PROFMAT da UNIRIO como requisito para obtenção do grau de MESTRE em Matemática.

Aprovada em: 03 de março de 2020.

BANCA EXAMINADORA:

Prof. Dr. Silas Fantin - Orientador

UNIRIO

Prof. Dra. Cecilia Fernanda Saraiva de Oliveira

UNIRIO

Prof. Dra. Christina Fraga Esteves Maciel Waga

UERJ

Dedicatória

Aos meus amados pais Alzira Domingos e Fernando da Silva e ao meu grande amor Everton Nascimento que sempre me apoiaram e foram fundamentais para a conclusão desse curso.

Resumo:

O objetivo principal deste trabalho é apresentar como podemos utilizar alguns recursos de teoria de grupos, em particular, grupos de simetria do quadrado, para construir todas as soluções de quadrados mágicos de ordem 3.

Para tanto, será feito uma fundamentação de alguns aspectos acerca da teoria de grupos, onde veremos o teorema de Lagrange, que diz de maneira informal, que um grupo finito pode ser dividido em pedaços com a mesma quantidade de elementos e com isso obter como consequência imediata o pequeno teorema de Fermat e o teorema de Euler vistos em um curso básico de aritmética.

Além disso, estudaremos algumas construções de quadrados mágicos de ordem n e apresentaremos uma seleção de possíveis atividades a serem implementadas numa perspectiva metodológica de resolução de problemas no ensino básico.

Palavras - chaves: Grupos; Subgrupos; Grupo S_n; Quadrado Mágico; Permutação.

Agradecimentos

A Deus, por sempre guiar todos os meus projetos e permitir a realização de mais um dos meus infinitos sonhos.

À minha mãe Alzira, minha maior incentivadora e meu maior exemplo de comprometimento.

Ao meu pai Fernando pelo exemplo de profissional e por sempre acreditar na minha capacidade.

Ao meu marido Everton, por se orgulhar de mim, por me amar em todos momentos e por entender minha ausência e falta de paciência.

À minha tia Ângela, por ser uma segunda mãe tão boa quanto a primeira.

Aos meus irmãos Rafael, Renan, Rômulo e Lucas, por serem os melhores companheiros da vida.

À minha afilhada Eduarda, por me motivar a progredir.

Aos meus professores do PROFMAT da UNIRIO, por todas aulas, paciência, dedicação e parceria.

Aos meus colegas de turma do PROFMAT da UNIRIO, em especial, aos meus amigos Ana Eliza, Bruno, Matheus e Stella por todo estudo, matéria compartilhada, risadas e muretas.

À CAPES pelo suporte financeiro.

Ao meu orientador Dr. Silas, que apesar de todos os problemas, não desistiu e não me deixou desistir, se predispondo, mesmo que forma bem peculiar, a me auxiliar e incentivar no que fosse necessário.

ABSTRACT

The aim of this work is to present a way that we can use some resources of group theory, in a particular way, symmetry of the square, in order to build all the solutions of magic squares of the third order.

To achieve this we will ground some aspects about group theories that we will look at Lagrange's theorem. It says, in a informal way, that a finite group can be divided in pieces with the same amount of elements and, because of it, to obtain the Fernat's and Euler's theorems as an immediate consequence in basic Arithmetics.

Besides, we will study some constructions of magic squares of order n and we will present a selection of possible activities to be implemented in a methodological perspective to solutions of problems in the Elementary and Secondary schools.

Keywords: groups, subgroups, Sn groups, magic square, permutation

SUMÁRIO

INTRODUÇÃO

A teoria de grupos é uma das ferramentas mais utilizadas na matemática moderna e nas diversas nas áreas da ciência. Este conceito é fundamental e estão incluídas a teoria quântica de campos, as estruturas atômicas e moleculares, além do próprio estudo de álgebra abstrata. Tal conceito é usado para a construção de outras estruturas algébricas, como anéis, corpos, módulos e espaços vetoriais, uma vez que estes podem ser vistos como grupos dotados de operações e axiomas adicionais.

A origem da teoria de grupos surgiu no trabalho do matemático Frances Evariste Galois (1811-1832) buscando descrever as simetrias de equações satisfeitas pelas soluções de uma equação polinomial. Em 1832, por meio de uma carta escrita ao seu amigo Auguste Chevalier, Galois esboçou o seu famoso trabalho sobre solubilidade por radicais, introduzindo o conceito de grupo solúvel. O problema consistia em mostrar que uma equação polinomial admite solução por radicais se seu grupo é solúvel.

A definição moderna que conhecemos do conceito de grupo foi dada por Arthur Cayley (1821-1895) em 1854 e permitiu que a teoria de grupos se desenvolvesse rapidamente, e foi tão influente que sua expansão rompeu os limites da álgebra. Grupos aparecem em todas as áreas da matemática e são usados nas ciências em geral para determinar a simetria interna de uma estrutura na forma de automorfismos de grupo. Uma simetria interna está normalmente associada a alguma propriedade constante. E o conjunto de transformações que preserva esta propriedade forma um grupo, chamado grupo de simetria.

Neste trabalho apresentaremos os principais conceitos, propriedades e resultados na teoria de grupos que servirão de base para o estudo do grupo de simetrias, também conhecido por grupo diedral ou grupo de permutações, onde os movimentos são representados por permutações, e iremos explorar o grupo de simetrias no triangulo equilátero e no quadrado.

Um quadrado mágico é uma matriz quadrada de números inteiros positivos, sendo que nenhum destes números se repetem, em que a soma de cada linha, de cada diagonal e de cada coluna tem o mesmo valor M, chamado de constante mágica.

Existem muitas histórias sobre o surgimento dos quadrados mágicos. Os primeiros a trabalhar com os quadrados mágicos foram os chineses, hindus e árabes. A versão mais antiga é o Loh-Shu encontrado na China por volta de 2850 a.C. e é referente a um quadrado mágico de ordem 3. Iremos mostrar como o grupo de simetria do quadrado pode ser útil para determinarmos todos os quadrados mágicos de ordem 3.

No Brasil os livros didáticos de matemática do ensino Fundamental e Médio raramente fazem alusão aos quadrados mágicos. E quando é feita, se limitam a apresentar os de ordem 3 e com pouquíssima referência sobre aplicações, tornando os Quadrados Mágicos apenas objetos de diversão e curiosidade.

Iremos também estudar Quadrados Mágicos e apresentaremos aplicações para os anos finais do ensino fundamental e ensino médio e algumas curiosidades sobre o tema como o misticismo de amuletos de metal com inscrição de quadrados mágicos.

A seguir faremos uma descrição sucinta de cada capitulo.

No capítulo 1 iremos apresentar os conceitos preliminares, necessários para o entendimento do trabalho, como noções básicas de grupos e subgrupos; permutações; grupos diedrais; teorema de Lagrange e homomorfismo. E obteremos como consequência do teorema de Lagrange, o Pequeno teorema de Fermat e o teorema de Euler, vistos em um curso de aritmética.

No capítulo 2, apresentaremos o grupo de simetria S_n, estudando com detalhes as permutações pares e impares que são fundamentais para elaboração, discursão e conclusão deste trabalho.

No capítulo 3, apresentaremos uma aplicação de teoria de grupos: os quadrados mágicos. Destacamos a história dos quadrados mágicos, sua origem, a magia dos amuletos, tipos, curiosidades, outros formatos "mágicos", e também as construções de alguns tipos de Quadrados Mágicos que possibilitam a construção de outros.

Finalmente no capítulo 4 iremos sugerir atividades com aplicação em sala de aula, relacionadas aos quadrados mágicos, mostrando o uso destes quadrados mágicos no Ensino da Matemática. Essas atividades podem ser trabalhadas com alunos dos anos finais do ensino fundamental ou alunos do ensino médio. Pois, envolvem sequência numérica, raciocínio lógico e progressão aritmética.

CAPÍTULO 1: PRÉ – REQUISITO

Este capítulo é destinado a apresentação dos pré-requisitos necessários para a compreensão deste trabalho. Será mencionado e discutido o conceito de grupo, permutações, subgrupos, teorema de Lagrange, grupos diedrais e homomorfismo.

1.1- Conceitos preliminares

Um conjunto não vazio G está munido com uma operação $*$ se, e somente se, para cada par de elementos de G sabemos associar um único $c \in G$, denotado por $c = a * b$. Equivalentemente, existe uma função

$$*: G\ x\ G \rightarrow G$$
$$(a.b) \rightarrow a * \text{b}$$

Definição 1.1 (Grupo): Um conjunto não vazio G munido de uma operação $*$ é chamado de grupo se as seguintes condições são satisfeitas:

(i) (Associativa) $a * (b * c) = (a * b) * c$, para quaisquer $a, b, c \in G$.

(ii) (Existência do elemento neutro) Existe e G, tal que $a * e = e * a = a$ para qualquer $a \in G$.

(iii) (Existência do Inverso) Para cada $a \in G$, existe $b \in G$, tal que $a * b = b * a = e$.

Denota - se um grupo G com a operação $*$ por $(G,*)$.

Exemplo 1.2: Seja $G = \{A \in M_{n\,x\,n}(R),\ det\ A \neq 0\}$ munido com a operação usual de multiplicação de matrizes. Então $(G,\ \cdot)$ é um grupo.

Definição 1.3 (Ordem de um Grupo): A ordem de um grupo $(G,\ *)$ é denotada por $|G|$ e é o número de elementos do conjunto G. Dizemos que G é um grupo finito se, e somente, se o conjunto G é um conjunto finito. Caso contrário, dizemos que G tem ordem infinita, escrevemos $|G| = \infty$ e G é dito grupo infinito.

Definição 1.4 (Grupo Abeliano): Dizemos que um $(G, *)$ é um grupo abeliano se, e somente se, $a * b = b * a$, para quaisquer $a, b \in G$.
Caso contrário, dizemos que G é um grupo não - abeliano.

Exemplo 1.5: Para todo $n > 1$ o grupo $(Z_n, + mod\ n)$ é exemplo de um grupo abeliano de n elementos.

Exemplo 1.6 (Grupo não Abeliano): Seja $G = \{A \in M_{n\,x\,n}(R),\ det\ A \neq 0\}$ munido com a operação usual de multiplicação de matrizes. Então $(G, \cdot)$ é um exemplo de grupo não abeliano.

Definição 1.7 (Permutação): Seja $C = \{1, \dots, n\}$. Toda bijeção $\sigma: C \to C$ é chamada uma permutação de C. O Grupo $S_n = \{\sigma : C \to C, \sigma \text{ é } uma\ bije\text{ção}\}$ também é chamado de grupo das permutações de n elementos.

Como há $n!$ Permutações de n elementos e o conjunto das permutações de n elementos está em bijeção com S_n , portanto a ordem de S_n é $|S_n| = n!$.

A bijeção $\sigma \in S_n$ definida por

$$\begin{array}{ccc} 1 & \to & \sigma(1) \\ 2 & \to & \sigma(2) \\ n & \to & \sigma(n) \end{array}$$

Pode ser representado por

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

O elemento neutro de S_n é a bijeção $I = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$.

Se

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \ e\ \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}.$$

Então:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \dots & \sigma(\tau(n)) \end{pmatrix}.$$

Exemplo 1.8: Seja $\sigma, \tau \in S_5$ dadas por:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} \quad \text{e} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}.$$

Então,

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \quad \text{e} \quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

Observamos que dado

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

trocando a primeira linha (domínio de σ) com a segunda (as correspondentes imagens por σ), temos que que

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(1) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

Depois, se necessário, permutamos as colunas, enumerando a primeira linha como $1, 2, \dots, n$. Por exemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \rightarrow \sigma^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Exemplo 1.9: S_2 tem 2 elementos, a saber, $I = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ *e* $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Observamos que

$$\sigma^2 = \sigma \circ \sigma = I.$$

O grupo S_3 tem 6 elementos, as bijeções:

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \sigma = r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \tau = r_{\frac{2\pi}{3}} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$f_4 = r_{\frac{4\pi}{3}} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f_5 = r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad f_6 = r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Observamos que S_3 pode ser descrito usando apenas as bijeções σ *e* τ , pois $f_4 = \tau^2$, $f_6 = \sigma \circ \tau$ *e* $f_5 = \sigma \circ \tau^2$. Temos que $\sigma^2 = I, \tau^3 = I.$ Como $r_3 . r_{\frac{2\pi}{3}} \neq r_{\frac{2\pi}{3}} . r_3$, vemos que S_3 é um grupo que não é abeliano.

Assim,

$$\text{Com } i = \{0,1\} \text{ e } j = \{0,1,2\},\ S_3 = \{\sigma^i \circ \tau^j\ , \sigma^2 = \text{I}, \tau^3 = \text{I}, \tau \circ \sigma = \sigma \circ \tau^2\}$$

Proposição 1.10: Para todo $n \geq 3$, S_n é um grupo não abeliano.

Prova: Seja $n \geq 3$ e seja $S = \{1, 2, \ldots, n\}$. Basta exibir duas bijeções do conjunto S, tais que $\sigma \circ \tau \neq \tau \circ \sigma$. Sejam σ e τ definidas por:

$$\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3 \text{ e } \sigma(x) = x, \text{ para todo } x \geq 4,$$

$$\tau(1) = 1, \tau(2) = 3, \tau(3) = 2 \text{ e } \tau(x) = x, \text{ para todo } x \geq 4.$$

Então:

$$(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(1) = 2 \text{ e } (\tau \circ \sigma)(1) = \tau(\sigma(1)) = \tau(2) = 3,$$

Logo:

$$\sigma \circ \tau \neq \tau \circ \sigma.$$

1.2- O conceito de subgrupo

Definição 1.11 (Subgrupo): Um subconjunto não-vazio H de um grupo (G,·) é um subgrupo se, e somente se,

(i) se $a, b \in H$, então $a \cdot b \in H$;

(ii) se $a \in H$, então $a^{-1} \in H$.

Observação 1: Se H é um subgrupo de G então denotaremos $H < G$.

Suponhamos que $H \subset G$ seja um subgrupo de G. Então, por definição de subgrupo, a operação de G está fechada em H, valendo (i) e (ii). Como $H \neq \emptyset$, existe $c \in H$. Então, de (ii) $c^{-1} \in H$ e de (i) e $e_G = c \cdot c^{-1} \in H$. Reciprocamente, suponhamos que $H \subset G$ seja um subconjunto que tenha as propriedades (i) e (ii) do enunciado. De (i) segue que H está munido com a operação de G e de (ii) a existência de inverso em H de cada elemento de H. Para mostrar que H é um grupo, basta observar que a operação sendo associativa em G é associativa em qualquer subconjunto, em particular, é associativa em H.

Exemplo 1.12: Seja $(G, .)$ um grupo. Então, $\{e\}$ e G são subgrupos de G, chamados de subgrupos triviais.

Exemplo 1.13:

Grupo	Subgrupo
$(\mathbb{Q}, +)$	$(\mathbb{Z}, +)$
$(\mathbb{R}, +)$	$(\mathbb{Q}, +)$
$(\mathbb{C}, +)$	$(\mathbb{R}, +)$
$(\mathbb{Q}^*, \cdot)$	$(\{-1, 1\}, \cdot)$
$(\mathbb{R}^*, \cdot)$	$(\mathbb{Q}^*, \cdot)$
$(\mathbb{C}^*, \cdot)$	$(\mathbb{R}^*, \cdot)$

1.3 - Teorema de Lagrange e aplicações:

Nesta seção iremos mostrar e estudar o teorema de Lagrange, a fim de obtermos como consequência, o pequeno teorema de Fermat e o teorema de Euler, que são muito úteis no estudo de congruências. E para isso foi necessário visitar algumas definições e proposições, tais como: classe lateral, cardinalidade de grupo e função φ.

Definição 1.14 (Classe Lateral): Seja G um grupo e H um subgrupo de G. Definimos sobre G a relação de equivalência $\sim E$ da seguinte forma:

$$y \sim_E x \text{ se e somente se , existe } h \in H \; tal \; que \; y = xh$$

Por definição, a classe lateral a esquerda de H em G que contem x é:

$$xH = \{xh \; ; \; h \in H\} = \{y \in G \; ; \; y \sim_E x\}$$

Analogamente, definimos a seguinte relação de equivalência:

$$y \sim_D x \text{ se e somente se , existe } h \in H \; tal \; que \; y = hx$$

Segue que a classe lateral a direita de H em G que contem x é:

$$Hx = \{hx \; ; \; h \in H\} = \{y \in G \; ; \; y \sim_D x\}$$

Proposição 1.15 : Todas as classes laterais tem a mesma cardinalidade de H. Se G é um grupo finito. Isto é,

$$\#\{xH\} = \#H$$

Prova: Considere a seguinte função dada por:

$$\varphi_x: H \to xH$$
$$h \to xh$$

Vamos mostrar que φ_x é uma bijeção.

De fato:

(1) $\varphi_x: H \to xH$ é injetiva.

$$\varphi_x(h_1) = \varphi_x(h_2) \implies xh_1 = xh_2 \implies x^{-1}xh_1 = x^{-1}xh_2 \implies h_1 = h_2$$

(2) $\varphi_x: H \to xH$ é sobrejetiva.

$$g \in xH\,, existe\ h \in H; g = xh\ e\ h = x^{-1}g \implies \varphi_x(h) = x(x^{-1}g) = g$$

Portanto φ_x é sobrejetiva ■

Definição 1.16 (Cardinalidade): A cardinalidade do conjunto das classes laterais à esquerda se chama o índice de H em G, denotado por $(G:H)$.

Observação 2: O índice de H em G também é a cardinalidade do conjunto das classes laterais à direita de H em G, pois a aplicação de φ é uma bijeção

$$\varphi: \{classes\ laterais\ \text{à}\ esquerda\} \to \{casses\ laterais\ \text{à}\ direita\}$$
$$xH \to Hx^{-1}$$

Portanto,

$$\#\{classes\ laterais\ \text{à}\ esquerda\} = (G:H) = \#\{classes\ laterais\ \text{à}\ direita\}$$

Teorema 1.17 (Teorema de Lagrange): Seja G um grupo finito e H um subgrupo de G. Então:

$$|G| = |H|.(G:H)$$

Em particular:

- A ordem de H divide a ordem de G.
- O índice de H em G divide ordem de G.

Prova: considerando

$$\text{Relação } \sim E \text{ em } G \implies \text{obtemos uma partição de } G \text{ em classes}$$
$$\implies \text{por definição, } (G:H) = \#\{xH\}, x \in G.$$
$$\underset{\substack{Prop \\ 1.15}}{\Longrightarrow} \text{cada classe tem } |H| \text{ elementos.}$$
$$\implies |G| = |H|.(G:H) \blacksquare$$

Corolário 1.18: Seja G um grupo finito e $\alpha \in G$. Então a ordem de α divide a ordem de G. Ou seja,

$$o(\alpha) \text{ divide } |G|$$

Prova: Pelo teorema de Lagrange

$$|G| = o(\alpha).\big(G:o(\alpha)\big) \implies o(\alpha) \mid |G|$$

Em particular:

$$\alpha^{|G|} = \alpha^{o(\alpha).(G:\langle\alpha\rangle)} = e^{(G:o(\alpha))} = e \blacksquare$$

Corolário 1.19 (Pequeno Teorema de Fermat): Seja p um número primo e $a \in \mathbb{Z}$. Com $mdc\,(a,p) = 1$. Então:

$$a^{p-1} \equiv 1\ mod\ p, \forall\ a \in\ \mathbb{Z}_p$$

Prova: Como

$$mdc\,(a,p) = 1 \implies a \in\ \mathbb{Z}\backslash\{p\mathbb{Z}\}$$
$$\implies \bar{a} \in\ \mathbb{Z}_p\backslash\{\bar{0}\} = G \text{ , grupo de } (p-1) \text{ elementos}$$
$$\implies \bar{a}^{|G|} = \bar{1}$$
$$\implies \bar{a}^{(p-1)} = \bar{1}$$
$$\implies a^{p-1} \equiv 1\ mod\ p \blacksquare$$

Observação 3: ϕ é a função de Euler, definida por:

$$\phi\,(n) = \#\{m \in \mathbb{N};\ 1 \le m \le n, mdc\,(m,n) = 1\}$$

Corolário 1.20 (Teorema de Euler): Sejam $x, n \in \mathbb{Z}$ com $mdc\ (m,n) = 1$. Então:

$$mdc\ (x,n) = 1 \Longrightarrow x^{\phi(n)} \equiv 1\ mod\ n.$$

Prova: Como

$$\overline{a} \in \mathbb{Z}_n \text{ é } invertível \Leftrightarrow mdc(a,n) = 1$$

Segue da definição da função de Euler (Observação 3)

$$G = \phi(n)$$

Deste modo:

$$\begin{aligned} mdc\ (x,n) = 1 &\Longrightarrow x \in G \\ &\Longrightarrow x^{|G|} = e \\ &\Longrightarrow \bar{x}^{\phi(n)} = \overline{1} \\ &\Longrightarrow x^{\phi(n)} \equiv 1\ mod\ n. \blacksquare \end{aligned}$$

Definição 1.21: Sejam G um grupo e $\alpha \in G$. Denotamos por $\langle \alpha \rangle$ o conjunto de todas as potências de α.

Ou seja,

$$\begin{aligned} \langle \alpha \rangle &= \{\alpha^n \,|n \in Z\} \\ &= \{\cdots, \alpha^{-2}, \alpha^{-1}, e, \alpha, \alpha^2, \cdots\}. \end{aligned}$$

Proposição 1.22 (O subgrupo cíclico gerado por α): Sejam $(G,\cdot)$ um grupo e $\alpha \in G$. Então $\langle \alpha \rangle$ é um subgrupo de G, chamado de subgrupo cíclico gerado por α.

Prova:

a. Para todo n, m inteiros temos que $\alpha^n \cdot \alpha^m = \alpha^{n+m} \in \langle \alpha \rangle$.
b. $e = \alpha^0 \in \langle \alpha \rangle$.
c. Para todo n inteiro, temos $(\alpha^n)^{-1} = \alpha^{-n} \in \langle \alpha \rangle$.

Corolário 1.23: Se G é um grupo de ordem prima, então G é cíclico.

Prova:
$$\alpha \in G \setminus \{e\} \overset{\substack{Teo \\ Lag.}}{\Longrightarrow} |\langle\alpha\rangle| \; divide \; |G| = p$$
$$\Longrightarrow |\langle\alpha\rangle| = |G| \blacksquare$$

Definição 1.24 (Ordem de um elemento): Seja $(G,\cdot)$ um grupo. Quando $\langle\alpha\rangle$ é um grupo finito, chamamos $\langle\alpha\rangle$ de ordem de α e escrevemos $\circ(\alpha) = \langle\alpha\rangle$

Exemplo 1.25: Mostre que se p é $primo \implies a^p \equiv a \; mod \; p$, para todo $a \in \mathbb{Z}$.
Como
$$a^{p-1} \equiv 1 \; mod \; p$$
e
$$a = a \; mod \; p$$
Multiplicando
$$a^{p-1}.a \equiv a \; .1 \; mod \; p \implies a^p \equiv a \; mod \; p$$

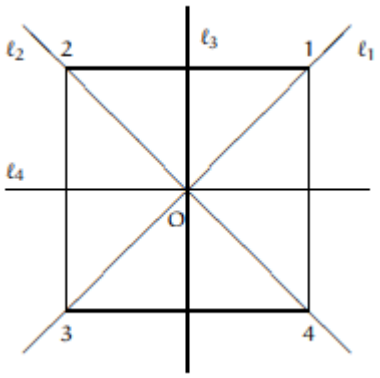
Observação 4 (Generalização do Teorema de Lagrange): Seja G grupo e sejam $K < H < G$. Temos então:
$$(G:K) = (G:H).(H:K)$$
Prova: caso $|G| < \infty$. Segue do Teorema de Lagrange:
$$H < G \Longrightarrow |G| = |H|.(G:H)$$
$$K < G \Longrightarrow |H| = |K|.(H:K)$$
$$\Longrightarrow |G| = |K|.(H:K).(G:H)$$
$$K < G \Longrightarrow |G| = |K|.(G:K)$$
Segue:
$$|K|.(G:K) = |K|.(G:H).(H:K)$$
$$\Longrightarrow (G:K) = (G:H).(H:K)$$
Este resultado vele também para grupos de ordem infinita. ■

Observação 5: Se G é um grupo abeliano e H subgrupo de G, temos:

$$G \; grupo \; abeliano, H < G \; então \; xH = Hx, para \; todo \; x \in G.$$

Prova: $xH = \{xh; h \in H\} = \{hx; h \in H\} = Hx$■

Observação 6: $D_{\square}$ grupo de simetrias especiais do quadrado não é abeliano.



De fato, seja:

$$H = \{id, R_1\}$$

Assim:

$$R_{\frac{\pi}{2}}.H = \{R_{\frac{\pi}{2}}, R_4\}$$

$$H.R_{\frac{\pi}{2}} = \{R_{\frac{\pi}{2}}, R_2\}$$

$$\Longrightarrow R_{\frac{\pi}{2}}.H \neq H.R_{\frac{\pi}{2}}$$

Exemplo 1.26: O grupo S_3 tem 6 elementos. Um subgrupo H de S_3, pelo Teorema de Lagrange, só pode ter $|H| \in \{1, 2, 3, 6\}$, que são os divisores de 6.

Classificando os subgrupos de S_3, temos:

O único subgrupo de ordem 1 é $\{I\}$

Os subgrupos de ordem 2 são: $\langle\sigma\rangle = \{I, \sigma\}, \langle\sigma \circ \tau\rangle = \{I, \sigma \circ \tau\}$ e $\langle\sigma \circ \tau^2\rangle = \{I, \sigma \circ \tau^2\}$

O único subgrupo de ordem 3 é $\langle\tau\rangle = \{I, \tau, \tau^2\} = \langle\tau^2\rangle$.

Lema 1.27: Seja $(G, \cdot)$ um grupo e seja $a \in G$ com $o(a) = n$. Então,

$$\langle a^s\rangle = \langle a^{mdc(s,n)}\rangle$$

Prova:($\subset$:) Como $s = m \cdot mdc(s, n)$, para algum $m \in \mathbb{Z}$, então

$$a^s = a^{m \cdot mdc(s,n)} = (a^{mdc(s,n)})^m \in \langle a^{mdc(s,n)} \rangle$$

Logo, $\langle a^s \rangle \subset \langle a^{mdc(s,n)} \rangle$

($\supset$:) Sejam $\alpha, \beta \in \mathbb{Z}$ tais que $mdc(s,n) = \alpha n + \beta s$. Então,

$$a^{mdc(s,n)} = a^{\alpha n + \beta s} = a^{\alpha n} \cdot a^{\beta s} = (a^n)^\alpha \cdot (a^s)^\beta = e \cdot (a^s)^\beta = (a^s)^\beta.$$

Logo,

$$a^{mdc(s,n)} \in \langle a^s \rangle \Longrightarrow \langle a^{mdc(s,n)} \rangle \subset \langle a^s \rangle. \blacksquare$$

Teorema 1.28: Todo subgrupo de um grupo cíclico é cíclico.

Prova: Seja $(G,\cdot)$ grupo cíclico gerado por a, $G = \langle a \rangle$. Se $H = \{e\}$, então $H = \{e\}$, com $e = a^0$. Suponhamos que H seja subgrupo de G, $H \neq \{e\}$. Então, existe $m \in \mathbb{Z}, m \neq 0$, tal que $a^m \in H$. Como $a^m, a^{-m} = (a^m)^{-1} \in H$, então existe um inteiro positivo n_0, tal que $a^{n_0} \in H$.

Seja $S = \{n > 0; a^n \in H\}$. S é não vazio e $S \subset \mathbb{N}$ então, pelo Princípio da Boa Ordenação, S tem um menor elemento, digamos s. Como $s \in S$, temos $a^s \in H$ e $s > 0$.

Afirmamos que $\langle a^s \rangle = H$. De fato, $\langle a^s \rangle \subset H$, pois $a^s \in H$.

Seja agora $b \in H \subset G = \langle a \rangle$. Logo, existe $n \in \mathbb{Z}$ tal que $b = a^n$. Pela divisão euclidiana de n por s, existem q, r em $\mathbb{Z}$, unicamente determinados tais que $n = qs + r$, com $0 \leq r < s$. Dessa forma,

$$b = a^n = a^{sq+r} = a^{sq} \cdot a^r = (a^s)^q \cdot a^r$$

Logo,

$$a^r = b \cdot (a^s)^{-q} \in H, \text{ com } 0 \leq r < s.$$

Pela escolha de s, temos $r = 0$. Portanto, $b = (a^s)^q \in \langle a^s \rangle$ e $H \subset \langle a^s \rangle$.$\blacksquare$

1.4 – Grupos Diedrais

Esse subcapítulo é destinado a apresentar os grupos diedrais, que é o grupo de simetrias de um polígono regular de n lados qualquer, que iremos representar por D_n.

Mostraremos que para cada $n \geq 3$ existe um grupo não - abeliano com $2n$ elementos, chamado de $grupo\ diedral\ n$ e denotado por D_n.

D_n é subgrupo de S_n e é o grupo das simetrias do polígono regular de n lados.

Fixando P um polígono regular de n lados. Considerando D_n o conjunto das bijeções do plano que deixam P invariante.

Denotando por $\prod o$ plano, se tem:

$$D_n = \left\{\sigma: \prod \to \prod, \ \sigma \text{ é } uma\ bije\text{ção } e\ \sigma(P) = P\right\}$$

D_n é subgrupo do grupo das bijeções do plano. De fato,

(i) Como $I : \prod \to \prod$ é uma bijeção tal que $I(P) = P$, então $I \in D_n$.

(ii) $(\sigma, \tau \epsilon D_n$ se, e somente se, $\sigma : \prod \to \prod$ e $\tau : \prod \to \prod$ são bijeções, tais que $\sigma\ (P) = P$ e $\tau(P) = P$, então $\sigma \circ \tau : \prod \to \prod$ é uma bijeção e

$$(\sigma \circ \tau)(P) = \sigma\big(\tau(P)\big) = \ \sigma(P) = P.$$

Logo, $\sigma \circ \tau \in D_n$.

(iii) Se $\sigma \in D_n$, então existe $\tau : \prod \to \prod$ tal que $\sigma \circ \tau = \tau \circ \sigma = I$, pois σ é uma bijeção no plano $\prod$. Como $\sigma\ (P) = P$, então

$$P = \ I(P) = (\sigma \circ \tau)(P) = \tau\big(\sigma(P)\big) = \ \tau(P)$$

Logo $\sigma^{-1} = \tau \in D_n$.

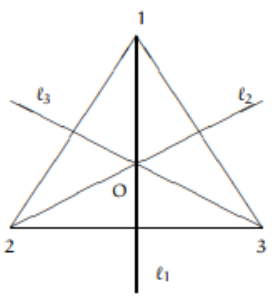
Portanto, D_n é grupo.

Faremos as construções detalhadas de D_3, o grupo das simetrias do triângulo equilátero, e de D_4, o grupo de simetrias do quadrado. A construção de D_n para n ímpar é análoga ao caso $n = 3$ e, para n par, ao caso $n = 4$

O grupo diedral 3 (D_3)

Fixamos um triângulo equilátero Δ. O grupo de bijeções do plano que deixam Δ invariante é o grupo de simetrias de Δ.

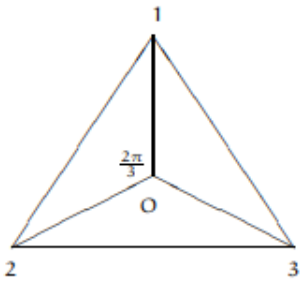
Para visualizarmos as bijeções e a imagem dos pontos de Δ, será considerado os vértices do triângulo numerados por 1,2 e 3. O triângulo Δ está inscrito em um círculo de centro O, como mostra a figura a seguir:



Temos 3 retas no plano, cujas simetrias do plano em relação a elas deixam Δ invariante. Para cada $j = 1, 2, 3$, seja l_j a reta que passa pelo vértice j e pelo centro O de Δ. A reta l_j é perpendicular ao lado oposto ao vértice j e o divide ao meio (mediana).

Sejam S_1', S_2', S_3' as simetrias do plano em relação às retas l_1, l_2, l_3, respectivamente. Essas bijeções do plano tem a propriedade de $S_j'(\Delta) = \Delta$.

O ângulo interno $1\hat{O}2$ do triângulo equilátero, em radianos, tem medida igual a $\frac{2\pi}{3}$.



Temos três rotações do plano em torno do ponto O, no sentido anti-horário, que deixam Δ invariante, isto é, $R_j(\Delta) = \Delta$, para $j = 1, 2, 3$: R_1, a rotação de $\frac{2\pi}{3}$; R_2, a rotação de $\frac{2(2\pi)}{3} = \frac{4\pi}{3}$ e R_3, a rotação de $\frac{3(2\pi)}{3} = 2\pi$. É claro que $R_3 = I$, a função identidade no plano.

As 6 bijeções estão perfeitamente determinadas pelas imagens dos vértices do triângulo. Podemos representar as 6 bijeções do plano que deixam Δ invariante por bijeções do conjunto $\{1, 2, 3\}$, os vértices do triângulo

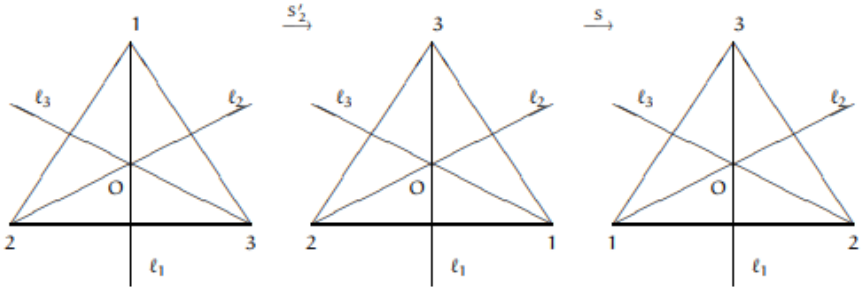
$$S = S_1' = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad S_2' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad S_3' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$R = R_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad R_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad R_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$$

Podemos descrever as 6 bijeções a partir de $S = S_1'$ *e* $R = R_1$.

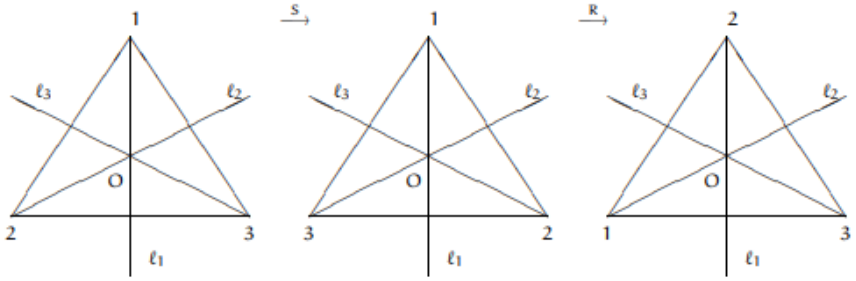
Inicialmente, observamos que $R_2 = R^2, R_3 = R^3 = I$ e $S^2 = I$. Temos que $S_2' = SR, S_3' = SR^2$ e $RS = SR^2$.

Na figura a seguir vamos visualizar a composição $S_1'S_2' = SS_2' = R$. Lembrando que as retas estão fixas.



Comparando a configuração inicial com a final, observamos que. Como $S_2 = I$, compondo com S à esquerda, obtemos que $S_2' = SR$. De modo análogo, é possível a verificação de que $SS_3' = R^2$ e conclusão que $S_3' = SR^2$.

Na figura a seguir vamos visualizar a composição $RS = SR^2 = S_3'$. Lembrando que as retas e o ponto O estão fixos. No processo, as retas l_1, l_2, l_3 determinam as simetrias.



Logo,

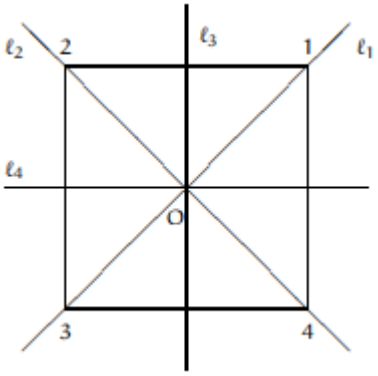
$$D_3 = \{I, R, R^2, S, SR, SR^2\}\ e\ S^2 = I, R^3 = I, RS = SR^2$$

$$= \{S^i R^j\}\ com\ i = 0{,}1, j = 0{,}1{,}2\ e\ S^2 = I, R^3 = I, RS = SR^2$$

O grupo diedral 4 (D_4)

Fixamos um quadrado □. O grupo das bijeções do plano que deixam o quadrado invariante é o grupo das simetrias do quadrado.

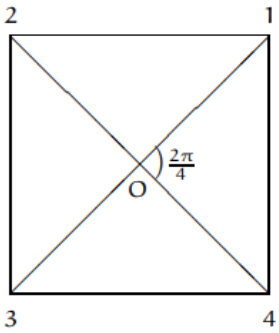
Para visualizarmos as bijeções do plano e a imagem dos vértices de □, consideramos os vértices do quadrado numerados por 1, 2, 3 e 4. O quadrado está inscrito num círculo de centro O, conforme a figura abaixo:



Temos 4 retas no plano, cujas simetrias do plano relacionadas a elas, deixam invariante. Para $j = 1,2$ seja l_j a reta que passa pelo centro O e pelo vértice j (tem um vértice do quadrado oposto a j). Para $j = 1,2$, seja l_{2+j} a reta que passa pelo centro O e é perpendicular ao lado que contém os vértices j *e* $j + 1$ (Existem dois lados do quadrado paralelos perpendiculares a l_{2+j} que os divide ao meio).

Sejam S_1', S_2', S_3' e S_4' as simetrias do plano em relação às retas l_1, l_2, l_3 ,e l_4 respectivamente. Essas bijeções do plano tem a propriedade de $S_j'(\square) = \square$.

O ângulo interno $4\hat{O}1$ do quadrado, em radianos, tem medida igual a $\frac{2\pi}{4} = \frac{\pi}{2}$.



Temos quatro rotações do plano em torno do ponto O, no sentido anti-horário, que deixam $\square$ invariante, isto é, $R_j(\square) = \square$, para j $= 1, 2, 3, 4$: R_1 , a rotação de $\frac{2\pi}{4} = \frac{\pi}{2}$; R_2, a rotação de $\frac{2(2\pi)}{4} = \pi$ e R_3, a rotação de $\frac{3(2\pi)}{4} = \frac{3\pi}{2}$. E R_4, a rotação de $\frac{4(2\pi)}{4} = 2\pi$, com $R_4 = I$.

Podemos representar as 8 bijeções do plano que deixa invariante por bijeções do conjunto {1,2,3,4}.

$$S = S_1' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} S_2' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

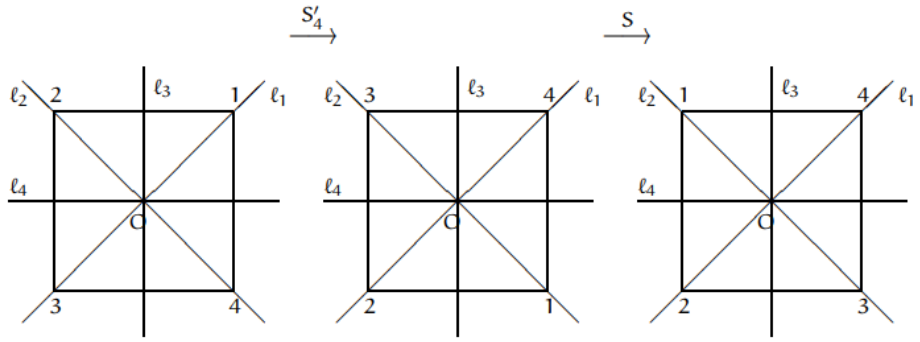
$$S_3' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} S_4' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$R = R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$
$$R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} R_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I$$

Podemos descrever as 8 bijeções a partir de $S = S_1'$ *e* $R = R_1 = R_{\frac{\pi}{2}}$

Inicialmente, observamos que $R_2 = R^2, R_3 = R^3, R_4 = R^4 = I, S^2 = I$ e $S_2' = SR^2, S_3' = SR^3, S_4' = SR$ e $RS = SR^3$.

Na figura a seguir vamos visualizar a composição $SS_4' = R$. Lembrando que as retas estão fixas.



A configuração do último quadrado corresponde a R(□). Logo, $SS_4' = R$ e como $S_2 = I$, compondo à esquerda da igualdade com S, temos:

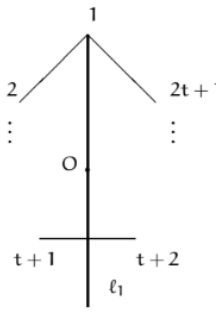
$$D_4 = \{I, R, R^2, R^3, S, SR, SR^2, SR^3\} \text{ e } R^4 = I, S^2 = I, RS = SR^3.$$
$$= \{S^i R^j\} \, com \, i = 0,1, j = 0,1,2,3 \, e \, S^2 = I, R^4 = I, RS = SR^3.$$

Sendo assim, $D_4 \subsetneq S_4$.

O grupo diedral n (D_n, com $n = 2t + 1$), $t \in \mathbb{N}$.

Fixamos um polígono regular P com $n = 2t + 1$. O grupo das bijeções do plano que deixam P invariante é o grupo de simetrias de P.

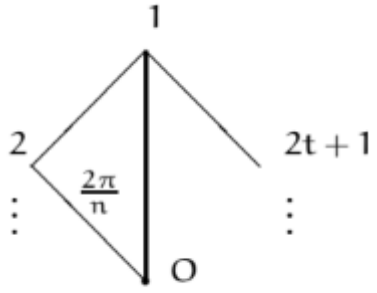
Para visualizarmos as bijeções e a imagem dos pontos de P serão considerados os vértices do polígono numerados por 1,2, ... $2t + 1$. O polígono P está inscrito em um círculo de centro O, como mostra a figura a seguir:



Temos $n = 2t + 1$ retas no plano, cujas simetrias do plano relacionadas a elas, deixam P invariante. Para $j = 1, \dots, 2t + 1$, seja l_j a reta que passa pelo centro O de P e pelo vértice j. A reta l_j é perpendicular ao lado oposto ao vértice j o divide ao meio.

Sejam $S'_1, \dots, S'_{2t+1}$ as simetrias do plano em relação às retas $l_1, \dots, l_{2t+1}$, respectivamente. Essas bijeções do plano tem a propriedade de $S'_j(P) = P$.

O ângulo interno $1\hat{O}2$ de P, em radianos, tem medida igual a $\frac{2\pi}{n}$, onde $n = 2t + 1$.



Temos $n = 2t + 1$ rotações do plano em torno do ponto O, no sentido anti-horário, que deixam P invariante, isto é, $R_j(P) = P$, para $j = 1, .., n$: R_1 , a rotação de $\frac{2\pi}{n}$; R_2, a rotação de $\frac{2(2\pi)}{3} = \frac{4\pi}{3}$, e assim por diante até R_{n-1}, a rotação de $\frac{(n-1)(2\pi)}{n}$; e R_n, a rotação de $\frac{n(2\pi)}{n} = 2\pi$, com $R_n = I$.

Podemos representar as $2n$ bijeções do plano que deixam P invariante por bijeções do conjunto $\{1,2, \dots, n\}$, usando apenas $S = S'_1$ e $R = R_1$.

$$S = S'_1 = \begin{pmatrix} 1 & 2 & \dots & t+1 & t+2/ & \dots & 2t+1 \\ 1 & 2t+1 & \dots & t+2 & t+1 & \dots & 2 \end{pmatrix}$$

$$R = R_1 = \begin{pmatrix} 1 & 2 & \dots & 2t & 2t+1 \\ 2 & 3 & \dots & 2t+1 & 1 \end{pmatrix}$$

Observamos que $R_j = R^j$, para cada $j = 1, \dots, n-1$ e $R^n = I$,$S^2 = I$, além disso SR^j é uma simetria para cada $j = 1, \dots, n-1$.

Logo,

$$D_n = \{ I, R, \dots, R^{n-1}, S, SR, \dots, SR^{n-1}\} \text{ e } R^n = I, S^2 = I, RS = SR^{n-1}$$

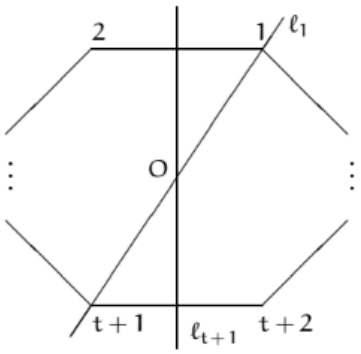
$$= \{S^i R^j\} \; com \; i = 0,1 \; ; j = 0, \dots, n-1 \; e \; S^2 = I, R^n = I, RS = SR^{n-1}$$

Sendo assim, $D_n \subsetneq S_n$, para n ímpar e $n > 3$.

O grupo diedral n (D_n, com $n = 2t$), $t \in \mathbb{N}$.

Fixamos um polígono regular P com $n = 2t$. O grupo das bijeções do plano que deixam P invariante é o grupo de simetrias de P.

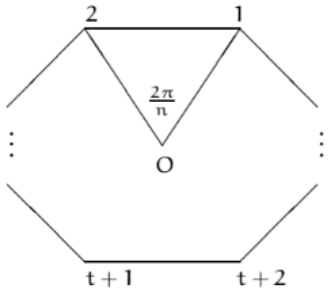
Para visualizarmos as bijeções e a imagem dos pontos de P serão considerados os vértices do polígono numerados por 1,2, ... $2t$. O polígono P está inscrito em um círculo de centro O, como mostra a figura a seguir:



Temos $n = 2t$ retas no plano, cujas simetrias do plano relacionadas a elas, deixam P invariante. Para cada $j = 1, \dots, t$, seja l_j a reta que passa pelo centro O de P e pelo vértice j. O vértice $t + j$ é oposto ao vértice j e está na reta l_j. Para cada $j = 1, \dots, t$, seja l_{t+j} a reta que passa pelo centro O e é perpendicular ao lado que contém os vértices j e $j + 1$. Existe t dessas retas que são perpendiculares a dois lados paralelos de P passando pelo ponto médio desses lados.

Sejam $S_1', \ldots, S_{2t}'$ as simetrias do plano em relação às retas $l_1, \ldots, l_{2t}$, respectivamente. Essas bijeções do plano tem a propriedade de $S_j'(P) = P$.

O ângulo interno $1\hat{O}2$ de P, em radianos, tem medida igual a $\frac{2\pi}{n}$, onde $n = 2t$.



Temos $n = 2t$ rotações do plano em torno do ponto O, no sentido anti-horário, que deixam P invariante, isto é, $R_j(P) = P, \text{para } j = 1, \ldots, n$: R_1 , a rotação de $\frac{2\pi}{n}$; R_2, a rotação de $\frac{2(2\pi)}{3} = \frac{4\pi}{3}$ e assim por diante até R_{n-1}, a rotação de $\frac{(n-1)(2\pi)}{n}$; e R_n, a rotação de $\frac{n(2\pi)}{n} = 2\pi$, com $R_n = I$.

Podemos representar as $2n$ bijeções do plano que deixam P invariante por bijeções do conjunto $\{1,2, \ldots, n\}$, usando apenas $S = S_1'$ e $R = R_1$

$$S = S_1' = \begin{pmatrix} 1 & 2 & 3 & \ldots & t & t+1 & t+2 \\ 1 & 2t & 2t-1 & \ldots & t+2 & t+1 & t \end{pmatrix}$$

$$R = R_1 = \begin{pmatrix} 1 & 2 & 3 & \ldots & 2t-1 & 2t \\ 2 & 3 & 4 & \ldots & 2t & 1 \end{pmatrix}$$

Logo,

$$D_n = \{ I, R \ldots, R^{n-1}, S, SR, \ldots, SR^{n-1}\} \text{ e } R^n = I, S^2 = I, RS = SR^{n-1}$$

$$= \left\{ S^i R^j \right\} com\ i = 0,1\ ;\ j = 0, \ldots, n-1\ e\ S^2 = I, R^n = I, RS = SR^{n-1}$$

1.5 - Homomorfismo

Essa seção é destinada a apresentar e estudar homomorfismo de grupos que é uma função entre dois grupos que preserva as operações binárias e veremos o Teorema de Cayley que permite representar qualquer grupo como um grupo de permutações.

Definição 1.29 (Homomorfismo de grupos): Sejam $(G,\cdot)$ e $(G',\star)$ grupos. A função $\varphi : G \to G'$ é chamada de homomorfismo de grupos, se e somente se, $\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$, para quaisquer $a, b \in \mathrm{G}$.

Exemplo 1.30: Seja $\mathbb{R}^+ = \{ x \in \mathbb{R} ; x > 0\}$ Como o produto de reais positivos é um também um real positivo, o inverso de real positivo também é um real positivo e 1 é um real positivo então, então $\mathbb{R}^+$ é um subgrupo de $\mathbb{R}^*$. Portanto,$(\mathbb{R}^+, \cdot)$ é um grupo. Considerando os grupos $(\mathbb{C}^*, \cdot)$ e $(\mathbb{R}^+, \cdot)$. A função

$$\varphi: \mathbb{C}^* \to \mathbb{R}^+$$
$$z \mapsto |z|$$

É um homomorfismo de grupos, pois

$$\varphi(z \cdot w) = |z \cdot w| = |z| \cdot |w| = \varphi(z) \cdot \varphi(w).$$

Proposição 1.31 (Propriedades de homomorfismo): Sejam $(G,\cdot)$ e $(G',\star)$ grupos e $\varphi : G \to G'$ um homomorfismo de grupos.

Então:

(i) $\varphi\,(e_G) = e_{G'}$

(ii) $\varphi\,(a^{-1}) = (\varphi\,(a))^{-1}$, para todo $a \in G$.

(iii) A imagem de φ é um subgrupo de G'.

Prova: (i) Temos $\varphi\,(e_G) = \varphi\,(e_G \cdot e_G) = \varphi\,(e_G) \star \varphi\,(e_G)$. Operando em ambos os lados da igualdade com $(\varphi\,(e_G))^{-1}$ obtemos $e_{G'} = \varphi\,(e_G)$.

(ii) Temos que $e_{G'} = \varphi\,(e_G) = \varphi\,(a \cdot a^{-1}) = \varphi(a) \star \varphi(a^{-1})$. Analogamente, $e_{G'} = \varphi(a^{-1}) \star \varphi(a)$. Dessas igualdades temos que $\varphi\,(a^{-1}) = (\varphi\,(a))^{-1}$, para todo $a \in G$.

(iii) Sejam $(G,\cdot)$, $(G',\star)$ grupos e $\varphi: G \to G'$ um homomorfismo de grupos. Mostre que $\varphi\,(G) = \{\varphi(a);\ a \in G\}$ é um subgrupo de G'. ■

Proposição 1.32: Sejam $(G,\cdot),(G',\star)$ e $(G'',\star')$ grupos. Se $\varphi : G \to G'$ e $\psi : G' \to G''$ são homomorfismo de grupos então $\psi \circ \varphi : G \to G''$ é um homomorfismo de grupos.

Prova: Seja $a, b \in G$. Então,

$$\begin{aligned}(\psi \circ \varphi)(a \cdot b) &= \psi(\varphi(a \cdot b) \\ &= \psi\big(\varphi(a) \star \varphi(b)\big) \\ &= \psi\big(\varphi(a) \star' \varphi(b)\big) \\ &= (\psi \circ \varphi)(a) \star' (\psi \circ \varphi)(b). \blacksquare\end{aligned}$$

Definição 1.33 (Núcleo): Sejam $(G,\cdot)$ e $(G',\star)$ grupos e $\varphi : G \to G'$ um homomorfismo de grupos. O núcleo de φ é o conjunto:

$$N\acute{u}cleo\ (\varphi) = \{x \in G; \varphi(x) = e_{G'}\}$$

Proposição 1.34 (Propriedades do núcleo): Sejam $(G,\cdot)$ e $(G',\star)$ grupos e $\varphi : G \to G'$ um homomorfismo de grupos. Então,

(i) $N\acute{u}cleo\ (\varphi)$ é um subgrupo de G.

(ii) φ é injetora se, e somente se, $N\acute{u}cleo\ (\varphi) = \{e_G\}$

Prova:

(i) Como $\varphi\ (e_G) = e_{G'}$, temos que $e_G \in N\acute{u}cleo\ (\varphi)$. Além disso, se $a, b \in N\acute{u}cleo\ (\varphi)$, então $\varphi(a \cdot b) = \varphi(a) \star \varphi(b) = e_{G'} \star e_{G'} = e_{G'}$ e $\varphi\ (a^{-1}) = (\varphi\ (a))^{-1} = e_{G'}^{-1} = e_{G'}$, logo $a \cdot b \in N\acute{u}cleo\ (\varphi)$ e $a^{-1} \in N\acute{u}cleo$. Portanto $N\acute{u}cleo\ (\varphi)$ é um subgrupo de G.

(ii) ($\Rightarrow$:) Suponhamos que φ seja injetora. Seja Então, $\varphi(a) = \varphi(e_G)$. Como φ é injetora, segue que $a = e_G$. Portanto, $N\acute{u}cleo\ (\varphi) = \{e_G\}$.

($\Leftarrow$:) Suponhamos que $N\acute{u}cleo\ (\varphi) = \{e_G\}$. Sejam $a, b \in G$ tais que $\varphi(a) = \varphi(b)$. Então, $e_{G'} = (\varphi\ (a) \star \varphi(b))^{-1} = \varphi\ (a) \star \varphi(b^{-1}) = \varphi(a \cdot b^{-1})$. Portanto, $a \cdot b^{-1} \in N\acute{u}cleo(\varphi) = \{e_G\}$. Logo, $a \cdot b^{-1} = e_G$, que nos dá $a = b$.

Então, φ é injetora. ■

Definição 1.34 (Isomorfismo de grupos): Sejam $(G,\cdot)$ e $(G',\star)$ grupos e $\varphi : G \to G'$ um isomorfismo de grupos se, somente se, φ é um homomorfismo de grupos bijetor.

Definição 1.36 (Grupos isomorfos): Sejam $(G,\cdot)$ e $(G',\star)$ são grupos isomorfos se, somente se, existe $\varphi : G \to G'$ isomorfismo de grupos.

Exemplo 1.37: Os grupos $(\mathbb{R}^+, \cdot)$ e $(\mathbb{R}, +)$ são isomorfos, pois a função $\varphi : \mathbb{R}^+ \to \mathbb{R}$ definida por $\varphi(x) = \log x$ é um isomorfismo de grupo.

Proposição 1.38: Sejam $(G,\cdot)$ e $(G',\star)$ grupos e $\varphi : G \to G'$ um isomorfismo de grupos. Então a função ψ, inversa de φ, é um isomorfismo de grupos.

Prova: Como φ é uma função bijetora, existe $\psi : G' \to G$ a função inversa de φ. Temos que $\varphi \circ \psi = I_{G'}$ *e* $\psi \circ \varphi = I_G$. Dessas composições segue, que ψ é função injetora e sobrejetora,
Para cada $b' \in G'$ temos que existe $b \in G$ tal que $\varphi(b) = b'$, pois φ é sobrejetora e b é único porque φ é injetora. Assim, a função ψ é definida por:

$$\psi(b') = b, \text{ se somente se, } \varphi(b) = b'.$$

Agora falta mostrar que ψ é um isomorfismo de grupos.
Sejam $a', b' \in G'$ e $a, b \in G$ tais que $\psi(a') = a$ e $\psi(b') = b$. Então, $\varphi(a) = a'$ e $\varphi(b) = b'$ e

$$\begin{aligned}
\psi(a' \star b') &= \psi(\varphi(a) \star \varphi(b)) \\
&= \psi\big(\varphi(a \cdot b)\big) \\
&= (\varphi \circ \psi)(a \cdot b) \\
&= a \cdot b \\
&= \psi(a') \cdot \psi(b')
\end{aligned}$$

Definição 1.39: Seja $(G,\cdot)$ um grupo. Um automorfismo de G é um isomorfismo $\varphi: G \to G$.
E será visto um resultado muito importante.

Teorema 1.40 (Cayley): Sejam $(G,\cdot)$ um grupo, $S_G = \{\sigma : G \to G; \sigma \text{ é uma bijeção}\}$ e $(S_G,\circ)$ o grupo das bijeções de G. Então G é isomorfo a um grupo de S_G.

Prova: Vamos construir φ, um homomorfismo injetor de grupos de G em S_G.
A imagem de φ é um subgrupo de S_G e é isomorfo de G.
Para cada $a \in G$ seja $\sigma_a: G \to G$ a função definida por $\sigma_a(x) = a \cdot x$. Então, para quaisquer $x, y \in G$.

$\sigma_a(x) = \sigma_a(y)$ se, e somente, se $a \cdot x = a \cdot y$

se, e somente, se $x = y$

Logo, σ_a é uma função injetora. Além do mais, para cada $b \in G$, temos que

$$b = a \cdot (a^{-1} \cdot b\ ) = \sigma_a(a^{-1} \cdot b),$$

mostrando que σ_a é uma função sobrejetora. Desta forma, $\sigma_a \in S_G$, para cada $a \in G$.

Definimos $\varphi: G \to S_G$ por $\varphi(a) = \sigma_a$.

Vamos mostrar que φ é um homomorfismo de grupos injetor.

Sejam $a, b \in G$. Temos que $\varphi(a \cdot b) = \sigma_{a \cdot b}$. Para entendermos esta função devemos aplicá – la nos elementos do seu domínio. Para isto, seja $x \in G$. Então,

$$\begin{aligned} \sigma_{a \cdot b}(x) &= (a \cdot b) \cdot x \\ &= a \cdot (b \cdot x) \\ &= \sigma_a(\sigma_b)(x) \\ &= \sigma_a \circ \sigma_b(x). \end{aligned}$$

Logo, $\sigma_{a \cdot b} = \sigma_a \circ \sigma_b$. Portanto,

$$\varphi(a \cdot b) = \sigma_{a \cdot b} = \sigma_a \circ \sigma_b = \varphi(a) \circ \varphi(b),$$

mostrando que φ é homomofismo de grupos.

Para mostrar que φ é injetora, devemos determinar o seu núcleo.

$$\begin{aligned} N\acute{u}cleo\ (\varphi) &= \{a \in G; \varphi(a) = I_G\} \\ &= \{a \in G; \sigma_a = I_G\} \\ &= \{a \in G, para\ todo\ x\ \in G, a \cdot x = x\} \\ &= \{e_G\}. \end{aligned}$$

Corolário 1.41 Seja $(G, \cdot)$ um grupo com n elementos. Então, G é um isomorfo a um subgrupo S_n.

Prova: É suficiente observar que se G é um grupo de n elementos, então S_G é isomorfo a S_n.

Os grupos finitos são realizados como subgrupos de S_n. Assim, S_n deve ser estudado como mais atenção, e será feito no próximo capítulo.

Observação:

(1) Os grupos de ordem 4, são o grupo cíclico de ordem 4 e o grupo de Klein, que são isomorfos a $\mathbb{Z}_4$ e $\mathbb{Z}_2\ x\ \mathbb{Z}_2$, respectivamente.

(2) Os grupos de ordem 8 são, a menos de isomorfismo, $\mathbb{Z}_2\ x\ \mathbb{Z}_2 x\ \mathbb{Z}_2$, $\mathbb{Z}_2\ x\ \mathbb{Z}_4, \mathbb{Z}_8$ todos esses grupos abelianos, e os grupos não – abelianos dos quatérnios Q e o Diedral D_4.

(3) Conhecemos dois exemplos de grupos com 4 elementos, cíclicos e S_3. E esse capítulo será encerrado mostrando que, a menos de isomorfismo, o único grupo não – cíclico de ordem 6 é o S_3.

De fato, Seja $(G,\cdot)$ um grupo não - cíclico com 6 elementos. Pelo teorema de Lagrange, para cada $x \in G$, temos que $\circ(x)$ divide 6, e como $\circ(x) \neq 6$, logo $\circ(x) \in \{1,2,3\}$.

Afirmamos que G tem elementos de ordem 3. Suponhamos, por absurdo, que todo elemento de G diferente de e_G tenha ordem 2. Então para todo $x \in G$, temos $x^2 = e_G$. Assim $(xy)(yx) = e$ implica $xy = yx$. Logo G é um grupo abeliano. Escolhendo $x, y \in G\backslash\{e_G\}$ tais que $x \neq y$ temos que $H = \{e_G, x, y, x \cdot y\}$ é um subgrupo de G com $|H| = 4$, contradizendo o teorema de Lagrange.

Seja $b \in G$ um elemento de ordem 3. Então, $\langle b\rangle = \{e_G, b, b^2\} \subsetneq G$. Existe $a \in G$ tal que $a \notin \langle b\rangle$.

Afirmamos que a ordem de a é 2. De fato, se $\circ(a) = 3$ então $e_G, b, b^2, a, a^2, b \cdot \text{a}, b \cdot a^2, b^2 \cdot a$ e $b^2 \cdot a^2$ são elementos distintos, contradizendo o fato de $|G| = 6$.

Sendo assim, $a^2 = e_G$ e $\{e_G, b, b^2, a, a \cdot b, a \cdot b^2\} \subset G$. Como os elementos do conjunto à esquerda são distintos temos que

$$G = \{e_G, b, b^2, a, a \cdot b, a \cdot b^2\}$$

Afirmamos que $a \cdot b \neq b \cdot a$. De fato, se $a \cdot b = b \cdot a$, então $c = a \cdot b$ é um elemento de G de ordem de 6, visto que o $mdc\big(\circ(a),\circ(b)\big) = mdc(2,3) = 1$,contradizendo o fato de G não ser grupo cíclico.

Como $b \cdot \text{a}$ é diferente de e_G, b, b^2, a e de $a \cdot b$, a única possibilidade é $b \cdot a = a \cdot b^2$. Assim,

$$G = \{e_G, b, b^2, a, a \cdot b, a \cdot b^2; b \cdot a = a \cdot b^2, a^2 = e_G, b^3 = e_G\},$$

Construindo o único isomorfismo $\varphi: G \to S_3$ definido por $\varphi(a) = \sigma$ e $\varphi(b) = \tau$, mostramos que G é isomorfo a S_3. ■

CAPÍTULO 2: GRUPOS DE SIMETRIAS

Este capítulo é destinado a apresentação e discussão dos grupos de permutações, que é um grupo cujo elementos são permutações de elementos de um conjunto *M* com a operação binária de composição de funções.

Já vimos que o Teorema de Cayley afirma que qualquer grupo é isomorfo a um grupo de permutações onde estudaremos o grupo de todas as permutações do conjunto $\{1,2,\dots,n\}$.

2.1 - O Grupo S_n

Pelo Teorema de Cayley, um grupo finito G pode ser visto como um subgrupo de S_n, onde $n = |G|$, o que motiva o estudo detalhado de S_n, o grupo de permutações no conjunto $S = \{1,2,\dots,n\}$.

Para estudarmos $S_n = \{\sigma: \{1,\dots,n\} \to \{1,\dots,n\}; \sigma \text{ é uma bijeção}\}$, definiremos uma relação de equivalência no conjunto $S = \{1,\dots,n\}$, a partir de um elemento σ de S_n fixado.

Definição 2.1 (Congruência módulo σ):

Seja $\sigma \in S_n$ fixado. Para $a, b \in S$, dizemos que a é congruente a b módulo σ se, somente se, $b = \sigma^j(a)$, para algum $j \in \mathbb{Z}$. Nesse caso, escrevemos $a \equiv_\sigma b$. Ou seja,

$$a \equiv_\sigma b \Leftrightarrow b = \sigma^j(a).$$

Definição 2.2 (Potência módulo σ): Seja $\sigma \in S_n$ e $j \in \mathbb{Z}$, então:

$$\sigma^j = \begin{cases} I_s, se\ j = 0 \\ \sigma, se\ j = 1 \\ \sigma \circ \sigma^{j-1}, se\ j > 1 \\ (\sigma - j)^{-1}, se\ j < 0 \end{cases}$$

Proposição 2.3: A congruência módulo σ é uma relação de equivalência em $S = \{1,\dots,n\}$.

Prova: De fato:

Reflexiva: Como $I_s = \sigma^0$, para todo $a \in S$, temos $a = I_s(a) = \sigma^0(a)$, logo $a \equiv_\sigma a$.

Simétrica: Se $a, b \in S$ e $a \equiv_\sigma b$, então existe $j \in \mathbb{Z}$ tal que $b = \sigma^j(a)$, logo $-j \in \mathbb{Z}$ e $\sigma^{-j}(b) = \sigma^{-j}\left(\sigma^j(a)\right) = (\sigma^{-j} \circ \sigma^j)(a) = a$, mostrando que $b \equiv_\sigma a$.

Transitiva: Por fim, se $a, b \in S$ e $a \equiv_\sigma b \; e \; b \equiv_\sigma c$, então existe $i, j \in \mathbb{Z}$ tais que

$$b = \sigma^i(a) \text{ e } c = \sigma^j(b),$$

Assim, $c = \sigma^j(\sigma^i(a)) = (\sigma^j \circ \sigma^i)(a) = \sigma^{j+i}(a)$, com $i + j \in \mathbb{Z}$. Portanto, $a \equiv_\sigma c$

Como a congruência módulo σ é reflexiva, simétrica e transitiva, concluímos que é uma relação de equivalência. ■

Toda relação de equivalência em um conjunto define uma partição do conjunto em subconjuntos disjuntos, tais subconjuntos são as classes de equivalência. Para cada $a \in S$, **classe do elemento** $\boldsymbol{a} = \overline{a} = [a] = \{b \in S; b = \sigma^j(a)$, para algum $j \in \mathbb{Z}\} = \{\sigma^j(a); j \in \mathbb{Z}\}$.

Definição 2.4 (Órbita de $\boldsymbol{a}$ por $\boldsymbol{\sigma}$): Para cada $a \in S$, chamamos a classe de equivalência de a módulo σ de órbita de a por σ.

Proposição 2.5: Para cada $a \in S$ existe $l = l_a \geq 1$ tal que $\sigma^l(a) = a$.

Prova: $\{\sigma^j(a); j \in \mathbb{Z}\} \subset S$. Logo, a órbita de a tem um número finitos de elementos. Em particular, $\{\sigma^j(a); j \in \mathbb{Z}, j \geq 1\}$ é finito.

Sendo assim, existem inteiros i, j com $1 \leq i < j$ tais que

$$\sigma^i(a) = \sigma^j(a).$$

Aplicando, σ^{-i} em ambos os lados dessa igualdade, obtemos $a = \sigma^{j-i}(a)$, com $j - i \geq 1$.

Portanto, o conjunto $C = \left\{j \in \mathbb{Z}\,; j \geq 1 \; e \; \sigma^j(a) = a\right\}$ é um subconjunto não – vazio de inteiros limitados inferiormente. Pelo Princípio da Boa Ordenação, C tem um menor elemento, que chamaremos de l. Então, $\sigma^l(a) = a$. ■

Definição 2.6 (Propriedade da órbita de $\boldsymbol{a}$ por $\boldsymbol{\sigma}$): A órbita de a por σ é $\{a, \sigma(a), \ldots \sigma^{l-1}(a)\}$, onde $l = l_a$ é o menor inteiro positivo j tal que $\sigma^l(a) = a$.

Exemplo 2.7 : Determinar a órbita de a por σ, para cada $a \in \{1,2,3,4,5,6\}$, onde

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

Órbita de $1 = \{\sigma(1) = 2, \sigma^2(1) = \sigma(\sigma(1)) = \sigma(2) = 1\} \Rightarrow l_1 = 2$;

Órbita de $3 = \{\sigma(3) = 3\} \Rightarrow l_3 = 1$;

Órbita de $4 = \{\sigma(4) = 5, \sigma^2(4) = \sigma(5) = 6 = \sigma^3(4) = \sigma(\sigma^2(4)) = \sigma(6) = 4\} \Rightarrow l_4 = 3$;

As classes de equivalência da congruência módulo σ, isto é, as órbitas de σ, são

$$\{1,2\}, \{3\} \text{ e } \{4,5,6\}.$$

Definição 2.8 (Ciclo a por σ): Dados $a \in S = \{1, \dots, n\}, \sigma \in S_n$ e $\{a, \sigma(a), \dots, \sigma^{l_a-1}(a)\}$, A órbita de a por σ, chamamos $(a, \sigma(a), \dots, \sigma^{l_a-1}(a))$, ou qualquer permutação circular, de um ciclo de σ.

Exemplo 2.9: Os ciclos de σ no Exemplo 1.46 são $(1,2), (3), (4,5,6)$.

Definição 2.10 (r-ciclo): Sejam $r \geq 2$ e $\{a_1, \dots, a_r\} \subset S = \{1, \dots, n\}$. Por um *r*-ciclo $(a_1, \dots, a_r)$ estendemos uma permutação $\sigma: S \to S$ definida por:

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3, \dots,\ \sigma(a_r) = a_1$$

e σ fixa todos os outros elementos S.

Por um 1-ciclo(a) entendemos como sendo a permutação $I: S \to S$.

Observação: Qualquer permutação circular do r-ciclo $(a_1, \dots, a_r)$ define a mesma bijeção de S.

Exemplo 2.11 : Seja $n = 9$ e consideramos o 5-ciclo $(1,3,4,2,6)$.

Esse ciclo corresponde a permutação $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 2 & 5 & 1 & 7 & 8 & 9 \end{pmatrix}$.

Claro que $(1,3,4,2,6) = \sigma$, assim como qualquer permutação circular 5-ciclo $(1,3,4,2,6)$, começando em qualquer um desses elementos.

Definição 2.12 (Multiplicação de ciclos): Sejam

$$S = \{1, \dots, n\}, \qquad \{i_1, \dots, i_r\} \subset S \text{ e } \qquad \{j_1, \dots, j_s\} \subset S.$$

Definimos o produto dos ciclos $\sigma = (i_1, \dots, i_r)$ e $\tau = (j_1, \dots, j_s)$ de S_n como a composição das permutações de S_n que eles representam, a saber.

$$(i_1, \dots, i_r)\ (j_1, \dots, j_s) = \sigma \circ \tau$$

Exemplo 2.13 : Calcular os produtos de alguns ciclos de S_7.

$$(1,3,5)(2,3,7,6,1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 4 & 1 & 3 & 6 \end{pmatrix}$$

$$(1,4,3,5,6)(2,3,7,6,1,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 2 & 6 & 4 & 1 \end{pmatrix}$$

$$(1,4,3)(2,5,7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 1 & 3 & 7 & 6 & 2 \end{pmatrix}$$

$$(2,5,7)(1,4,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 1 & 3 & 7 & 6 & 2 \end{pmatrix}$$

Definição 2.14 (Ciclos disjuntos): Sejam

$$S = \{1, \dots, n\}, \qquad \{i_1, \dots, i_r\} \subset S \text{ e } \qquad \{j_1, \dots, j_s\} \subset S.$$

Dizemos que $(i_1, \dots, i_r)$ e $(j_1, \dots, j_s)$ são ciclos disjuntos se, e somente se,

$$\{i_1, \dots, i_r\} \cap \{j_1, \dots, j_s\} = \emptyset \ .$$

Exemplo 2.15: Vimos no exemplo anterior que no S_7 temos $(1,4,3)$ *e* $(2,5,7)$ são ciclos disjuntos.

Proposição 2.16 (Propriedade de ciclos disjuntos): Se $\sigma = (i_1, \dots, i_r)$ e $\tau = (j_1, \dots, j_s)$ são ciclos de S_n disjuntos, então $\sigma \circ \tau = \tau \circ \sigma$.

Prova: De fato, sejam

$$A = \{i_1, \dots, i_r\} \text{ e } B = \{j_1, \dots, j_s\}, \text{ tais que } A \cap B = \emptyset \text{ e } S = \{1, \dots, n\}.$$

Se $j \in S \backslash (A \cup B)$, então e σ e τ fixam j, logo

$$\sigma\big(\tau(j)\big) = j = \tau(\sigma(j)).$$

Se $j \in A$, então

$$j = i_k, \ \sigma\,(i_k) = i_l \ , \ \tau(j) = j \quad \text{e} \quad \tau(i_l) = i_l.$$

Assim,

$$\sigma\big(\tau(j)\big) = \sigma(j) = i_l \ \text{ e } \ \tau(\sigma(j)) = \tau(i_l) = i_l.$$

Se $j \in B$ então

$$j = j_k, \ \ \tau(j_k) = j_l \ , \ \sigma(j) = j \ \text{ e } \ \sigma(j_l) = j_l.$$

Assim,

$$\sigma(\tau(j)) = \sigma(j_l) = j_l \quad \text{e} \quad \tau(\sigma(j)) = \tau(j) = j_l.$$

Logo, $\sigma \circ \tau = \tau \circ \sigma$.■

Proposição 2.17: Toda permutação de σ em S, pode ser escrita de maneira única, a menos da ordem, como produto dos seus ciclos disjuntos.

Prova: Seja $\sigma \in S$. Para cada $a \in S$, o ciclo de σ por S é da forma $(a, \sigma(a), \dots, \sigma^{l_a-1}(a))$, para algum $l_a \geq 1$ e os ciclos de σ são disjuntos. Seja ψ a permutação que é o produto dos ciclos de σ. Então, $\psi(b) = \sigma(b)$, pois para cada $b \in S$ ocorre em um único ciclo de σ.

Corolário 2.18: Toda permutação $\sigma \in S_n, \sigma \neq I$, se escreve, de maneira única, a menos da ordem, como produto de *r*-ciclos disjuntos, onde $r \geq 2$.

Prova: Como $\sigma \neq I$, existe $\sigma \in S$ tal que $\sigma(a) \neq a$, existem órbitas com pelo menos 2 elementos. Consideremos os ciclos de σ provenientes dessas órbitas. Esses ciclos determinam σ e são *r*-ciclos disjuntos com $r \geq 2$. ■

Exemplo 2.19: Escreveremos as seguintes permutações de S_{10} como produto de r-ciclos disjuntos com $r \geq 2$.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 & 10 & 8 & 9 \end{pmatrix} = (1,3,5,7)(2,4,6)(8,10,9)$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 9 & 7 & 2 & 1 & 5 & 3 & 6 & 10 & 4 \end{pmatrix} = (1,8,6,5)(2,9,10,4)(3,7)$$

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 5 & 1 & 8 & 9 & 6 & 10 & 3 & 2 & 7 \end{pmatrix} = (1,4,8,3)(2,5,9)(6)(7,10)$$
$$= (1,4,8,3)(2,5,9)(7,10)$$

Consideremos o *r*-ciclos disjuntos com $r \geq 2$. Observamos que

$$(1,2,\dots,r) = (1,r)(1,r-1)\dots(1,3)(1,2).$$

Em geral,

$$(i_1,\dots,i_r) = (i_1,i_r)(i_1,i_{r-1})\dots(i_1,i_3)(i_1,i_2).$$

Lema 2.20: Seja $n \geq 2$. Toda permutação em S_n é o produto de 2-ciclos.

Prova: Seja $\sigma \in S_n$, onde $n \geq 2$. Se $\sigma \neq I$. Seja σ como o produto dos seus r-ciclos disjuntos, onde $r \geq 2$. Escrevendo cada r-ciclo como produto de 2-ciclos, obtemos o resultado.

Temos $I = (1,2)(1,2)$. Logo I é produto de 2-ciclos. Se $n > 2$ existe outras formas de escrever I como produto de 2-ciclos. ■

Corolário 2.21: S_n, $n \geq 2$ é gerado pelo conjunto de todos os 2-ciclos.

Definição 2.22 (Transposições): Os 2 – ciclos em S_n são chamados de transposições.

Exemplos 2.23: Todo r – ciclo com $r \geq 2$ é o produto de $r - 1$ transposições.
De fato, $(i_1, \dots, i_r) = (i_1, i_r) \dots (i_1, i_3)(i_1, i_2)$.

Definição 2.24 (Permutação par ou permutação ímpar): Uma permutação $\sigma \in S_n$, é chamada permutação par se, e somente se, σ é um produto de um número par de transposições. Caso contrário, σ é chamada de uma permutação ímpar.

Exemplo 2.25: Como r-ciclo $\sigma = (i_1, i_2, \dots, i_r) = (i_1, i_r) \dots (i_1, i_2)$ é o produto de $r - 1$ transposições, então σ é par se, somente se, r é ímpar.

O produto das duas permutações pares é par, I é par e a inversa de uma permutação par é par, então o conjunto das permutações pares e é um subgrupo de S_n.

Definição 2.24 (Grupo Alternado): Seja $A_n = \{ \sigma \in S_n; \sigma \text{ é par} \}$. A_n é chamado de grupo alternado.

A congruência módulo A_n define uma partição de S_n em dois subconjuntos disjuntos, as classes de equivalência módulo A_n, onde uma das classes é A_n e a outra é $A_n\sigma$, onde σ é qualquer permutação ímpar.
De fato, dadas $\sigma \circ \tau$ em S_n temos:

$\sigma \equiv \tau \bmod A_n \Leftrightarrow \sigma \circ \tau^{-1} \in A_n$

$\Leftrightarrow \sigma \circ \tau^{-1}$ são ambas pares ou ambas ímpares

$\Leftrightarrow \sigma \circ \tau$ são ambas pares ou ambas ímpares

Assim, duas permutações estão na mesma classe se, e somente se, são ambos pares ou ambas ímpares. Tomando σ ímpar, temos que $A_n\sigma \neq A_n$, a classe das permutações pares. Assim,

$$n! = |S_n| = 2 \cdot |A_n|, \text{ isto é, } |A_n| = \frac{n!}{2}. \blacksquare$$

CAPÍTULO 3- Algumas Aplicações de Teorias de Grupo

Este capítulo é destinado a aplicação de teoria de grupo: os quadrados mágicos. Apresentando um pouco de sua história, tipos, origens, curiosidades e construção dos Quadrados Mágicos de qualquer ordem.

3.1 - Quadrados Mágicos:

Existem muitas histórias sobre o surgimento dos Quadrados Mágicos. E os primeiros a trabalhar com os quadrados mágicos foram os chineses, hindus e árabes. A versão mais antiga é o Loh- Shu encontrado na China por volta de 2850 a.C. e é referente a um quadrado mágico de ordem 3.

Um quadrado mágico é uma matriz quadrada de números inteiros positivos, sendo que nenhum destes números se repetem, em que a soma de cada linha, de cada diagonal e de cada coluna tem o mesmo valor M, chamado de constante mágica. Por exemplo,

Figura 1

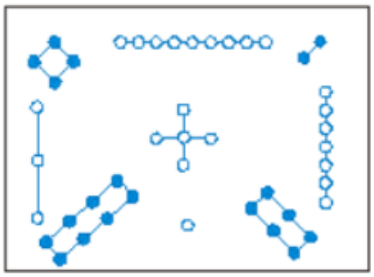


Figura 2

Um **quadrado do mágico puro** é um quadrado mágico contendo apenas números inteiros consecutivos.

A constante M pode ser facilmente calculada em função de n. Para isto, basta observar que a soma das n linhas da matriz é igual a:

$$M + M + \ldots + M = nM$$

Por outro lado, esta soma é igual a

$$1 + 2 + \cdots + n^2 = \frac{n^2.(n^2+1)}{2}$$

Assim, $$nM = \frac{n^2.(n^2+1)}{2} \Longrightarrow M = \frac{n.(n^2+1)}{2}$$

Neste caso, a constante mágica M, deve ser igual a:

$$M_3 = \frac{3.(3^2+1)}{2} = \frac{30}{2} = 15$$

Muitos também pensam que os quadrados mágicos tenham sido criados na Índia, chegando no século IX à Arábia e espalharam - se pelo Oriente Médio e Japão, onde foram associados à astrologia para cálculos de horóscopos. Os quadrados Mágicos tornaram objetos de estudos, na transição entre Idade Média e o Renascimento, segundo Figueiredo (1999). Chegando a Europa no século XV por Manuel Moschopoulos.

Em 1514 o pintor alemão Albrecht Dürer, pintou um quadrado mágico em sua gravura com título Melancolia I, ligada as influências astrais do planeta Júpiter. Essa relação dos planetas com os quadrados mágicos pode ter sido iniciada pela sabeísta, que eram adoradores de astros, especialmente do sol.

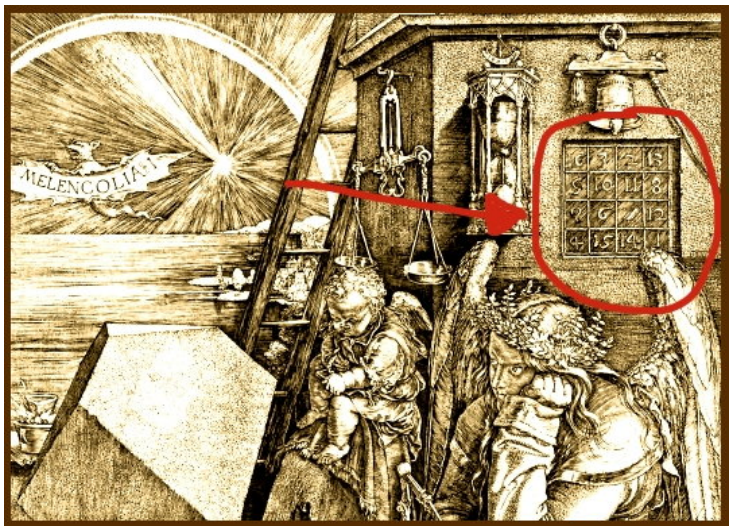
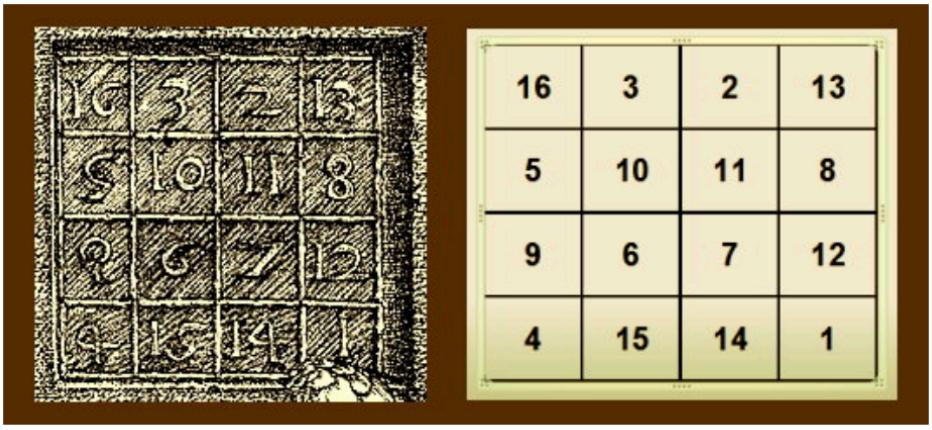


Figura 3: Melancolia I



16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Figura 4: Melancolia I – quadrado mágico ampliado

Em torno de 1533, Heinrich Cornelius Agrippa Von Nettesheim, mago, alquimista, médico, cabalista, astrólogo, escritor, físico e filósofo, estabeleceu uma ligação dos quadrados mágicos com os metais e planetas. Para entender o sobrenatural, Agrippa estudou Pitágoras e Porfírio, entre outros filósofos e físicos.

Por influência dos estudos de Agrippa, era comum o uso de amuletos de metal, embasados nos Quadrados Mágicos. Agrippa fez o primeiro amuleto, com os sete quadrados, relacionando cada a um planeta. Na época, o Sol e a Lua, eram considerados como planetas e os cientistas só conheciam sete astros. Acreditava - se que tais amuletos protegiam de forças negativas e doenças.

- 9 elementos simbolizando Saturno, em chumbo;
- 16 elementos simbolizando Júpiter, em estanho;
- 25 elementos simbolizando Marte, em ferro;
- 36 elementos simbolizando o Sol, em ouro;

Saturno=15		
4	9	2
3	5	7
8	1	6

Jupiter=34			
4	14	15	1
9	7	6	12
5	11	10	8
16	2	3	13

Marte=65				
11	24	7	20	3
4	12	25	8	16
17	5	13	21	9
10	18	1	14	22
23	6	19	2	15

Solenóide=111					
6	32	3	34	35	1
7	11	27	28	8	30
19	14	16	15	23	24
18	20	22	21	17	13
25	29	10	9	26	12
36	5	33	4	2	31

Figura 5

- 49 elementos simbolizando Vênus, em cobre;
- 64 elementos simbolizando Mercúrio, em liga de prata;

· 81 elementos simbolizando a Lua, em prata;

Venus=175						
22	47	16	41	10	35	4
5	23	48	17	42	11	29
30	6	24	49	18	36	12
13	31	7	25	43	19	37
38	14	32	1	26	44	20
21	39	8	33	2	27	45
46	15	40	9	34	3	28

Mercúrio=260							
8	58	59	5	4	62	63	1
49	15	14	52	53	11	10	56
41	23	22	44	45	19	18	48
32	34	35	29	28	38	39	25
40	26	27	37	36	30	31	33
17	47	46	20	21	43	42	24
9	55	54	12	13	51	50	16
64	2	3	61	60	6	7	57

Luna=369								
37	78	29	70	21	62	13	54	5
6	38	79	30	71	22	63	14	46
47	7	39	80	31	72	23	55	15
16	48	8	40	81	32	64	24	56
57	17	49	9	41	73	33	65	25
26	58	18	50	1	42	74	34	66
67	27	59	10	51	2	43	75	35
36	68	19	60	11	52	3	44	76
77	28	69	20	61	12	53	4	45

Figura 6

Figura 7 Figura 8 Figura 9

Além de serem estudados pela astrologia e magia, os quadrados mágicos, despertaram também o interesse de alguns matemáticos, pelos problemas difíceis que originados em relação à construção, classificação e enumeração dos quadrados de uma dada ordem. Bernard Frénicle de Bessy (1602 - 1675), Claude - Gaspar Bachet (1581 - 1638), Pierre Fermat (1601 - 1665) e Leonhard Euler (1707 - 1783) estudaram quadrados mágicos e cubos mágicos.

O menor quadrado mágico possível é o de ordem 3 com 9 elementos, ou seja, com 3 linhas e 3 colunas, ou seja, de ordem 3.

8	**1**	**6**
3	**5**	**7**
4	**9**	**2**

Quadrado Mágico 3x3

Nota - se que não é possível formar um Quadrado Mágico Puro 2 x 2, pois não é possível apresentar os elementos 1, 2, 3, 4 de forma que a soma de dois desses números fosse igual à soma dos outros dois, como acontece no quadrado mágico de ordem 3.

Definição 3.1: Um Quadrado Mágico Puro de ordem n é uma matriz $(a_{ij})_{nxn}$ cujos elementos pertencem aos subconjuntos dos naturais $\{1,2,3,\dots n^2\}$ e são dois a dois distintos e tais que a soma de cada linha, coluna e diagonal é igual a uma constante *M*, vista anteriormente e dada por:

$$M = \frac{n.(n^2+1)}{2}$$

Vejamos dois exemplos de quadrados mágicos formados apenas por números primos:

3	61	19	37
43	31	5	41
7	11	73	29
67	17	23	13

17	79	101	43	73
13	113	89	61	37
109	11	41	47	97
107	71	53	59	23
67	31	29	103	83

3.2 - Quadrado Mágico 3

Será apresentado um método de resolução do Quadrado Mágico de ordem 3. Seguindo a definição 3.1 e calculando a constante M temos que um Quadrado Mágico de ordem 3 é uma matriz 3 x 3 onde os elementos pertencem ao conjunto 1,2,3,4,5,6,7,8,9 e a soma de qualquer coluna, linha ou diagonal é igual a 15.

Método de Resolução:

Observamos que entre o intervalo $[1,9] = \{1,2,3,4.5,6,7,8,9\}$ tem 5 algarismos ímpares $= \{1,3,5,7,9\}$ e 4 algarismos pares $= \{2,4,6,8\}$ Assim, as possíveis somas de 3 parcelas são:

- PAR + PAR + PAR = PAR
- PAR + PAR + ÍMPAR = ÍMPAR
- PAR + ÍMPAR + ÍMPAR = PAR
- ÍMPAR + ÍMPAR + ÍMPAR = ÍMPAR

No caso do Quadrado Mágico de ordem 3, o resultado da soma é 15, então as únicas situações possíveis são a segunda e quarta.

O número que ocupa o centro do quadrado merece um olhar diferenciado, pois ele é parcela de 4 das 8 somas.

Considerando um Quadrado Mágico da forma:

a_{11}	a_{12}	a_{13}
a_{21}	a_{22}	a_{23}
a_{31}	a_{32}	a_{33}

Para os lemas a seguir usaremos a notação P para um número par e I para um número ímpar.

Lema 3.2: O elemento a_{22} é ímpar.

Prova: Por contradição, suponha que $\boldsymbol{a_{22}}$ seja par. Dessa forma, se tem as seguintes possibilidades para a configuração do Quadrado Mágico:

P		P
	P	
I		I

P		I
	P	
P		I

I		P
	P	
I		P

I		I
	P	
P		P

Sabendo - se as possíveis combinações para a soma resultarem em ímpar, completa - se as possibilidades nos quadrados e chega - se em:

I) A linha central resulta em par;

P		P
P	**P**	P
I		I

II) A coluna central resulta em par;

P	P	I
	P	
P	P	I

III) A coluna central resulta em par;

I	P	P
	P	
I	P	P

IV) A linha central resulta em par;

I		I
P	**P**	P
P		P

Assim, é visto que para todas as possibilidades, o elemento a_{22} par é uma contradição. Logo, conclui-se que o elemento a_{22} é ímpar. ■

Lema 3.3: Os elementos $a_{11}, a_{13}, a_{31}, a_{33}$ são pares.

Prova: Pelo lema anterior, o elemento central é ímpar. Para mostrar o lema, são analisadas todas as possibilidades de elementos ímpares e pares que ocupam os cantos do quadrado (os elementos $\boldsymbol{a_{11}, a_{13}, a_{31}, a_{33}}$**).**

- Possibilidade I:

I		I
	I	
I		I

Só resta completar as posições vagas com algarismos pares, mas notamos que ao fazer isso, a soma da primeira linha, por exemplo, resulta em um número par. Sendo assim, descartamos essa possibilidade.

- Possibilidade II:

I		I
	I	
P		I

Essa possibilidade também é descartada, pois a soma da diagonal secundária está resultando em par.

- Possibilidade III:

I		P
	I	
P		I

Para ter a soma resultando um número ímpar, todas as posições vazias deveriam ser preenchidas com algarismos pares, o que é impossível, pois temos apenas 4 algarismos pares entre 1 e 9

- Possibilidade IV:

P		P
	I	
I		P

A soma da diagonal secundária está resultando em par.

- Possibilidade V:

P		P
	I	
P		P

É uma possibilidade válida, pois as posições vazias são completadas por algarismos ímpares e as somas de todas as linhas, colunas e diagonais resultam em par.

Logo, os elementos $a_{11}, a_{13}, a_{31}, a_{33}$ são pares.

Lema 3.4: O elemento a_{22} é igual a 5.

Prova: O elemento a_{22} é parcela comum da soma de duas diagonais. Listando a somas que resultam em 15 e que tenham parcelas como parcelas um algarismo ímpar e dois pares.

1 + 8 + 6

4 + 5 + 6

2 + 8 + 5

2 + 9 + 4

3 + 4 + 8

2 + 6 + 7

O único algarismo que aparece em mais de uma soma é o 5. Assim, a_{22} = 5. Seja um quadrado mágico 3 x 3 da forma:

$\boldsymbol{a_{11}}$	$\boldsymbol{a_{12}}$	$\boldsymbol{a_{13}}$
$\boldsymbol{a_{21}}$	**5**	$\boldsymbol{a_{23}}$
$\boldsymbol{a_{31}}$	$\boldsymbol{a_{32}}$	$\boldsymbol{a_{33}}$

Com a_{11}, a_{13} , a_{31} e a_{12}, a_{21} , a_{23} $a_{32} \in \{1, 3, 7, 9\}$.

E sabemos que a soma de cada coluna, cada linha e cada diagonal é igual a 15, dessa forma temos o seguinte sistema linear:

$$\begin{cases} a_{11} + a_{12} + a_{13} = 15 \\ a_{21} + a_{23} = 10 \\ a_{31} + a_{32} + a_{33} = 15 \\ a_{11} + a_{21} + a_{31} = 15 \\ a_{12} + a_{32} = 10 \\ a_{13} + a_{23} + a_{33} = 15 \\ a_{11} + a_{33} = 10 \\ a_{31} + a_{13} = 10 \end{cases}$$

Reescrevendo o sistema, e deixando a_{11}, a_{12} como variáveis livres, temos:

$$\begin{cases} a_{13} = 15 - a_{11} - a_{12} \\ a_{21} = 20 - a_{11} - a_{12} \\ a_{23} = -10 - a_{11} + a_{12} \\ a_{31} = -5 + a_{11} + a_{12} \\ a_{32} = 10 - a_{12} \\ a_{33} = 10 - a_{11} \end{cases}$$

sendo que $a_{11} \in \{2,4,6,8\}$ e $a_{12} \in \{1,3,7,9\}$.

Podemos ficar tentado afirmar que o sistema tem infinitas soluções; isso só ocorreria se a_{11} e a_{12} pudessem assumir qualquer valor real mas, $a_{11} \in \{2,4,6,8\}$ e $a_{12} \in \{1,3,7,9\}$ e o valor de qualquer a_{ij} deve pertencer ao conjunto $\{1,2,3,4,6,7,8,9\}$ e devem ser dois a dois distintos. Por exemplo, se a_{11} = 2 e a_{12} = 1, que pelos lemas anteriores são valores que eles poderiam assumir. Como $a_{13} = 15 - 2 - 1 = 12 \notin \{1,2,3,4,6,7,8,9\}$,essa possibilidade é eliminada.

Outro caso para ser eliminado, é

$a_{11} = 6$ e $a_{12} = 3$, pois $a_{13} = 15 - 6 - 3 = 6 = a_{11}$, o que não pode ocorrer.

Eliminando todos esses casos, temos:

$(a_{11}, a_{11}) \in \{(2, 7), (2, 9), (4, 3), (4, 9), (6, 7), (6, 1), (8, 1), (8, 3)\}$

E resolvendo o sistema para cada um dos pares possíveis, chegamos a 8 configurações do quadrado mágico, mostradas a seguir:

2	7	6
9	5	1
4	3	8

2	9	4
7	5	3
6	1	8

4	3	8
9	5	1
2	7	9

4	9	2
3	5	7
8	1	6

6	7	2
1	5	9
8	3	4

6	1	8
7	5	3
2	9	4

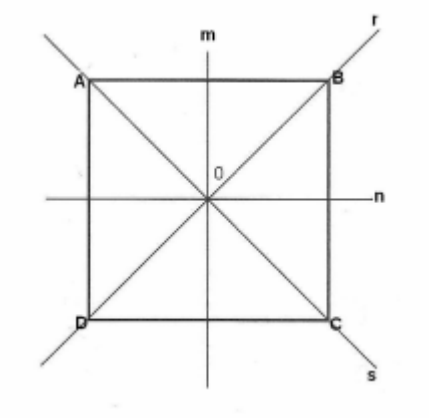
8	1	6
3	5	7
4	9	2

8	3	4
1	5	9
6	7	2

Falta mostrar que os oito quadrados que encontramos pertencem a mesma classe, ou seja, o quadrado mágico 3 x 3 é único a menos de simetrias e isso será feito usando o que foi visto de teoria de grupos.

O grupo das simetrias do quadrado

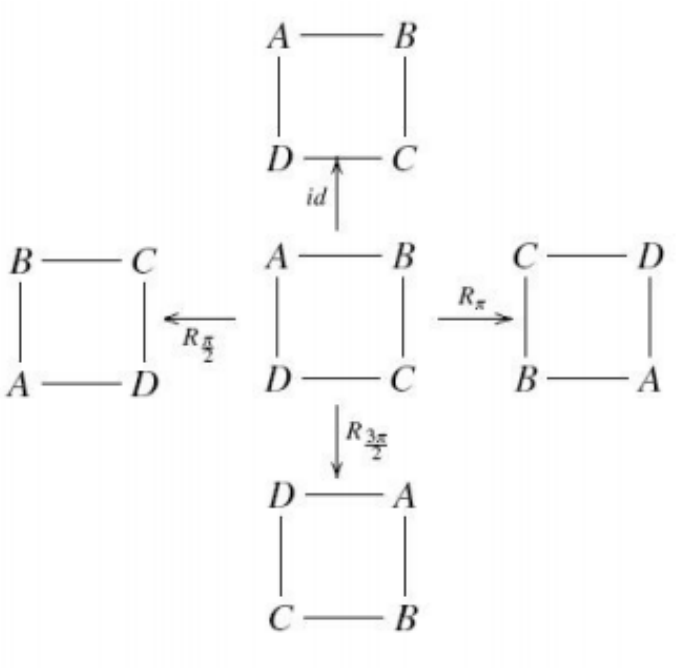
Sejam A, B, C, D, os vértices de um quadrado. Considere *O*, o ponto de interseção das duas diagonais do quadrado e denote $r, s, m\ e\ n$ as retas determinadas pelas diagonais e pelas mediatrizes do quadrado, como mostra na figura.



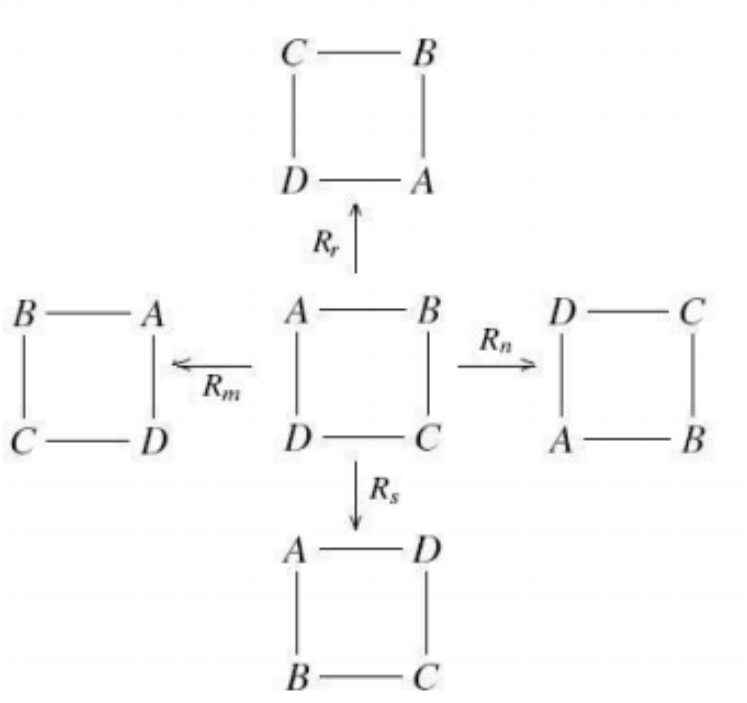
Denotaremos por

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

Abaixo foi ilustrado cada uma dessas transformações aplicados no quadrado de vértices A, B, C e D.



- R_r, R_s, R_m, R_n as rotações de ângulo com eixos r, m, n, s respectivamente.



É fácil ver que o conjunto de transformações

$$D_4 = \left\{ id, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}, R_r, R_s, R_m, R_n \right\}$$

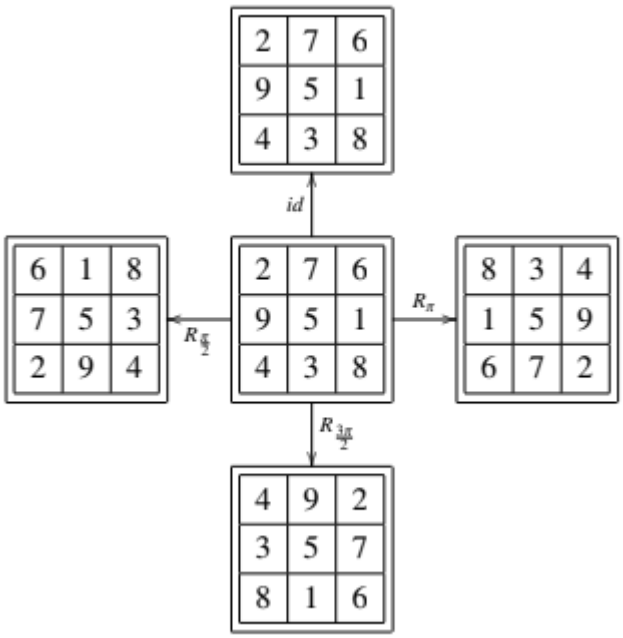
Com a operação de composição de funções é um grupo.

Analisando os quadrados 3 x 3 obtidos, e levando em considerações as informações vistas acima e tomando as retas r, s, m, n como coluna central, a linha central, a diagonal principal e a diagonal secundária respectivamente.

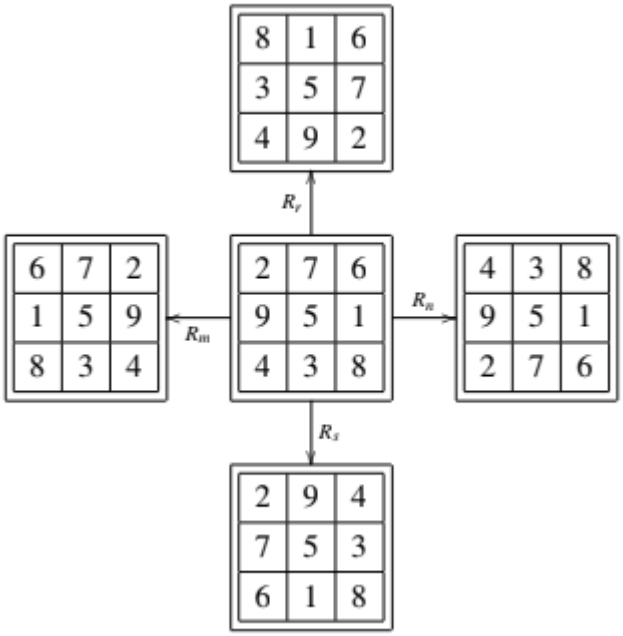
Seja o quadrado a seguir o elemento inicial:

2	7	6
9	5	1
4	3	8

Aplicando as transformações $id, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}$ temos:



E aplicando as transformações R_r, R_s, R_m, R_n, obtemos:



A partir de um dos quadrados obtidos é gerado, com as transformações do quadrado, todos os outros quadrados. Com isso, concluimos que, a menos de simetrias, existe um único Quadrado Mágico 3 x 3.

3.3 - Quadrado Mágico de Ordem *n*:

A construção do quadrado mágico é feita de formas distintas. Existem técnicas específicas para Quadrados Mágicos de ordem ímpar, outras para os de ordem par e não múltipla de 4 e outras para os de ordem múltipla de 4. E apresentaremos tais construções respeitando as especificações.

Quadrados Mágicos de ordem ímpar.

Inicialmente, o inteiro 1 deve ser posicionado no meio da primeira linha. Uma vez definida a posição de um inteiro r, a posição seguinte deverá ser preenchida com o inteiro $r + 1$, levando em consideração os seguintes critérios:

- A posição a ser preenchida depois do a_{ij} é a posição do elemento $a_{i-1,1}$ se $i > 1$ e $j < n$.

- A posição que segue a_{in} , com $i > 1$ é $a_{i-1,1}$ .Logo, se a posição atual preenchida com n estiver na última coluna, a próxima posição a ser preenchida com $n + 1$ será da linha acima na primeira coluna.

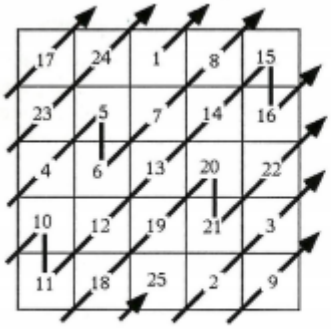
- A posição que segue a_{1j}, com $j < n$ é $a_{n,j+1}$. Portanto, se a posição atual preenchida com n estiver na primeira linha, a próxima posição a ser preenchida com $n + 1$ será na coluna anterior na última linha.

- Se a posição que segue a_{ij} segundos os critérios anteriores já tiver sido usada, será preenchida a posição do elemento $a_{i+1,j}$. Portanto, se a posição seguinte já estiver preenchida, será usada como próxima posição a que estiver imediatamente abaixo da atual.

Ou mais condensamente, iniciamos com $a_{1,\frac{n+1}{2}} = 1$ e dado $a_{i,j} = 1$, preenchemos com $n + 1$ a posição

- $a_{n,j+1}$ se $i = 1$ e $j < n$
- $a_{i-1,1}$ se $i > 1$ e $j = n$
- $a_{i-1,j+1}$ se $i > 1$ e $j < n$
- $a_{i+1,j}$ se a posição estiver ocupada.

O processo encerra quando preenchemos a última célula vazia com n^2. As figuras abaixo mostram um Quadrado Mágico de ordem 5 e um Quadrado Mágico de ordem 9 completos. A figura do Quadrado Mágico de ordem 5 nos dá uma ideia de como essa técnica funciona e que depois de nos habituarmos com ela podemos acelerar o preenchimento do quadrado fazendo alguns movimentos, que são equivalentes a seguir os passos da técnica.



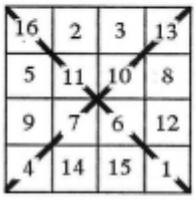
Quadrado mágico de ordem 5

47	58	69	80	1	12	23	34	45
57	68	79	9	11	22	33	44	46
67	78	8	10	21	32	43	54	56
77	7	18	20	31	42	53	55	66
6	17	19	30	41	52	63	65	76
16	27	29	40	51	62	64	75	5
26	28	39	50	61	72	74	4	15
36	38	49	60	71	73	3	14	25
37	48	59	70	81	2	13	24	35

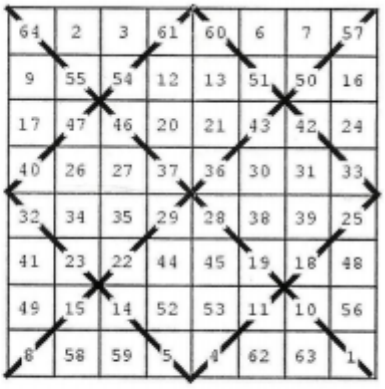
Quadrado mágico de ordem 9

Quadrados Mágicos de ordem n múltipla de 4.

Neste método basta preencher a primeira linha com inteiros de 1 a n, a segunda linha de $n+1$ a $2n$ e assim por diante, até preencher a última linha com os inteiros de n^2-n+1 a n^2. Depois, subdividir o quadrado $n \times n$ em $(\frac{n}{4})^2$ quadrados 4×4 e, para cada um desses quadrados menores, trocar cada elemento a_{ij} que apareça em qualquer uma de suas diagonais pelo elemento n^2+1-a_{ij}. A figura abaixo ilustra os Quadrados Mágicos de ordem 4 e 8, que exemplificam a técnica de preenchimento do Quadrado Mágico de ordem n múltipla de 4.



Quadrado mágico de ordem 4



Quadrado mágico de ordem 8

Tomemos um quadrado 4×4 e preencha-o com os números de 1 a 16, como descrito acima e ilustrado na figura abaixo:

1	2	3	**4**
5	**6**	**7**	8
9	**10**	**11**	12
13	14	15	**16**

Identificamos os elementos das diagonais, que estão em negrito e permutamos os elementos das diagonais em posições opostas em relação ao centro, o que equivale a substituir o elemento a_{ij} das diagonais pelo elemento $n^2 + 1 - a_{ij}$. Assim o elemento 1 é substituído pelo 16 e reciprocamente. Analogamente os elementos 4,6 e 7 são permutados com os elementos 13,11 e 10 respectivamente. Fazendo as trocas obtemos o Quadrado Mágico 4 × 4 ilustrado na figura abaixo.

16	2	3	**13**
5	**1 1**	**10**	8
9	**7**	**6**	12
4	14	15	**1**

Agora aplicaremos o método para obter um quadrado mágico 8 × 8. Preenchemos o quadrado da maneira proposta pelo método dispondo os elementos de 1 a 64 por linha, como ilustrado na figura abaixo.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Subdividimos o quadrado 8 × 8 em $(\frac{8}{4})^2$ quadrados 4 × 4 e identificamos os elementos das diagonais como ilustrado na figura abaixo

1	2	3	**4**	**5**	6	7	**8**
9	**10**	**11**	12	13	**14**	**15**	16
17	**18**	**19**	20	21	**22**	**23**	24
25	26	27	**28**	**29**	30	31	**32**
33	34	35	**36**	**37**	38	39	**40**
41	**42**	**43**	44	45	**46**	**47**	48
49	**50**	**51**	52	53	**54**	**55**	56
57	58	59	**60**	**61**	62	63	**64**

Permutamos os elementos das diagonais principais e secundárias em posições opostas do quadrado 8 × 8. Além disso, permutamos os elementos, que não sofreram qualquer modificação, das diagonais dos quadrados 4 × 4. Isto equivale a substituir os elementos a_{ij} das diagonais dos quadrados pelo elemento $n^2 + 1 - a_{ij}$ Assim, por exemplo, temos as seguintes trocas:

$$1 \Rightarrow 64 + 1 - 1 = 64$$
$$4 \Rightarrow 64 + 1 - 4 = 61$$
$$5 \Rightarrow 64 + 1 - 5 = 60$$
$$8 \Rightarrow 64 + 1 - 8 = 57$$
$$10 \Rightarrow 64 + 1 - 10 = 55$$
$$11 \Rightarrow 64 + 1 - 11 = 54$$
$$\vdots$$
$$25 \Rightarrow 64 + 1 - 25 = 40$$
$$29 \Rightarrow 64 + 1 - 29 = 36$$
$$\vdots$$

Fazendo as respectivas permutas, obtemos o Quadrado Mágico 8 × 8 desejado, conforme ilustrado na figura abaixo.

64	2	3	**61**	**60**	6	7	**57**
9	**55**	**54**	12	13	**51**	**50**	16
17	**47**	**46**	20	21	**43**	**42**	24
40	26	27	**37**	**36**	30	31	**33**
32	34	35	**29**	**28**	38	39	**25**
41	**23**	**22**	44	45	**19**	**18**	48
49	**15**	**14**	52	53	**11**	**10**	56
8	58	59	**5**	**4**	62	63	**1**

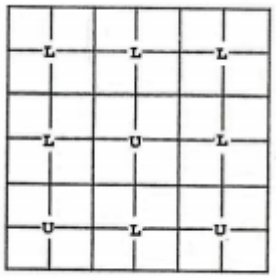
Quadrados Mágicos de ordem n par não múltipla de 4.

Dado um quadrado $n \times n$ onde n é par não múltiplo de 4, podemos escrever $n = 2(2m+1)$, com $m \in$ N. Divide-se o quadrado $n \times n$ em $(2m+1)^2$ quadrados 2×2. No centro de cada quadrado coloque uma letra L, U ou X de maneira que as $m + 1$ primeiras fileiras de quadrados 2×2 sejam as que tem L, a próxima fileira tenha a letra U e as $m - 1$ fileiras tenham a letra X. Depois de feito isso, troque o U que esta no quadrado 2×2 central da fileira pelo L logo acima dele. Se $n = 6$, por exemplo, temos a seguinte configuração ilustrada na figura abaixo.

1ª fileira $2\ x\ 2 \implies$ colocar L

2ª fileira $2\ x\ 2 \implies$ colocar L

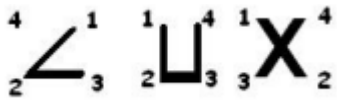
3ª fileira $2\ x\ 2 \implies$ colocar U



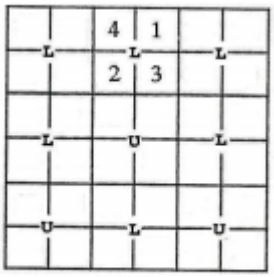
Agora, iremos considerar o Quadrado Mágico auxiliar de ordem ímpar $(2m + 1)$. No exemplo é um quadrado de ordem 3, preenchido pela técnica de Quadrados Mágicos de ordem ímpar, como mostra a figura abaixo.

8	1	6
3	5	7
4	9	2

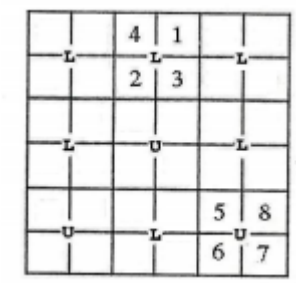
Preenchemos agora cada um dos quadrados 2 × 2, que estão compondo o quadrado original, distribuindo os inteiros de 1 a n^2 de 4 em 4, levando em consideração a ordem sugerida pelo quadrado auxiliar da figura acima e pelo formato de cada letra como mostra a figura abaixo.



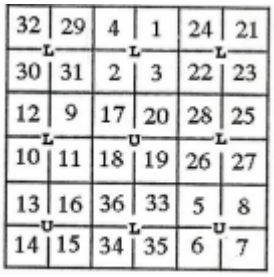
O primeiro quadrado 2×2 a ser preenchido é o quadrado central que está na primeira fileira:



O próximo é o quadrado que está no canto inferior direito:



Assim por diante até que temos o quadrado desejado:



Note que a soma de cada linha, coluna e diagonal é 111.

CAPÍTULO 4 – Atividades Propostas para a Sala de Aula

Este capítulo é destinado a apresentação de atividades propostas para sala de aula que envolvam o uso ou construção de Quadrados Mágicos para o Ensino da Matemática.

4.1- Atividade I: Quadrado Mágico Fundamental:

Objetivo:

- Apresentar os Quadrados Mágicos.
- Conceituar elemento numérico.
- Apresentar o Quadrado Mágico aditivo fundamental.
- Descobrir termo central e constante mágica.
- Estimular o raciocínio lógico.

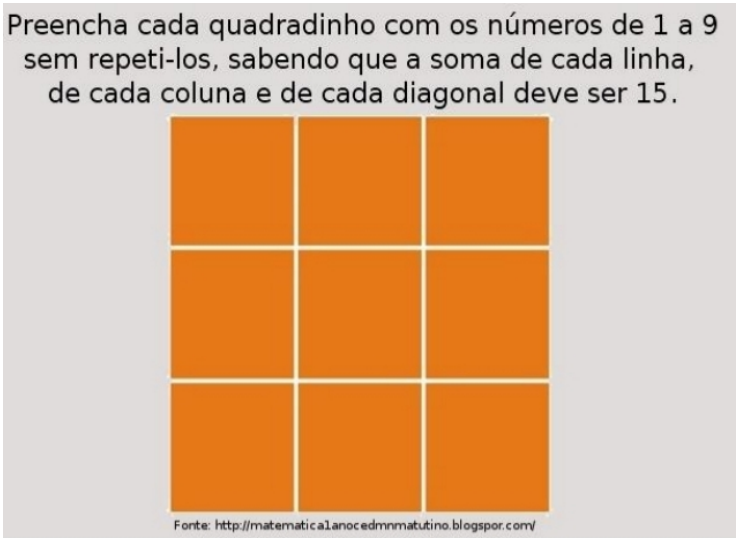
Público alvo: Alunos do 1° ano do Ensino Médio, de preferência divididos em 8 grupos.
Material utilizado: Material impresso.
Duração: ~100 minutos.

Comentário inicial: Um Quadrado Mágico é uma tabela quadrada de lado *n*, cuja soma dos termos de cada linha, coluna e diagonal (principal e secundária) é constante. Esse valor é chamado de constante mágica. O quadrado mágico estudado a seguir é conhecido como quadrado mágico fundamental. Suas principais características são: 3 quadradinhos cada lado, formando 9 quadradinhos a ser preenchido com valores de 1 a 9 com constante mágica igual a 15.

Questionário para ser respondido pelos grupos:

I) Quantos elementos (números) possuem o quadrado mágico fundamental?
II) Quais são os elementos (números)?
III) Complete a figura abaixo de acordo com as orientações contidas nelas:

Figura 3: QUADRADO MÁGICO FUNDAMENTAL



Fonte: Dia a dia educação PR.

IV) O número ocupante da parte central de um quadrado mágico recebe o nome de termo central. Qual elemento é o termo central do quadrado mágico acima?

V) No quadrado mágico acima denominado fundamental o resultado da soma de cada linha, de cada coluna e de cada diagonal é:_____. Esse resultado é denominado soma mágica sendo igual a constante mágica.

VI) Em caso afirmativo, explique com suas palavras.

4.2- Atividade II

Objetivo:

- Apresentar os Quadrados Mágicos e suas permutações.
- Construir novos Quadrados Mágicos
- Estimular o raciocínio lógico.

Público alvo: Alunos do 1° ano do Ensino Médio, de preferência divididos em 8 grupos.
Material utilizado: Material impresso.
Duração: ~100 minutos.

Objetivo: Conceituar elemento numérico, quadrado mágico aditivo fundamental, termo central e constante mágica e suas permutações.

Parte I

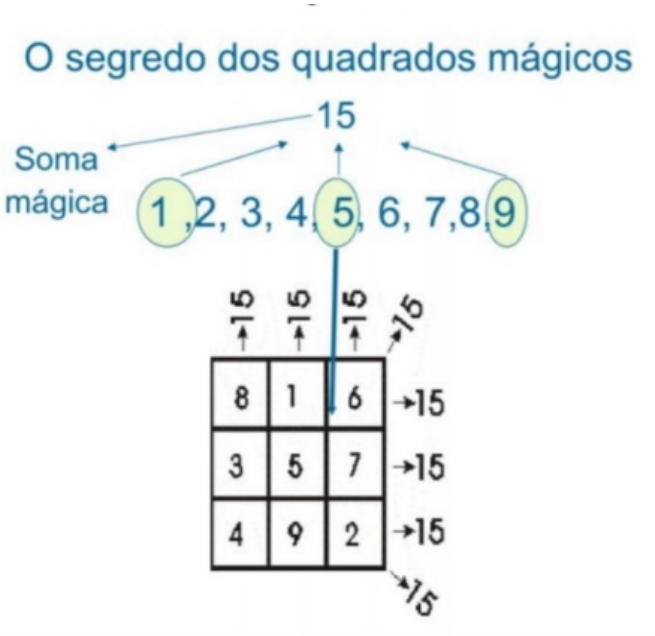
Questionário para grupos.

I) Reunir os 7 os grupos e comparar os 7 quadrados mágicos encontrados. E responder: Os 7 quadrados mágicos encontrados são iguais? Caso não, anotarem os quadrados mágicos fundamentais que estão faltando para completarem os 7 distintos.

Parte II

COMENTÁRIO INICIAL: Considere o quadrado mágico a seguir, podemos observar que no centro do quadrado está um número ímpar, nos cantos temos números pares. Esse padrão observado se repete em outros quadrados mágicos. Assim, se no centro do quadrado colocamos um número ímpar, nos cantos temos que colocar números pares e depois os espaços que sobram completamos com números ímpares. E se no centro for utilizado um número par, nos cantos vamos colocar ímpares.

Figura 4



Fonte: artigo: KOLODZIEISKI e NASCIMENTO 2011: O Quadrado Mágico: O Lúdico Contribuindo no Processo Ensino Aprendizagem de Matemática. (p.07)

Questionário para os grupos:

I) Responda: Se utilizarmos uma sequência com os números de 4 a 12, ou seja: 4, 5, 6, 7, 8, 9, 10, 11, 12. A soma mágica é:_____, Logo em todas as linhas, colunas e diagonais a soma deve ser igual a _____.

II) Dado um conjunto de nove números que preenchem um quadrado mágico, como saber qual será a constante mágica? Responda essa questão sem resolver o quadrado mágico.

III) Atividade (para casa): Essa atividade vai ser recolhida no início da próxima aula. O que os quatro conjuntos de números dados têm em comum:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9\},$$

$$\{1, 3, 5, 7, 9, 11, 13, 15, 17\},$$

$$\{2, 4, 6, 8, 10, 12, 14, 16, 18\}$$

$$\{2,3,4,5,6,7,8,9,10\}$$

4.3- Atividade III

Objetivo:

- Debater o conceito de elemento em um conjunto numérico utilizando a tarefa de casa.
- Reforçar o conceito de termo central e constante mágica.
- Iniciar o conteúdo de Progressão Aritmética
- Estimular a pesquisa matemática
- Estimular o raciocínio lógico.

Público alvo: Alunos do 1° ano do Ensino Médio

Material utilizado: Material impresso.

Duração: ~100 minutos.

Parte I

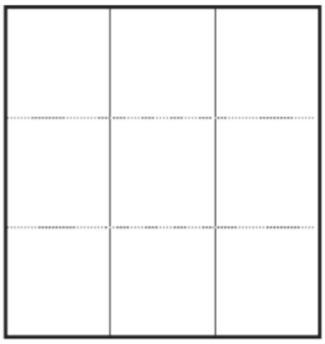
Debates, comentários e argumentações sobre o dever de casa da aula anterior. Resposta correta: Todos os conjuntos de números possuem 9 elementos.

Parte II

Em qualquer quadrado mágico, somando-se todos os elementos de cada linha vertical, assim como, todos os elementos de cada coluna vertical e todas suas diagonais o valor deve ser o mesmo.

Questionário para grupos:

I) Pedir para os alunos preencherem o quadrado mágico abaixo com conjunto de números: $\{2, 3, 4, 5, 6, 7, 8, 9, 10\}$



II) Após finalizar a atividade anterior, pedir para os alunos montarem dois quadrados mágicos com os seguintes conjuntos de números: $\{1, 3, 5, 7, 9, 11, 13, 15, 17\}$ e $\{2, 4, 6, 8, 10, 12, 4, 16, 18\}$.

III) Qual elemento é o termo central do primeiro quadrado mágico acima?

IV) Esse termo é o mesmo encontrado nos outros dois? Por quê?

V) No primeiro quadrado mágico o resultado da soma de cada linha, de cada coluna e de cada diagonal é:_____. Esse resultado é denominado constante mágica.

VI) Essa constante é a mesmo encontrado nos outros dois? Por quê?

VII) Atividade para casa: Pesquise sobre Sequências Numéricas e Progressão Aritmética PA: (Razão e termo geral).

4.4- Atividade IV: Quadrado Mágico e Progressão Aritmética

Objetivo:

- Multiplicar e Somar constantes ao Quadrado Mágico e Debater os resultados.
- Relacionar o Quadrado Mágico e Progressão Aritmética.
- Estimular o raciocínio lógico.

Público alvo: Alunos do 1° ano do Ensino Médio, de preferência divididos em 8 grupos.
Material utilizado: Material impresso.
Duração: ~100 minutos.

Parte I:

Questionário para os grupos:

I) Em um quadrado mágico de ordem 3, se multiplicarmos o termo central por 3, já temos o resultado da soma mágica. Isso é verdade? Se for, explique com suas palavras porque isso acontece.

8	1	6
3	5	7
4	9	2

II) Em um quadrado Mágico de ordem três, se multiplicarmos todos os elementos por 2, encontraremos outro quadrado Mágico. Isso é verdade? Se for, explique com suas palavras porque isso acontece.

16	2	12
6	10	14
8	18	4

III) Em um quadrado Mágico de ordem três, se multiplicarmos todos os elementos por 5, encontraremos outro quadrado Mágico. Isso é verdade? Se for, explique com suas palavras porque isso acontece

40	5	30
15	25	35
20	45	10

Sendo assim, sem realizar uma demonstração rigorosa do resultado, vamos afirmar que: qualquer sequência de nove múltiplos consecutivos de um número inteiro pode ser arranjada na forma de um quadrado mágico.

IV) Com argumentos matemáticos, explique essa afirmação.

V) Considere a afirmação: em um quadrado Mágico de ordem três, se multiplicarmos todos os elementos por 3 e depois somamos 2, encontraremos outro quadrado Mágico. Isso é verdade? Se for, explique com suas palavras porque isso acontece.

8	1	6		26	5	20
3	5	7	⇢	11	17	23
4	9	2		14	29	8

Com algumas somas, podemos verificar que o quadrado resultante também é mágico e sua constante mágica é igual a 51 $(15 \times 3 + 2 + 2 + 2)$. Mas o que podemos dizer sobre os termos? Qual é a padrão que apresentam?

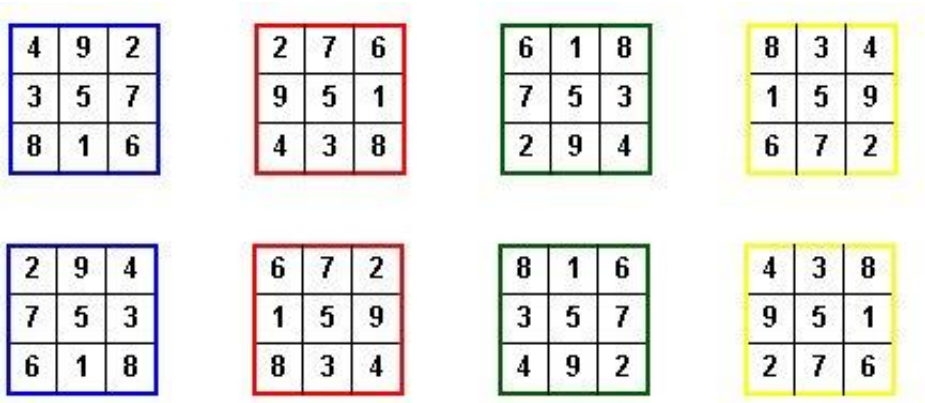
4.5 - Solução da Atividade I:

Questionamento para ser respondido pelos grupos:

I) 9

II) 1,2,3,4,5,6,7,8,9

III) Possíveis Quadrados Mágicos encontrados:



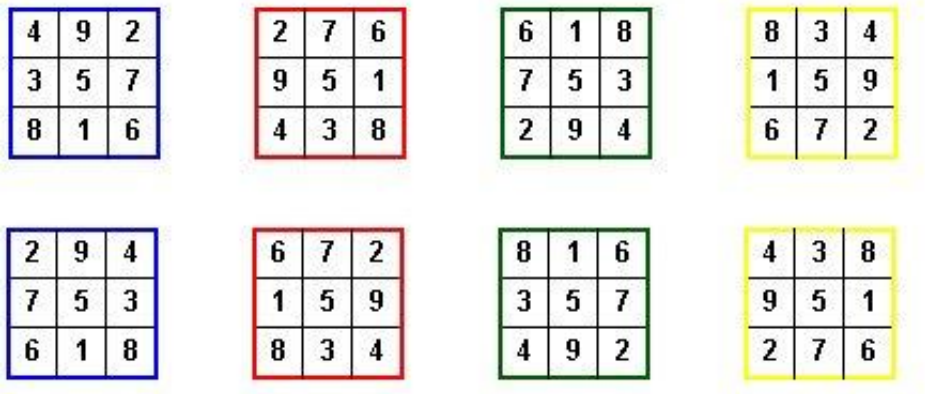
IV) 5

V) 15

VI) A constate mágica é o termo central somado com o primeiro e último termo da sequência; o termo central é um terço da constante mágica.

4.6 - Solução da Atividade II:

I) Todos os Quadrados Mágicos possíveis são:



II) 24;24.

III) A constante mágica será o triplo do termo do centro da sequência organizada de forma crescente.

IV) Todos os conjuntos são sequências numéricas com 9 elementos, que podem formar Quadrados Mágicos.

4.7 - Solução da Atividade III:

I)

9	4	5
2	6	10
7	8	3

II)

3	13	11
17	9	1
7	5	15

4	14	12
18	10	2
8	6	16

III) 6

IV) Não, porque os quadrados mágicos são formados por sequência numéricas diferentes.

V) 18

VI) Não. Porque a constante central tem relação com a constante mágica.

4.8 - Solução da Atividade IV:

I) Sim. Isso acontece porque em um quadrado mágico de ordem 3 , a soma mágica é o triplo é da constante mágica.

II) Sim.

III) Sim.

IV) Toda sequência de nove múltiplos pode ser escrita da forma K. (1,2,3,4,5,6,7,8,9), onde K é inteiro e (1,2,3,4,5,6,7,8,9) sequência que de fato forma o quadrado mágico puro fundamental de ordem 3.

V) Quando ordenamos seus termos, podemos ver facilmente que se trata dos termos de uma Progressão Aritmética de razão igual a 3 e primeiro termo igual a 5:

$$5, 8, 11, 14, 17, 20, 23, 26\ e\ 29.$$

E com isso, concluímos que:

Dada uma Progressão Aritmética de nove termos, quando posicionados todos os seus termos a_i na posição que o número i ocupa no Quadrado de Mágico, o quadrado resultante também será mágico.

CONCLUSÃO:

Ao aprendermos um pouco sobre de teoria de grupos, podemos ver como uma simples divisão de elementos de um grupo finito foi possível a obtenção de dois resultados clássicos de aritmética, além do uso desta teoria na construção de quadrados mágicos de ordem 3.

Por outro lado, vimos que os quadrados mágicos tornaram-se objetos de estudos, na transição entre a Idade Média e o Renascimento, onde alguns aparecem em gravuras, alguns estão relacionados com os metais e planetas e despertaram o interesse de alguns matemáticos, pelos problemas difíceis que originaram a sua construção, classificação e enumeração dos quadrados de uma determinada ordem.

Propomos atividades para sala de aula relacionando quadrados mágicos, sequências numéricas e progressão aritmética, apresentando tópicos matemáticos de forma lúdica com metodologia simples, estimulando o raciocínio lógico e solidificando o conhecimento matemático de modo natural e mais divertido, apresentando como inspiração didática para os professores de matemática em sua prática diária.

REFERÊNCIA BIBLIOGRÁFICA:

ANDRADE, L. **Mais sobre Quadrados Mágicos.** Revista do Professor de Matemática, volume 41.

ARSIE, K. **Jogos Sudoku e Quadrado Mágico.** 2010. Disponível em: <https://docs.ufpr.br/~ewkaras/ic/karla10.pdf> Acesso em: 23/03/2018.

BARICHELLO, L. **Quadrado Mágico Aditivo - Experimento.** 2018. Disponível em: <https://m3.ime.unicamp.br/recursos/1028> Acesso em : 23/11/2019.

FERREIRA, D. **Grupo de Simetria ao Quadrado mágico.** 2019. Disponível em: <http://riu.ufam.edu.br/bitstream/prefix/5665/6/TCC-DirleiFerreira.pdf> Acesso em: 15/01/2020.

JANUARIO, G. **Quadrados Mágicos: Uma Proposta de Aprendizado com Enfoque Etnomatemático**. 2008. Disponível em: <http://www.educadores.diaadia.pr.gov.br/arquivos/File/2010/artigos_teses/MATEMATICA/Artigo_Gilberto_02.pdf> Acesso em: 11/02/2019.

LOPES, T. **A História dos Quadrados Mágicos.** 2011. Disponível em: <http://www.mat.uc.pt/~mat0717/public_html/Cadeiras/1Semestre/O%20que%20%C3%A9%20um%20quadrado%20m%C3%A1gico.pdf > Acesso em: 6/02/2018.

VILELLA, M. **Grupos.** Universidade Federal Fluminense. 2009. Disponível em: <http://www.professores.uff.br/jcolombo/wp-content/uploads/sites/124/2017/09/1-2016-grupos-mod1.pdf>