



**UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS E TECNOLOGIA
CURSO DE LICENCIATURA EM MATEMÁTICA**

ESTUDANDO ALGUNS GRUPOS INESPERADOS

MATHEUS AZEVEDO MAIA

CAMPINA GRANDE

2019

MATHEUS AZEVEDO MAIA

ESTUDANDO ALGUNS GRUPOS INESPERADOS

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade Estadual da Paraíba em cumprimento as exigências para obtenção do título de Licenciado em Matemática.

Orientadora: Profa. Emanuela Régia de Sousa Coelho

CAMPINA GRANDE

2019

É expressamente proibido a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano do trabalho.

M217e Maia, Matheus Azevedo.
Estudando alguns grupos inesperados [manuscrito] /
Matheus Azevedo Maia. - 2019.
43 p.
Digitado.
Trabalho de Conclusão de Curso (Graduação em
Matemática) - Universidade Estadual da Paraíba, Centro de
Ciências e Tecnologia, 2019.
"Orientação : Profa. Dra. Emanuela Régia de Sousa
Coelho, Coordenação do Curso de Matemática - CCT."
1. Teoria dos grupos. 2. Matrizes singulares. 3. Classes de
restos. I. Título
21. ed. CDD 512.9434

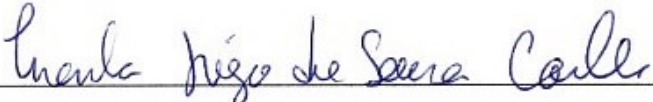
MATHEUS AZEVEDO MAIA

ESTUDANDO ALGUNS GRUPOS INESPERADOS

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade Estadual da Paraíba em cumprimento as exigências para obtenção do título de Licenciado em Matemática.

Aprovado em: 28/06/2019.

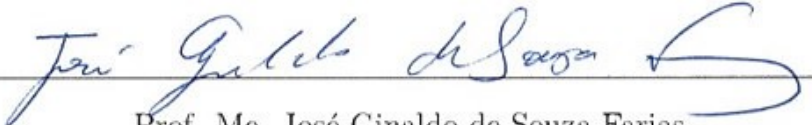
BANCA EXAMINADORA



Profa. Dra. Emanuela Régia de Sousa Coelho (Orientadora)
Universidade Estadual da Paraíba (UEPB)



Prof. Esp. Adailson Ribeiro da Silva
Universidade Estadual da Paraíba (UEPB)



Prof. Me. José Ginaldo de Souza Farias
Universidade Estadual da Paraíba (UEPB - Campus VII)

Dedicatória

À minha querida família,
DEDICO.

Agradecimentos

”Agradecemos a Deus o presente que ele nos dá, um presente que palavras não podem descrever”(2Cor9.15). Agradeço a Deus pela oportunidade concedida de estar concluindo essa importante etapa na minha vida.

Agradeço aos meus familiares em especial aos meus pais, Severino e Paula, pelo incentivo, apoio e todo suporte, aos meus irmãos Jônathas e em especial Dayvid, que na sua condição autista, me traz alegria, me leva a lutar para sempre conquistar mais e me motivou durante essa jornada. Agradeço a minha madrinha, Maria José que me acolheu e cuidou super bem, sendo uma segunda mãe.

Agradeço aos meus professores que ajudaram a moldar meu caráter profissional, e contribuíram na minha formação acadêmica. Para não correr o risco do esquecimento optei por não citar nomes, mas que tenho apreço e carinho enorme. Em especial quero agradecer a minha orientadora Emanuela Régia, pelo grandioso apoio para realização desse trabalho, pelos ensinamentos em salas de aula e ensinamentos para a vida.

Agradeço a Isaías, Marcos, Everaldo e Junior os motoristas de ônibus da cidade de Solânea pela época em que estive com eles. Foram muito pacientes, se tornaram amigos e sempre fizeram o possível para cumprir seu trabalho.

Agradeço meus amigos de curso que estiveram presentes e sempre me ajudaram durante essa jornada, Henrique, Geovane, Raylson, Jamerson, Newton, Jailson, Wesley, Jessica, Mariana, Ketllen, Rivanio entre outros que peço desculpas por não citar nominalmente. Agradeço também aos meus amigos Thainá, Rafael, Tales, Cássio, Wagner e Daiana que estão sempre comigo.

Resumo

O presente trabalho trata de estudar alguns subconjuntos de matrizes singulares 2×2 e da classe de restos \mathbb{Z}_n que, quando munidos da operação de multiplicação usual, formam um grupo. Esses grupos não são comuns quando estudamos Estruturas Algébricas, uma vez não estamos trabalhando com elementos invertíveis desses conjuntos, no sentido usual. Para isso vamos utilizar de algumas Definições, Exemplos, Proposições e Teoremas da Álgebra linear, Teoria dos números, além dos importantes resultados encontrados na Teoria dos Grupos.

Palavras-chave: Grupos Inesperados. Matrizes Singulares. Classes de restos.

Abstract

The present work tries to study some subsets of singular matrices 2×2 and the class of residues \mathbb{Z}_n that, when equipped with the multiplication operation, form a group. These groups are not common when we study Algebraic Structures since we are not working with invertible elements of these arrays in the usual sense. For this we will use some Definitions, Examples, Propositions and Theorems of Linear Algebra, Number Theory, besides the important results found in the Theory of Groups.

Keywords: Unexpected Groups. Single Matrices. Classes of remains.

Sumário

Introdução	7
1 Preliminares	9
1.1 Tópicos em Álgebra linear	9
1.1.1 Matrizes	9
1.1.2 Espaço Vetorial	13
1.1.3 Transformação Linear	19
1.1.4 Teorema do Núcleo e da Imagem	20
1.2 Tópicos em Teoria dos Números	23
1.3 Tópicos em Teoria dos Grupos	27
1.3.1 Subgrupos	28
1.3.2 Grupos Cíclicos	29
1.3.3 Homomorfismo de Grupos	29
2 Alguns Grupos Inesperados	30
2.1 Grupos não invertíveis em \mathbb{Z}_n	30
2.2 Grupos de Matrizes singulares 2×2	33
Considerações Finais	41

Introdução

Entendemos por Estrutura Algébrica um conjunto munido de uma(ou mais) operação(ões) binária(s). O que diferencia uma Estrutura Algébrica de outra são as propriedades que sua(s) operação(ões) satisfaz. Dentre as Estruturas Algébricas mais usuais, encontramos a estrutura de Grupo que é caracterizada pela associatividade, existência de elemento neutro e existência de elemento inverso, para cada elemento dado. Como em qualquer teoria, há exemplos usuais de objetos que satisfazem a definição dada. No caso dessa Estrutura, os conjuntos

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}); \det A \neq 0\}$$

e

$$U(\mathbb{Z}_n) = \{\bar{a} \in \mathbb{Z}_n^*; \text{mdc}(a, n) = 1\}$$

munidos dos seus respectivos produtos, são exemplos clássicos de Grupos.

No presente trabalho vamos utilizar dos conceitos da Teoria de Grupos para estudar alguns grupos multiplicativos não usuais que também são subconjuntos de $M_n(\mathbb{R})$ e \mathbb{Z}_n . Para esse objetivo, seguimos o que foi feito por W. R. Brakes no artigo "Unexpected Groups" em [3], apresentando uma exposição didática do mesmo.

O trabalho está organizado da seguinte forma: o primeiro capítulo traz uma apresentação de conceitos e resultados imprescindíveis da Álgebra Linear que vão desde uma simples definição de matrizes até o Teorema do Núcleo e da Imagem. Já na Teoria dos Números apresentamos conceitos de congruência e introduzimos o conjunto \mathbb{Z}_n e na Teoria dos Grupos explanamos definições iniciais como operações binárias e seguindo até homomorfismo de grupos, para que o resultado principal do trabalho seja entendido abordando o que de fato é importante. As Teorias apresentadas nesse primeiro capítulo estão resumidas e não detalhadas, com o intuito apenas de deixar o texto autossuficiente, mas

referenciamos os livros onde possam ser encontrados de forma mais detalhada.

Já no segundo capítulo temos os resultados principais do nosso trabalho, que é a apresentação de alguns grupos inesperados, no caso deste trabalho os Grupos não invertíveis sob a multiplicação no sentido usual em \mathbb{Z}_n e os grupos de matrizes singulares 2×2 .

Capítulo 1

Preliminares

Neste capítulo serão explorados conceitos e resultados necessários ao desenvolvimento do trabalho.

1.1 Tópicos em Álgebra linear

Um dos temas que será abordado no próximo capítulo deste trabalho terá seu foco em mostrar quais subconjuntos de matrizes singulares de ordem 2×2 formam um grupo sob a multiplicação. Por isto, nesta seção serão introduzidas algumas definições como de Matrizes, Espaço Vetorial, Transformação Linear, dentre outras; também será apresentado algumas propriedades e teoremas importantes como o Teorema do Núcleo e da Imagem, Teorema da Representação Matricial dentre outros que serão explorados no sentido de dar um suporte ao capítulo seguinte. Algumas propriedades e teoremas não terão suas demonstrações apresentadas, para não fugirmos da proposta do trabalho, mas podem ser encontradas em [1], [4], [5], [2] e [8] tais referências também servem de embasamento para a construção dessa seção.

1.1.1 Matrizes

Definição 1.1. (*Matrizes*) Consideremos os seguintes subconjuntos de inteiros positivos:

$$Im = \{1, 2, \dots, m\} \text{ e } In = \{1, 2, \dots, n\}.$$

Uma função,

$$a : Im \times In \rightarrow \mathbb{R} \\ (i, j) \mapsto a(i, j) = a_{ij} ,$$

é chamada matriz.

Observação 1.1. A imagem da matriz é denotada por $A = (a_{ij})_{m \times n}$ e é representada por uma tabela com m linhas e n colunas. Nessas condições, identificamos a matriz a com sua imagem A . Em geral, omitimos o termo $a(i, j)$ e escrevemos os termos a_{ij} e dizemos que A é uma matriz $m \times n$, da seguinte forma:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Quando $m = n$ dizemos que A é uma matriz quadrada.

Exemplo 1.1. (Matriz Identidade) A matriz identidade de ordem $n \times n$:

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

é chamada matriz identidade.

Exemplo 1.2. (Matriz Nula) É a matriz cujos elementos são todos nulos. Indica-se a matriz nula por 0:

$$0 = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

Definição 1.2. (Multiplicação de Matrizes) Sejam $A = (a_{ij})$ uma matriz $m \times p$ e $B = (b_{ij})$ uma matriz $p \times n$. O produto AB é dado pela matriz $C = (c_{ij})_{m \times n}$ da seguinte forma:

$$c_{ij} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + \cdots + a_{ip} \cdot b_{pj} = \sum_{k=1}^p a_{ik} \cdot b_{kj}, \quad (1.1)$$

para $i = 1, 2, \dots, m$ e $j = 1, 2, \dots, n$.

Escrevemos,

$$C = AB \text{ ou } [AB]_{i,j} = \sum_{k=1}^p a_{ik} \cdot b_{kj}.$$

A igualdade da equação 1.1 está dizendo que o elemento i, j do produto é igual a soma dos produtos dos elementos de i -ésima linha de A pelos elementos correspondentes da j -ésima coluna de B .

Exemplo 1.3. Dadas as matrizes

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \text{ e } B = \begin{bmatrix} -2 & 1 \\ 0 & 3 \end{bmatrix}.$$

então

$$AB = \begin{bmatrix} -2 & 7 \\ -6 & 15 \end{bmatrix} \text{ e } BA = \begin{bmatrix} 1 & 0 \\ 9 & 12 \end{bmatrix}$$

Observação 1.2. A matriz identidade I_n é tal que: $AI_n = A$, para todo $A = (a_{ij})_{m \times n}$ e $I_n B = B$, para todo $B = (b_{ij})_{n \times m}$

Observação 1.3. Do exemplo anterior nota-se $AB \neq BA$, ou seja, o produto de matrizes não é comutativo.

Proposição 1.1. (Multiplicação de Matrizes) Admitindo que as ordens das matrizes possibilitem as operações, tem-se:

- (i) $(AB)C = A(BC)$
- (ii) $(A + B)C = AC + BC$
- (iii) $C(A + B) = CA + CB$
- (iv) $(\alpha A)B = \alpha(AB), \alpha \in \mathbb{R}$.

Prova. A prova da Proposição encontra-se em STEINBRUCH, A., 1997. [4]

Definição 1.3. (Matriz Invertível) Uma matriz quadrada $A = (a_{ij})_{n \times n}$ é invertível ou não-singular, se existir uma matriz $B = (b_{ij})_{n \times n}$, tal que $AB = BA = I_n$. A matriz B é chamada inversa de A . Se A não tem inversa dizemos que A é não invertível ou singular. Denotamos a inversa de A , quando existir, por A^{-1} .

Teorema 1.1. Se uma matriz $A = (a_{ij})_{(n \times n)}$ possui inversa, então a inversa é única.

Prova. Suponha que B e C são inversas de A . Então

$$AB = BA = I_n = AC = CA$$

e assim:

$$B = BI_n = B(AC) = (BA)C = I_n C = C.$$

Portanto, $B = C$.

Definição 1.4. (*Operações Elementares*) Uma operação elementar sobre as linhas de uma matriz é uma das seguintes operações:

- Trocar a posição das linhas da matriz;
- Multiplicar uma linha da matriz por um escalar diferente de zero;
- Somar a uma linha da matriz um múltiplo escalar de outra linha.

Se uma matriz B puder ser obtida de uma matriz A através de um número finito de operações elementares, dizemos que B é equivalente à A . E escrevemos $A \sim B$.

Teorema 1.2. Uma matriz A é invertível se, e somente se, $I_n \sim A$.

Prova. A prova do Teorema encontra-se em LOURÊDO, ALDO TRAJANO, 2015.[1]

Exemplo 1.4. A matriz:

$$A = \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} \sim I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Solução: De fato,

$$\begin{aligned} \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ -1 & 2 & 0 & 1 \end{array} \right) &\xrightarrow{L_1 + L_2} \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 3 & 1 & 1 \end{array} \right) \xrightarrow{\frac{1}{3}L_2} \\ \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 1 & \frac{1}{3} & \frac{1}{3} \end{array} \right) &\xrightarrow{-L_1 + L_2} \left(\begin{array}{cc|cc} 1 & 0 & \frac{2}{3} & \frac{-1}{3} \\ 0 & 1 & \frac{1}{3} & \frac{1}{3} \end{array} \right). \end{aligned}$$

Portanto, $A \sim I_2$, e além disso

$$A^{-1} = \begin{pmatrix} \frac{2}{3} & \frac{-1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

Observação 1.4. Neste caso, a mesma sucessão de operações elementares que transforma A em I_n , transforma I_n em A .

Definição 1.5. (*Matrizes Semelhantes*) Diz-se que duas matrizes $P, Q \in M_n(\mathbb{R})$ são semelhantes quando existe uma matriz invertível $R \in M_n(\mathbb{R})$ tal que $Q = RPR^{-1}$.

Teorema 1.3. Se $A = (a_{ij})$ e $B = (b_{ij})$ matrizes semelhantes então, $TrA = TrB$ são

iguais

$$\text{Tr}A = \sum_{i=1}^n a_{ii} = \text{Tr}B \sum_{i=1}^n b_{ii}.$$

Prova. A prova do Teorema encontra-se em FINKBEINER, DANIEL T. [2]

Definição 1.6. (*Determinante*) Seja $A = (a_{ij})_{n \times n}$. O determinante de A , denotado por $\det(A)$, é definido por

$$\det(A) = a_{11}b_{11} + a_{12}b_{12} + \cdots + a_{1n}b_{1n} = \sum_{j=1}^n a_{1j}b_{1j},$$

em que $b_{1j} = (-1)^{1+j}\det(A_{ij})$ é cofator do elemento a_{ij} . A expressão acima é chamada desenvolvimento em cofatores do determinante de A em termos da 1ª linha da matriz A .

1.1.2 Espaço Vetorial

Definição 1.7. (*Espaço Vetorial*) Dizemos que um conjunto $V \neq \emptyset$ munido de duas operações uma "soma" e outra "multiplicação" por escalar:

$$+ : V \times V \rightarrow V$$

$$(u, v) \mapsto u + v$$

e

$$\cdot : \mathbb{R} \times V \rightarrow V$$

$$(\alpha, v) \mapsto \alpha \cdot v;$$

é um espaço vetorial sobre \mathbb{R} , se satisfaz as seguintes propriedades:

1. $v + u = u + v, \forall u, v \in V$;
2. $(v + u) + w = v + (u + w), \forall u, v, w \in V$;
3. $\exists 0 \in V$, tal que $0 + v = v + 0, \forall v \in V$;
4. $\forall v \in V, \exists (-v) \in V$, tal que $v + (-v) = -v + v = 0$;
5. $\forall v$ e $\forall \alpha, \beta \in \mathbb{R}, (\alpha\beta)v = \alpha(\beta v)$;
6. $\forall u, v \in V$ e $\forall \alpha \in \mathbb{R}, \alpha(u + v) = \alpha u + \alpha v$;
7. $\forall \alpha, \beta \in \mathbb{R}$ e $\forall v \in V, (\alpha + \beta)v = \alpha v + \beta v$;
8. $\forall v \in V, 1v = v$.

Exemplo 1.5. Sejam $V = \mathbb{R}^2 = \{(x, y), x, y \in \mathbb{R}\}$, sendo u e v vetores $\in \mathbb{R}^2$ munido das operações:

$$u + v = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

e

$$\alpha(x_1, y_1) = (\alpha x_1, \alpha y_1).$$

onde $u, v \in \mathbb{R}^2$ e $\alpha \in \mathbb{R}$. Então, $(\mathbb{R}^2, +, \cdot)$ é um espaço vetorial.

Solução: De fato, dados $u = (x_1, y_1), v = (x_2, y_2), w = (x_3, y_3) \in \mathbb{R}^2$ e $\alpha, \beta \in \mathbb{R}$

$$1. \quad u + v = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) = \\ (x_2 + x_1, y_2 + y_1) = (x_2, y_2) + (x_1, y_1) = v + u.$$

Portanto, $u + v = v + u$.

$$2. \quad (u + v) + w = u + (v + w) = [(x_1, y_1) + (x_2, y_2)] + (x_3, y_3) = \\ (x_1 + x_2, y_1 + y_2) + (x_3, y_3) = (x_1 + x_2) + x_3, (y_1 + y_2) + y_3 = \\ x_1 + (x_2 + x_3), y_1 + (y_2 + y_3) = (x_1, y_1) + [(x_2, y_2) + (x_3, y_3)] = u + (v + w).$$

Portanto, $(u + v) + w = u + (v + w)$.

3. Seja $0 = (0, 0) \in \mathbb{R}^2$. Então,

$$0 + u = (0, 0) + (x_1, y_1) = (0 + x_1, 0 + y_1) = (x_1, y_1) = u,$$

e

$$u + 0 = (x_1, y_1) + (0, 0) = (x_1 + 0, y_1 + 0) = (x_1, y_1) = u$$

Portanto, $u + 0 = 0 + u = u$.

4. Seja $-u = (-x_1, -y_1) \in \mathbb{R}^2$, o simétrico do vetor u . Então,

$$u + (-u) = (x_1, y_1) + (-x_1, -y_1) = (x_1 + (-x_1), y_1 + (-y_1)) = (0, 0) = 0.$$

Por outro lado,

$$-u + u = (-x_1, -y_1) + (x_1, y_1) = (-x_1 + x_1, -y_1 + y_1) = (0, 0) = 0.$$

Portanto, $u + (-u) = -u + u = 0$.

$$5. \quad (\alpha\beta)u = (\alpha\beta)(x_1, y_1) = ((\alpha\beta)x_1, (\alpha\beta)y_1) = \\ = \alpha(\beta x_1), \alpha(\beta y_1) = \alpha(\beta u).$$

Portanto, $(\alpha\beta)u = \alpha(\beta u)$.

$$6. \quad \alpha(u + v) = \alpha[(x_1, y_1) + (x_2, y_2)] = \alpha(x_1 + x_2, y_1 + y_2) = (\alpha x_1 + \alpha x_2, \alpha y_1 + \alpha y_2) \\ = (\alpha x_1, \alpha y_1) + (\alpha x_2, \alpha y_2) = \alpha(x_1, y_1) + \alpha(x_2, y_2) = \alpha u + \alpha v.$$

Portanto, $\alpha(u + v) = \alpha u + \alpha v$.

$$7. \quad (\alpha + \beta)u = (\alpha + \beta)(x_1, y_1) = ((\alpha + \beta)x_1, (\alpha + \beta)y_1) = \\ = (\alpha x_1 + \beta x_1, \alpha y_1 + \beta y_1) = (\alpha x_1, \alpha y_1) + (\beta x_1, \beta y_1) = \\ = \alpha(x_1, y_1) + \beta(x_1, y_1) = \alpha u + \beta v.$$

Portanto, $(\alpha + \beta)u = \alpha u + \beta v$.

8. Seja $1 \in \mathbb{R}$, tem-se $1u = 1(x_1, y_1) = (1x_1, 1y_1) = (x_1, y_1) = u$.

Portanto, $1u = u$.

Como as oito axiomas de espaço vetorial são satisfeitos, segue que $(\mathbb{R}^2, +, \cdot)$ é um

espaço vetorial sobre \mathbb{R} .

Observação 1.5. De forma análoga, tem-se \mathbb{R}^n , para qualquer $n \in \mathbb{N}$ é espaço vetorial.

Exemplo 1.6. Seja $V = M_n(\mathbb{R})$ o conjunto das matrizes de ordem $n \times n$ munido das operações:

$$A + B = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} =$$

$$\begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \cdots & a_{nn} + b_{nn} \end{pmatrix}.$$

ou

$$A + B = [a_{ij} + b_{ij}]$$

e

$$\alpha A = \alpha \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} & \cdots & \alpha a_{1n} \\ \alpha a_{21} & \alpha a_{22} & \cdots & \alpha a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha a_{n1} & \alpha a_{n2} & \cdots & \alpha a_{nn} \end{pmatrix}.$$

ou

$$\alpha A = (\alpha a_{ij}).$$

Então, $(M_n(\mathbb{R}), +, \cdot)$ é um espaço vetorial sobre \mathbb{R} .

Definição 1.8. (Subespaço Vetorial) Seja V um espaço vetorial sobre \mathbb{R} e W um subconjunto de V . Dizemos que W é um subespaço vetorial de V ou simplesmente subespaço de V , se as seguintes condições são satisfeitas:

- (i) $0 \in W$;
- (ii) $\lambda u \in W$, para todo $\lambda \in \mathbb{R}$ e todo $u \in W$;
- (iii) $u + v \in W$, para todo $u, v \in W$.

Exemplo 1.7. Seja $W = \{(x, 0) : x \in \mathbb{R}\}$ um subconjunto do \mathbb{R}^2 . Vamos mostrar que W é um subespaço do \mathbb{R}^2

Solução. De fato,

i) $(0, 0) \in W$;

ii) Sejam $\lambda \in \mathbb{R}$ e $u = (x, 0) \in W$. Então, $\lambda u = (\lambda x, \lambda 0) = (\lambda x, 0) \in W$

iii) Sejam $u = (a, 0), v = (b, 0) \in W$. Então, $u + v = (a, 0) + (b, 0) = (a + b, 0) \in W$.

Portanto, de (i)-(iii), obtemos W é um subespaço do \mathbb{R}^2 . Geometricamente W é o eixo das abscissas.

Exemplo 1.8. Seja o conjunto $W = \{(1, y) : y \in \mathbb{R}\}$ não é um subespaço do \mathbb{R}^2 , pois, basta notar que $0 = (0, 0) \notin W$.

Teorema 1.4. Sejam V e W subespaços do espaço vetorial \mathbb{R}^2 . Temos que $\mathbb{R}^2 = V + W$ se, e somente se, todo vetor v em \mathbb{R}^2 se escreve de modo único como $v = v_1 + w_1$, onde $v_1 \in V$ e $w_1 \in W$.

Prova. A prova do Teorema encontra-se em HEFEZ, ABRAMO.[8]

Definição 1.9. (Combinação Linear) Sejam V um espaço vetorial real, $v_1, \dots, v_n \in V$ e $a_1, a_2, \dots, a_n \in \mathbb{R}$. Então, o vetor:

$$v = a_1 v_1 + \dots + a_n v_n,$$

é um elemento de V ao qual chamamos de combinação linear de v_1, \dots, v_n .

Proposição 1.2. Fixados os vetores $v_1, v_2, \dots, v_n \in \mathbb{R}$, o conjunto W de todos os vetores de V , que são combinação linear destes, o qual é denotado por

$$W = [v_1, v_2, \dots, v_n] = \{v \in V : v = a_1 v_1 + \dots + a_n v_n : a_i \in \mathbb{R}, 1 \leq i \leq n\},$$

é um subespaço de V e W é chamado de **subespaço gerado por** v_1, \dots, v_n .

Prova. (i) $0 \in W$, pois

$$0 = 0v_1 + \dots + 0v_n.$$

(ii) Sejam $v = a_1 v_1 + \dots + a_n v_n$ e $w = b_1 v_1 + \dots + b_n v_n \in W$. Então, pelas propriedades da associatividade e comutatividade em V , podemos escrever:

$$v + w = (a_1 v_1 + \dots + a_n v_n) + (b_1 v_1 + \dots + b_n v_n) = (a_1 + b_1)v_1 + \dots + (a_n + b_n)v_n \in W$$

(iii) Sejam $\alpha \in \mathbb{R}$ e $v = a_1 v_1 + \dots + a_n v_n \in W$. Então,

$$\alpha v = \alpha(a_1 v_1 + \dots + a_n v_n) = (\alpha a_1)v_1 + \dots + (\alpha a_n)v_n \in W$$

Portanto, de (I)-(III), segue $[v_1, \dots, v_n]$ é um subespaço de V .

Definição 1.10. Sejam V um espaço vetorial e $A = \{v_1, \dots, v_n\} \subset V$. O conjunto A diz-se ser linearmente independente (LI) ou que os vetores v_1, \dots, v_n são LI caso a equação

$$a_1v_1 + \cdots + a_nv_n = 0$$

admita apenas a solução trivial, isto é,

$$a_1 = a_2 = \cdots = a_n = 0.$$

Se existir $a_i \neq 0$, para algum $i = 1, \dots, n$, diz-se que o conjunto A é linearmente dependente(LD), ou que os vetores v_1, \dots, v_n , são LD.

Definição 1.11. (Base de um Espaço Vetorial) Um conjunto $B = \{v_1, \dots, v_n\} \subset V$ é uma base para o espaço vetorial V se :

- i) B é LI;
- ii) B gera V .

Teorema 1.5. Se $\beta = \{v_1, \dots, v_n\}$ for uma base de um espaço vetorial V , então todo conjunto com mais de n vetores em V será linearmente dependente.

Prova. A prova do Teorema encontra-se em LOURÊDO, ALDO TRAJANO, 2015.[1]

Dimensão de um Espaço Vetorial

Seja V um espaço vetorial sobre \mathbb{R} .

- Se V possui uma base com n vetores, então V tem dimensão n e anota-se $\dim V = n$.
- Quando um espaço vetorial V admite uma base finita, dizemos que V é um espaço vetorial de dimensão finita.
- Se $V = \{0\}$, convencionou-se que $\dim V = 0$.
- Se V tem uma base com infinitos vetores, então a dimensão de V é infinita e anota-se $\dim V = \infty$

Exemplo 1.9. $\dim \mathbb{R}^n = n$, pois $\beta = (1, 0, \dots, 0), \dots, (0, 0, \dots, 1)$ é base de \mathbb{R}^n .

Exemplo 1.10. $\dim M_2(\mathbb{R}) = 4$, pois

$$\beta = \left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right]$$

é base para o espaço M_2 .

Proposição 1.3. Sejam V um espaço vetorial e $\beta = \{v_1, \dots, v_n\}$ um conjunto LI em V . Se $v \notin [\beta]$, então o conjunto $A = \{v_1, \dots, v_n, v\}$ é LI.

Prova. Como $v \notin [\beta]$ e $v \in A$ o conjunto A não pode ser escrito como combinação linear de β , logo o conjunto é LI.

Proposição 1.4. Sejam V um espaço vetorial com $\dim V = n$ e $\beta = \{v_1, \dots, v_n\}$ um

conjunto LI em V . Então, β é um base de para V .

Prova. Se β gerar V , então β é uma base para V . Se β não gerar V , então existe um vetor $v \in V$, tal que $v \notin [\beta]$. Logo, pela Proposição 1.3, o conjunto $A = \{v_1, \dots, v_n, v\}$ é LI, o que contraria o Teorema 1.5, pois $n(A) = n + 1 > \dim V = n$.

Proposição 1.5. *Seja V um espaço vetorial com $\dim V = n$ e β um conjunto gerador para V . Então, β pode ser reduzida a uma base β' para V .*

Prova. A prova da Proposição encontra-se em LOURÊDO, ALDO TRAJANO, 2015.[1]

Teorema 1.6. *(Completamento) Qualquer conjunto de vetores LI de um espaço vetorial V de dimensão finita pode ser completado de modo a formar uma base V .*

Prova. A prova da Proposição encontra-se em LOURÊDO, ALDO TRAJANO, 2015.[1]

Proposição 1.6. *Seja V um espaço vetorial sobre \mathbb{R} com $\dim V = n$ e W é um subespaço de V ,*

i) W é de dimensão finita e $\dim W \leq \dim V$;

ii) $\dim W = \dim V$ se, e somente se, $W = V$.

Prova. (i) Se $W = \{0\}$, então $\dim W = 0 \leq n = \dim V$. Se $W \neq \{0\}$, então qualquer base B para V gera W , pois $W \subset V$. Logo, pela Proposição 1.4, conjunto gerador β de W pode ser reduzida a uma base β' para W , a qual tem no máximo n vetores. Portanto, W é de dimensão finita e $\dim W \leq n = \dim V$.

(ii) (\Leftarrow) Se $W = V$, é claro que $\dim V = \dim W$.

(\Rightarrow) Suponha que $\dim W = \dim V = n$ e seja $\beta = \{w_1, \dots, w_n\}$ uma base de W . Logo, $[\beta] = W$. Como $W \subset V$, esses n vetores são LI em V e, pela Proposição 1.6, segue-se que β é uma base para V . Portanto, $V = [\beta] = W$.

Retas em \mathbb{R}^2

Supondo W como subespaço de \mathbb{R}^2 , tem-se pela proposição 1.6 que $\dim W = 0, 1$ ou 2 . Sabendo que necessariamente o vetor $\{(0, 0)\}$ tem que estar no conjunto, pois é uma das condições para que seja subespaço, vamos analisar $W \in \mathbb{R}^2$ no que se refere ao aspecto geométrico, com isso:

- Se $\dim W = 0$, então $W = \{(0, 0)\}$
- Se $\dim W = 1$, então $W = r$, em que r é uma reta que passa pela origem, como no Exemplo 1.7.
- Se $\dim W = 2$, então pela proposição 1.6, $W = \mathbb{R}^2$.

1.1.3 Transformação Linear

Definição 1.12. (*Transformação Linear*) Sejam V e W espaços vetoriais sobre \mathbb{R} . Dizemos que uma aplicação $T : V \rightarrow W$ é uma transformação linear se satisfaz as seguintes condições:

- i) $T(\alpha v), \forall \alpha \in \mathbb{R}$ e $v \in V$;
- ii) $T(v + u) = T(v) + T(u), \forall u, v \in V$.

Exemplo 1.11. A aplicação $T : \mathbb{R}^2 \rightarrow M_2(\mathbb{R})$ definida por

$$T(x, y) = \begin{pmatrix} x + y & -x \\ x - y & y \end{pmatrix} \text{ é uma transformação linear.}$$

Solução. i) De fato, sejam $\alpha \in \mathbb{R}$ e $v = (x, y) \in \mathbb{R}^2$. Então, $\alpha v = \alpha(x, y) = (\alpha x, \alpha y) \in \mathbb{R}^2$ e

$$T(\alpha v) = T(\alpha x, \alpha y) = \begin{pmatrix} \alpha x + \alpha y & -(\alpha x) \\ \alpha x - (\alpha y) & \alpha y \end{pmatrix} = \alpha \begin{pmatrix} x + y & -x \\ x - y & y \end{pmatrix} = \alpha T(v);$$

ii) Sejam $v = (x_1, y_1), w = (x_2, y_2) \in \mathbb{R}^2$. Então, $v + w = (x_1 + x_2, y_1 + y_2) \in \mathbb{R}^2$ e

$$\begin{aligned} T(v + w) &= T(x_1 + x_2, y_1 + y_2) = \begin{pmatrix} (x_1 + x_2) + (y_1 + y_2) & -(x_1 + x_2) \\ x_1 + x_2 - (y_1 + y_2) & (y_1 + y_2) \end{pmatrix} = \\ &= \begin{pmatrix} (x_1 + y_1) & -x_1 \\ x_1 - y_1 & y_1 \end{pmatrix} + \begin{pmatrix} x_2 + y_2 & -x_2 \\ x_2 - y_2 & y_2 \end{pmatrix} = T(v) + T(w). \end{aligned}$$

Portanto, de (i)-(ii), segue-se que T é uma transformação linear.

Matriz de uma Transformação Linear

Sejam $T : V \rightarrow W$ uma transformação linear e $\beta = \{v_1, v_2, \dots, v_n\}$ e $\gamma = \{w_1, w_2, \dots, w_m\}$ bases ordenadas de V e W respectivamente. Então,

$$T(v_j) = a_{1j}w_1 + a_{2j}w_2 + \dots + a_{mj}w_m,$$

para cada j , com $1 \leq j \leq n$. A matriz de T relativa as bases ordenadas β e γ é a matriz $m \times n$ com entradas em \mathbb{R} , denotada por $[T]_{\gamma}^{\beta}$ é organizada na forma:

$$[T]_{\gamma}^{\beta} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

1.1.4 Teorema do Núcleo e da Imagem

Definição 1.13. (*Núcleo e Imagem de uma Transformação Linear.*) Sejam V e W dois espaços vetoriais sobre \mathbb{R} e $T : V \rightarrow W$ uma transformação linear.

- a) O conjunto $\{v \in V : T(v) = 0\}$ é chamado núcleo de T e é denotado por $Ker(T)$;
 b) O conjunto $\{w \in W : \exists v \in V \text{ com } T(v) = w\}$ é chamado de imagem de T e será denotado por $Im(T)$.

Observa-se que uma transformação linear $T : V \rightarrow W$ é sobrejetora se, e somente se $Im(T) = W$.

Proposição 1.7. Seja $T : V \rightarrow W$ uma transformação linear. Então, T é injetiva se, e somente se $Ker(T) = \{0\}$.

Prova. (\Rightarrow) Supondo que T é injetiva. Seja $u \in Ker(T)$, então, $T(u) = 0 = T(0)$ e como T é injetiva, essa igualdade implica em $u = 0$. Portanto, $Ker(T) = \{0\}$.

(\Leftarrow) Agora, supondo que $Ker(T) = \{0\}$ vamos mostrar que T é injetiva. Sejam $u, v \in V$, tais que $T(u) = T(v)$. Então, $T(u - v) = 0$, o que implica em $u - v \in Ker(T) = \{0\}$. Dai obtêm-se $u - v = 0$, e portanto $u = v$ o que mostra que T é injetiva.

Proposição 1.8. Sejam V e W dois espaços vetoriais sobre \mathbb{R} e $T : V \rightarrow W$ uma transformação linear. Então $Ker(T)$ é um subespaço vetorial de V e $Im(T)$ é um subespaço vetorial de W .

Prova. Sejam $v \in Ker(T)$, isto é, $T(v) = 0$, e $\alpha \in \mathbb{R}$, então: $T(\alpha v) = \alpha T(v) = \alpha 0 = 0$, logo $\alpha v \in Ker(T)$. Agora, se $u, w \in Ker(T)$, isto é, $T(u) = 0$ e $T(w) = 0$, então: $T(v + w) = T(v) + T(w) = 0 + 0 = 0$, portanto $v + w \in Ker(T)$. Logo, o $Ker(T) \subset V$ é um subespaço de V .

Sejam $\lambda \in \mathbb{R}$ e $w \in Im(T)$. Então, existe $v \in V$, tal que $T(v) = w$. Logo, $\lambda w = \lambda T(v) = T(\lambda v)$, o que implica $\lambda w \in Im(T)$. Agora, sejam $w_1, w_2 \in Im(T)$. Então, existem $v_1, v_2 \in V$, tais que $T(v_1) = w_1$ e $T(v_2) = w_2$. Logo, $w_1 + w_2 = T(v_1 + v_2)$. Dai obtêm-se $w_1 + w_2 \in Im(T)$. Portanto, $Im(T)$ é um subespaço de V .

Teorema 1.7. (*Teorema do Núcleo e da Imagem*) Sejam V e W espaços vetoriais sobre

\mathbb{R} e $T : V \rightarrow W$ uma transformação linear com $\dim V = n$. Então,

$$\dim V = \dim \text{Ker}(T) + \dim \text{Im}(T).$$

Prova. Seja $\beta = \{u_1, \dots, u_n\}$ uma base do $\text{Ker}(T)$. Como β é LI, então β pode ser completado pelo teorema 1.6 até formar uma base para V . Digamos que

$$\gamma = \{u_1, \dots, u_r, u_{r+1}, \dots, u_n\},$$

é uma base para V . Mostraremos que,

$$\alpha = \{T(u_{r+1}), \dots, T(u_n)\},$$

é uma base para $\text{Im}(T)$. De fato, dado $w \in \text{Im}(T)$ existe $u \in V$, tais que $T(u) = w$.

Como $u \in V$, então existem escalares $a_i \in \mathbb{R}$, $1 \leq i \leq n$, tais que

$$u = a_1 u_1 + \dots + a_r u_r + a_{r+1} u_{r+1} + \dots + a_n u_n.$$

Agora, usando o fato de que $T(u_i) = 0$, para $1 \leq i \leq r$, pois $u_i \in \text{Ker}(T)$, obtemos:

$$\begin{aligned} w &= T(u) = T(a_1 u_1 + \dots + a_r u_r + a_{r+1} u_{r+1} + \dots + a_n u_n) \\ &= a_1 T(u_1) + \dots + a_n T(u_n) + a_{r+1} T(u_{r+1}) + \dots + a_n T(u_n) \\ &= a_{r+1} T(u_{r+1}) + \dots + a_n T(u_n). \end{aligned}$$

Dai, obtemos que $w \in [T(u_{r+1}), \dots, T(u_n)]$ e, conseqüentemente,

$$\text{Im}(T) \subset [T(u_{r+1}), \dots, T(u_n)].$$

Como $[T(u_{r+1}), \dots, T(u_n)] \subset \text{Im}(T)$, resulta que $\text{Im}(T) = [T(u_{r+1}), \dots, T(u_n)]$. Agora vamos mostrar que,

$$\alpha = \{T(u_{r+1}), \dots, T(u_n)\}, \text{ é LI.}$$

De fato, consideremos a combinação linear $a_{r+1} T(u_{r+1}) + \dots + a_n T(u_n) = 0$, o que implica, $T(a_{r+1} u_{r+1}) + \dots + T(a_n u_n) = 0$ que acarreta,

$$T(a_{r+1} u_{r+1} + \dots + a_n u_n) = 0.$$

Dai, obtemos $a_{r+1} u_{r+1} + \dots + a_n u_n \in \text{Ker}(T)$. Logo escreve-se,

$$a_{r+1} u_{r+1} + \dots + a_n u_n = a_1 u_1 + \dots + a_r u_r,$$

donde segue,

$$a_1 u_1 + \dots + a_r u_r + (-a_{r+1}) u_{r+1} + \dots + (-a_n) u_n = 0$$

Agora, usando o fato de que $\gamma = \{u_1, \dots, u_r, u_{r+1}, \dots, u_n\}$, é uma base para V , obtêm-se $a_1 = \dots = a_r = a_{r+1} = \dots = a_n = 0$.

Portanto, $\alpha = \{T(u_{r+1}), \dots, T(u_n)\}$ é LI, e conseqüentemente um base para $\text{Im}(T)$. Logo,

$$\dim V = n = r + (n - r) = \dim \text{Ker}(T) + \dim \text{Im}(T).$$

Corolário 1.1. Se $T : V \rightarrow W$ é uma transformação linear e $\dim V = \dim W$, então T é injetora se, somente se, T é sobrejetora.

Prova. (\Leftarrow) Por suposição seja T injetora. Logo pela Proposição 1.7 tem-se $\text{Ker}(T) = \{0\}$. Portanto, $\dim \text{Ker}(T) = 0$ e usando o fato que $\dim V = \dim W$, pelo Teorema 1.7 obtemos,

$$\dim V = \dim \text{Ker}(T) + \dim \text{Im}(T) \text{ logo, } \dim W = 0 + \dim \text{Im}(T) = \dim \text{Im}(T).$$

Como a $\text{Im}(T) \subset W$ é um subespaço de W e $\dim W = \dim \text{Im}(T)$, obtemos pela Proposição 1.6 item (ii) $\text{Im}(T) = W$, isto é, T é sobrejetora.

(\Rightarrow) Supondo que T é sobrejetora, isto é, $\text{Im}(T) = W$. Logo, $\dim \text{Im}(T) = \dim W$. Agora usando a hipótese de que $\dim V = \dim W$, segue do Teorema do Núcleo e da Imagem que,

$$\begin{aligned} \dim V = \dim \text{Ker}(T) + \dim \text{Im}(T) &\Rightarrow \dim W = \dim \text{Ker}(T) + \dim \text{Im}(T) \Rightarrow \\ \dim \text{Ker}(T) &= 0 \end{aligned}$$

o que implica que $\text{Ker}(T) = 0$ e pela Proposição 1.7, obtemos T é injetora.

Definição 1.14. (*Isomorfismo*) Seja $T : V \rightarrow W$ uma transformação linear. Dizemos que T é isomorfismo linear ou simplesmente um isomorfismo, se T é bijetora.

Quando $T : V \rightarrow W$ é isomorfismo, diz-se que os espaços V e W são isomorfos.

Notação: $V \sim W$.

Dois espaços de dimensões finitas isomorfos preservam dimensões, isto é, $\dim V = \dim W$. Agora, denotando o conjunto de todas as transformações lineares $T : V \rightarrow W$ por $\mathcal{L}(V, W)$, temos o seguinte Teorema:

Teorema 1.8. (*Teorema da Representação Matricial*) Sejam V e W dois espaços vetoriais sobre \mathbb{R} e β e γ bases ordenadas de V e W , respectivamente, com $\#\beta = n$ e $\#\gamma = m$. Então, a aplicação

$$\begin{aligned} \psi : \mathcal{L}(V, W) &\rightarrow M_{m \times n}(\mathbb{R}) \\ T &\mapsto \psi(T) = [T]_{\gamma}^{\beta} \end{aligned}$$

é um isomorfismo linear. Em particular, $\dim \mathcal{L}(V, W) = \dim V \cdot \dim W$.

Prova. A prova da Proposição encontra-se em LOURÊDO, ALDO TRAJANO, 2015.[1]

Observação 1.6. Seja $A \in M_2(\mathbb{R})$ do Teorema 1.5 podemos identificar A como uma transformação linear $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$. Se A é invertível, segue que T é isomorfismo, portanto, $\dim \text{Im}(T) = \dim \mathbb{R}^2$, assim é bijetora e não singular. Se A é nula então $\dim \text{Ker}(T) = 2$ e $\dim \text{Im}(T) = 0$, então tem-se uma transformação linear nula. Agora se A é não invertível e não nula, da proposição 1.6, segue

$$1 \leq \dim \text{Ker}(T) \leq 2,$$

e

$$1 \leq \dim \text{Im}(T) \leq 2.$$

Logo, comparando obtém-se $\dim \text{Ker}(T) = 1$ e $\dim \text{Im}(T) = 1$ e, pelos comentários sobre retas em \mathbb{R}^2 , concluímos que $\text{Ker}(T)$ e $\text{Im}(T)$ são retas que passam pela origem.

1.2 Tópicos em Teoria dos Números

Como o trabalho também se atenta a mostrar subconjuntos de elementos, não invertíveis, de Z_n que formam um grupo sob a multiplicação, precisamos, como no Tópico Anterior, de alguns conceitos de Teoria dos Números. Para essa seção, nos guiamos pelas referências [7] e [6].

Definição 1.15. (*Divisibilidade*) Dizemos que a divide b , em símbolos $a|b$, se existir um número c , com $c \in \mathbb{Z}$, tal que:

$$b = a.c$$

Neste caso, diremos também que a é divisível por b , que b é um divisor de a ou ainda que a é um múltiplo de b . Assim,

$$b|a \Leftrightarrow a = bc, \text{ para algum } c \in \mathbb{Z}.$$

Teorema 1.9. (*Algoritmo da Divisão*) Sejam a, b inteiros, com $b > 0$. Então, existem únicos inteiros q e r tais que:

$$a = bq + r, \text{ com } 0 \leq r < b.$$

Prova. A prova do Teorema encontra-se em VIEIRA, VANDEBERG LOPES, 2015.[6]

Definição 1.16. Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Dizemos que $d \in \mathbb{N}$ é máximo divisor comum de a e b quando as seguintes condições são satisfeitas:

(a) $d|a$ e $d|b$

(b) Se $c|a$ e $c|b$, então $c|d$.

Em outras palavras, o máximo divisor comum de a e b é um número natural que os divide e é divisível por todo divisor comum de a e b .

Notação: $d = \text{mdc}(a, b)$

Definição 1.17. Dois inteiros a e b são ditos primos entre si ou relativamente primos quando o $\text{mdc}(a, b) = 1$.

Proposição 1.9. Os inteiros a e b são relativamente primos se, e somente se, existem $x, y \in \mathbb{Z}$ tais que

$$1 = ax + by$$

Prova. A prova da Proposição encontra-se em VIEIRA, VANDEBERG LOPES, 2015.[6].

Proposição 1.10. *Todo número natural $a > 1$ pode ser escrito de modo único, a menos da ordem dos fatores, na forma*

$$a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \quad (1.2)$$

em que p_1, p_2, \dots, p_k são primos distintos e r_1, r_2, \dots, r_k são números naturais.

A representação de um inteiro $a > 1$ dada em (1.2) é sua fatoração ou decomposição primária em fatores primos.

Propriedades Básicas da Congruência

Sejam m um número natural e a e b inteiros quaisquer. Dizemos que a é congruente a b módulo m , em símbolos,

$$a \equiv b \pmod{m},$$

quando m divide $a - b$. O número m é chamado módulo da congruência.

Exemplo 1.12. Tem-se

$$4 \equiv 1 \pmod{3}; 16 \equiv -4 \pmod{5}; -7 \equiv 5 \pmod{2};$$

pois, $3|(4 - 1)$; $5|(16 + 4)$ e $2|(-7 - 5)$.

A notação $a \equiv b \pmod{m}$ significa afirmar que existe um inteiro k tal que:

$$a = b + km.$$

Proposição 1.11. *Dados a e b inteiros, tem-se $a \equiv b \pmod{m}$ se, e somente se, a e b tem o mesmo resto quando divididos por m .*

Prova. Se $a \equiv b \pmod{m}$, então $a = b + km$, com k inteiro. Pelo algoritmo da divisão ,

$$b = qm + r, \text{ com } 0 \leq r < m.$$

Assim,

$$a = b + km = qm + r + km = (q + k)m + r,$$

ou seja, r também é o resto da divisão de a por m . Reciprocamente, suponha que

$$a = q_1m + r \text{ e } b = q_2m + r, \text{ em que } 0 \leq r < m.$$

Logo,

$$a - b = (q_1 - q_2)m,$$

de modo que $m|(a - b)$, isto é, $a \equiv b \pmod{m}$.

Definição 1.18. *(Relação de Equivalência) Uma relação \mathcal{R} em um conjunto A é chamado de relação de equivalência quando as seguintes condições são satisfeitas:*

- i) $x\mathcal{R}x, \forall x \in A$. (\mathcal{R} é reflexiva)
- ii) Se $x\mathcal{R}y$, então $y\mathcal{R}x, \forall x, y \in A$. (\mathcal{R} é simétrica)
- iii) Se $x\mathcal{R}y$ e $y\mathcal{R}z$ então $x\mathcal{R}z, \forall x, y \in A$. (\mathcal{R} é transitiva).

Quando uma relação \mathcal{R} em A for de equivalência, usaremos em geral a notação \sim ao invés de \mathcal{R} .

Definição 1.19. *Seja \sim uma relação de equivalência sobre o conjunto A . O conjunto dos x tais que $x \sim a$ é chamado de classe de equivalência de a e indicado por \bar{a} , ou seja,*

$$\bar{a} = \{x \in A : x \sim a\}.$$

Um elemento $b \in \bar{a}$ é dito um representante da classe \bar{a} . O conjunto de todas as classes de equivalência segundo a relação \sim é chamado conjunto quociente de A por \sim e indicado por A/\sim . Assim,

$$A/\sim = \{\bar{a} : a \in A\}.$$

Denotemos o conjunto quociente de \mathbb{Z} pela relação de congruência \equiv_n por \mathbb{Z}_n .

Proposição 1.12. *A congruência módulo n ($\equiv \pmod{n}$) é uma relação de equivalência.*

Prova. Para provarmos que a congruência módulo n é uma relação de equivalência, temos que mostrar que ela é reflexiva, simétrica e transitiva.

Reflexiva: Para qualquer $a \in \mathbb{Z}$, temos que

$$a - a = 0 = 0.n,$$

isto é, $a \equiv a \pmod{n}$. Portanto $\equiv \pmod{n}$ é reflexiva.

Simétrica: Para todo $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{n}$, então $a - b = c.n$, para algum $c \in \mathbb{Z}$, e, assim,

$$b - a = -(a - b) = (-c).n$$

Logo, $b \equiv a \pmod{n}$, o que implica que a relação é simétrica.

Transitiva: Sejam $a, b, c \in \mathbb{Z}$, tais que $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a - b = e.n$ e $b - c = f.n$, para algum $e, f \in \mathbb{Z}$. Logo,

$$a - c = a - b + b - c = e.n + f.n = (e + f).n$$

Portanto, $a \equiv c \pmod{n}$, o que implica que a relação é transitiva.

Logo, tem-se que tal relação é de equivalência.

Conjunto Quociente \mathbb{Z}_n

Analisando o conjunto quociente de \mathbb{Z} pela relação de congruência modulo n

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

formado por n classes de equivalência, cujos representantes são possíveis restos obtidos da divisão de inteiros por n . cada elemento \bar{r} de \mathbb{Z}_n , com $0 \leq r < n$, representa um conjunto infinito de inteiros, a saber,

$$\bar{r} = \{x \in \mathbb{Z} : x \equiv r \pmod{n}\}$$

Proposição 1.13. *Seja n um número natural. Então,*

$$\begin{aligned} + : \mathbb{Z}_n \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n & e & & \cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n \\ (\bar{a}, \bar{b}) &\mapsto \bar{a} + \bar{b} = \overline{a+b} & & & (\bar{a}, \bar{b}) &\mapsto \bar{a} \cdot \bar{b} = \overline{a \cdot b} \end{aligned}$$

definem duas operações de adição e multiplicação sobre \mathbb{Z}_n .

Prova. A prova da Proposição encontra-se em VIEIRA, VANDEBERG LOPES, 2013.[6]

Teorema 1.10. *A operação \odot multiplicação usual sobre \mathbb{Z}_n tem as seguintes propriedades:*

- (1) $\bar{a} \odot (\bar{b} \odot \bar{c}) = (\bar{a} \odot \bar{b}) \odot \bar{c}, \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ (\odot é associativa);
- (2) $\bar{a} \odot \bar{b} = \bar{a} \odot \bar{b}, \forall \bar{a}, \bar{b} \in \mathbb{Z}_n$ (\odot é comutativa);
- (3) $\bar{a} \odot \bar{1}, \forall \bar{a} \in \mathbb{Z}_n$ (\odot tem elemento neutro);
- (4) Dado $\bar{a} \in \mathbb{Z}_n$, existe $\bar{b} \in \mathbb{Z}_n$ com $\bar{a} \odot \bar{b} = \bar{1}$, se, e somente se, $\text{mdc}(a, n) = 1$ (existência do inverso sob \odot)

Prova. (1) $\bar{a} \odot (\bar{b} \odot \bar{c}) = \bar{a} \odot \overline{b \odot c} = \overline{a \odot b \odot c} = \overline{(a \odot b) \odot c} = (\bar{a} \odot \bar{b}) \odot \bar{c}$.

$$(2) \bar{a} \odot \bar{b} = \overline{a \odot b} = \overline{b \odot a} = \bar{b} \odot \bar{a}.$$

$$(3) \bar{a} \odot \bar{1} = \overline{a \odot 1} = \bar{a}.$$

- (4) Para $\bar{a} \in \mathbb{Z}_n$, suponhamos que existe $\bar{b} \in \mathbb{Z}_n$ tal que $\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \bar{1}$. Logo, $a \cdot b \equiv 1 \pmod{n}$ ou seja,

$$a \cdot b + k \cdot n = 1, \text{ com } k \in \mathbb{Z}.$$

Portanto, pela Proposição 1.9, concluímos que o $\text{mdc}(a, n) = 1$. Reciprocamente, seja $a \in \mathbb{Z}$, com $\text{mdc}(a, n) = 1$. Pela Proposição 1.9, existem $x, y \in \mathbb{Z}$ tais que $a \cdot x + n \cdot y = 1$. Assim,

$$\overline{a \cdot x + n \cdot y} = \bar{1} \Leftrightarrow \overline{a \cdot x} + \overline{n \cdot y} = \bar{1} \Leftrightarrow \bar{a} \cdot \bar{x} + \bar{n} \cdot \bar{y} = \bar{1} \Leftrightarrow \bar{a} \cdot \bar{x} + \bar{n} \cdot \bar{y} = \bar{1}$$

ou seja, $\bar{a} \cdot \bar{x} = \bar{1}$, de modo que \bar{a} tem inverso multiplicativo.

1.3 Tópicos em Teoria dos Grupos

Como pretendemos estudar subconjuntos das matrizes singulares 2×2 e dos \mathbb{Z}_n não invertíveis formam grupos sob a operação de multiplicação, nesta seção será apresentado as definições de operações binárias, grupos, subgrupos, grupos cíclicos e homomorfismo de grupos além de alguns exemplos e proposições que serão importantes para o desenvolvimento do trabalho.

Definição 1.20. (*Operação binária*) Seja A um conjunto não vazio. Uma função $\star : A \times A \rightarrow A$ chama-se operação binária sobre A .

Definição 1.21. Seja G um conjunto não vazio munido com a operação binária \star . Dizemos que G é um grupo se satisfazer as seguintes condições:

i) \star é associativa, ou seja,

$$a \star (b \star c) = (a \star b) \star c \text{ para todo } a, b, c \in G;$$

ii) Existe um elemento neutro para \star , ou seja,

$$\exists e \in G \text{ tal que } a \star e = e \star a = a, \text{ para todo } a \in G;$$

iii) Todo elemento em G possui inverso em relação a \star , ou seja,

$$\text{para todo } a \in G, \exists a' \in G \text{ tal que } a \star a' = e.$$

O elemento a' inverso de a será denotado por a^{-1} .

Indicaremos um grupo G munido da operação \star pela notação: (G, \star) , ou, denota-se apenas por G .

Exemplo 1.13. O conjunto \mathbb{Z}_n dotado da operação de multiplicação não é um grupo, pois $\bar{0}$ não possui inverso. Embora $\bar{1}$ é neutro, mas

$$\text{não existe } \bar{a} \in \mathbb{Z}_n \text{ tal que } \bar{0} \cdot \bar{a} = \bar{1}$$

Exemplo 1.14. Tem-se o conjunto \mathbb{R}^* munido com a operação de multiplicação é um grupo. De fato, o produto em \mathbb{R} é associativo e sabemos que o número 1 é o neutro multiplicativo dos reais e dado $a \in \mathbb{R}^*$ daí $\frac{1}{a}$ é o inverso de a e $\frac{1}{a} \in \mathbb{R}^*$. Logo, (\mathbb{R}^*, \cdot) é grupo.

Exemplo 1.15. O conjunto $GL_2(\mathbb{R}) = \{X \in M_2(\mathbb{R}) : \det X \neq 0\} \subset G$ é um grupo multiplicativo:

De fato,

(i) $X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z, \forall X, Y, Z \in GL_2(\mathbb{R})$.

(ii) Além disso I_2 a matriz identidade de ordem 2, é o elemento neutro do produto, pois,

$$X \cdot I_2 = I_2 \cdot X, \forall X \in GL_2(\mathbb{R}).$$

(iii) Dados $X, Y \in GL_2(\mathbb{R})$ tal que $X \cdot Y = Y \cdot X = I_2$, isso só é possível pelo fato de $\det X \cdot \det Y \neq 0$.

Assim, $GL_2(\mathbb{R})$ é fechado sob o produto, logo é um grupo.

Exemplo 1.16. Em geral, dado $n \leq 2$, o conjunto Z_n com a multiplicação definida na proposição 1.13 não é um grupo, pois $\bar{0}$ não possui inverso. Além disso, pelo item (4) do teorema 1.10, dado $\bar{a} \in Z_n$, existe $\bar{b} \in Z_n$ tal que $\bar{a} \cdot \bar{b} = \bar{1}$ se, somente se, $\text{mdc}(a, n) = 1$. No entanto, pelo mesmo teorema, considerando o fato de a multiplicação ser associativa, segue que o subconjunto próprio $U(Z_n)$ de Z_n

$$U(Z_n) = \{\bar{a} \in Z_n : \text{mdc}(a, n) = 1\},$$

é um grupo multiplicativo. Quando n for primo, então é claro que

$$U(Z_n) = \{\bar{1}, \bar{2}, \dots, \overline{n-1}\}.$$

Para $n = 4$, por exemplo, $U(Z_4) = \{\bar{1}, \bar{3}\}$; e com $n = 7$, $U(Z_7) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

1.3.1 Subgrupos

Definição 1.22. Seja G um grupo. Um subconjunto não vazio H de G é um subgrupo de G quando, munido com a operação de G , também é um grupo. Para indicar que H é um subgrupo de G , usaremos a seguinte notação: $H < G$.

Exemplo 1.17. Seja $G = Z_4$. Tem-se $H = \{\bar{0}, \bar{2}\}$ é um subgrupo de G . De fato, note que a soma é bem definida em H e como a soma em Z_n é associativa, então em H a soma é associativa, pois H é um subconjunto de Z_n para $n = 4$. Note também que $\bar{0} \in H$ e sabemos que $\bar{0}$ é o neutro de Z_n , ademais temos que todos os elementos de H possuem seus inversos em H , pois o inverso de $\bar{0}$ é o próprio e o inverso de $\bar{2}$ também é o próprio. Logo, H também é um grupo, portanto por definição $H < G$.

Exemplo 1.18. O conjunto $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) : \det A = 1\}$ é um subgrupo do grupo (GL_2, \cdot) . De fato, dados $A, B \in SL_2(\mathbb{R})$ tem-se $\det A = \det B = 1$. Por isso,

$$\det(A \cdot B) = \det A \cdot \det B = 1$$

isto é, $A \cdot B \in SL_2(\mathbb{R})$. Por outro lado,

$$\det A^{-1} = (\det A)^{-1} = 1 \Rightarrow A^{-1} \in SL_2(\mathbb{R}).$$

Logo, $SL_2(\mathbb{R}) < GL_2(\mathbb{R})$.

1.3.2 Grupos Cíclicos

Definição 1.23. Um grupo G é dito cíclico quando existir $a \in G$ de maneira que

$$G = \langle a \rangle$$

Exemplo 1.19. Para cada $n \in \mathbb{N}$, o grupo $(\mathbb{Z}_n, +)$ é cíclico. De fato, dado $\bar{a} \in \mathbb{Z}_n$,

$$\bar{a} = 1 + 1 + \dots + 1 = \bar{1} + \bar{1} + \dots + \bar{1} \text{ (} a \text{ vezes)},$$

ou seja, $\bar{a} = a\bar{1}$, de modo que $\bar{a} \in \langle \bar{1} \rangle$. Isso mostra que $\mathbb{Z}_n \subset \langle \bar{1} \rangle$, e como $\langle \bar{1} \rangle \subset \mathbb{Z}_n$, então $\langle \bar{1} \rangle = \mathbb{Z}_n$.

1.3.3 Homomorfismo de Grupos

Definição 1.24. Sejam (G_1, \star) e (G_2, \cdot) dois grupos. Uma função $f : G_1 \rightarrow G_2$ chama-se homomorfismo de G_1 em G_2 quando

$$f(a \star b) = f(a) \cdot f(b), \forall a, b \in G_1$$

Observação 1.7. Nas condições da definição anterior, se e_1 e e_2 neutros de G_1 e G_2 , respectivamente e $a \in G_1$, então

$$(i) f(e_1) = e_2$$

$$(ii) f(a^{-1}) = f(a)^{-1}.$$

Proposição 1.14. Seja $f : G_1 \rightarrow G_2$ um homomorfismo de grupos. Então, $Im(f) = \{f(a) : a \in G_1\}$ é subgrupo de G_2 , chamado de imagem de f .

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

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

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

Capítulo 2

Alguns Grupos Inesperados

No capítulo anterior, vimos no exemplo 1.15 que o conjunto $GL_2(\mathbb{R})$ é um grupo com a multiplicação, portanto, todos os elementos desse grupo são invertíveis. Também no exemplo 1.16 vimos que $\mathbb{Z}_n \setminus \{0\}$, com n primo é também um grupo. Nessa seção pretendemos estender esses conceitos, ou seja, procurar outros subconjuntos de GL_2 e de \mathbb{Z}_n que também são grupos com o produto, mas que são diferentes desses grupos usuais. Ressaltamos que esse Capítulo refere-se a uma abordagem mais didática do texto "Unexpected Groups", de autoria W. R. Brakes, encontrado na referência [3].

2.1 Grupos não invertíveis em \mathbb{Z}_n

Seja n natural com $n > 1$ e não primo e suponha que G é um subconjunto de \mathbb{Z}_n que forma um grupo sob a multiplicação. Suponha que G não contenha $\bar{0}$ e que todos os elementos sejam "não invertíveis", isto é, que tenham fatores em comum com n . Suponha também que o elemento identidade de G seja \bar{e} . Tem-se

$$\bar{e}^2 = \bar{e} \cdot \bar{e} = \bar{e},$$

isto é,

$$e^2 \equiv e \pmod{n},$$

logo,

$$e^2 - e = e(e - 1) \equiv 0 \pmod{n}.$$

Como e e $e - 1$ são números consecutivos, ambos maiores que 1 e menores que $n - 1$ e $e(e - 1) = kn$, para algum $k \in \mathbb{Z}$, segue que tal elemento e só pode ocorrer como correspondente a alguma fatoração não trivial de n , ou seja, considerando $n = ab$ existe

inteiros positivos λ e μ , tais que $e = \lambda a$ e $e - 1 = \mu b$. Como consequência,

$$\lambda a - \mu b = 1 \quad (2.1)$$

então pela Proposição 1.9 a e b são primos entre si (e assim devem ser λ e b , a e μ).

Agora, seja g um elemento de G , daí

$$\overline{ge} = \overline{g},$$

isto é,

$$ge \equiv g(\text{mod } n) \text{ ou } g(e - 1) \equiv 0(\text{mod } n),$$

daí

$$g\mu b \equiv 0(\text{mod } n),$$

logo, lembrando que $n = ab$,

$$ab|g\mu b$$

e portanto $a|g\mu$.

Assim, $g\mu$ é múltiplo de a . Como μ e a são primos entre si, tem-se g múltiplo de a .

Agora multiplicando por a a Equação 2.1, tem-se

$$a = a^2\lambda - \mu ba \Leftrightarrow a - a^2\lambda = -\mu ba \Leftrightarrow a \equiv \lambda a^2(\text{mod } n) \Leftrightarrow a \equiv \lambda a \cdot a(\text{mod } n) \Leftrightarrow a \equiv ea(\text{mod } n).$$

Assim, a é múltiplo de e logo, todos os elementos de G são múltiplos de e , pois g é múltiplo de a . Como $e = \lambda a$ e λ e b primos entre si pela Equação 2.1, tem-se $b\bar{e} = ba\lambda \equiv 0(\text{mod } n)$ daí, be é o menor múltiplo positivo de e congruente a 0 módulo n .

Como

$$(\overline{xe})(\overline{ye}) = (\overline{xy})\bar{e},$$

então, $xe \equiv ye(\text{mod } n)$ se, e somente se, $x \equiv y(\text{mod } b)$. De fato,

$$xe \equiv ye(\text{mod } n)$$

se, e somente se, existe $k \in \mathbb{Z}$, tal que,

$$xe - ye = kab$$

$$\Leftrightarrow x\lambda a - y\lambda a = kab$$

$$\Leftrightarrow x\lambda - y\lambda = kb,$$

como $\text{mdc}(\lambda, b) = 1$, logo, $\lambda|k$.

$$x - y = \left(\frac{k}{\lambda}\right)b$$

$$\Leftrightarrow x \equiv y(\text{mod } b).$$

Assim, a busca por grupos com identidade \bar{e} se reduz ao conjunto,

$$\{\bar{e}, \bar{2e}, \bar{3e}, \dots, \overline{(b-1)e}\}.$$

E esses conjuntos podem ser identificados como grupos multiplicativos com identidade $\bar{1}$ dentro do conjunto \mathbb{Z}_b .

Diante do exposto, vamos proceder para encontrar valores possíveis para e . Como já foi descrito para cada fatoração de n , $n = ab$ onde a e b são primos entre si, buscamos $e = \lambda a$ de tal forma que existe um μ satisfazendo

$$\lambda a - \mu b = 1.$$

Para a, b e λ nas condições acima, do algoritmo da divisão, existe λ_0 de tal forma que

$$\lambda = \lambda_0 + kb,$$

logo,

$$\lambda a = \lambda_0 a + kn,$$

portanto, $\lambda a \equiv \lambda_0 a \pmod{n}$. Assim, a escolha de tal \bar{e} (como elemento de \mathbb{Z}_n) é única (para a escolha de a e b). Dai, a quantidade desses possíveis \bar{e} coincide precisamente com o número de maneiras pelas quais n pode ser decomposto não trivialmente em um produto ordenado de dois fatores primos entre si.

Se $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$ é a fatoração primária de n , então o número de tais escolhas é $2^r - 2$. Agora, os critérios para decidir se um elemento de \mathbb{Z}_n está dentro de um grupo multiplicativo, é a determinação de seu inverso e que ele é único (se existir). A conclusão é que um inteiro m ($1 < m < n$) tal que \bar{m} está dentro do grupo se, somente se, o seu maior fator comum com n é d , onde n/d e d são primos entre si. Seja m escrito da forma xe e o inverso é unicamente dado e denotado por x^{-1} no grupo multiplicativo $U(\mathbb{Z}_b)$, o conjunto dos inteiros positivos menores que b e primos com b .

Exemplo 2.1. Considere $n = 14 = 2 \cdot 7$. O par ordenado (a, b) é $(2, 7)$ ou $(7, 2)$. As possibilidades para \bar{e} são $\bar{8}$ (pela equação 2.1 tem-se $1 = \lambda a - \mu b \Leftrightarrow 4 \times 2 - 1 \times 7 = 1$) ou $\bar{7}$. Se $\bar{e} = \bar{8}$, então $b = 7$ e, portanto,

$$G = \{\bar{e}, \bar{2e}, \bar{3e}, \bar{4e}, \bar{5e}, \overline{(7-1)e}\} \Leftrightarrow G = \{\bar{8}, \bar{2}, \bar{10}, \bar{4}, \bar{12}, \bar{6}\},$$

logo G é um grupo multiplicativo (isomorfo a $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ sob a multiplicação módulo 7) porque 7 é primo. Os subgrupos multiplicativos em \mathbb{Z}_7 com identidade 1 são $\{\bar{1}\}$, $\{\bar{1}, \bar{6}\}$, $\{\bar{1}, \bar{2}, \bar{4}\}$ e $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$, e assim os subgrupos em \mathbb{Z}_{14} com $\bar{8}$ como identidade são $\{\bar{8}\}$, $\{\bar{8}, \bar{6}\}$, $\{\bar{8}, \bar{2}, \bar{4}\}$ e $\{\bar{8}, \bar{2}, \bar{10}, \bar{4}, \bar{12}, \bar{6}\}$, com $\bar{e} = \bar{7}$ o único grupo é $\{\bar{7}\}$, pois com $\bar{e} = 7$ então $b = 2$.

$$G = \{\overline{(2-1)e}\} \Leftrightarrow G = \{\bar{e}\} \Leftrightarrow G = \{\bar{7}\}$$

Exemplo 2.2. Agora considere $n = 60$. Como $60 = 2^2 \cdot 3 \cdot 5$, então existem 6 opções para o par ordenado (a, b) :

$$(4, 15), (3, 20), (5, 12), (15, 4), (20, 3), (12, 5).$$

Em cada caso, os valores possíveis de $\bar{e}(\text{mod}60)$, são respectivamente

$$\overline{16}, \overline{21}, \overline{25}, \overline{45}, \overline{40}, \overline{36}.$$

Para $\bar{e} = \overline{16}$, os múltiplos não nulos de \bar{e} são:

$$\{\overline{16}, \overline{32}, \overline{48}, \overline{4}, \overline{20}, \overline{36}, \overline{52}, \overline{8}, \overline{24}, \overline{40}, \overline{56}, \overline{12}, \overline{28}, \overline{44}\}.$$

Para ver quais subconjuntos formam um grupo a atenção se concentra no conjunto \mathbb{Z}_{15} , tendo $\bar{1}$ como elemento identidade cujos subgrupos são $\{\bar{1}\}, \{\bar{1}, \bar{4}\}, \{\bar{1}, \bar{11}\}, \{\bar{1}, \bar{14}\}, \{\bar{1}, \bar{2}, \bar{4}, \bar{8}\}, \{\bar{1}, \bar{7}, \bar{4}, \bar{13}\}, \{\bar{1}, \bar{4}, \bar{11}, \bar{14}\}.$

Assim, os grupos multiplicativos em \mathbb{Z}_{60} com $\overline{16}$ como identidade são: $\{\overline{16}\}, \{\overline{16}, \overline{4}\}, \{\overline{16}, \overline{56}\}, \{\overline{16}, \overline{44}\}, \{\overline{16}, \overline{32}, \overline{4}, \overline{8}\}, \{\overline{16}, \overline{52}, \overline{4}, \overline{28}\}, \{\overline{16}, \overline{4}, \overline{56}, \overline{44}\}, \{\overline{16}, \overline{32}, \overline{4}, \overline{52}, \overline{8}, \overline{56}, \overline{28}, \overline{44}\}.$

O procedimento é semelhante para as demais escolhas para \bar{e} . Cada elemento será incluindo em um ou mais desses grupos.

2.2 Grupos de Matrizes singulares 2x2

Agora será apresentado os grupos de matrizes singulares 2×2 sob a multiplicação, onde será mostrado o porquê esse grupo G não é subgrupo de $GL_2(\mathbb{R})$, uma vez que matriz nula não pertence a esse grupo, também será mostrado as possíveis formas dos elementos neutros desse grupo, e ainda que qualquer matriz 2×2 singular com $A^2 \neq 0$ pertence a um grupo do tipo que iremos discutir no Lema 2.9.

Teorema 2.1. *Se G é um grupo de matrizes singulares 2×2 que não incluem a matriz nula então, G é um subgrupo $\langle E \rangle = \{xE : x \in \mathbb{R}, x \neq 0\}$, onde E possui uma das formas*

$$\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix} \text{ ou } \frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix}$$

Supondo que G é um conjunto de matrizes 2×2 que formam um grupo sob a operação de multiplicação. Denota-se o elemento identidade de G por E , e para qualquer elemento A de G denota-se seu inverso por A^{-1} .

Lema 2.1. *Se G contém uma matriz não singular então G é um subgrupo de $GL_2(\mathbb{R})$.*

Prova. Seja A em G não singular, então $A \in GL_2(\mathbb{R})$ pois, o E que satisfaz $AE = A$ e

$A \cdot A^{-1} = E$ é único daí, $E = I_n$. Agora, para qualquer B em G , tem-se, $B \cdot B^{-1} = I_n = B^{-1} \cdot B$, o que mostra que B não singular com B^{-1} seu inverso. Então G é sub conjunto de $GL_2(\mathbb{R})$, portanto um subgrupo de $GL_2(\mathbb{R})$.

Como estamos procurando grupos que não sejam subgrupos de $GL_2(\mathbb{R})$, daqui em diante será assumido que todos os elementos de G são matrizes singulares.

Lema 2.2. *Se G contém a matriz nula, então G não contém outros elementos.*

Prova. Como $0^2 = 0 \cdot 0 = 0$, se G contém 0 , então 0 é o elemento identidade, mas para qualquer elemento A em G , $0A = A$ enquanto também $A0 = 0$, assim $A = 0$, daí o único elemento de G é a matriz nula.

Como esse também não é um caso interessante é assumido daqui em diante que G não contém a matriz nula. Segundo a seção Retas em \mathbb{R}^2 o elemento identidade E não sendo nem nulo nem não singular, pode ser identificado como uma transformação linear $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, que tem o núcleo e imagem representados por retas que passam pela origem, uma vez que ambos são subespaços de dimensão 1 de \mathbb{R}^2 que serão designadas por L_1 e L_2 respectivamente.

Lema 2.3. *$E|_{L_2} = \text{identidade}$, isto é, $Ew = w$ para todo $w \in L_2$*

Prova. Como $E^2 = E \cdot E = E$, portanto $E(Ev) = E(v)$ para qualquer v em \mathbb{R}^2 . Daí, pela definição 1.13(b) qualquer $w \in L_2$ pode ser escrito como $w = E(v)$, para algum $v \in \mathbb{R}^2$ portanto, $w = E(v) = E(Ev) = E(w)$.

Suponha agora que A é qualquer elemento de G . Por suposições já feitas A não é nem singular nem matriz nula.

Lema 2.4. *O núcleo de A é L_1 . A imagem de A é L_2 .*

Prova. De $AE = A$, para qualquer $v_1 \in L_1$ da Definição 1.13 (a) obtém-se $Av_1 = AE(v_1) = A(0) = 0$, daí tem-se $Av_1 = 0$. Logo, o núcleo de A tem L_1 como um subconjunto. Como L_1 e o núcleo de A são retas que passam pela origem, segue que $\text{Ker}(A) = L_1$. Agora, $EA = A$ logo, para qualquer $v \in \mathbb{R}^2$, $Av = E(A(v))$ que do lema anterior garante que Av pertence a $L_2 = \text{Im}(E)$. Portanto, a imagem de A está contido em L_2 . Como a imagem de A e L_2 são retas que passam pela origem, tem-se $\text{Im}(A) = L_2$.

Daí, segue que $A|_{L_2}$ é uma transformação linear não singular em um espaço unidimensional e assim $A|_{L_2}$ é simplesmente multiplicação por algum escalar t , ou seja, $Av = tv, \forall v \in L_2$.

Lema 2.5. *$A = tE$.*

Prova. Seja $v \in \mathbb{R}^2$, escrevemos v da forma $v_1 + v_2$ onde $v_1 \in L_1$ e $v_2 \in L_2$. Assim,

$$E(v) = E(v_1 + v_2) = E(v_1) + E(v_2)$$

como $v_1 \in L_1$ então do Lema anterior, $E(v_1) = 0$ e mais, sendo $v_2 \in L_2$ então $E(v_2) = v_2$, daí

$$E(v_1) + E(v_2) = 0 + v_2 = v_2.$$

Ainda,

$$A(v) = A(v_1 + v_2) = A(v_1) + A(v_2) = 0 + A(E(v_2)) = tv_2.$$

Então, $Av = tEv$, para qualquer $v \in \mathbb{R}^2$.

Recordemos do Exemplo 1.14 que \mathbb{R}^* é grupo dos números reais diferentes de zero sob a multiplicação.

Lema 2.6. *Para algum subgrupo H de \mathbb{R}^**

$$G = \{xE : x \in H\}$$

Prova. Pelo Lema anterior os elementos A de G são múltiplos de E .

Seja $x, y \in H$ a função.

$$\begin{aligned} f : G &\rightarrow \mathbb{R}^* \\ xE &\mapsto x \end{aligned}$$

é um homomorfismo, pois

$$xEyE = xyE^2 = xyE$$

logo,

$$f(xEyE) = f(xyE) = xy = f(xE)f(yE)$$

da Proposição 1.14 tomando H como imagem deste homomorfismo tem-se o resultado.

Se E é qualquer matriz 2×2 satisfazendo $E^2 = E$ fica claro que o conjunto de todos os múltiplos não nulos de E formam um grupo sob a multiplicação de matrizes, pois, dados $a, b \in A$ em que A é esse conjunto dos múltiplos de E , então $a = xE$ e $b = yE$.

$$(xE) \cdot (yE) = (xy)E \in A$$

$$(1E) \cdot (yE) = yE \text{ onde } 1E \text{ é elemento neutro de } A.$$

$$\left(\frac{1}{x}\right)E \cdot (xE) = \left(\frac{1}{x} \cdot x\right)E = 1E = \left(x \cdot \frac{1}{x}\right)E = (xE) \cdot \left(\frac{1}{x}\right)E. \text{ Daí } \left(\frac{1}{x}\right)E \text{ é elemento inverso de } xE.$$

denotamos esse grupo de $\langle E \rangle$, então, $\langle E \rangle = \{xE : x \in \mathbb{R}^*\}$. Do lema 2.6 tem-se que o grupo G do tipo que estamos buscando é um subgrupo de $\langle E \rangle$ para algum E .

Para completar a classificação desses grupos em termos de subgrupos de \mathbb{R}^* resta

identificar as possibilidades para E .

Lema 2.7. *Temos $E^2 = E$ se, e somente se,*

$$E = \frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix} \text{ ou } E = \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix} \text{ ou } E = \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix},$$

com para a, b distintos, e $a, b, c \in \mathbb{R}$.

Prova. (\Leftarrow) Suponha

$$E^2 = \left[\frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix} \right]^2 = \left[\frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix} \right] = E,$$

pois,

$$\begin{aligned} E^2 &= \left[\frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix} \right]^2 = \left[\frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix} \right] \cdot \left[\frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix} \right] \\ &= \frac{1}{(a-b)^2} \begin{pmatrix} a^2 - ab & -a + b \\ a^2b - ab^2 & -ab - b^2 \end{pmatrix} = \frac{1}{(a-b)^2} \begin{pmatrix} a(a-b) & -1(a-b) \\ ab(a-b) & -b(a-b) \end{pmatrix} \\ &= \frac{1}{(a-b)} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix} = E. \end{aligned}$$

Agora para

$$E = \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix},$$

tem-se

$$\begin{aligned} E^2 &= \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 0 \cdot c & 1 \cdot 0 + 0 \cdot 0 \\ c \cdot 1 + 0 \cdot c & c \cdot 0 + 0 \cdot 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix} = E. \end{aligned}$$

Já na última fórmula

$$E = \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix},$$

tem-se

$$\begin{aligned} E^2 &= \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} 0 \cdot 0 + 0 \cdot c & 0 \cdot 0 + 0 \cdot 1 \\ c \cdot 0 + 1 \cdot c & c \cdot 0 + 1 \cdot 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix} = E. \end{aligned}$$

(\Rightarrow) Sejam L_1 e L_2 o núcleo e a imagem de E . Como já mencionado L_1 e L_2 são retas que passam pela origem, digamos $y = ax$ e $y = bx$, respectivamente. Se $a, b \neq 0$,

$$E = \frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix}$$

e $v = (x, ax) \in L_1$, então

$$E(v) = \frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix} \cdot \begin{pmatrix} x \\ ax \end{pmatrix} = \frac{1}{a-b} \begin{pmatrix} ax - ax \\ abx - abx \end{pmatrix} = \frac{1}{a-b} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

dai segue que leva L_1 para $\{0\}$. Agora, se $u = (x, bx) \in L_2$, então

$$E(u) = \frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix} \cdot \begin{pmatrix} x \\ bx \end{pmatrix} = \frac{1}{a-b} \begin{pmatrix} ax - bx \\ abx - b^2x \end{pmatrix} = \frac{1}{a-b} \begin{pmatrix} x \\ bx \end{pmatrix} = \begin{pmatrix} x \\ bx \end{pmatrix},$$

assim L_2 é a identidade. No caso de L_1 ser a reta $x = 0$, L_2 ser a reta $y = cx$, $c \neq 0$,

$v = (0, y)$, $u = (x, cx)$ e

$$E = \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix},$$

tem-se

$$\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ y \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + 0 \cdot y \\ c \cdot 0 + 0 \cdot y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

ou seja, leva L_1 para $\{0\}$. Agora,

$$\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ cx \end{pmatrix} = \begin{pmatrix} 1 \cdot x + 0 \cdot cx \\ c \cdot x + 0 \cdot cx \end{pmatrix} = \begin{pmatrix} x \\ cx \end{pmatrix},$$

que é a identidade L_2 . Para o último caso, isto é, L_1 é a reta $x = -cx$, $c \neq 0$ e L_2 é a reta $x = 0$, $v = (x, -cx)$, $u = (x, 0)$ e

$$E = \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix},$$

tem-se

$$\begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ -cx \end{pmatrix} = \begin{pmatrix} 0 \cdot x + 0 \cdot (-cx) \\ c \cdot x + 1 \cdot (-cx) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

ou seja, leva L_1 em $\{0\}$

$$\begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ y \end{pmatrix} = \begin{pmatrix} 0 \cdot 0 + 0 \cdot y \\ c \cdot 0 + 1 \cdot y \end{pmatrix} = \begin{pmatrix} 0 \\ y \end{pmatrix},$$

que é a identidade em L_2 . Agora, se

$$P = \begin{pmatrix} 1 & 1 \\ b & a \end{pmatrix}, \text{ daí } P^{-1} = \frac{1}{a-b} \begin{pmatrix} a & -1 \\ -b & 1 \end{pmatrix},$$

logo,

$$\begin{aligned} P \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P^{-1} &= \left[\begin{pmatrix} 1 & 1 \\ b & a \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \frac{1}{a-b} \begin{pmatrix} a & -1 \\ -b & 1 \end{pmatrix} \right] = \\ &= \frac{1}{a-b} \begin{pmatrix} a & -1 \\ ab & -b \end{pmatrix}. \end{aligned}$$

Assim,

$$E = P \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P^{-1} \text{ simplifica para a primeira fórmula.}$$

Agora para as demais formulas, tem-se

$$P = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \text{ e } P^{-1} = \begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix},$$

onde,

$$P \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P^{-1} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -c & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

e, por fim, para a última fórmula de E , tem-se

$$P = \begin{pmatrix} 0 & -1 \\ 1 & c \end{pmatrix} \text{ e } P^{-1} = \begin{pmatrix} c & 1 \\ -1 & 0 \end{pmatrix},$$

onde,

$$P \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & c \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix}.$$

O que prova o Teorema 2.1. Agora,

Teorema 2.2. a) *Qualquer matriz 2×2 singular com $A^2 \neq 0$ pertence a um grupo do tipo que iremos discutir nos lemas a seguir e tem inversa dada pela fórmula do Lema 2.9.*

b) *A matriz nula tem como inversa ela mesma.*

c) *As matrizes excepcionais A que satisfazem $A \neq 0$ e $A^2 = 0$ são precisamente matrizes singulares mas não nulas que possuem traço zero, e assim a fórmula do Lema 2.9 é inválida, estes não pertencem a nenhum desses grupos.*

Lema 2.8. *Se $A = 0$, ele está exatamente no grupo $\{0\}$, e assim tem um inverso, ou seja, ela mesma.*

Prova. Se $A = 0$, então do Lema 2.2 o grupo tem apenas a matriz nula, logo sua inversa é ela mesma.

Lema 2.9. *Se $L_1 \neq L_2$ então A tem uma inversa única, $A^{-1} = \frac{1}{t^2}A$, onde t é o traço da matriz A , $t = \text{Tr}(A)$.*

Prova. Como E é a matriz que restringe a transformação identidade em L_2 e a matriz nula em L_1 pelo lema 6 sabe-se que E será o elemento identidade em qualquer grupo contendo A . Assim, existe um número real t , não nulo, satisfazendo, $A = tE$ como $A \cdot A^{-1} = E$ temos $AA^{-1} = \frac{1}{t}A \Leftrightarrow A^{-1}AA^{-1} = A^{-1}\frac{1}{t}A$ daí, $A^{-1} = \frac{1}{t}E = \frac{1}{t^2}A$, onde t é um fator

escalar da transformação de $A|L_2$. Pela possível forma de E no Lema 2.7, tem-se $A = tE$

$$A = t \left[P \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P^{-1} \right] \Leftrightarrow A = \left[Pt \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P^{-1} \right] \Leftrightarrow A = \left[P \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix} P^{-1} \right].$$

Logo,

$$\text{Tr}(A) = \text{Tr} \left[P \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix} P^{-1} \right] = \text{Tr}(P) \text{Tr} \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix} \text{Tr}(P^{-1}) = t.$$

Lema 2.10. *Se $L_1 = L_2$, A não está em nenhum grupo de matrizes singulares.*

Prova. Para essa matriz A e qualquer vetor $v \in \mathbb{R}^2$, Av está em L_2 então também está em L_1 , logo $Av = 0$. Portanto, A é a matriz nula, daí qualquer grupo multiplicativo contendo A também conteria a matriz nula mas, pelo Lema 2.2 isto é impossível.

Exemplo 2.3. Seja,

$$A(\mathbb{R}^*) = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix}, a \in \mathbb{R}^* \right\},$$

considere

$$E = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix},$$

matriz singular de ordem 2×2 , observe que

$$E = \frac{1}{-1-1} \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix} = \frac{1}{-2} \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$$

que é um dos elementos no Lema 2.7, com $a = -1$ e $b = 1$. Nesse caso,

$$\langle E \rangle = \{xE : x \in \mathbb{R}^*\} = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \in \mathbb{R}^* \right\}.$$

é um grupo com a multiplicação, cujo elemento neutro é E . Ainda, o núcleo de E ; pela prova do Lema 2.7 é a reta $y = ax$ e a imagem é a reta $y = bx$, donde o núcleo de E é a reta, $y = -x$ e a imagem é a reta $y = x$.

Considerações Finais

O estudo de alguns grupos inesperados nos propiciou um rico itinerário sobre a Teoria dos Grupos, onde englobou vários conceitos de Álgebra Linear e Teoria dos Números. Vimos que nesse trabalho algo incomum do que vemos no curso de Estruturas Algébricas, Alguns Grupos Inesperados, onde é possível encontrar subconjuntos de matrizes 2×2 que formam um grupo sob a multiplicação, e também da classe de restos \mathbb{Z}_n , não invertíveis que também formam grupo sob a multiplicação.

Referências Bibliográficas

- [1] LOURÊDO, ALDO TRAJANO; OLIVEIRA, ALEXANDO MARINHO. **Um primeiro curso de Álgebra Linear**. 21.ed. Campina Grande: EDUEPB, 2015;
- [2] FINKBEINER, DANIEL T. **Introduction to Matrices and Linear Transformations**. W. H. FREEMAN AND COMPANY.
- [3] BRAKES, W.R. **Unexpected Groups**. the Mathematical Association. Disponível em: < <http://www.jstor.org/stable/3618078> >
- [4] STEINBRUCH, ALFREDO; WINTERLE, PAULO. **Álgebra Linear**. São Paulo: PEARSON EDUCATION DO BRASIL, 1997;
- [5] COELHO, FLÁVIO U.; LOURENÇO, MARY L. **Um Curso de Álgebra Linear**. São Paulo: EDUSP, 2007.
- [6] VIEIRA, VANDEBERG LOPES. **Álgebra abstrata para licenciatura**. Campina Grande: EDUEPB, 2013;
- [7] VIEIRA, VANDEBERG LOPES. **Um curso Básico em Teoria dos Números**. Campina Grande: EDUEPB, 2015;
- [8] HEFEZ, ABRAMO; FERNANDES, CECÍLIA DE SOUZA. **Introdução à Álgebra Linear**. SBM, 2016.