UNIVERSIDADE FEDERAL DO ACRE

CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

CORPOS FINITOS:

Processo para obtenção de corpos de ordem p^2 com elementos matriciais

por

WILLIAM MAIA CAVALCANTE

2024

Rio Branco - AC

UNIVERSIDADE FEDERAL DO ACRE

CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL PROFMAT

CORPOS FINITOS:

PROCESSO PARA OBTENÇÃO DE CORPOS DE ORDEM p^2 COM ELEMENTOS MATRICIAIS

por

William Maia Cavalcante

sob a orientação do

Prof. Dr. Josean da Silva Alves

Co- orientação do

Prof. Dr. Sergio Brazil Jr.

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT/CCET/UFAC,como requisito parcial para a obtenção do título de Mestre.

Agosto / 2024

Rio Branco - AC

Ficha catalográfica elaborada pela Biblioteca Central da UFAC

C377c Cavalcante, William Maia, 1997 -
Corpos finitos: processo para obtenção de corpos de ordem p2 com elementos matriciais / William Maia Cavalcante; orientador: Prof. Dr. Josean da Silva Alves; coorientador Prof. Dr. Sérgio Brasil Jr. – 2024.
65 f. ; 30 cm.

Dissertação apresentada ao Corpo Docente de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/CCET/UFAC, como requisito parcial para a obtenção do título de Mestre.

1. Corpos finitos. 2. Anel de Polinômios. 3. Elemento primitivo. 4. Extensão algébrica. 5. Matriz simétrica. I. Alves, Josean da Silva (Orientador). II. Brasil Jr., Sérgio (Coorientador). III. Título.

CDD: 512.5

Marcelino G. M. Monteiro Bibliotecário CRB 11ª / 258

UNIVERSIDADE FEDERAL DO ACRE
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU PROFISSIONAL EM MATEMÁTICA

FOLHA DE APROVAÇÃO

Titulo da dissertação: Corpos Finitos: processo para obtenção de corpo de ordem p^2 com elementos matriciais.

Autor: William Maia Cavalcante

Orientador: Prof. Dr. Josean da Silva Alves

Dissertação aprovada como parte das exigências para obtenção do título de Mestre em Matemática, pelo Programa de Mestrado em Matemática em Rede Nacional (PPGPROFMAT).

DATA DA APROVAÇÃO:13 de agosto de 2024.

BANCA EXAMINADORA:

Assinado Eletronicamente
Prof. Dr. Josean da Silva Alves
Orientador
Universidade Federal do Acre - UFAC

Assinado Eletronicamente
Prof. Dr. Cleber Pereira
Membro Interno
Universidade Federal do Acre - UFAC

Assinado Eletronicamente
Profa. Dra. Sara Raissa Silva Rodrigues
Membra Externa
Universidade do Estado do Pará - UEPA

Documento assinado eletronicamente por **Sara Raissa Silva Rodrigues**, **Usuário Externo**, em 16/08/2024, às 10:46, conforme horário de Rio Branco - AC, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Josean da Silva Alves**, **Professor do Magisterio Superior**, em 19/08/2024, às 08:03, conforme horário de Rio Branco - AC, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Cleber Pereira**, **Professor do Magisterio Superior**, em 20/08/2024, às 21:45, conforme horário de Rio Branco - AC, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade do documento pode ser conferida no site https://sei.ufac.br/sei/valida_documento ou click no link Verificar Autenticidade informando o código verificador **1347594** e o código CRC **4F6B35E0**.

Referência: Processo nº 23107.019828/2024-24 SEI nº 1347594

Agradecimentos

À minha querida mãe, Maria Carmelita M. Cavalcante, que sempre me direcionou ao caminho dos estudos e nunca me deixou desistir.

Ao meu pai, Floriano F. Cavalcante, que sempre me apoiou nas minhas decisões.

À minha irmã, Wilanice Maia.

À minha companheira, Mikaely S. Santos, por ter me ajudado nos momentos difíceis.

Ao professor Dr. Josean da Silva, meu orientador, por me orientar com paciencia durante todo o trabalho.

Ao professor Dr. Sergio Brazil, por todo apoio e auxilio durante o trabalho.

Ao professor Dr. José Ivan da Silva Ramos, por todo o apoio durante o curso.

Aos professores do PROFMAT, que contribuiram para o meu crescimento profissional e acadêmico.

Aos meus amigos, Douglas Wilson e Tharles Araujo, por me ajudarem nessa jornada.

Ao Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) e a Universidade Federal do Acre (UFAC).

À minha mãe Maria C. M. Cavalcante e ao meu Pai Floriano F. Cavalcante dedico!

Resumo

O presente trabalho trata do estudo da estrutura algébrica de corpos. O objetivo foi obter um processo para determinar os elementos de corpos finitos de ordem potência de primo, de forma diferente do habitual, além disso, baseou-se esta dissertação em pesquisas bibliográficas de textos acadêmicos e artigos a respeito do tema. Durante esse trabalho são apresentados os resultados principais da teoria de matrizes, grupos, anéis e corpos, estabelecendo os critério necessários para o estudo de extensão de corpos que fornece os princípios para construir tais corpos de forma que seus elementos sejam matrizes quadradas.

Palavras-chaves: Corpos finitos; Anel de Polinômios; Elemento primitivo; Extensão algébrica; Matriz simétrica.

Abstract

The present work deals with the study of the algebraic structure of fields. The objective was to obtain a process to determine the elements of finite fields of order, power of prime in a different way from the usual, in addition, this dissertation was based on bibliographical research of academic texts and articles on the subject. During this work, the main results of the theory of matrices, groups, rings and fields are presented, establishing the necessary directions for the study of the extension of fields that provides the principles for constructing such fields so that their elements are square matrices.

Keywords: Finite fields; Ring of Polynomials; Primitive element; Algebraic extension; Symmetrical matrix.

“A Matemática é a honra do espírito humano.”
(Gottfried Leibniz)

Sumário

INTRODUÇÃO

Esse trabalho consiste no estudo, apresentação e construção de corpos finitos matriciais sobre corpos de característica p, onde p é um primo. A primeira menção a estrutura algébrica corpo foi dada pelo alemão Richard Dedekind (1831 – 1916) em 1879, Richard Dedekind foi o primeiro a dar uma definição explícita de corpo numérico como sendo uma coleção de números que formam um grupo abeliano que é comutativo em relação à adição e multiplicação, no qual a multiplicação é distributiva em relação à adição. Este conceito, foi fundamental para o desenvolvimento da Álgebra.

Os corpos finitos são objetos matemáticos muito importantes, pois têm aplicações em diversas áreas, como teoria de códigos, criptografia, geometria algébrica, teoria dos números e combinatória. Ao longo da vida como estudante começando no ensino médio não me recordo do fato de ser mencionado pelos professores que o conjunto dos números racionais, reais e complexos constituíam uma estrutura de corpos. No início da graduação, em Matemática, tive o primeiro contato com a definição de corpos onde os exemplos apresentados eram exatamente os racionais, reais e complexo, todos corpos infinitos. Prosseguindo com a graduação, em um curso de tópicos de álgebra me foi apresentado o conjunto $\mathbb{Z}_p$, um exemplo de corpo finito com p elementos, quando me deparei com essas estruturas fiquei me perguntando como seria outros tipos de corpos finitos, além de saber qual a forma desses elementos, visto que nas disciplinas estudadas na graduação não existia um aprofundamento no assunto de criação desses corpos, mais após ingressar no Mestrado Profissional em Matemática e estudar os conceitos de aritmética novamente, vi uma oportunidade de me aprofundar um pouco mais nesse assunto, ao escolher meu orientador e após uma conversa começamos a indagar sobre as seguintes questões: Por que a ordem de um corpo finito tem que ser sempre uma potência de primo? Como construir um corpo finito de uma dada ordem? Ao construir um corpo finito de ordem potência de primo ele será o único com aquela ordem? É possível construir um corpo cujo os elementos são matrizes? Diante disso, concordamos que um processo para obter corpos finitos em uma estrutura algébrica, seria ótimo para os docentes do magistério superior usarem para criar exemplos de corpos finitos com p^n elementos.

No capítulo 1, abordaremos uma revisão bibliográfica sobre alguns componentes e operações entre matrizes quadradas, salvo que o assunto é de extrema importância para o desenvolvimento do trabalho, nessa revisão veremos algumas definições e teoremas envolvendo matrizes, onde serão abordados, produto e soma de matrizes, determinantes e matrizes simétricas. Também faremos uma breve revisão sobre congruência módulo n, grupos, anéis e anéis de polinômios, onde veremos um pouco de suas propriedades e principais teoremas.

No capítulo 2, será feito uma coleção de teoremas e proposições sobre teoria de corpos. Esses resultados serão a base para construção do trabalho e para atender os objetivos, nesse capítulo, abordaremos assuntos sobre a característica de um corpo, ordem de um corpo, corpo finito, corpo de decomposição, visto que esses resultados serão cruciais para o entendimento deste trabalho e para sua conclusão.

O capítulo 3, será o ápice do nosso trabalho, onde será construído os corpos finitos de ordem p^2 menores que 121. Nesse capítulo, vamos apresentar de forma matricial os elementos dos corpos de ordem 4, 9, 25 e 49. Apresentaremos, também, as ordens dos elementos e seus geradores. Também serão exibidos alguns corpos de ordem p^3.

GENERALIDADES

Como neste trabalho veremos alguns exemplos de corpos matricial, vamos verificar a finitude e como são gerados. De início, devemos entender o que é necessário para ser um corpo.

Definição: Um corpo é um conjunto $\mathbb{K}$ munido com duas operações, adição e multiplicação, que satisfaz as seguintes propriedades:

- Para todo $\alpha, \beta, \delta \in \mathbb{K}$, $\alpha + (\beta + \delta) = (\alpha + \beta) + \delta$, (Associatividade).
- Para todo $\alpha \in \mathbb{K}$, $\exists!\,(-\alpha) \in \mathbb{K}$, $(-\alpha) + \alpha = \alpha + (-\alpha) = 0$. (existência do elemento simétrico da adição).
- Para todo $\alpha \in \mathbb{K}$, $\exists!\, 0 \in \mathbb{K}; 0+\alpha = \alpha + 0 = \alpha$. (existência do elemento neutro da adição).
- Para todo $\alpha, \beta \in \mathbb{K}$, $\alpha + \beta = \beta + \alpha$. (Comutatividade)
- Para todo $\alpha, \beta, \delta \in \mathbb{K}$, $\alpha.(\beta.\delta) = (\alpha.\beta).\delta$. (Associatividade).

- Para todo $\alpha \in \mathbb{K}$, $\exists! 1 \in \mathbb{K}; 1.\alpha = \alpha.1 = \alpha$. (Elemento neutro da multiplicação).
- Para todo $\alpha, \beta \in \mathbb{K}$, $\alpha.\beta = \beta.\alpha$; (comutatividade)
- Para todo $\alpha \neq 0$, $\exists!\ \alpha^{-1}$; $\alpha^{-1}.\alpha = \alpha.\alpha^{-1} = 1$ (Existência do elemento inverso com relação a multiplicação).
- Para todo $\alpha, \beta, \delta \in \mathbb{K}$, $\alpha.(\beta + \delta) = (\alpha.\beta) + (\alpha\delta)$ (Distributividade).

Neste trabalho, definiremos um **Corpo finito** $\mathbb{K}$, como sendo o corpo que possui um número finito de elementos. Como já foi estudado em teoria de grupos, sabemos que todo corpo finito é **cíclico**, com relação ao grupo multiplicativo de $\mathbb{K}$, ou seja, o corpo finito $\mathbb{K}$ é gerado por um único elemento. Um exemplo de corpo finito, como já foi falado, são os $\mathbb{Z}_p$. Para mais detalhes consultar o livro $[4]$.

O $\mathbb{Z}_p$ é o conjunto dos inteiros módulo p, onde p é um número primo. Eles formam um corpo finito, ou seja, um conjunto no qual podemos realizar as operações de soma, subtração, multiplicação e divisão por não nulo, respeitando as propriedades usuais dessas operações. O $\mathbb{Z}_p$, denotaremos por $\mathbb{F}_p$, possui p elementos, ou seja, $\mathbb{F}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Por exemplo, $\mathbb{Z}_2$ ou $\mathbb{F}_2$ é o corpo finito formado pelos elementos $\overline{0}$ e $\overline{1}$.

CAPÍTULO 1- CONCEITOS BÁSICOS

1.1 CONGRUÊNCIA

Os resultados sobre congruência foram de extrema importância para o desenvolvimento da teoria dos números, nesta secção destacaremos alguns desses resultados que foram introduzidos por Gauss (1777-1855) em um trabalho publicado em 1801 (*Disquisitiones Arithmeticae).* Nesta seção serão utilizados resultados que podem ser encontrados nos livros [1], [3] e [14].

Definição 1.1.1. Se a, b e m são inteiros com $m > 0$ dizemos que a é *congruente* a b módulo m se $m|(a-b)$.

Denotamos isto por $a \equiv b\ (mod\ m)$.

Caso $m \nmid (a-b)$ dizemos que a é *incongruente* a b módulo m e escrevemos

$$a \not\equiv b\ (mod\ m).$$

Exemplo 1.1.1. $12 \equiv 5\ (mod\ 7)$ pois $7|(12-5)$. Como $4 \nmid 5$ e $5 = 17 - 12$, temos que $17 \not\equiv 12\ (mod\ 4)$.

Proposição 1.1.1. Se a e b são inteiros, temos que $a \equiv b\ (mod\ m)$ se, e somente se, existir um inteiro k tal que $a = b + km$.

Demonstração: Se $a \equiv b\ (mod\ m)$, então $m|(a-b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. A recíproca é trivial, veja, se

$$a = b + km,$$

Isso implica que

$$(a-b) = km,$$

como k é inteiro, temos que $m|(a-b)$, isto é, $a \equiv b\ (mod\ m)$.

O próximo resultado nos diz que a congruência modular, definida no conjunto dos números inteiros, é uma relação de equivalência, ou seja, vale as propriedades reflexiva, simétrica e transitiva.

Proposição 1.1.2. Se a, b, m e d são inteiros, com $m > 0$, as seguintes sentenças são verdadeiras:

i) $a \equiv a\ (mod\ m)$

ii) Se $a \equiv b\ (mod\ m)$, então $b \equiv a\ (mod\ m)$

iii) Se $a \equiv b\ (mod\ m)$ e $b \equiv d\ (mod\ m)$, então $a \equiv d\ (mod\ m)$.

Demonstração: (i) como $m|0$, então $m|(a-a)$, o que implica que $a \equiv a\ (mod\ m)$. (ii) Se $a \equiv b\ (mod\ m)$, então $a = b + k_1 m$ para algum inteiro k_1. Logo $b = a + k_1 m$, o que implica, pela Proposição 1.1.1, $b \equiv a\ (mod\ m)$.

(iii) Se $a \equiv b\ (mod\ m)$ e $b \equiv d\ (mod\ m)$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - d = k_2 m$. Somando-se membro a membro, estas duas últimas equações, obtemos $a - d = (k_1 + k_2)m$, o que implica $a \equiv d\ (mod\ m)$. ■

A seguir, destacamos as principais propriedades aritméticas da congruência modular.

Teorema 1.1.1. Se a, b, c e m são inteiros tais que $a \equiv b\ (mod\ m)$, então

i) $a + c \equiv b + c\ (mod\ m)$

ii) $a - c \equiv b - c\ (mod\ m)$

iii) $ac \equiv bc\ (mod\ m)$

Demonstração: (i) como $a \equiv b\ (mod\ m)$, temos que $a - b = km$ para algum inteiro k, e, portanto, como

$$a - b = (a + c) - (b + c),$$

temos $a + c \equiv b + c\ (mod\ m)$.

(ii) como $(a - c) - (b - c) = a - b$ e por hipótese, $a - b = km$. Temos que

$$a - c \equiv b - c\ (mod\ m).$$

(iii) Como $a - b = km$ então $ac - bc = ckm$ o que implica $m|(ac - bc)$ e, portanto, $ac \equiv bc\ (mod\ m)$. ■

Teorema 1.1.2. Se a, b, c, d e m são inteiros tais que $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então

i) $a + c \equiv b + d\ (mod\ m)$;

ii) $a - c \equiv b - d\ (mod\ m)$;

iii) $ac \equiv bd\ (mod\ m)$.

Demonstração: (i) De $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$ temos

$$a - b = km \text{ e } c - d = k_1 m,$$

onde k, k_1 são inteiros.

Somando-se, membro a membro as duas últimas equações, obtemos,

$$(a + c) - (b + d) = (k + k_1)m$$

e isto implica $a + c \equiv b + d \ (mod\ m)$.

(ii) subtraindo membro a membro $a - c = km$ e $c - d = k_1 m$ obtemos,

$$(a - b) - (c - d) = (a - c) - (b - d) = (k - k_1)m,$$

o que implica $a - c \equiv b - d \ (mod\ m)$.

(iii) Multiplicando ambos os lados de $a - b = km$ por c e ambos os lados de

$$c - d = k_1 m$$

por b, obtendo $ac - bc = ckm$ e $bc - bd = bk_1 m$. Basta agora, somarmos membro a membro, estas duas últimas igualdades, obtendo

$$ac - bc + bc - bd = ac - bd = (ck + bk_1)m,$$

o que implica $ac \equiv bd \ (mod\ m)$. ■

A Definição 1.1.2 e Proposição 1.1.3 que veremos abaixo podem ser consultados em [3].

Definição 1.1.2. Seja $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ o conjunto das classes de congruência $mod\ m$, dados $\bar{x}$ e $\bar{y}$ em $\mathbb{Z}_m$, vamos definir as seguintes operações:

$$\bar{x} + \bar{y} = \overline{x + y};$$

$$\bar{x}.\bar{y} = \overline{xy}.$$

Pode-se mostrar que essas operações estão bem definidas e delas podemos listar as seguintes propriedades:

Proposição 1.1.3. Sejam $\bar{x}$, $\bar{y}$ e $\bar{z}$ pertencentes a $\mathbb{Z}_m$, temos:

i) $\bar{x} + \bar{y} = \bar{y} + \bar{x}$

ii) $\bar{x}.\bar{y} = \bar{y}.\bar{x}$

iii) $(\bar{x} + \bar{y}) + \bar{z} = \bar{x} + (\bar{y} + \bar{z})$

iv) $(\bar{x}.\bar{y}).\bar{z} = \bar{x}.(\bar{y}.\bar{z})$

v) $\bar{x}.(\bar{y} + \bar{z}) = \bar{x}.\bar{y} + \bar{x}.\bar{z}$

vi) $\bar{0} + \bar{x} = \bar{x}$

vii) $\bar{1}.\bar{x} = \bar{x}$

Vale que, se $m = p$ onde p é um número primo e se $\bar{a} \neq \bar{0}$, está em $\mathbb{Z}_p$, então existe um elemento $\bar{b}$ em $\mathbb{Z}_p$, tal que $\bar{a}.\bar{b} = \bar{1}$.

Demonstração:

O conjunto $\mathbb{Z}_p$ é muito importante para a álgebra e teoria dos números, ele é chamando de *conjunto dos inteiros* $mod\ p$, então devemos está bem familiarizados com ele para que possamos entender todos os resultados apresentados nesse trabalho.

Observação: Nas seções seguintes trabalharemos com os elementos pertencentes aos $\mathbb{Z}_p$ sem a barra.

1.2 MATRIZES

Para entendermos esse trabalho faz-se necessário conhecer algumas propriedades e operações das matrizes, portanto, nesta seção, abordaremos alguns fatos que serão utilizados no decorrer do trabalho, tais fatos podem ser encontrados nos livros [1],[2], [5], [6] e [15] . Ao longo da seção, $\mathbb{K}$ representará um corpo.

Definição 1.2.1. Dados m, n dois números inteiros positivos, uma matriz A de ordem m por n, sobre $\mathbb{K}$, é formada por valores $a_{ij} \in \mathbb{K}$, com $1 \leq i \leq m, 1 \leq j \leq n$, distribuídos em m linhas e n colunas, onde o índice i indica a linha e o índice j a coluna as quais os elementos estão posicionados, como podemos ver a seguir:

$$A = (a_{ij})_{i,j} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

No conjunto $\mathbb{M}_{m\times n}(\mathbb{K})$ formado por todas as matrizes de ordem $m \times n$ sobre um corpo $\mathbb{K}$ podemos definir duas operações:

I. SOMA DE MATRIZES.

Se $A = (a_{ij})_{i,j}, B = (b_{ij})_{i,j} \in \mathbb{M}_{m\times n}(\mathbb{K})$, então a soma $A + B$ é a matriz

$$C = \left(c_{ij}\right)_{i,j} \in \mathbb{M}_{m\times n}(\mathbb{K}),$$

tal que, para cada par (i,j), temos $c_{ij} = a_{ij} + b_{ij}$, isto é,

$$A + B = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{pmatrix}.$$

II. PRODUTO DE MATRIZES.

Sejam $A = \left(a_{ij}\right)_{i,j} \in \mathbb{M}_{m\times n}(\mathbb{K})$ e $B = \left(b_{ij}\right)_{i,j} \in \mathbb{M}_{n\times p}(\mathbb{K})$, isto é, com o número de colunas de A igual ao número de linhas de B. Definimos o produto de A por B como sendo a matriz $C = \left(c_{ij}\right)_{i,j} \in \mathbb{M}_{m\times p}(\mathbb{K})$ tal que

$$c_{ij} = \sum_{l=1}^{n} a_{il} b_{lj},$$

para $i = 1, \ldots, m$ e $j = 1, \ldots, p$ ou seja,

$$A \cdot B = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \cdots & b_{1p} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{np} \end{pmatrix} = \begin{pmatrix} \sum_{l=1}^{n} a_{1l} \cdot b_{l1} & \cdots & \sum_{l=1}^{n} a_{1l} \cdot b_{lp} \\ \vdots & \ddots & \vdots \\ \sum_{l=1}^{n} a_{ml} \cdot b_{l1} & \cdots & \sum_{l=1}^{n} a_{ml} \cdot b_{lp} \end{pmatrix}.$$

No produto entre matrizes devemos tomar cuidado, pois, em geral essa operação não é comutativa e nem todo elemento possui inverso multiplicativo.

Exemplo 1.2.1. sejam $A = \begin{pmatrix} 1 & 1 & 3 \\ 2 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix}$ e $B = \begin{pmatrix} 2 & 5 & 6 \\ 2 & 2 & 1 \\ 4 & 3 & 3 \end{pmatrix} \in \mathbb{M}_{3\times 3}(\mathbb{R})$, calcule $A + B$.

Por definição, a soma das matrizes $A, B \in \mathbb{M}_{3\times 3}(\mathbb{R})$ é dada por uma matriz

$$C \in \mathbb{M}_{3\times 3}(\mathbb{R}),$$

onde

$$C = A + B = \begin{pmatrix} 1 & 1 & 3 \\ 2 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 5 & 6 \\ 2 & 2 & 1 \\ 4 & 3 & 3 \end{pmatrix} = \begin{pmatrix} 1+2 & 1+5 & 3+6 \\ 2+2 & 1+2 & 2+1 \\ 3+4 & 2+3 & 1+3 \end{pmatrix} = \begin{pmatrix} 3 & 6 & 9 \\ 4 & 3 & 3 \\ 7 & 5 & 4 \end{pmatrix}.$$

Exemplo 1.2.2. Dada as matrizes $A = \begin{pmatrix} 3 & 1 \\ -1 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{M}_{2\times 2}(\mathbb{R})$ a seguir, calcule $A \cdot B$.

Temos que o produto de A, B e dado por uma matriz $C \in \mathbb{M}_{2\times 2}(\mathbb{R})$, onde

$$C = A \cdot B = \begin{pmatrix} 3 & 1 \\ -1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3\cdot 2 + 1\cdot 1 & 3\cdot 1 + 1\cdot 1 \\ -1\cdot 2 + 3\cdot 1 & -1\cdot 1 + 3\cdot 1 \end{pmatrix} = \begin{pmatrix} 7 & 4 \\ 1 & 2 \end{pmatrix}.$$

No estudo sobre corpos, uma propriedade importante é que todos os elementos não nulos possuem inverso multiplicativo. Portanto, devemos definir um fato importante sobre matrizes, para nos auxiliar nessa análise.

Definição 1.2.2. Seja n um número inteiro positivo. Definimos $\mathbb{M}_n(\mathbb{K})$ como sendo o conjunto das matrizes quadradas n por n, sobre um corpo $\mathbb{K}$.

Definição 1.2.3. Dizemos que duas matrizes A e $B \in \mathbb{M}_n(\mathbb{Z}_m)$ são congruentes se, e somente se $a_{ij} \equiv b_{ij}\ (mod\ m)$ com $i, j < n$ e denotamos $A \equiv B\ (mod\ m)$.

Exemplo 1.2.3. Calcule a soma e o produto das matrizes

$$A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 0 \end{pmatrix} \text{ e } B = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix} \in \mathbb{M}_3(\mathbb{Z}_3).$$

A soma de A com B é dada por:

$$A + B = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 0 \end{pmatrix} + \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1+2 & 2+0 & 2+1 \\ 2+0 & 1+1 & 2+2 \\ 2+1 & 2+2 & 0+1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 1 \end{pmatrix}.$$

Observe que $\begin{pmatrix} 3 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 2 & 0 \\ 2 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ (mod 3), segue que $A + B = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

O produto, de A por B, é dado por:

$$A.B = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 0 \end{pmatrix}.\begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1.2 + 2.0 + 2.1 & 1.0 + 2.1 + 2.2 & 1.1 + 2.2 + 2.1 \\ 2.2 + 1.0 + 2.1 & 2.0 + 1.1 + 2.2 & 2.1 + 1.2 + 2.1 \\ 2.2 + 2.0 + 0.1 & 2.0 + 2.1 + 0.2 & 2.1 + 2.2 + 0.1 \end{pmatrix} =$$

$$\begin{pmatrix} 4 & 6 & 7 \\ 6 & 5 & 6 \\ 4 & 2 & 6 \end{pmatrix}.$$

Como $\begin{pmatrix} 4 & 6 & 7 \\ 6 & 5 & 6 \\ 4 & 2 & 6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 2 & 0 \end{pmatrix}$ (mod 3), segue que $A.B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 2 & 0 \end{pmatrix}$.

Agora definiremos o determinante de uma matriz $A \in \mathbb{M}_n(\mathbb{K})$ de maneira indutiva, sobre $n \geq 1$. A definição que veremos a seguir pode ser encontrada em $[2]$.

Definição 1.2.4. Se $n = 1$, então a matriz $A \in \mathbb{M}_1(\mathbb{K})$ é dada por um único elemento $a = a_{11}$. Definimos, neste caso, $\det A = a$. Suponha agora que $n > 1$ e que $\det B$ esteja definido para todas as matrizes $B \in \mathbb{M}_m(\mathbb{K})$ com $m < n$ e seja $A \in \mathbb{M}_n(\mathbb{K})$. Para cada par (i, j), defina a matriz A_{ij} formada a partir de A retirando-se a sua i-énesima linha e sua j-ésima coluna. É claro que $A_{ij} \in \mathbb{M}_{n-1}(\mathbb{K})$ e, portanto, já está definido $\det A_{ij}$. Agora podemos definir o determinante de A como sendo

$$det\, A = \sum_{j=1}^{n} (-1)^{j+1} a_{1j} \cdot det\, A_{1j}.$$

Observe que o $det\ A \in \mathbb{K}$.

Exemplo 1.2.4. Seja $A = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix} \in \mathbb{M}_2(\mathbb{Z}_5)$. Pela definição 1.2.4, temos que o determinante da matriz A é dado por:

$$\det A = (-1)^{1+1} \cdot 1 \det A_{11} + (-1)^{1+2} \cdot -3 \det A_{12} = 1 \det A_{11} - 3 \det A_{12}.$$

Como $\det A_{11} = 2$ e $\det A_{12} = 3$, temos que $\det A = 1 \cdot 2 - 3 \cdot 3 = -7$. Como os elementos pertencem ao corpo primo $(\mathbb{Z}_5)$, temos $\det A = -7 \equiv 3\ (mod\ 5)$, ou seja, $\det A = 3$.

O próximo resultado é crucial para decidirmos quando uma matriz é ou não invertível.

Teorema 1.2.1. Uma matriz $A \in \mathbb{M}_n(\mathbb{K})$ é *invertível* se, e somente se, $\det A \neq 0$.

Demonstração: Essa demonstração pode ser vista em $[1]$. ■

Definição 1.2.5. Se A é uma matriz $m \times n$, então a matriz $transposta$ de A, denotada por A^T, é a matriz $n \times m$ obtida transformando as linhas de A em colunas; ou seja, a primeira coluna de A^T é a primeira linha de A, a segunda coluna de A^T é a segunda

linha de A, e assim por diante. Assim, a entrada na linha i e coluna j de A se transforma na entrada na linha j e coluna i de A^T, ou seja,

$$A = (a_{ij})_{i,j} \text{ e } A^T = (a_{ji})_{ji}.$$

Exemplo 1.2.5. Veja os exemplos de matrizes e suas transpostas.

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, C = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix},$$

$$A^T = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \\ a_{13} & a_{23} \end{pmatrix}, B^T = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}, C^T = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}.$$

Agora, veremos um tipo de matriz essencial que vamos abordar no nosso trabalho, essa matriz é chamada de matriz simétrica.

Definição 1.2.6. Uma matriz quadrada é dita *simétrica* quando $(a_{ij}) = (a_{ji})$, ou seja, $\forall\, i, j \in \{1, 2, \dots, n\}$ tem -se $A = (a_{ij}) = (a_{ji}) = A^T$.

Exemplo 1.2.6. Vejamos alguns exemplos de matrizes simétricas.

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}, B = \begin{pmatrix} 1 & 3 & 1 \\ 3 & 2 & 2 \\ 1 & 2 & 2 \end{pmatrix}, C = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ e } D = \begin{pmatrix} 4 & -3 & -3 \\ -3 & 4 & -3 \\ -3 & -3 & 4 \end{pmatrix}.$$

A seguir, veremos um teorema que lista as principais propriedades das matrizes simétricas.

Teorema 1.2.2. O produto de duas matrizes simétricas é uma matriz simétrica se, e somente se, as matrizes comutam.

Demonstração: Seja A e B duas matrizes simétricas de mesmo tamanho. Então,

$$(AB)^T = AB.$$

Pela propriedade de matriz transposta,

$(AB)^T = B^T A^T = BA.$

Logo, $AB = BA$, ou seja, A e B comutam.

Por outro lado, temos que

$$AB = BA.$$

Daí,

$$(AB)^T = (BA)^T = A^T B^T = AB.$$

Logo, AB é simétrica. ■

Teorema 1.2.3. Se A é uma matriz simétrica invertível, então A^{-1} é simétrica.

Demonstração: Suponha que A é simétrica e invertível. Para provar que A^{-1} é simétrica, devemos mostrar que A^{-1} é igual a sua transposta, contudo, pelo teorema 3.2.11, do livro $[1]$ e pela simetria de A temos que

$$(A^{-1})^T = (A^T)^{-1} = A^{-1}$$

O que conclui a prova. ■

Agora, vejamos algumas definições e teoremas que relacionam matrizes com polinômios, esses resultados são muito importantes, pois, tratam de mostrar como é obtido o polinômio mínimo, polinômio característico e polinômio matricial de uma matriz pertencente a $\mathbb{M}_n(\mathbb{K})$.

Definição 1.2.7. Seja $p(x)$ um polinômio de grau m na variável x, isto é,

$$p(x) = a_m x^m + \cdots + a_1 x + a_0$$

com, $a_j \in \mathbb{K}$ e $a_m \neq 0$. Para uma matriz $A \in \mathbb{M}_n(\mathbb{K})$ definimos o *polinômio matricial* $p(A)$ por

$$p(A) = a_m A^m + \cdots + a_1 A + a_0 I_n.$$

Obviamente, $p(A) \in \mathbb{M}_n(\mathbb{K})$.

Definição 1.2.8. Seja $A \in \mathbb{M}_n(\mathbb{K})$ uma matriz cujos os elementos são a_{ij}. A expressão

$$\det(A - xI_n) = det\begin{pmatrix} a_{11} - x & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - x & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - x \end{pmatrix}.$$

Define, um polinômio de grau n na variável x, com coeficientes no corpo $\mathbb{K}$, os quais dependem dos elementos $a_{ij} \in A$. Esse polinômio é denominado $polinômio\ característico$ da matriz A, e será denotado por p_A.

Proposição 1.2.1. Sejam $A, B \in \mathbb{M}_n(\mathbb{K})$. Então, $o\ polinômio\ característico$ de AB é igual ao $polinômio\ característico$ de BA, ou seja, $p_{AB} = p_{BA}$.

Demonstração: A demonstração dessa proposição pode ser encontrada em $[6]$.

Teorema 1.2.4. (Teorema de Hamilton-Cayley) Seja $A \in \mathbb{M}_n(\mathbb{K})$ e seja

$$p_A(x) = \det(xI_n - A)$$

o $polinômio\ característico\ de\ A$ (e que tem grau n). Então, $p_A(A) = 0$.

Demonstração: A demonstração deste teorema pode ser encontrada em $[6]$.

Definição 1.2.9. Um polinômio $p(x)$ com coeficiente em $\mathbb{K}$, de grau n, é dito ser um $polinômio\ mônico$ se for da forma

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

ou seja, se o coeficiente do monômio de maior grau for igual a 1.

Note que, polinômios mônicos nunca são identicamente nulos.

Definição 1.2.10. Dada uma matriz $A \in \mathbb{M}_n(\mathbb{K})$, o *polinômio mínimo* de A é o polinômio mônico de menor grau da forma $M(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$. Para o qual $M(A) = 0$.

Teorema 1.2.5. O $polinômio\ mínimo\ ou\ mínimal\ M(x)$ de uma matriz $A \in \mathbb{M}_n(\mathbb{K})$ é único. Fora isso, se p é um polinômio não identicamente nulo que também se anula em A, ou seja, $p(A) = 0$, então $p(x)$ é divisível por $M(x)$, ou seja, existe um polinômio $f(x)$ tal que

$$p(x) = f(x)M(x)$$

para todo $x \in \mathbb{K}$.

Demonstração: Dada uma matriz $A \in \mathbb{M}_n(\mathbb{K})$, o polinômio mínimo de A é da forma

$$M(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0.$$

Onde $M(A) = 0$.

Vamos supor que haja outro polinômio N da forma

$$N(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0,$$

para o qual $N(A) = 0$. Subtraindo um do outro, teríamos o polinômio

$$(M - N)(x) = (a_{m-1} - b_{m-1})x^{m-1} + \cdots + (a_1 - b_1)x + (a_0 - b_0),$$

que tem grau menor ou igual a $m - 1$ e para o qual vale

$$(M - N)(A) = M(A) - N(A) = 0 - 0 = 0.$$

Como, por hipótese, não há polinômios não nulos com grau menor que o de M que anulam A, isso é uma contradição, a menos que $M = N$. Isso prova a unicidade.

Seja P um polinômio não identicamente nulo para o qual valha $P(A) = 0$. Se p é o grau de P, deve-se ter $p \geq m$, onde m é o grau do polinômio mínimo de A. Logo, pelos conhecidos fatos sobre divisão de polinômios, podemos encontrar dois polinômios F e R, cujos graus são, respectivamente $p - m$ e r com $0 \leq r \leq m$, tais que

$$P(x) = F(x)M(x) + R(x),$$

para todo $x \in \mathbb{K}$. Ora, isso diz que

$$P(A) = F(A)M(A) + R(A).$$

Como $P(A) = 0$ e $M(A)$=0, isso implica $R(A) = 0$. Como, porém, o grau de R é menor que m, tem-se que R deve ser identicamente nulo. Isso completa a prova. ■

Exemplo 1.2.7. Dada a matriz $A = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} \in \mathbb{M}_2(\mathbb{F}_5)$, o polinômio $f(x) \in \mathbb{F}_5[x]$, dado por $f(x) = x^2 + x + 2$, é o polinômio minimal da matriz A, pois, aplicando a matriz A no polinômio temos:

$$f(A) = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}^2 + \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 4 & 0 \end{pmatrix} + \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Portanto, $f(A) = 0$, o que implica que o polinômio $f(x) = x^2 + x + 2$ é o polinômio minimal de A.

1.3 ESTRUTURAS ALGÉBRICAS

Nesta seção abordaremos alguns conceitos e resultados da álgebra, mais precisamente sobre grupos, anéis, anéis de polinômios, no qual apresentaremos suas definições e alguns exemplos. Para mais detalhes consultar os livros [4], [7], [8], [9] e [10].

Vamos começar definindo a estrutura algébrica grupo, além disso definiremos algumas classes como grupo abeliano e grupo cíclico.

Definição 1.3.1. Chama-se $grupo$ um conjunto não vazio G munido de uma operação $*$ que possui as seguintes propriedades:

i) Associativa:

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

ii) Admite elemento neutro θ:

$$a * \theta = \theta * a = a, \forall\, a \in G$$

iii) Para todo elemento $a \in G$, existe um elemento $a' \in G$ tal que

$$a * a' = a' * a = \theta$$

Temos que quando um grupo G é munido da operação de adição $(+)$, então esse grupo G é chamado de grupo aditivo; já o grupo munido pela operação de multiplicação $(\cdot)$ é chamado de grupo multiplicativo.

Definição 1.3.2. (Grupo Finito) Um grupo $(G,*)$ é dito $finito$ quando o conjunto G for $finito$.

Definição 1.3.3. Se $(G,*)$ é um grupo e a operação $*$ é comutativa, isto é:

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

Diz-se que $(G,*)$ é um $grupo\ comutativo$ ou $grupo\ abeliano$ (do nome de NIELS HENRIK ABEL, matemático norueguês do século XIX (1802 – 1829)).

Exemplos de grupos aditivos abelianos são os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$, pois a operação de adição nesses conjuntos possui as seguintes propriedades:

- Associativa;
- Existência de elemento neutro (aditivo);
- Existência de elemento inverso (aditivo);
- Comutatividade.

Definição 1.3.4. Seja $(G,*)$ um grupo. Dados $x \in G$ e $n \in \mathbb{Z}$. Então, definimos x^n por

$$x^n = \begin{cases} \theta, se\ n = 0 \\ x^{n-1} * x, se\ n > 0 \\ (x^{-n})^{-1}, se\ n < 0 \end{cases}.$$

Proposição 1.3.1. Seja $(G,*)$ um grupo. Dados $a \in G$ e $m, n \in \mathbb{Z}$. Então,

i) $a^n * a^m = a^{m+n}$;

ii) $(a^n)^m = a^{mn}$.

Demonstração: A demonstração desta proposição pode ser encontrada em [8].

Definição 1.3.5. (Grupo cíclico) Um grupo G é dito $cíclico$ se existir $x \in G$, tal que para qualquer elemento $y \in G$ tem-se

$$y = x^n,$$

para algum $n \in \mathbb{Z}$.

Escrevemos

$$G = \langle x \rangle = \{x^n; n \in \mathbb{Z}\},$$

e dizemos que x gera o conjunto G.

Proposição 1.3.2. Todo grupo $cíclico$ é $abeliano$.

Demonstração: Sejam G um grupo $cíclico$ e $a, x_1, x_2 \in G$, onde $G = \langle a \rangle$. Temos,

$$x_1 = a^{n_1}\ e\ x_2 = a^{n_2},$$

para $n_1, n_2 \in \mathbb{Z}$. Assim, pela Proposição 1.3.1, segue que

$$x_1 \cdot x_2 = a^{n_1} \cdot a^{n_2}$$

$$= a^{n_1+n_2}$$

$$= a^{n_2+n_1}$$

$$= a^{n_2} \cdot a^{n_1}$$

$$= x_2 \cdot x_1.$$

Portanto, G é um grupo $abeliano$. ■

Agora, vamos fazer um breve estudo sobre anéis, uma estrutura munida de duas operações uma de adição e outra de multiplicação, que satisfaz algumas condições.

Definição 1.3.6. Um conjunto não vazio A é dito um $anel$ se em A estão definidas duas operações, indicadas por $+$ (chamada adição) e $\cdot$ (chamada multiplicação), denotado por $(A, +, \cdot)$, tais que para todo $a, b, c \in A$, tem-se:

i) $a + b \in A$ (A é fechado para a adição);
ii) $a + b = b + a$ (comutatividade da adição);
iii) $(a + b) + c = a + (b + c)$ (Associatividade da adição);
iv) Existe $0 \in A$ tal que $a + 0 = a$, para todo $a \in A$ (Elemento neutro da adição);
v) Existe $-a \in A$ tal que $a + (-a) = 0$ (Elemento inverso da adição);
vi) $a \cdot b \in A$ (A é fechado para multiplicação);
vii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Associatividade da multiplicação);
viii) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$ (Leis distributivas).

Da definição, temos que A é um grupo abeliano com relação a adição (itens iv *ao* v*)* e é um conjunto fechado com relação à multiplicação (item vi). Se em relação à multiplicação de A temos que $a \cdot b = b \cdot a$, para todo $a, b \in A$, então A é um anel comutativo e se existe $1 \in A$ tal que, $a \cdot 1 = 1 \cdot a = a$, para todo $a \in A$, então *A* é um anel com unidade.

Definição 1.3.7. Se A é um anel comutativo, então $a \in A$, com $a \neq 0$, é dito um divisor de zero se existe $b \in A$ com $b \neq 0$, tal que $ab = 0$.

Definição 1.3.8. Um anel comutativo é um *domínio de integridade* se não possui divisores de zero.

Definição 1.3.9. (Corpo) Seja A um anel comutativo. Se A é um domínio de integridade e para qualquer $a \in A - \{0\}$, existe $b \in A$ tal que $a \cdot b = b \cdot a = 1$, diremos que $(A, +, \cdot)$ é um $corpo$.

Exemplo 1.3.1. Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ e $n \cdot \mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ munidos da soma e produto usuais são exemplos de $anéis$.

Definição 1.3.10. Seja A um anel e B um subconjunto não vazio de A. Dizemos que B é um $subanel$ de A, se velem as seguintes condições:

i) $\forall\, x, y \in B \Longrightarrow x - y \in B$;

ii) $\forall\, x, y \in B \Longrightarrow x \cdot y \in B$.

Exemplo 1.3.2. Temos que $n\mathbb{Z}$ é um subanel de $\mathbb{Z}$, por sua vez, $\mathbb{Z}$ é um subanel de $\mathbb{Q}$, já o $\mathbb{Q}$ é um subanel de $\mathbb{R}$ e $\mathbb{R}$ é um subanel de $\mathbb{C}$.

Observação 1.3.1. Chama-se de $subdomínio$ um subanel que não possui divisores de zeros.

Definição 1.3.11. Um subanel B de um corpo $\mathbb{K}$ é chamado um $subcorpo$ de $\mathbb{K}$, se dado $a \in B - \{0\}$ existe $b \in B$ tal que $a \cdot b = 1$.

Exemplo 1.3.3. Observe que $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$ que, por sua vez, é um subcorpo de $\mathbb{C}$.

Definição 1.3.12. Sejam A um anel e I um subanel de A. Dizemos que I é um $ideal$ de A se, $a \cdot x \in I$, $\forall a \in A$, $\forall x \in I$ e $x \cdot a \in I, \forall a \in A, \forall x \in I$.

Os subanéis $\{0\}$ e A são ideias de A e são chamados de ideais triviais de A.

Definição 1.3.13. Sejam A um anel e M um ideal de A. Dizemos que M é um $ideal\ maximal$ de A se, $M \neq A$ e se J é um ideal de A tal que $M \subset J \subset A$, então $J = M$ ou $J = A$.

Teorema 1.3.1. Seja $\mathbb{K}$ um anel comutativo com unidade, $1 \in \mathbb{K}$. Então, as seguintes condições são equivalentes:

i) $\mathbb{K}$ é um corpo;

ii) $\{0\}$ é um ideal maximal em $\mathbb{K}$;

iii) Os únicos ideais de $\mathbb{K}$ são os triviais.

Demonstração: De $\mathrm{i}) \Rightarrow \mathrm{ii})$. Sejam $\mathbb{K}$ um corpo e J um ideal de $\mathbb{K}$ tal que $\{0\} \subset J \subset \mathbb{K}$. Suponhamos $J \neq \{0\}$. Assim existe $a \in J$, com $a \neq 0$. Como $\mathbb{K}$ é um corpo, existe $b \in \mathbb{K}$ tal que $b \cdot a = 1$ e, portanto, $1 \in J$ e daí segue imediatamente que $J = \mathbb{K}$.

Temos que de $\mathrm{ii}) \Rightarrow \mathrm{iii})$. Seja J um ideal de $\mathbb{K}$. Logo, $\{0\} \subset J \subset \mathbb{K}$ e como $\{0\}$ é maximal, então, $J = \{0\}$ ou $J = \mathbb{K}$. Portanto, os únicos ideais de $\mathbb{K}$ são os triviais.

De iii) ⇒ i) resta mostrar que todo elemento não nulo tem inverso. Seja $0 \neq a \in \mathbb{K}$ e $I = \mathbb{K} \cdot a$ o ideal principal de $\mathbb{K}$ que é gerado por a. Como $1 \in \mathbb{K}$, temos $a = 1 \cdot a \in I$, logo $I \neq 0$ e assim pela nossa hipótese, teremos $I = \mathbb{K}$. Portanto,

$$1 \in \mathbb{K} = \mathbb{K} \cdot a,$$

donde existe $b \in \mathbb{K}$ tal que $1 = b \cdot a$. Logo, a é invertível em $\mathbb{K}$. Portanto, $\mathbb{K}$ é um corpo.

■

Definição 1.3.14. Se $A \neq \{0\}$ for um anel e existir um inteiro positivo n tal que, para todo $a \in A$,

$$n.a = a + \cdots + a = 0, \quad (n \text{ vezes}),$$

Então o menor desses inteiros positivos será chamado de a $característica$ do anel A. Diremos, nesse caso, que A tem $característica\ positiva$. Se não existir nenhum inteiro positivo com a propriedade acima, diremos que A tem $característica\ zero$.

Dizemos que um corpo $\mathbb{K}$ tem característica 0 ou característica p se, como anel, tiver característica 0 ou p. Onde p representa um número primo.

Exemplo 1.3.4. Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ tem característica 0, pois se $n \neq 0$, então $n \cdot 1 = n$ e, portanto, $n \cdot 1 \neq 0$.

Observação 1.3.2. Aqui definiremos A/J como sendo um anel, chamado de $anel\ quociente$, que é munido das seguintes operações:

$$+ \colon A/J \times A/J \to A/J$$

$$\left(\bar{a}, \bar{b}\right) \mapsto \overline{a+b}$$

$$\cdot \colon A/J \times A/J \to A/J$$

$$\left(\bar{a}, \bar{b}\right) \mapsto \overline{a.b}$$

Teorema 1.3.2. Sejam A um anel comutativo com unidade 1 e J um ideal de A. Então J é um ideal maximal de A se, e somente se, A/J é um corpo.

Demonstração: A demonstração desse teorema pode ser encontrada em [9].

Podemos descobrir muitos resultados analisando interações entre anéis, fazemos isso utilizando o conceito de homomorfismo, veja a definição.

Definição 1.3.15. Dados A e B anéis, uma função $f: A \longrightarrow B$ diz-se um $homomorfismo$ de A em B se satisfaz as seguintes condições:

i) $f(x+y) = f(x) + f(y), \forall x, y \in A$;

ii) $f(x \cdot y) = f(x) \cdot f(y), \forall x, y \in A$.

Definição 1.3.16. Um homomorfismo bijetor de anéis será chamado de $isomorfismo$. Dois anéis são ditos $isomorfos$ se existir um isomorfismo entre eles.

Exemplo 1.3.5. Sejam A e B dois anéis quaisquer. Note que, $f: A \longrightarrow B$, dada por $f(a) = 0$, para todo $a \in A$, é claramente um homomorfismo de anéis.

Vejamos, sejam $a, b \in A$. Têm-se:

$$f(a + b) = 0 = 0 + 0 = f(a) + f(b),$$

$$f(a \cdot b) = 0 = 0 \cdot 0 = f(a) \cdot f(b).$$

Teorema 1.3.3. Sejam A e B anéis e $f: A \longrightarrow B$ um homomorfismo de anéis. Então:

i) $Im\,(f) = \{f(a) \mid a \in A\}$ é um subanel de B.

ii) $\ker(f) = \{a \in A \mid f(a) = 0'\}$ é um ideal de A e f é injetiva se, se somente se, $\ker(f) = \{0\}$;

iii) Os anéis $\frac{A}{\ker\,(f)}$ e $Im\,f$ são isomorfos.

Demonstração. A demonstração deste teorema pode ser encontrada em [9].

Veremos agora alguns resultados interessantes sobre um tipo específico de anel, o anel de polinômios.

Definição 1.3.17. Seja A um anel. Um *polinômio em uma variável* x é uma série finita de monômios em uma variável da forma

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

onde $a_i \in A$, *com* $0 \leq i \leq n$.

Definição 1.3.18. Seja R um anel comutativo, temos que $R[x]$ denota o conjunto de todos os polinômios na variável x com coeficientes em R, ou seja,

$$R[x] = \{f(x) = a_0 + a_1 x + \cdots + a_n x^n \mid n \geq 0, a_j \in R, \forall j\}.$$

Em $R[x]$ definimos duas operações $+$ e $\cdot$: Sejam

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n\ ,\ g(x) = b_0 + b_1 x + \cdots + b_m x^m\ \in R[x]$$

então,

$f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_k+b_k)x^k$, onde $k=max\{n,m\}$ e

$f(x)\cdot g(x)=c_0+c_1x+\cdots+c_{n+m}x^{n+m}$, onde $c_j=a_jb_0+a_{j-1}b_1+\cdots+a_0b_j$.

Proposição 1.3.3. $(R[x],+,\cdot)$ é um anel, chamado $anel\ de\ polinômios$ em uma variável com coeficientes no anel R.

Demonstração: A demonstração desta proposição pode ser encontrada em $[5]$.

Definição 1.3.19. (Grau) Sejam R um anel e $R[x]$ o anel de polinômios com coeficientes em R. Se $f\in R[x], f=a_0+a_1x+\cdots+a_nx^n$, com $a_n\neq 0$, então o *grau* de f é definido por grau $(f)=n$ e a_n é dito ser o *coeficiente líder* de f.

Em particular, quando $a_n=1$, tem-se

$$f(x)=a_0+a_1x+\cdots+x^n,$$

e dizemos que $f(x)$ é um polinômio *mônico*.

Definição 1.3.20. Seja R um anel comutativo com identidade. Dados

$$f(x),g(x)\in R[x],$$

dizemos que $g(x)$ divide $f(x)$ se existe $h(x)\in R[x]$ tal que $f(x)=g(x)h(x)$.

Teorema 1.3.4. (Algoritmo da divisão de Euclides). Sejam $\mathbb{K}$ um corpo e $f(x),g(x)\in\mathbb{K}[x]$, com $g\neq 0$, então existem únicos $q(x),r(x)\in\mathbb{K}[x]$ tais que

$$f(x)=q(x)g(x)+r(x)$$

Onde $r(x)=0$ ou grau $(r(x))<$ grau $(g(x))$.

Demonstração: A demonstração deste teorema pode ser encontrada em $[10]$.

Observe que o resultado do Teorema 1.3.4 não pode ser verdadeiro se $\mathbb{K}$ não for um corpo. Vejamos os exemplos

i) Em $\mathbb{Z}[x]$ não existem polinômios $q(x),r(x)\in\mathbb{Z}[x]$ tal que

$$1+3x^2=q(x)(1+2x)+r(x).$$

ii) Em $\mathbb{Z}_4[x]$ temos que

$$2x^3+2x^2+3x+3=q_1(x)(2x^2+3)+r_1(x).$$

Onde

$$q_1(x) = x + 1, r_1(x) = 0$$

e também

$$2x^3 + 2x^2 + 3x + 3 = q_2(x)(2x^2 + 3) + r_2(x).$$

Onde $q_2(x) = 3x + 1, r_2(x) = 2x$, logo os $q(x)$ e $r(x)$ não são únicos. ■

Exemplo 1.3.6. Determine polinômios $q(x)$ e $r(x)$ tais que $f(x) = g(x)q(x) + r(x)$, onde $r(x) = 0$ ou grau $r(x) <$ grau $g(x)$ sabendo que

$$f(x) = 2x^2 + 4x + 3, g(x) = 7x + 3 \in \mathbb{Z}_8[x].$$

$2x^2$	$+$	$4x$	$+$	3	$7x$	$+$	3
$-2x^2$	$-$	$2x$			$6x$	$+$	6
		$2x$	$+$	3			
	$-$	$2x$	$-$	2			
				1			

Portanto, $q(x) = 6x + 6, r(x) = 1$ e $f(x) = q(x)g(x) + r(x)$.

Definição 1.3.21. (Raiz de um polinômio). Seja R um anel comutativo e seja

$$f(x) \in R[x] \backslash \{0\}.$$

Um elemento $a \in R$ é chamado de *raiz* de $f(x)$ se $f(a) = 0$.

Exemplo 1.3.7. Seja $f(x) = x^2 + 5 \in \mathbb{Z}_6[x]$, temos que as raízes desse polinômio são $1, 5 \in \mathbb{Z}_6$, pois, $f(1) = 1^2 + 5 = 6 \equiv 0\ (mod\ 6)$ e $f(5) = 5^2 + 5 = 30 \equiv 0\ (mod\ 6)$.

Definição 1.3.22. (Polinômios irredutível). Seja R um domínio de integridade. Um polinômio $f(x) \in R[x]$ é dito *irredutível* sobre R se

i) $f(x) \neq 0$ e grau $f(x) \geq 1$ (isto é, $f(x)$ é um polinômio não constante) e
ii) Se $f(x) = p(x)q(x)$ em $R[x]$, então ou $p(x)$ é a unidade ou $q(x)$ é a unidade. Ou seja, $p(x) = 1$ ou $q(x) = 1$.

Dizemos que $f(x)$ é *redutível* em $R[x]$, quando ele não for irredutível, ou seja, se $f(x) = p(x)q(x)$, com $p(x)$ e $q(x)$ são unidades. Nesse caso, $p(x)$ e $q(x)$ são chamados de *fatores* de $f(x)$.

Definição 1.3.23. Se $\mathbb{K}$ é um corpo, então $f(x) \in \mathbb{K}[x]$ é redutível se, e somente se, existe uma fatorização da forma:

$$f(x) = p(x)q(x), \text{ com } p(x), q(x) \in \mathbb{K}[x], \text{ grau } p(x) \geq 1 \text{ e grau } g(x) \geq 1.$$

Teorema 1.3.5. Seja $\mathbb{K}$ um corpo e seja $f(x) \in \mathbb{K}[x]$ com grau $f(x) \geq 2$. Então, $f(x)$ é irredutível sobre $\mathbb{K}$, se $f(x)$ não tem raízes em $\mathbb{K}$.

Demonstração: Se $f(x)$ tem uma raiz $a \in \mathbb{K}$, então $f(x) = (x-a)p(x)$, para algum $p(x) \in \mathbb{K}[x]$, com grau $p(x) \geq 1$. Como ambos $(x-a)$ e $p(x)$ não são unidades de $\mathbb{K}[x]$, segue que $f(x)$ é redutível. Portanto, se $f(x)$ é irredutível sobre $\mathbb{K}$, então $f(x)$ não tem raízes em $\mathbb{K}$. ■

Exemplo 1.3.8. Note que o polinômio $x^2 + 2$ é irredutível em $\mathbb{R}[x]$, mas se pegarmos o mesmo polinômio com coeficientes em $\mathbb{Z}_3$, esse polinômio será redutível em $\mathbb{Z}_3[x]$ (em particular, $x^2 + 2 = (x+2)(x+1) \in \mathbb{Z}_3[x]$).

Agora vamos falar brevemente de anéis quocientes de polinômios sobre um corpo, onde veremos dois teoremas que tratam da estrutura $\mathbb{K}[x]/_I$, onde $\mathbb{K}$ é um corpo e I é um ideal de $\mathbb{K}[x]$.

Teorema 1.3.6. Sejam $\mathbb{K}$ um corpo e I um ideal não nulo de $\mathbb{K}[x]$. Então, existe um único polinômio mônico $f(x) \in \mathbb{K}[x]$ tal que I é gerado por $f(x)$, isto é,

$$I = \langle f(x) \rangle = f(x)\mathbb{K}[x] = \{f(x)g(x) \mid g(x) \in \mathbb{K}[x]\}.$$

Demonstração: Essa demonstração desse teorema pode ser encontrada em [10].

Teorema 1.3.7. Sejam $\mathbb{K}$ um corpo, $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$ e $I = \langle f(x) \rangle$, com $n = grau\, f(x)$. Então, todo elemento de $R = \mathbb{K}[x]/_I$ tem uma representação única de $grau \leq n-1$. Portanto, o anel quociente $R = \mathbb{K}[x]/_I$ é dado por

$$R \cong \{b_{n-1}t^{n-1} + \cdots + b_2 t^2 + b_1 t + b_0 \mid b_0, \ldots, b_{n-1} \in \mathbb{K}\}.$$

Além disso, $f(t) = 0$.

Demonstração. A demonstração desse teorema pode ser encontrada em [10]. Teorema 2.5.21.

Exemplo 1.3.9. Descrever o anel quociente $\frac{\mathbb{Q}[x]}{\langle x^3-2 \rangle}$.

Pelo Teorema 1.3.7, temos que:

$$\frac{\mathbb{Q}[x]}{\langle x^3-2\rangle} \cong \{at^2 + bt + c \mid a, b, c \in \mathbb{Q}\}, \text{ com } t^3 - 2 = 0.$$

CAPÍTULO 2- UM POUCO SOBRE TEORIA DOS CORPOS

Nesse capítulo, falaremos sobre alguns resultados da teoria de corpos finitos e extensões algébricas. Esses resultados serão de extrema importância para o ápice do capítulo final, onde serão construídos os corpos de ordem p^2 menores do que 121. A teoria de corpos finitos é uma teoria que envolve grandes resultados da álgebra. Os resultados que veremos nas seções seguintes podem ser encontrados em [3] e [9].

2.1 EXTENÇÃO ALGÉBRICA

Definição 2.1.1 Um corpo $\mathbb{K}$ é dito uma extensão de um corpo $\mathbb{F}$, se $\mathbb{F}$ for um subcorpo de $\mathbb{K}$ e denotamos por $\mathbb{K} \supset \mathbb{F}$.

Exemplo 2.1.1 O corpo $\mathbb{R}$ é uma extensão do corpo $\mathbb{Q}$.

Definição 2.1.2 Sejam $\mathbb{K}$ uma extensão de $\mathbb{F}$ e $\alpha \in \mathbb{K}$. Dizemos que α é $algébrico$ sobre $\mathbb{F}$ se existe $f(x) \in \mathbb{F}[x] - \{0\}$ tal que $f(\alpha) = 0$. Caso o contrário, dizemos que α é $transcedente$ sobre $\mathbb{F}$**.**

Proposição 2.1.1. Se $\alpha \in \mathbb{K}$, então α é algébrico sobre $\mathbb{K}$.

Demonstração. Basta tomar $f(x) = x - \alpha \in \mathbb{K}[x]$ e temos $f(\alpha) = \alpha - \alpha = 0$. Logo α é algébrico sobre $\mathbb{F}$. ■

Observação 2.1.1. Se $\alpha \in \mathbb{K} \supset \mathbb{F}$ definimos $\mathbb{F}[\alpha] = \{f(\alpha) \mid f(x) \in \mathbb{F}[x]\}$. Ademais, $\mathbb{F}[\alpha]$ é um subdomínio de $\mathbb{K}$ que contém $\mathbb{F}$.

Proposição 2.1.2. Sejam $\alpha \in \mathbb{K}$ algébrico sobre $\mathbb{F}$ e $p(x) \in \mathbb{F}[x]$, mônico e de menor grau, tal que $p(\alpha) = 0$. Pela minimalidade do grau de $p(x)$, segue que $p(x)$ é o único polinômio mônico irredutível em $\mathbb{F}[x]$, tal que $p(\alpha) = 0$, o qual será denotado aqui por $p(x) = irr(\alpha, \mathbb{F})$.

Demonstração: A Demonstração desta proposição pode ser encontrada em [9].

Teorema 2.1.1. Se $\alpha \in \mathbb{K} \supset \mathbb{F}$ e se $\Psi : \mathbb{F}[x] \longrightarrow \mathbb{K}$ é definida por $\Psi\big(f(x)\big) = f(\alpha)$, então Ψ é um $homomorfismo$ de corpos, tal que:

i) $Im\,(\Psi) = \mathbb{F}[\alpha], \mathbb{F} \subset \mathbb{F}[\alpha] \subset \mathbb{K}$;
ii) α é transcendente sobre $\mathbb{F}$ se, e somente se, $\ker(\Psi) = 0$;
iii) Se α é algébrico sobre $\mathbb{F}$ e $p(x) = irr(\alpha, \mathbb{F})$, então $\ker(\Psi) = \mathbb{F}[x] \cdot p(x)$ é um ideal maximal de $\mathbb{F}[x]$;

iv) $\mathbb{F}[x]/\ker(\Psi) \simeq \mathbb{F}[\alpha]$.

Demonstração. A demonstração deste teorema pode ser encontrada em [9].

Corolário 2.1.1. Sejam $\mathbb{K}$ uma extensão de $\mathbb{F}$ e $\alpha \in \mathbb{K}$**.** Então:

i) Se α é algébrico sobre $\mathbb{F}$, então $\mathbb{F}[\alpha]$ é um subcorpo de $\mathbb{K}$.
ii) Se α é transcendente sobre $\mathbb{F}$, então $\mathbb{F}[\alpha]$ é um subdomínio de $\mathbb{K}$ isomorfo ao domínio $\mathbb{F}[x]$ dos polinômios em uma indeterminada x.

Demonstração. A demonstração deste corolário pode ser encontrada em [9].

Corolário 2.1.2. Se $\mathbb{K}$ é uma extensão de $\mathbb{F}$ e se $\alpha, \beta \in \mathbb{K}$ são raízes de um mesmo polinômio irredutível sobre $\mathbb{F}$, então $\mathbb{F}[\alpha]$ e $\mathbb{F}[\beta]$ são corpos isomorfos.

Demonstração: Por hipótese, $p(x) = irr(\alpha, \mathbb{F}) = irr(\beta, \mathbb{F})$. Agora, pelo item (iii), do Teorema 2.1.1, obtemos

$$J = \mathbb{F}[x] \cdot p(x),$$

e, por (iv), temos $\mathbb{F}[\alpha] \simeq \frac{\mathbb{F}[x]}{J}$ e da mesma forma $\frac{\mathbb{F}[x]}{J} \simeq \mathbb{F}[\beta]$. Logo, $\mathbb{F}[\alpha] \simeq \mathbb{F}[\beta]$. ■

Proposição 2.1.3. Sejam $\mathbb{K}$ uma extensão de $\mathbb{F}$ e $\alpha \in \mathbb{K}$ algébrico sobre $\mathbb{F}$. Se o grau do polinômio $irr(\alpha, \mathbb{F})$ é n, então:

i) Para qualquer $f(x) \in \mathbb{F}[x], f(\alpha)$ pode ser expresso de modo único na forma, $f(\alpha) = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$, onde $a_i \in \mathbb{F}$, com $1 \leq i \leq n$.
ii) $\mathbb{F}[\alpha] = \{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \mid a_i \in \mathbb{F}\}$ é um subcorpo de $\mathbb{K}$ que contém $\mathbb{F}$.
iii) Se $\mathbb{F} = \mathbb{Z}_p$, então $\mathbb{F}[\alpha]$ é um corpo contendo exatamente p^n elementos.

Demonstração. A demonstração desta proposição pode ser encontrada em [9].

Definição 2.1.4. Seja $\mathbb{K}$ uma extensão de $\mathbb{F}$. Dizemos que $\mathbb{K}$ é uma extensão algébrica de $\mathbb{F}$, se todo $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{F}$.

Exemplo 2.1.2. O corpo $\mathbb{R}$ é uma extensão do corpo $\mathbb{Q}$. Desde que $\sqrt{2}$ é uma raiz do polinômio $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, temos que $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$. Note que $i \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$, pois é raiz de $p(x) = x^2 + 1 \in \mathbb{C}[x]$.

Vejamos agora alguns conceitos sobre o grau de uma extensão.

Observação 2.1.2. Seja S um conjunto finito, digamos que $S = \{a_1, \ldots, a_n\}$, denotaremos $\mathbb{F}(S)$ por $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$.

Definição 2.1.5. Se $\mathbb{K}$ é uma extensão de $\mathbb{F}$, então ele é um espaço vetorial sobre $\mathbb{F}$. Este tem uma dimensão sobre $\mathbb{F}$, que pode ser finita. Tal dimensão é chamada de $grau$ de $\mathbb{K}$ sobre $\mathbb{F}$, e é denotada por $[\mathbb{K}: \mathbb{F}]$.

Uma extensão $\mathbb{K}$ de $\mathbb{F}$ é dita finita se tem o grau da extensão finito. Caso contrário, dizemos $\mathbb{K} \supset \mathbb{F}$ é uma extensão infinita.

Exemplo 2.1.3. O corpo $\mathbb{C}$, visto como espaço vetorial sobre $\mathbb{R}$ tem dimensão 2, pois $\{1, i\}$ é base desse espaço vetorial. Assim, $\mathbb{C}$ é uma extensão de grau 2 sobre $\mathbb{R}$, ou seja, $[\mathbb{C} : \mathbb{R}] = 2$.

Proposição 2.1.4. Sejam $\mathbb{F}$ um corpo e $\mathbb{K} \supset \mathbb{F}$ uma extensão de $\mathbb{F}$. Então:

i) Se $\mathbb{K} \supset \mathbb{F}$ é finita, então $\mathbb{K} \supset \mathbb{F}$ é algébrica;
ii) Se $\alpha \in \mathbb{K} \supset \mathbb{F}$ é um elemento algébrico sobre $\mathbb{F}$ e o grau de $irr(\alpha, \mathbb{K}) = n$, então $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base do espaço vetorial $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$ e $[\mathbb{K}[\alpha] : \mathbb{K}] = n < \infty$;
iii) Se $\alpha \in \mathbb{K} \supset \mathbb{F}$ é um elemento transcendente sobre $\mathbb{K}$, então $\mathbb{K}[\alpha] \supset \mathbb{K}$ é uma extensão infinita.

Demonstração: i) Suponha $[\mathbb{K}: \mathbb{F}] = m < \infty$ e $\alpha \in \mathbb{K} \supset \mathbb{F}$, como $\mathbb{K}[\alpha]$ é um subespaço de $\mathbb{K}$, segue que $[\mathbb{K}[\alpha]: \mathbb{K}] \leq m < \infty$. Se $[\mathbb{K}[\alpha]: \mathbb{K}] = n$, então o conjunto $\{1, \alpha, \ldots, \alpha^n\}$ é L.D., pois n é o número máximo de elementos L.I. e, portanto existem escalares $a_0, a_1, \ldots, a_n \in \mathbb{F}$ não nulos, tais que

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0,$$

e isso significa que α é algébrico sobre $\mathbb{F}$, pois anula o polinômio

$$p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}[x].$$

ii) Seja $\alpha \in \mathbb{K} \supset \mathbb{F}$ um elemento sobre $\mathbb{F}$ tal que grau de $irr(\alpha, \mathbb{F}) = n$. Mas, pela Proposição 2.1.1, todo elemento de $\mathbb{F}[\alpha]$ pode ser escrito de modo único como combinação linear, sobre $\mathbb{F}$, de $1, \alpha, \ldots, \alpha^{n-1}$. Assim, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{F}[\alpha]$ sobre $\mathbb{F}$. Logo, $[\mathbb{F}[\alpha] : \mathbb{F}] = n$.

iii) Segue de imediato do item i). ■

Vejamos agora o corolário que segue desta proposição.

Corolário 2.1.3. Seja $\alpha \in \mathbb{K} \supset \mathbb{F}$. Então, as seguintes afirmações são equivalentes:

i) α é algébrico sobre $\mathbb{F}$;
ii) $[\mathbb{F}[\alpha]: \mathbb{F}] < \infty$;
iii) $\mathbb{F}[\alpha]$ é uma extensão algébrica de $\mathbb{F}$.

Demonstração: (i) ⇒ (ii) Note que, se $\alpha \in \mathbb{K} \supset \mathbb{F}$ é algébrico sobre $\mathbb{F}$, então existe $p(x) \in \mathbb{F}[x]$, tal que $p(\alpha) = 0$. Seja $f(x) = irr(\alpha, \mathbb{F})$, com grau de $irr(\alpha, \mathbb{F}) = n$. Pela minimalidade do grau de $f(x)$ e por resultado da Proposição 2.1.4, item (ii), temos que, $\{1, \alpha, \dots, \alpha^{n-1}\}$ é uma base de $\mathbb{F}[x]$ e $[\mathbb{F}[\alpha] : \mathbb{F}] = n < \infty$.

(ii) ⇒ (iii) Suponha $[\mathbb{F}[\alpha] : \mathbb{F}] = n < \infty$. Então, pela Proposição 2.1.3, item (i), temos que $\mathbb{F}[\alpha]$ é uma extensão algébrica de $\mathbb{F}$.

(iii) ⇒ (i) Sendo $\mathbb{F}[\alpha]$ uma extensão algébrica sobre $\mathbb{F}$, por definição, α é algébrico sobre $\mathbb{F}$. ■

Proposição 2.1.5. Sejam $\mathbb{J} \supset \mathbb{K} \supset \mathbb{F}$ corpos tais que $[\mathbb{J} : \mathbb{K}]$ e $[\mathbb{K} : \mathbb{F}]$ são finitos, então $[\mathbb{J} : \mathbb{F}]$ é finito e $[\mathbb{J} : \mathbb{F}] = [\mathbb{J} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}]$.

Demonstração. A demonstração desta proposição ser encontrada em [9].

2.2 CORPOS FINITOS

Lema 2.2.1. Seja $\mathbb{F}$ um corpo finito com q elementos. Se $\mathbb{F} \subset \mathbb{K}$, onde $\mathbb{K}$ também é um corpo finito, então $\mathbb{K}$ tem q^n elementos, onde $n = [\mathbb{K}: \mathbb{F}]$.

Demonstração: $\mathbb{K}$ é um espaço vetorial sobre $\mathbb{F}$ e como $\mathbb{K}$ é finito e, certamente $\mathbb{K}$ tem dimensão finita como um espaço vetorial sobre $\mathbb{F}$. Suponha que $[\mathbb{K}: \mathbb{F}] = n$, então $\mathbb{K}$ tem uma base de n elementos sobre $\mathbb{F}$. Seja essa base $\{v_1, v_2, v_3, \dots, v_n\}$. Então, cada elemento em $\mathbb{K}$ tem uma representação única na forma $\alpha_1 v_1 + \cdots + \alpha_n v_n$, onde α_1,..., α_n estão todos em $\mathbb{F}$. Portanto, o número de elementos de $\mathbb{K}$ é o número de $\alpha_1 v_1 + \cdots + \alpha_n v_n$, como α_1,..., α_n é um intervalo acima de $\mathbb{F}$, cada coeficiente pode ter q valores, logo $\mathbb{K}$ deve ter q^n elementos. ■

Corolário 2.2.1. Se o corpo finito $\mathbb{F}$ tem p^m elementos, então todo $a \in \mathbb{F}$ satisfaz

$$a^{p^m} = a.$$

Demonstração: Se a = 0 a afirmação do corolário é trivialmente verdadeira. Por outro lado, os elementos de $\mathbb{F}$ diferentes de zero, formam um grupo multiplicativo de ordem $p^m - 1$, pelo Corolário 2 e o Teorema 2.4.1, em [3] segue que, $a^{p^m-1} = 1$, para todo $a \neq 0$ em $\mathbb{F}$. Multiplicando essa relação por a, obtemos que, $a^{p^m} = a$. ■

Desse último corolário, podemos facilmente seguir para os resultados abaixo.

Definição 2.2.1 Considere o conjunto $\mathbb{F}_p[x]$ como sendo o anel de polinômios sobre um corpo de ordem p, onde p é um primo, isto é,

$$\mathbb{F}_p[x] = \{\alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 | \alpha_i \in \mathbb{F}_p, 0 \leq i \leq n\}.$$

Lema 2.2.2. Um polinômio de grau m sobre um corpo pode ter no máximo m raízes em qualquer corpo de extensão.

Demonstração: A demonstração deste lema pode ser encontrada em [3].

Corolário 2.2.2. Se $a \in \mathbb{K}$ é uma raiz de $p(x) \in \mathbb{F}[x]$, onde $\mathbb{K} \supset \mathbb{F}$, então em $\mathbb{K}[x]$,

$$(x - a)|p(x).$$

Demonstração. A demonstração deste corolário pode ser encontrada em [3].

Lema 2.2.3. Se o corpo finito $\mathbb{F}$ tem p^m elementos, então o polinômio $x^{p^m} - x$ em $\mathbb{F}[x]$ é fatorado em $\mathbb{F}[x]$ como $x^{p^m} - x = \prod_{\lambda \in \mathbb{F}}(x - \lambda)$.

Demonstração: Pelo Lema 2.2.2, o polinômio $x^{p^m} - x$ tem no máximo p^m raízes em $\mathbb{F}$. No entanto, pelo Corolário 2.2.1, conhecemos essas p^m raízes, ou seja, todos os elementos de $\mathbb{F}$. Pelo corolário 2.2.2, podemos concluir que $x^{p^m} - x = \prod_{\lambda \in \mathbb{F}}(x - \lambda)$.■

Definição 2.2.2. Uma extensão $\mathbb{K} \supset \mathbb{F}$ é dita um $corpo\ de\ decomposição$ para um polinômio $f(x) \in \mathbb{F}[x]$ se $\mathbb{K}$ contém todas as raízes de f e é da forma

$$\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n).$$

Corolário 2.2.3. Se o corpo $\mathbb{F}$ tem p^m elementos, então $\mathbb{F}$ é um corpo de decomposição do polinômio $x^{p^m} - x$.

Demonstração: Pelo Lema 2.2.3, o polinômio $x^{p^m} - x$ certamente é decomposto em $\mathbb{F}$. No entanto, ele não pode ser dividido em nenhum corpo, com ordem menor que a de $\mathbb{F}$, pois, esse corpo teria que ter todas as raízes deste polinômio e, portanto, teria que ter pelo menos p^m elementos. Assim, $\mathbb{F}$ é um corpo de decomposição de $x^{p^m} - x$.

■

Lema 2.2.4. Quaisquer dois corpos finitos com o mesmo número de elementos são isomórficos.

Demonstração: Se esses corpos possuem p^m elementos, pelo Corolário 2.2.3 acima ambos são corpos de decomposição do polinômio $x^{p^m} - x$, sobre $\mathbb{J}_p$ que é o corpo dos inteiros $mod\ p$, de onde são isomorfos. ■

Corolário 2.2.4. Seja p um primo. Se $\mathbb{F}$ é um corpo de característica p, então o polinômio $x^{p^m} - x \in \mathbb{F}[x]$, $n \geq 1$,tem raízes distintas.

Demonstração: A demonstração deste corolário pode ser encontrada em $[3]$.

O objetivo do próximo lema é demonstrar que para qualquer número primo p e qualquer inteiro m existe um corpo com p^m elementos.

Lema 2.2.5. Para todo número primo p e todo número inteiro positivo m, existe um corpo com p^m elementos.

Demonstração: Considere o polinômio $x^{p^m} - x$ em $\mathbb{F}[x]$, o anel de polinômios em x sobre $\mathbb{F}_p$, o corpo dos inteiros $mod\ p$. Sejam $\mathbb{K}$ um corpo de decomposição deste polinômio e $\mathbb{F} = \{a \in \mathbb{K} | a^{p^m} = a\}$ um subconjunto de $\mathbb{K}$. Os elementos de $\mathbb{F}$ são as raízes de $x^{p^m} - x$ e, pelo Corolário 2.2.4, são distintas, de onde $\mathbb{F}$ tem p^m elementos. Afirmamos agora que $\mathbb{F}$ é um corpo. Se $a, b \in \mathbb{F}$ então temos $a^{p^m} = a$, $b^{p^m} = b$ e então $(ab)^{p^m} = a^{p^m} b^{p^m} = ab$; portanto, $a, b \in \mathbb{F}$. Também como p é a característica de $\mathbb{F}$, $(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m} = a \pm b$, portanto, $a \pm b \in \mathbb{F}$. Consequentemente, $\mathbb{F}$ é um subcorpo de $\mathbb{K}$ e, portanto, um corpo. Tendo exibido o corpo $\mathbb{F}$ com p^m elementos provamos o Lema 2.2.5.

Utilizando os Lemas 2.2.4 e 2.2.5, chegamos ao seguinte teorema.

Teorema 2.2.2. Para todo número primo p e todo número inteiro positivo m, existe um único corpo com p^m elementos.

Demonstração: A demonstração desse teorema pode ser encontrada em [3].

Teorema 2.2.3. Seja $\mathbb{K}$ um corpo finito. Se G é o grupo multiplicativo de elementos diferentes de zero do corpo $\mathbb{K}$, então G é um grupo cíclico.

Demonstração: Essa demonstração deste teorema pode encontrada em [3].

Definição 2.2.3. Se α sobre $\mathbb{K}$ é algébrico sobre $\mathbb{F}$, então o polinômio mônico unicamente determinado $g(x) \in \mathbb{K}[x]$ que gera o ideal $J = \{f(x) \in \mathbb{K}[x]; f(\alpha) = 0\}$ de $\mathbb{K}[x]$ é chamado de *polinômio minimal* ou *polinômio irredutível* de α *sobre* $\mathbb{K}$. Pelo grau de α sobre $\mathbb{K}$ temos o grau de $g(x)$.

CAPÍTULO 3 - CORPOS DE ORDEM p^2

Nesse capítulo, será apresentado um processo de construção dos corpos de ordem potência de primo, representando seus elementos por matrizes simétricas, tais corpos são extensões algébricas do corpo primo $\mathbb{F}_p = \mathbb{Z}_p$. Uma vez que $\mathbb{K}$ é uma extensão algébrica de $\mathbb{F}_p$, sabemos que o grupo multiplicativo $\mathbb{K}^*$ é gerado por um elemento $\alpha \in \mathbb{K}$. Como o objetivo do nosso trabalho é estabelecer uma representação matricial dos elementos de um corpo finito a partir do grau da extensão, um desafio foi escolher o tipo de matriz quadrada sobre o corpo primo $\mathbb{F}_p$. No entanto, diante de várias observações conclui-se que as matrizes simétricas são as mais adequadas para desenvolver a teoria, porém, notou-se que para cada ordem a disposição das entradas são unicamente estabelecidas.

Neste trabalho, vamos criar um método para obter os elementos na forma matricial de corpos com ordem p^2, isto é, utilizaremos matrizes simétricas de ordem 2×2. Após algumas investigações, percebemos que um modelo mais adequado tem o seguinte formato:

$$\begin{pmatrix} a & b \\ b & a + nb \end{pmatrix},$$

onde a, b e $n \in \mathbb{F}_p$.

Para estabelecer as condições necessárias para descrever o processo, veremos, a seguir, algumas definições e resultados que são importantes na construção das extensões algébricas.

Observação 3.1. O *grupo multiplicativo* de $\mathbb{F}_p$ é denotado por $\mathbb{F}_p^*$.

Definição 3.2. O gerador do grupo cíclico $\mathbb{F}_p^*$ é chamado $elemento\ primitivo$ de $\mathbb{F}_p$.

Exemplo 3.2. O elemento primitivo do corpo finito $\mathbb{F}_3$ é o 2, pois o 2 gera $\mathbb{F}_3^*$, veja $\mathbb{F}_3^* = \{2^1 = 2, 2^2 = 4 \equiv 1\}$.

Exemplo 3.3. O corpo finito $\mathbb{F}_5$ possui dois elementos primitivos que são o 2 e o 3, ambos os elementos geram o grupo multiplicativo $\mathbb{F}_5^*$. Vejamos os grupos gerados pelo 2 e pelo 3 respectivamente,

$$\mathbb{F}_5^* = \{2^1 = 2, 2^2 = 4, 2^3 \equiv 3, 2^4 \equiv 1\}$$

$$\mathbb{F}_5^* = \{3^1 = 3, 3^2 \equiv 4, 3^3 \equiv 2, 3^4 \equiv 1\}.$$

Definição 3.3. Para $\alpha \in \mathbb{K} = \mathbb{F}_{p^m}$ e $\mathbb{F} = \mathbb{F}_p$, a $norma$, $N_{\frac{\mathbb{K}}{\mathbb{F}}}(\alpha)$, e o $traço$, $Tr_{\frac{\mathbb{K}}{\mathbb{F}}}(\alpha)$, de α sobre $\mathbb{K}$ são definidos, respectivamente, por:

i) $N_{\frac{\mathbb{K}}{\mathbb{F}}}(\alpha) = \alpha\alpha^q \dots \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}$;

ii) $Tr_{\frac{\mathbb{K}}{\mathbb{F}}}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}$.

Definição 3.4. Sejam $\mathbb{F}$ corpo finito e $\mathbb{K}$ uma extensão finita de $\mathbb{F}$. Então as duas bases $\{\alpha_1, \dots, \alpha_m\}$ e $\{\beta_1, \dots, \beta_m\}$ de $\mathbb{K}$ sobre $\mathbb{F}$ são ditas *bases duais* (ou *complementares*) se para $1 \leq i, j \leq m$, temos

$$Tr_{\frac{\mathbb{K}}{\mathbb{F}}}(\alpha_i\beta_j) = \begin{cases} 0, & se\ i \neq j \\ 1, & se\ i = j \end{cases}.$$

Definição 3.5. um polinômio $f(x) \in \mathbb{F}_p[x]$, de grau $n \geq 1$, é chamado $polinomio\ primitivo$ sobre $\mathbb{F}_p$, se for o polinômio minimal sobre $\mathbb{F}_p$ de um elemento primitivo de $\mathbb{F}_{p^n}$.

Teorema 3.1. Um polinômio $f(x) \in \mathbb{F}_p[x]$ de grau m é um polinômio primitivo $\mathbb{F}_p[x]$ se, e somente se, $f(x)$ é mônico, $f(0) \neq 0$, e $ord(f) = p^m - 1$.

Demonstração: A demonstração deste teorema pode ser encontrada em [5].

Corolário 3.1. Se $f(x) \in \mathbb{F}_p[x]$ é um polinômio irredutível sobre $\mathbb{F}_p$ de grau m, então $ord(f)$ divide $p^m - 1$.

Demonstração: A demonstração deste lema pode ser encontrada em [5].

Lema 3.1. Seja $c \in \mathbb{Z}_+$, onde $\mathbb{Z}_+$ é o conjunto dos inteiros não negativos. Então, o polinômio $f(x) \in \mathbb{F}_p[x]$ com $f(0) \neq 0$ divide $x^c - 1$, se e somente se, $ord(f)$ divide c.

Demonstração: A demonstração deste lema pode ser encontrada em [5].

Lema 3.2. Seja $f \in \mathbb{F}_p[x]$ um polinômio de grau positivo com $f(0) \neq 0$. Seja r o menor inteiro positivo para o qual x^r é congruente a algum elemento de $\mathbb{F}_p$ módulo $f(x)$, de modo que $x^r \equiv a\ mod\ f(x)$, sendo $a \in \mathbb{F}_p^*$ unicamente determinado. Então $ord\big(f(x)\big) = hr$, onde h é a ordem, de a no grupo multiplicativo $\mathbb{F}_p^*$.

Demonstração: A demonstração deste lema pode ser encontrada em [5].

Podemos escrever um polinômio primitivo sobre $\mathbb{F}_p$, de grau m, como um polinômio mônico sobre $\mathbb{F}_p$ que é irredutível e tem uma raiz em $\mathbb{F}_{p^n}$, e, por sua vez, essa raiz gera o grupo multiplicativo de $\mathbb{F}_{p^n}$. Vejamos como os polinômios primitivos podem ser caracterizados

Teorema 3.2. O polinômio mônico $f \in \mathbb{F}_p[x]$, de grau $n \geq 1$, é um polinômio primitivo sobre $\mathbb{F}_p$ se, e somente se, $(-1)^n f(0)$ é um elemento primitivo de $\mathbb{F}_p$ e o menor inteiro positivo r para o qual x^r é congruente a algum elemento de $\mathbb{F}_p$ módulo $f(x)$ é

$$r = \frac{(p^n - 1)}{(p - 1)}.$$

No caso em que $f(x)$ é primitivo sobre $\mathbb{F}_p$, temos

$$x^r \equiv (-1)^n f(0)\ mod\ f(x).$$

Os teoremas, lemas e proposições usados na demonstração abaixo podem ser encontrados em [5]**.**

Demonstração: Se $f(x)$ é primitivo sobre $\mathbb{F}_p$, então f tem uma raiz $\alpha \in \mathbb{F}_{p^n}$ que é um elemento primitivo de $\mathbb{F}_{p^n}$. Calculando a norma de $N_{\frac{\mathbb{F}_{p^n}}{\mathbb{F}_p}}(\alpha)$, pelas Definições 3.3 e 3.4**,** e observando que f é o polinômio característico de α sobre $\mathbb{F}_p$, chegamos à identidade $(-1)^n f(0) \equiv \alpha^{(p^n-1)/(p-1)}$. (3.2) Segue que a ordem de $(-1)^n f(0)$ em $\mathbb{F}_p^*$ é $p - 1$, logo, $(-1)^n f(0)$ é um elemento primitivo de $\mathbb{F}_p$. Uma vez, que f é o polinômio minimal de α sobre $\mathbb{F}_p$, a identidade (3.2) implica que

$$x^{(p^n-1)/(p-1)} \equiv (-1)^n f(0)\ \big(mod f(x)\big).$$

E, assim, $r \leq (p^n - 1)/(p - 1)$. Mas pelo Teorema 3.1 e Lema 3.2, temos que

$$p^n - 1 = ord(f(x)) \leq (p - 1)r,$$

logo

$$r \geq \frac{p^n - 1}{p - 1}.$$

Portanto,

$$r = \frac{p^n - 1}{p - 1}.$$

Reciprocamente, suponha que as condições do teorema sejam satisfeitas. Segue que

$$r = \frac{p^n - 1}{p - 1}$$

e pelo Lema 3.2**,** temos que a $ord(f)$ é relativamente prima com p. Então, o Teorema 3.11, em [5], mostra que f pode ser fatorado na forma $f = f_1 \dots f_k$, onde os f_i são polinômios mônicos distintos irredutíveis sobre $\mathbb{F}_p$ se $n_i = gr(f_i)$. Logo, $ord(f_i)$ divide $p^{n_i} - 1$, para $1 \leq i \leq k$, de acordo com o Corolário 3.1. Agora, $p^{n_i} - 1$ divide

$$d = (p^{n_i} - 1) \dots (p^{n_i} - 1)/(p - 1)^{k-1}.$$

Então, $ord(f_i)$ divide d, para $1 \leq i \leq k$. E, assim, pelo Lema 3.1, tem-se que $f(x)$ divide $x^d - 1$, para $1 \leq i \leq k$ e assim, $f(x)$ divide $x^d - 1$. Se $k \geq 2$, então

$$d < \frac{p^{n_1 + \dots + n_k} - 1}{p - 1} = \frac{p^n - 1}{p - 1} = r,$$

Contradizendo a definição de r. Portanto, $k = 1$ e f é irredutível sobre $\mathbb{F}_p$.

Se $\beta \in \mathbb{F}_{p^n}$ é uma raiz de f, segue, pelo argumento principal (3.2), que

$$\beta^r = (-1)^n f(0),$$

e assim, temos

$$x^r \equiv (-1)^n f(0) \ (mod f(x)).$$

Uma vez que, a ordem de $(-1)^n f(0)$ em $\mathbb{F}_p^*$ é $p - 1$, resulta, pelo Lema 3.2, que $ord(f) = p^n - 1$. Deste modo pelo Teorema 3.1. f é primitivo sobre $\mathbb{F}_p$.

Exemplo 3.4. Dada a matriz $A = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$, com entradas em $\mathbb{F}_3$, verifique se o polinômio característico de A é primitivo em $\mathbb{F}_3$.

Pela Definição 1.2.8, temos que o polinômio característico de A é dado por

$$f(x) = \det(A - xI) =$$

$$det \begin{pmatrix} 0 - x & 1 \\ 1 & 2 - x \end{pmatrix} =$$

$$det \begin{pmatrix} -x & 1 \\ 1 & 2 - x \end{pmatrix} =$$

$$-x.(2-x)-1=$$

$$x^2-2x-1.$$

Logo, $f(x)=x^2-2x-1$. Como $f(x)\in\mathbb{F}_3[x]$, tem-se que seus coeficientes estão em $\mathbb{F}_3$,daí

$$f(x)=x^2-2x-1\equiv x^2+x+2.$$

Portanto, o polinômio característico de A é $f(x)=x^2+x+2$. Note que $f(x)$ é mônico.

Agora pela Definição 1.2.10, veremos se $f(x)$ é minimal. Vejamos:

$$f(A)=A^2+A+2I=\begin{pmatrix}0&1\\1&2\end{pmatrix}^2+\begin{pmatrix}0&1\\1&2\end{pmatrix}+\begin{pmatrix}2&0\\0&2\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}.$$

Portanto, $f(x)$ é minimal de A.

Agora, veremos se o polinômio $f(x)\in\mathbb{F}_3[x]$ satisfaz o Teorema 3.2, ou seja, veremos se $f(x)$ satisfaz a seguinte congruência

$$x^{\frac{p^n-1}{p-1}}\equiv(-1)^n f(0)\ (mod f(x))\Rightarrow$$

$$x^{\frac{3^2-1}{3-1}}\equiv(-1)^2.2(\ mod(x^2+x+2))\Rightarrow$$

$$x^4\equiv 2\ (mod(x^2+x+2))\Leftrightarrow$$

$$(x^2+x+2)|x^4-2$$

Como $x^4-2=\ (x^2+x+2).(x^2-x-1)+3x$ temos que $(x^2+x+2)|x^4-2$, pois, $3x\equiv 0\ (mod\ 3)$. Concluímos que $f(x)=x^2+x+2$ é o polinômio primitivo.

3.1 PROCESSO PARA CRIAÇÃO DE CORPOS DE ORDEM p^2.

A partir de todos os resultados e definições vistos até aqui, foi possível estabelecer um processo para obter a representação matricial de um corpo de ordem p^n. Mesmo que a matriz utilizada para obter corpos de ordem p^2 tenha sido obtida através de experimentação, notou-se que este tipo de matriz é eficaz no processo de criação dos corpos de ordem p^2 menores que 121.

Passo 1: Escolher o valor do primo p para determinar o corpo $\mathbb{F}_p$ que deseja estender.

Passo 2: Escolher os valores de $a, b, n \in \mathbb{F}_P$ para determinar uma matriz simétrica $A = \begin{pmatrix} a & b \\ b & a+nb \end{pmatrix} \in \mathbb{M}_2(\mathbb{F}_p)$, onde o determinante de A seja o $elemento\ primitivo\ de\ \mathbb{F}_p$.

Passo 3: Calcular o polinômio característico $f(x) \in \mathbb{F}_p[x]$ da matriz A, ou seja,

$$f(x) = \det(A - xI).$$

Passo 4: Verificar se $p+1$ é o menor inteiro positivo que satisfaz a seguinte congruência

$$x^{p+1} \equiv (-1)^2 f(0)\ \big(mod f(x)\big).$$

(Caso o passo 4 tenha falhado, escolha uma nova matriz e refaça todos os passos até obter sucesso).

Passo 5: Calcular as potências de A para determinar o grupo multiplicativo

$$\mathbb{F}_{p^2}^* = \{A, A^2, \dots, A^{p^2-1}\}.$$

Passo 6: Acrescentar o $elemento\ neutro$ da adição das matrizes ao grupo multiplicativo $\mathbb{F}_{p^2}^*$. Note que, $\mathbb{F}_{p^n}$ é uma representação matricial do corpo de ordem p^2 cujo os elementos são: $0, I, A, A^2, \dots, A^{p^2-2}$.

Exemplo 3.1.1. Determinar a representação matricial do corpo de ordem 25.

Para determinar essa representação matricial, vamos utilizar o processo visto anteriormente.

Passo 1: Para determinar o corpo de ordem 25, vamos estender o corpo primo $\mathbb{F}_5$, ou seja, usaremos $p = 5$.

Passo 2: Determinar uma matriz simétrica $C = \begin{pmatrix} a & b \\ b & a+nb \end{pmatrix} \in \mathbb{M}_2(\mathbb{F}_p)$, onde o determinante de A seja o $elemento\ primitivo\ de\ \mathbb{F}_p$. Utilizaremos a matriz

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} \in \mathbb{M}_2(\mathbb{F}_5),$$

Note que, $\det C = 3 - 1 = 2$, e 2 é um elemento primitivo de $\mathbb{F}_5$.

Passo 3: Vamos calcular o polinômio característico $f(x) \in \mathbb{F}_5[x]$ da matriz A que é dado por $f(x) = \det(C - xI)$. Veja

$$f(x) = \det(C - xI) =$$

$$\det\left(\begin{pmatrix}1 & 1\\ 1 & 3\end{pmatrix} - \begin{pmatrix}x & 0\\ 0 & x\end{pmatrix}\right) =$$

$$\det\begin{pmatrix}1-x & 1\\ 1 & 3-x\end{pmatrix} =$$

$$(1-x)(3-x) - 1 =$$

$$x^2 - 3x - x + 3 - 1 =$$

$$x^2 - 4x + 2.$$

Logo, $f(x) = x^2 - 4x + 2$. Como $f(x) \in \mathbb{F}_5[x]$, tem-se que seus coeficientes estão em $\mathbb{F}_5$,daí

$$f(x) = x^2 - 4x + 2 \equiv x^2 + x + 2.$$

Portanto, o polinômio característico de C é $f(x) = x^2 + x + 2$.

Passo 4: Verificar se $p + 1$, ou seja, $5 + 1 = 6$ é o menor inteiro positivo que satisfaz a seguinte congruência

$$x^6 \equiv (-1)^2 f(0)\ (mod(x^2 + x + 2)).$$

veja que esse polinômio é mônico e que satisfaz a congruência

$$x^6 \equiv (-1)^2 f(0)\ \big(mod(x^2 + x + 2)\big),$$

pois, fazendo $f(x) = 0$, e isolando o monômio de maior grau, temos:

$$x^2 + x + 2 = 0 \Rightarrow x^2 = -x - 2 \equiv 4x + 3$$

Assim, $x^2 = 4x + 3$. Agora, vamos calcular as potências de x utilizando essa igualdade. Veja:

$$x^3 = x.x^2 = 4x^2 + 3x = 4(4x + 3) + 3x = 16x + 12 + 3x \equiv 4x + 2$$

$$x^4 = x.x^3 = 4x^2 + 2x = 4(4x + 3) + 2x = 16x + 12 + 2x \equiv 3x + 2$$

$$x^5 = x.x^4 = 3x^2 + 2x = 3(4x + 3) + 2x = 12x + 9 + 2x \equiv 4x + 4$$

$$x^6 = x.x^5 = 4x^2 + 4x = 4(4x + 3) + 4x = 16x + 12 + 4x \equiv 2.$$

Desta última igualdade, concluímos que $x^6 \equiv 2\ mod(x^2 + x + 2)$ e $r = 6$ é o menor inteiro para o qual a congruência é válida. Portanto, $f(x) = x^2 + x + 2$ é primitivo em $\mathbb{F}_5$ e, com isso, constatamos que $f(x) = x^2 + x + 2$ gera o grupo multiplicativo de ordem 24, como ele é associado a matriz C, temos que C é um elemento primitivo, portanto, também gera o grupo $\mathbb{F}_{25}^*$.

Passo 5: Calcular as potências de C e determinar o grupo $\mathbb{F}_{25}^* = \{C, C^2, \dots, C^{24}\}$.

Passo 6: Acrescentar o elemento neutro da adição das matrizes ao grupo $\mathbb{F}_{25}^*$.

Feito isso, obtermos a representação matricial do corpo de ordem 25 que é formado por $\mathbb{F}_{25} = \{0, I, C, C^2, \dots, C^{23}\}$. Veja a tabela 3 com os elementos deste corpo e suas ordens.

3.2 CORPOS DE ORDEM p^2 MENORES QUE 121.

Nesta secção, veremos exemplos da representação dos corpos que foram construídos utilizando o processo da secção anterior, grande parte dos cálculos serão ocultados, pois, o objetivo da secção é mostrar como são as representações matriciais dos elementos desse corpo.

Para construir o corpo de ordem $4 = 2^2$, vamos estender o corpo $\mathbb{F}_2$ utilizando o processo visto na seção anterior. A matriz utilizada para isso é a matriz $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{M}_2(\mathbb{F}_2)$, note que $\det A = -1 \equiv 1\ mod\ 2$, e que 1 é o elemento primitivo de $\mathbb{F}_2$. O polinômio característico de A é dado por

$$f(x) = \det(A - xI) =$$

$$det\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} - x\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) =$$

$$det\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\right) =$$

$$det\begin{pmatrix} 1-x & 1 \\ 1 & -x \end{pmatrix} =$$

$$(1 - x)(-x) - 1 =$$

$$x^2 - x - 1.$$

Portanto o polinômio característico da matriz A é $f(x) = x^2 - x - 1$.

Temos que o polinômio satisfaz a congruência $x^3 \equiv 1\ (mod f(x))$, pois, fazendo $f(x) = 0$. Temos:

$$x^2 - x - 1 = 0 \Rightarrow x^2 = x + 1.$$

Assim,

$$x^3 = x.x^2 = x^2 + x = (x + 1) + x = 2x + 1 \equiv 1.$$

Portanto, $x^3 \equiv 1$.

Logo, o polinômio $f(x)$ é primitivo e possui uma raiz em $\mathbb{F}_4$ que é o elemento primitivo de $\mathbb{F}_4^*$. Este elemento é a matriz A, assim, a matriz A gera o grupo multiplicativo $\mathbb{F}_4^* = \{I, A, A^2\}$. Acrescentando o elemento neutro da adição ao grupo temos o corpo $\mathbb{F}_4 = \{0, I, A, A^2\}$. Veja a tabela abaixo com os elementos e suas ordens.

Tabela 1 - Elementos do corpo $\mathbb{F}_4$		
A	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	Ordem 3
A^2	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	Ordem 3
$A^3 = I$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	Ordem 1
0	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	

No caso do corpo de ordem $9 = 3^2$, vamos estender o corpo $\mathbb{F}_3$. A matriz utilizada para isso é a matriz $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{M}_2(\mathbb{F}_3)$. Note que, $\det B = -1 \equiv 2\ mod\ 3$, e que 2 é o elemento primitivo de $\mathbb{F}_3$. O polinômio característico de B é dado por

$$f(x) = x^2 - x - 1.$$

Temos que o polinômio satisfaz a congruência $x^4 \equiv 2\ (mod f(x))$, pois, fazendo $f(x) = 0$. Temos:

$$x^2 - x - 1 = 0 \Rightarrow x^2 = x + 1.$$

Assim,

$$x^3 = x.x^2 = x^2 + x = (x+1) + x = 2x + 1.$$

$$x^4 = x.x^3 = 2x^2 + x = 2.(x+1) + x = 3x + 2 \equiv 2.$$

Portanto, $x^4 \equiv 2$.

Logo, o $f(x)$ é primitivo. Portanto, a matriz B gera o grupo multiplicativo

$$\mathbb{F}_9^* = \{ I, B, B^2, B^3, B^4, B^5, B^6, B^7\}.$$

Acrescentando o elemento neutro da adição ao grupo temos o corpo

$$\mathbb{F}_9 = \{0, I, B, B^2, B^3, B^4, B^5, B^6, B^7\}.$$

Veja a tabela abaixo com os elementos e suas ordens.

Tabela 2 - Elementos do corpo $\mathbb{F}_9$		
B	$\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$	Ordem 8
B^2	$\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}$	Ordem 4
B^3	$\begin{pmatrix}0 & 2\\ 2 & 1\end{pmatrix}$	Ordem 8
B^4	$\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$	Ordem 2
B^5	$\begin{pmatrix}2 & 2\\ 2 & 0\end{pmatrix}$	Ordem 8
B^6	$\begin{pmatrix}1 & 2\\ 2 & 2\end{pmatrix}$	Ordem 4
B^7	$\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}$	Ordem 8
$B^8 = I$	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	Ordem 1
0	$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$	

Vejamos, agora, a tabela com os elementos do corpo $\mathbb{F}_{25} = \{0, I, C, C^2, \dots, C^{23}\}$, o passo-a-passo da criação desse corpo pode ser vista no Exemplo 3.1.1, da seção anterior.

Tabela 3 - Elementos do corpo $\mathbb{F}_{25}$

C	$\begin{pmatrix}1 & 1\\1 & 3\end{pmatrix}$	Ordem 24
C^2	$\begin{pmatrix}2 & 4\\4 & 0\end{pmatrix}$	Ordem 12
C^3	$\begin{pmatrix}1 & 4\\4 & 4\end{pmatrix}$	Ordem 8
C^4	$\begin{pmatrix}0 & 3\\3 & 1\end{pmatrix}$	Ordem 6
C^5	$\begin{pmatrix}3 & 4\\4 & 1\end{pmatrix}$	Ordem 24
C^6	$\begin{pmatrix}2 & 0\\0 & 2\end{pmatrix}$	Ordem 4
C^7	$\begin{pmatrix}2 & 2\\2 & 1\end{pmatrix}$	Ordem 24
C^8	$\begin{pmatrix}4 & 3\\3 & 0\end{pmatrix}$	Ordem 3
C^9	$\begin{pmatrix}2 & 3\\3 & 3\end{pmatrix}$	Ordem 8
C^{10}	$\begin{pmatrix}0 & 1\\1 & 2\end{pmatrix}$	Ordem 12
C^{11}	$\begin{pmatrix}1 & 3\\3 & 2\end{pmatrix}$	Ordem 24
C^{12}	$\begin{pmatrix}4 & 0\\0 & 4\end{pmatrix}$	Ordem 2
C^{13}	$\begin{pmatrix}4 & 4\\4 & 2\end{pmatrix}$	Ordem 24
C^{14}	$\begin{pmatrix}3 & 1\\1 & 0\end{pmatrix}$	Ordem 12
C^{15}	$\begin{pmatrix}4 & 1\\1 & 1\end{pmatrix}$	Ordem 8
C^{16}	$\begin{pmatrix}0 & 2\\2 & 4\end{pmatrix}$	Ordem 3
C^{17}	$\begin{pmatrix}2 & 1\\1 & 4\end{pmatrix}$	Ordem 24
C^{18}	$\begin{pmatrix}3 & 0\\0 & 3\end{pmatrix}$	Ordem 4
C^{19}	$\begin{pmatrix}3 & 3\\3 & 4\end{pmatrix}$	Ordem 24
C^{20}	$\begin{pmatrix}1 & 2\\2 & 0\end{pmatrix}$	Ordem 6
C^{21}	$\begin{pmatrix}3 & 2\\2 & 2\end{pmatrix}$	Ordem 8
C^{22}	$\begin{pmatrix}0 & 4\\4 & 3\end{pmatrix}$	Ordem 12

C^{23}	$\begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}$	Ordem 24
$C^{24} = I$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	Ordem 1
0	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	

Por fim, para construir o corpo de ordem $49 = 7^2$, vamos estender o corpo $\mathbb{F}_7$ utilizando o processo que foi mostrado na seção anterior. A matriz utilizada para isso é a matriz $D = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix} \in \mathbb{M}_2(\mathbb{F}_7)$. Note que,

$$\det D = 4 - 1 = 3,$$

e que 3 é o elemento primitivo de $\mathbb{F}_7$. O polinômio característico de D é dado por

$$f(x) = x^2 - 5x + 3.$$

Temos que o polinômio satisfaz a congruência $x^8 \equiv 3\ (mod f(x))$, pois, fazendo $f(x) = 0$. Temos:

$$x^2 - 5x + 3 = 0 \Rightarrow x^2 = 5x - 3 \equiv 5x + 4\ mod\ 7.$$

Assim,

$$x^3 = x.x^2 = 5x^2 + 4x = 5(5x + 4) + 4x = 25x + 20 + 4x = 29x + 20 \equiv x + 6,$$

$$x^4 = x.x^3 = x^2 + 6x = 5x + 4 + 6x = 11x + 4 \equiv 4x + 4.$$

Fazendo agora $x^4.x^4$, temos:

$$x^8 = x^4.x^4 = (4x + 4)(4x + 4) =$$

$$16x^2 + 32x + 16 \equiv 2x^2 + 4x + 2 =$$

$$2(5x + 4) + 4x + 2 =$$

$$10x + 8 + 4x + 2 =$$

$$14x + 10 \equiv 3.$$

Portanto, $x^8 \equiv 3$. Logo, o polinômio $f(x)$ é primitivo e a matriz D, também. Assim, a matriz D gera o grupo multiplicativo $\mathbb{F}_{49}^* = \{ I, D, D^2, \dots, D^{47}\}$. Acrescentando

o elemento neutro da adição ao grupo temos o corpo $\mathbb{F}_{49} = \{0, I, D, D^2, \dots, D^{46}, D^{47}\}$. Veja a tabela abaixo com os elementos e suas ordens.

Tabela 4 - Elementos do corpo $\mathbb{F}_{49}$.		
D	$\begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}$	Ordem 48
D^2	$\begin{pmatrix} 2 & 5 \\ 5 & 3 \end{pmatrix}$	Ordem 24
D^3	$\begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix}$	Ordem 16
D^4	$\begin{pmatrix} 1 & 4 \\ 4 & 6 \end{pmatrix}$	Ordem 12
D^5	$\begin{pmatrix} 5 & 3 \\ 3 & 0 \end{pmatrix}$	Ordem 48
D^6	$\begin{pmatrix} 1 & 3 \\ 3 & 3 \end{pmatrix}$	Ordem 8
D^7	$\begin{pmatrix} 4 & 6 \\ 6 & 1 \end{pmatrix}$	Ordem 48
D^8	$\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$	Ordem 6
D^9	$\begin{pmatrix} 3 & 3 \\ 3 & 5 \end{pmatrix}$	Ordem 16
D^{10}	$\begin{pmatrix} 6 & 1 \\ 1 & 2 \end{pmatrix}$	Ordem 24
D^{11}	$\begin{pmatrix} 0 & 3 \\ 3 & 2 \end{pmatrix}$	Ordem 48
D^{12}	$\begin{pmatrix} 3 & 5 \\ 5 & 4 \end{pmatrix}$	Ordem 4
D^{13}	$\begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$	Ordem 48
D^{14}	$\begin{pmatrix} 3 & 2 \\ 2 & 2 \end{pmatrix}$	Ordem 24
D^{15}	$\begin{pmatrix} 5 & 4 \\ 4 & 3 \end{pmatrix}$	Ordem 16
D^{16}	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	Ordem 3
D^{17}	$\begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$	Ordem 48
D^{18}	$\begin{pmatrix} 4 & 3 \\ 3 & 6 \end{pmatrix}$	Ordem 6

D^{19}	$\begin{pmatrix} 0 & 2 \\ 2 & 6 \end{pmatrix}$	Ordem 48
D^{20}	$\begin{pmatrix} 2 & 1 \\ 1 & 5 \end{pmatrix}$	Ordem 12
D^{21}	$\begin{pmatrix} 3 & 6 \\ 6 & 0 \end{pmatrix}$	Ordem 16
D^{22}	$\begin{pmatrix} 2 & 6 \\ 6 & 6 \end{pmatrix}$	Ordem 24
D^{23}	$\begin{pmatrix} 1 & 5 \\ 5 & 2 \end{pmatrix}$	Ordem 48
D^{24}	$\begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	Ordem 2
D^{25}	$\begin{pmatrix} 6 & 6 \\ 6 & 3 \end{pmatrix}$	Ordem 48
D^{26}	$\begin{pmatrix} 5 & 2 \\ 2 & 4 \end{pmatrix}$	Ordem 24
D^{27}	$\begin{pmatrix} 0 & 6 \\ 6 & 4 \end{pmatrix}$	Ordem 16
D^{28}	$\begin{pmatrix} 6 & 3 \\ 3 & 1 \end{pmatrix}$	Ordem 12
D^{29}	$\begin{pmatrix} 2 & 4 \\ 4 & 0 \end{pmatrix}$	Ordem 48
D^{30}	$\begin{pmatrix} 6 & 4 \\ 4 & 4 \end{pmatrix}$	Ordem 8
D^{31}	$\begin{pmatrix} 3 & 1 \\ 1 & 6 \end{pmatrix}$	Ordem 48
D^{32}	$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$	Ordem 3
D^{33}	$\begin{pmatrix} 4 & 4 \\ 4 & 2 \end{pmatrix}$	Ordem 16
D^{34}	$\begin{pmatrix} 1 & 6 \\ 6 & 5 \end{pmatrix}$	Ordem 24
D^{35}	$\begin{pmatrix} 0 & 4 \\ 4 & 5 \end{pmatrix}$	Ordem 48
D^{36}	$\begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}$	Ordem 4
D^{37}	$\begin{pmatrix} 6 & 5 \\ 5 & 0 \end{pmatrix}$	Ordem 48
D^{38}	$\begin{pmatrix} 4 & 5 \\ 5 & 5 \end{pmatrix}$	Ordem 24
D^{39}	$\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$	Ordem 16
D^{40}	$\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$	Ordem 6

D^{41}	$\begin{pmatrix} 5 & 5 \\ 5 & 6 \end{pmatrix}$	Ordem 48
D^{42}	$\begin{pmatrix} 3 & 4 \\ 4 & 1 \end{pmatrix}$	Ordem 8
D^{43}	$\begin{pmatrix} 0 & 5 \\ 5 & 1 \end{pmatrix}$	Ordem 48
D^{44}	$\begin{pmatrix} 5 & 6 \\ 6 & 2 \end{pmatrix}$	Ordem 12
D^{45}	$\begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix}$	Ordem 16
D^{46}	$\begin{pmatrix} 5 & 1 \\ 1 & 1 \end{pmatrix}$	Ordem 24
D^{47}	$\begin{pmatrix} 6 & 2 \\ 2 & 5 \end{pmatrix}$	Ordem 48
$D^{48} = I$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	Ordem 1
0	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	

3.3 ALGUNS EXEMPLOS DE CORPOS COM ORDEM p^3

Agora, vejamos alguns exemplos de corpos com ordem p^3. Para criar os corpos de ordem p^3 utilizaremos uma matriz simétrica de ordem 3x3, visto que a ordem está relacionada com o grau da extensão, a matriz utilizada possui o seguinte formato:

$$\begin{pmatrix} a & a+c & a+b+2c \\ a+c & b & b+c \\ a+b+2c & b+c & c \end{pmatrix},$$

onde $a = b \; ou \; a \neq c$ são elementos do corpo primo $\mathbb{F}_p$, que está sendo estendido. Esse modelo de matriz apresentado foi obtido através de experimentação e testes.

Exemplo 3.3.1. Representação matricial do corpo de ordem 8.

Para construir o corpo de ordem $8 = 2^3$, vamos estender o corpo $\mathbb{F}_2$. A matriz utilizada para isso é a matriz $E = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in \mathbb{M}_3(\mathbb{F}_2)$. Note que,

$$\det E = -1 \equiv 1 \; mod \; 2,$$

e que 1 é o elemento primitivo de $\mathbb{F}_2$. O polinômio característico de E é dado por $f(x) = x^3 - 2x^2 + 3x - 1 \equiv x^3 + x - 1$, ou seja, $f(x) = x^3 + x - 1$.

Temos que o polinômio satisfaz o Teorema 3.2, ou seja, satisfaz a congruência

$$x^7 \equiv 1\ (mod f(x)),$$

pois, fazendo $f(x) = 0$. Temos:

$$x^3 + x - 1 = 0 \Rightarrow x^3 = -x + 1 \equiv x + 1$$

Assim, fazendo agora $x^6 = x^3.x^3$, temos:

$$x^6 = x^3.x^3 = (x+1)(x+1) =$$

$$x^2 + 2x + 1 \equiv x^2 + 1.$$

Logo,

$$x^7 = x.x^6 = x^3 + x = x + 1 + x = 2x + 1 \equiv 1.$$

Portanto $x^7 \equiv 1$. Logo, o polinômio $f(x)$ é primitivo, e a matriz E também. Assim, a matriz E gera o grupo multiplicativo $\mathbb{F}_7^* = \{ I, E, E^2, \dots, E^6\}$. Acrescentando o elemento neutro da adição ao grupo temos o corpo $\mathbb{F}_8 = \{0, I, E, E^2, \dots, E^6\}$. Veja a tabela abaixo com os elementos e suas ordens.

Tabela 5 - Elementos do Corpo $\mathbb{F}_8$		
E	$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	Ordem 7
E^2	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$	Ordem 7
E^3	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$	Ordem 7
E^4	$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$	Ordem 7
E^5	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	Ordem 7
E^6	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$	Ordem 7

$E^7 = I$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	Ordem 1
0	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	

Exemplo 3.3.2. Corpo de ordem 27.

Para construir o corpo de ordem $27 = 3^3$, vamos estender o corpo $\mathbb{F}_3$. A matriz utilizada para isso é a matriz $G = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in \mathbb{M}_3(\mathbb{F}_3)$. Note que, $\det E = -1 \equiv 2$, e que 2 é o elemento primitivo de $\mathbb{F}_3$. O polinômio característico de G é dado por

$$f(x) = x^3 - 2x^2 + 3x - 1$$

Como $f(x) \in \mathbb{F}_3[x]$, temos que

$$f(x) = x^3 - 2x^2 + 3x - 1 \equiv x^3 + x^2 - 1,$$

ou seja,

$$f(x) = x^3 + x^2 - 1.$$

Temos que o polinômio satisfaz o Teorema 3.2, ou seja, satisfaz a congruência $x^7 \equiv 1\ (mod f(x))$, pois, fazendo $f(x) = 0$. Temos:

$$x^3 + x^2 - 1 = 0 \Rightarrow x^3 = -x^2 + 1 \equiv 2x^2 + 1,$$

Agora fazendo,

$$x^4 = x.x^3 =$$

$$x(2x^2 + 1) =$$

$$2x^3 + x,$$

Como $x^3 = 2x^2 + 1$, tem-se

$$2x^3 + x =$$

$$2.(2x^2 + 1) + x =$$

$$4x^2 + x + 2 \equiv x^2 + x + 2 \ (mod\ 3).$$

Assim,

$$x^6 = x^3.x^3 = (2x^2 + 1)(2x^2 + 1) =$$

$$2x^2 + x + 3 \equiv 2x^2 + x, (mod\ 3).$$

Logo,

$$x^{12} = x^6.x^6 = (2x^2 + x)(2x^2 + x) =$$

$$4x^4 + 4x^3 + x^2 \equiv x^4 + x^3 + x^2.$$

Por outro lado, utilizando as potências de x^3 e x^4 vistas acima. Temos:

$$x^4 + x^3 + x^2 =$$

$$(x^2 + x + 2) + (2x^2 + 1) + x^2 =$$

$$4x^2 + x + 3 \equiv x^2 + x \ (mod\ 3).$$

Assim, chegamos a seguinte congruência:

$$x^{12} \equiv x^2 + x \ \ (mod\ 3),$$

Daí, temos que,

$$x^{13} = x.x^{12} =$$

$$x(x^2 + x) =$$

$$x^3 + x^2 =$$

$$2x^2 + 1 + x^2 \equiv 1.$$

Portanto, $x^{13} \equiv 1$. Logo, o polinômio $f(x)$ é primitivo, e a matriz G também. Assim, a matriz G gera o grupo multiplicativo $\mathbb{F}_{26}^{*} = \{ I, G, G^2, \dots, G^{25}\}$. Acrescentando o elemento neutro da adição ao grupo temos o corpo $\mathbb{F}_{27} = \{0, I, G, G^2, \dots , G^{25} \}$. Veja a tabela abaixo com os elementos e suas ordens.

Tabela 6 - Elementos do corpo $\mathbb{F}_{27}$		
G	$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	Ordem 26

G^2	$\begin{pmatrix} 2 & 2 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$	Ordem 13
G^3	$\begin{pmatrix} 1 & 1 & 2 \\ 2 & 0 & 0 \\ 2 & 0 & 1 \end{pmatrix}$	Ordem 26
G^4	$\begin{pmatrix} 0 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 0 \end{pmatrix}$	Ordem 13
G^5	$\begin{pmatrix} 2 & 1 & 2 \\ 1 & 1 & 2 \\ 2 & 2 & 0 \end{pmatrix}$	Ordem 26
G^6	$\begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 2 \end{pmatrix}$	Ordem 13
G^7	$\begin{pmatrix} 2 & 0 & 2 \\ 0 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix}$	Ordem 26
G^8	$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}$	Ordem 13
G^9	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix}$	Ordem 26
G^{10}	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$	Ordem 13
G^{11}	$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$	Ordem 26
G^{12}	$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix}$	Ordem 13
G^{13}	$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	Ordem 2
G^{14}	$\begin{pmatrix} 2 & 2 & 0 \\ 2 & 2 & 2 \\ 0 & 2 & 0 \end{pmatrix}$	Ordem 13
G^{15}	$\begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 2 \\ 2 & 2 & 2 \end{pmatrix}$	Ordem 26
G^{16}	$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 2 \end{pmatrix}$	Ordem 13

G^{17}	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	Ordem 26
G^{18}	$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix}$	Ordem 13
G^{19}	$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 2 & 1 \end{pmatrix}$	Ordem 26
G^{20}	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 2 \\ 1 & 2 & 2 \end{pmatrix}$	Ordem 13
G^{21}	$\begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 2 \\ 0 & 2 & 2 \end{pmatrix}$	Ordem 26
G^{22}	$\begin{pmatrix} 0 & 0 & 2 \\ 0 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix}$	Ordem 13
G^{23}	$\begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}$	Ordem 26
G^{24}	$\begin{pmatrix} 2 & 2 & 2 \\ 2 & 1 & 0 \\ 2 & 0 & 2 \end{pmatrix}$	Ordem 13
G^{25}	$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}$	Ordem 26
$G^{26} = I$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	Ordem 1
0	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	

Aqui encerramos os exemplos sobre corpos finitos, espera-se que o leitor tenha compreendido todo passo a passo para criação de um corpo finito de ordem p^n e que esse processo possa ser utilizado nos cursos de graduação ou mestrado como um método para exemplificar os corpos de ordem p^n.

CONSIDERAÇÕES FINAIS

Neste trabalho, vimos que a construção de corpos finitos com elementos matriciais e polinômios é um tópico fascinante na álgebra e na teoria dos números. Neste contexto, exploramos como combinar estruturas matriciais e polinomiais para criar corpos finitos, conteúdos que têm aplicações em criptografia, teoria de códigos e geometria aritmética. Na teoria de códigos os corpos finitos tem uma grande importância nos códigos de Goppa, que são um tipo especifico de código utilizados em correção de erros e armazenamento de dados $[16]$.

Neste trabalho, buscamos investigar como representar os elementos de um corpo finito usando matrizes. Isto envolve a definição de operações de adição, multiplicação e inversão compatíveis com as propriedades dos corpos. Além disso, os polinômios desempenham um papel crucial na construção desses corpos. Essa interseção entre matrizes e polinômios nos leva a explorar questões como minimalidade, irredutibilidade e extensões de corpos. A compreensão desses conceitos foi fundamental para construir os corpos de ordem p^2. Em resumo, a construção de corpos finitos com elementos matriciais e polinômios é um campo rico e desafiador, onde a álgebra encontra aplicações práticas e teóricas. Espera-se que este trabalho sirva como inspiração e norteie novas pesquisas nesse ramo belíssimo da álgebra que são os corpos finitos, que este trabalho possa abrir as portas para a criação de novos corpos com ordens maiores e mais complexos.

REFERÊNCIAS

[1] ANTON, Howard; BUSBY, Robert C. **Álgebra Linear Contemporânea**: Grupo A, 2006. *E-book.* ISBN 9788577800919. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788577800919/ Acesso em: 15 fev. 2024

[2] COELHO, Flavio. Um curso de álgebra linear. São Paulo: Editora da Universidade de São Paulo (USP),2007.

[3] HERSTEIN, I. N. Topics in Algebra. 2nd ed, J. Wiley, 1975.

[4] MARTINS, P. A. Grupos, corpos e teoria de Galois. LF Editorial, 2009.

[5] MORAES, M.M. Polinômios de corpos finitos, 2014, 36f. Monografia - Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

[6] Denis Serre. Matrices: Theory and Applications. Springer (Graduate Texts in Mathematics); 2 edition (2010). ISBN-13: 978-1441976826.

[7] SANTOS, Francicarlos. Uma introdução a teoria dos grupos. Caicó: UFRN, 2018.

[8] VIEIRA, V. L. Álgebra abstrata para licenciatura. 2.ed. Campina Grande: EDUEPB, 2015.

[9] SOUZA, Marcio. Introdução a teoria de galois. Rio grande: FURG, 2017.

[10] YARTEY, J. N. A. Álgebra II. Salvador, BA: UFBA, Instituto de Matemática e Estatística; Superintendência de Educação a Distância, 2017. 244p.

[11] DOMINGUES, H. H.; Iezzi, G. Álgebra Moderna. 4 a edição. Atual Editora 2003.

[12] ARAÚJO, Taciana. Álgebra de corpos finitos aplicada à teoria da codificação: Estudo do codificador BCH. João Pessoa: UFPB, 2012.

[13] Matrix calculator, 2024. Disponivel em: https://matrixcalc.org/pt/ . Acesso em: 23, abril de 2024.

[14] SANTOS, José Plínio de Oliveira. Introdução à teoria dos números. Rio de Janeiro: IMPA, 2016.

[15] CABRAL, Marcos A. P. e GOLDFELD, Paulo. Curso de Álgebra Linear. Rio de Janeiro: Instituto de Matemática, 2008.

[16] ARAUJO, Murillo Lozano Rubinho de. Corpos de funções algébricas e teoria dos códigos. São José do Rio Preto: Unesp, 2023.